МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ по дисциплине
«АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»
для студентов направления подготовки
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Ставрополь

СОДЕРЖАНИЕ

Практическая работа №1. Сканирование системы и сетевых ресурсов с помощью улучшенного IP сканнера

Цели работы

Целью практической является помощь студентам по сканированию сети и выявлению всех ее ресурсов.

Вам необходимо:

1) Поставить систему и выполнить ее сканирование.
2) Перечислить учетные записи пользователей.
3) Выполнить удаленное проникновение.
4) Собрать информацию о локальных сетевых компьютерах.

Средства для выполнения практической работы

В практической вам необходимо:

1) Улучшенный IP сканнер.
2) Вы можете загрузить его по ссылке http://www.advanced-ip-scanner.com. При этом скриншоты могут отличаться.
3) Windows 8 – как физическую систему. Другую систему Windows server 2008 как виртуальную.
4) Браузер и доступ в интернет.
5) Двойное нажатие по ipscan20.msi, установит с помощью мастера улучшенный IP сканнер.
6) Привилегии администратора.

Краткие теоретические сведения

Сканирование сети необходимо для сбора информации о живых системах, открытых портах и сетевых уязвимостях. Собранная информация полезна в определении угроз и уязвимостей сети.

Постановка задачи

l. Нажмите Пуск.

Рисунок 1.1: Windows 8 – Рабочий стол

2. Запустите улучшенный IP сканнер (Windows 8).

Рисунок 1.2.: Windows 8 – Приложения

3. Главное окно программы.

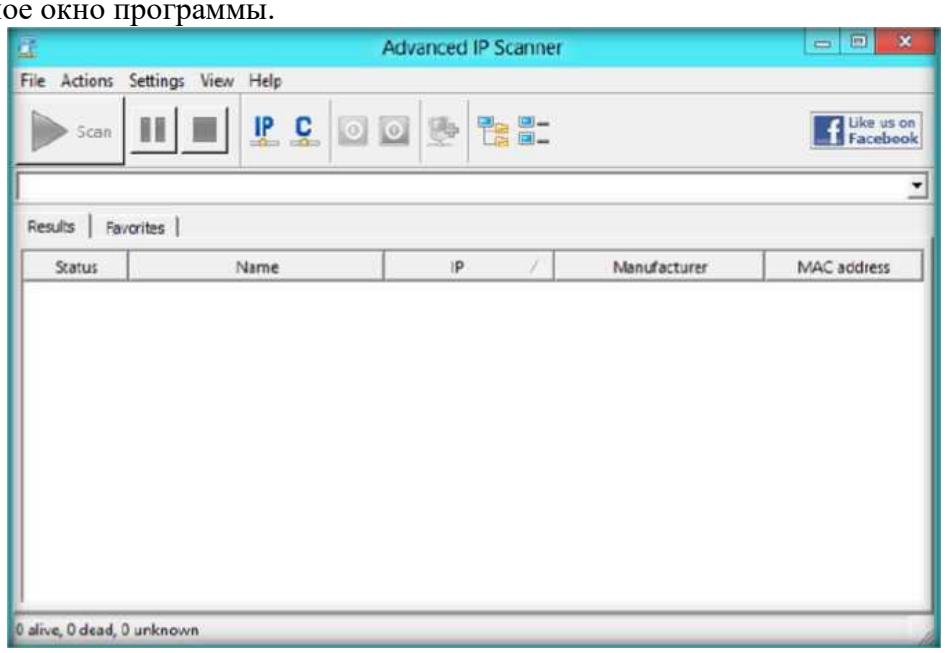


Рисунок 1.3.: Главное окно программы

4. Теперь запустите виртуальную машину Server 2008.

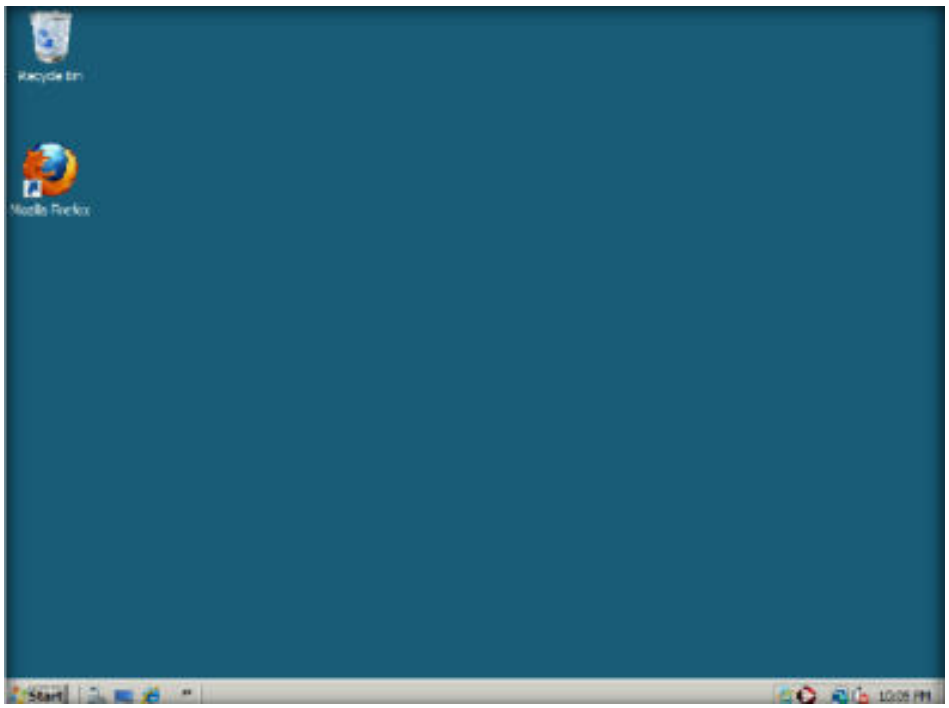


Рисунок 1.4: Windows server 2008

5. Теперь вернитесь в атакующую машину Windows 8 и введите IP адрес в поле.

6. Начните сканирование.

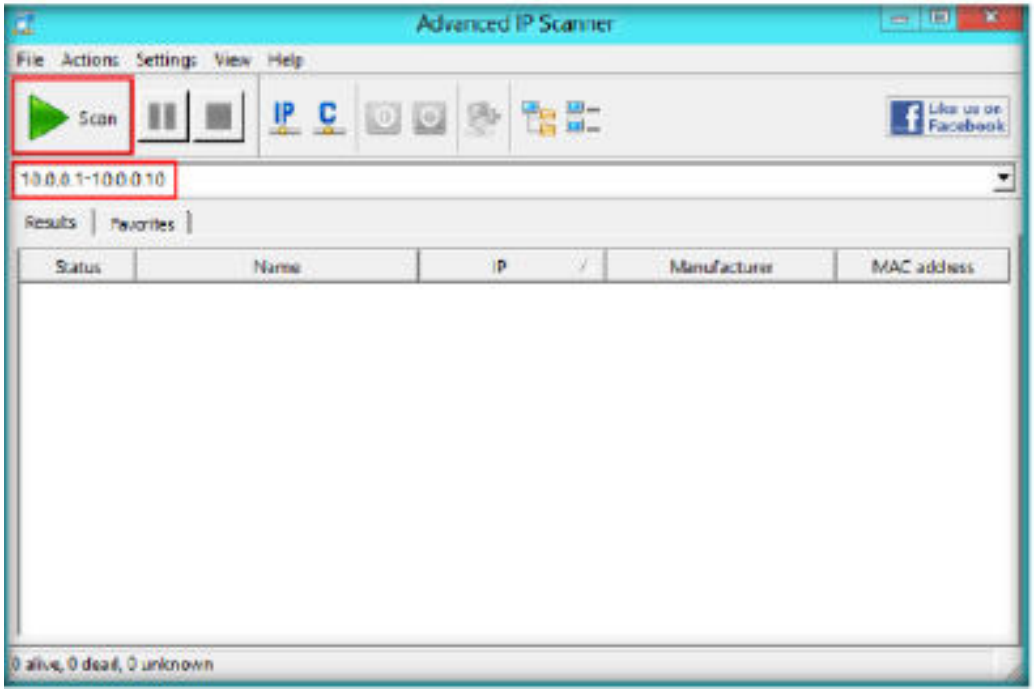


Рисунок 1.5: Сканирование

7. Усовершенствованный сканер IP сканирует все IP-адреса в диапазоне и выводит на экран результаты сканирования после завершения.

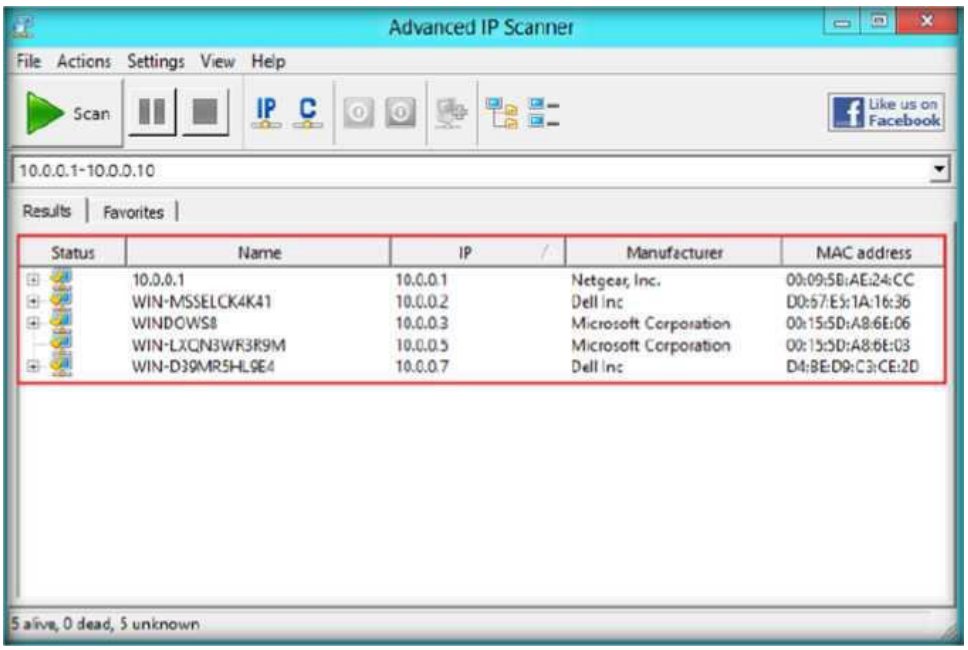


Рисунок 1.6: Результат сканирования

8. Сканер обнаружил IP адрес жертвы и ее состояние, как живое.
9. Правой мышкой на IP вызовите меню.

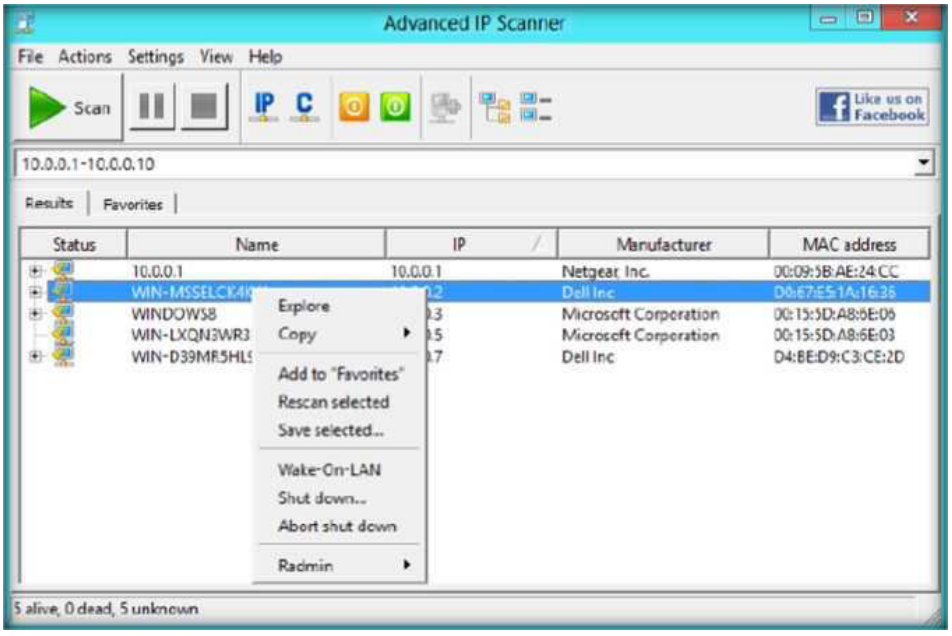


Рисунок 1.7: Меню

10. В результате сканер выводит на экран свойства обнаруженного компьютера, такие как IP-адрес. Имя, MAC и информация о NetBIOS.
11. Вы можете завершить работу, перезагрузить или аварийное выключить машину жертвы.

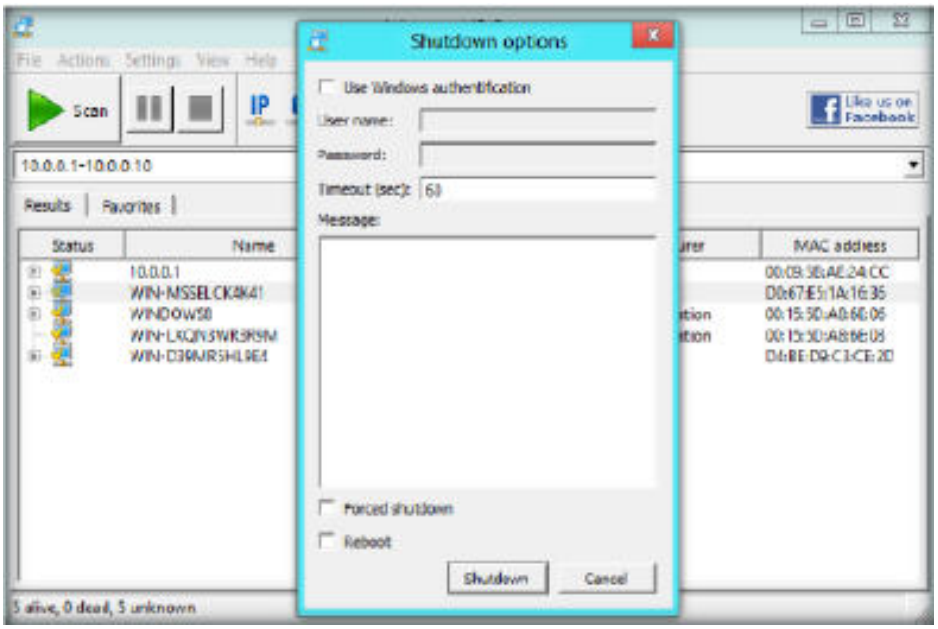


Рисунок 1.8: Дополнительные свойства

12. Теперь у вас есть информация о машине жертвы.

Анализ практической работы

Запишите все IP адреса, открытые порты, запущенные приложения и протоколы найденные в практическому занятию.

Средства	Собранная информация
Advanced IP Scanner	Информация: – IP адрес; – Имя системы; – MAC адрес; – Информация NetBIOS; – производитель; – статус системы.

Вопросы

1. Исследуйте и оцените IP-адреса и диапазон IP-адресов.

Практическое занятие №2. Сбор баннеров для определения удаленной целевой системы с помощью ID сервиса

Цели работы

Целью работы является помощь студентам в сборе баннеров, захвату веб-сайта и обнаружении приложений.

Вы научитесь:

1) Идентифицировать доменный IP адрес.
2) Идентифицировать информацию домена.

Средства для выполнения практической работы

Вам необходимо:

1) ID Server (IDS).
2) Можно загрузить по ссылке http://www.grc.com/id/idserve.htm.
3) Скриншоты могут отличаться из за версии IDS.
4) Административные привилегии для ID Serve tool.
5) Windows Server 2012.

Краткие теоретические сведения

Представление о ID Serve

ID Serve может соединиться с любым портом сервера и вывести на экран сообщение приветствия сервера, если оно имеется.

Постановка задачи

1. В главном окне ID Serve выбирайте Sever.

Рисунок 2.1.: Главное окно

2. Введите IP адрес или URL, как на примере.

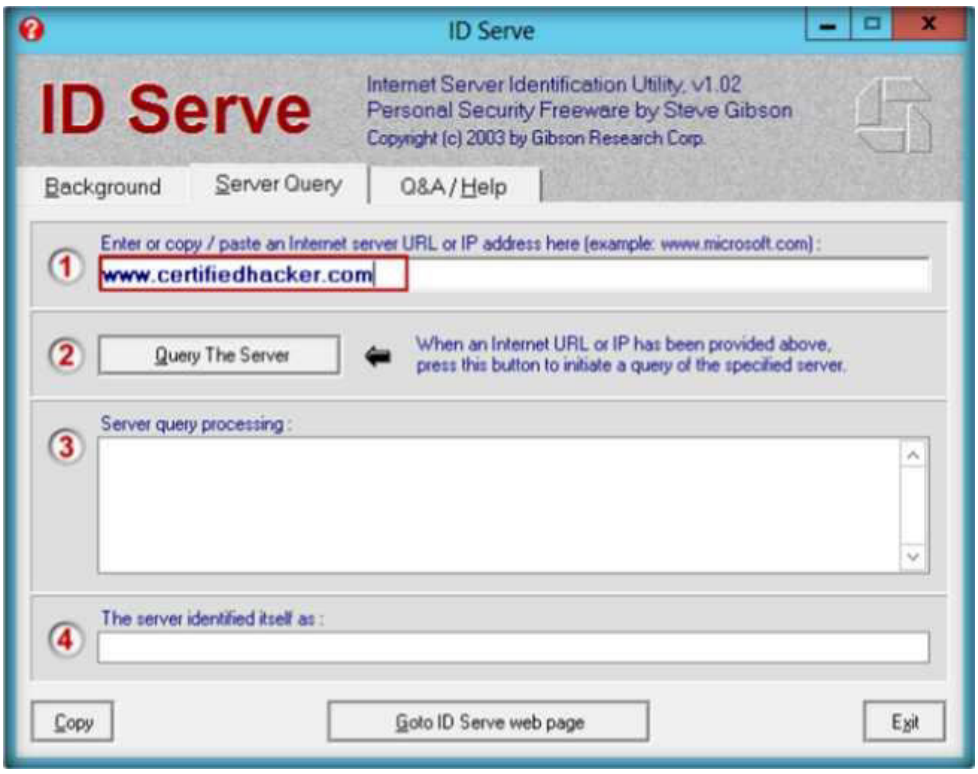


Рисунок 2.2.: Ввод адреса

3. Нажмите Query The Server.

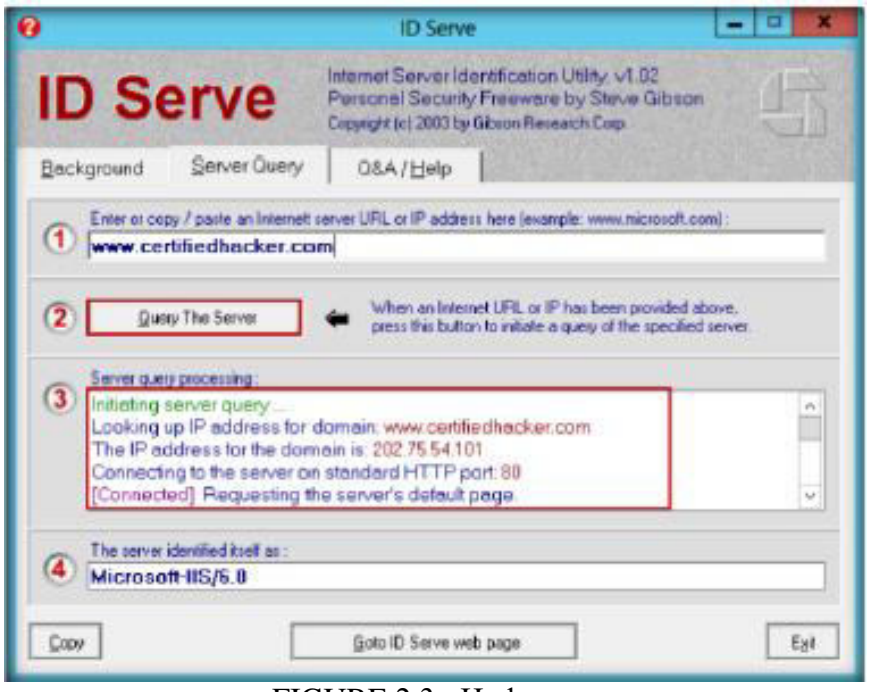


FIGURE 2.3.: Информация о сервере

Анализ практической работы

Запишите все IP адреса, приложения, протоколы которые вы открыли в ходе практической.

Средства	Собранная информация
ID Serve	IP адрес: 202.75.54.101
	Server Connection: Standard HTTP port: 80

	Заголовки ответа сервера: – HTTP/1.1 200. – Server: Microsoft-IIS/6.0. – X-Powered-By: PHP/4.4.8. – Transfer-Encoding: chunked. – Content-Type: text/html.

Вопросы

1. Проверьте, какие протоколы используются.
2. Проверьте, поддерживается ли SSL соединения.

Практическое занятие №3. Цифровой отпечаток открытых портов с Amap Tool

Цели работы

Целью практической является помочь студентам просканировать порты и обнаружить приложения работающие на них.

Вы изучите:

1. Идентифицируйте прикладные протоколы на открытых портах 80.
2. Обнаружьте прикладные протоколы.

Средства для выполнения практической работы

Вам необходимо:

1. Amap.
2. Можно загрузить по ссылке http://wwvw.thc.org/thc-amap.
3. Скриншоты могут отличаться.
4. Компьютер с Web Services port 80.
5. Права администратора для Amap tool.
6. Windows Server 2012.

Краткие теоретические сведения.

Представление о цифровом отпечатке

Снятие отпечатков пальцев используется, чтобы обнаружить приложения, работающие на каждом открытом порту, найденном в сети.

Постановка задачи

1. Запустите amap www.certifiedhacker.com 80.

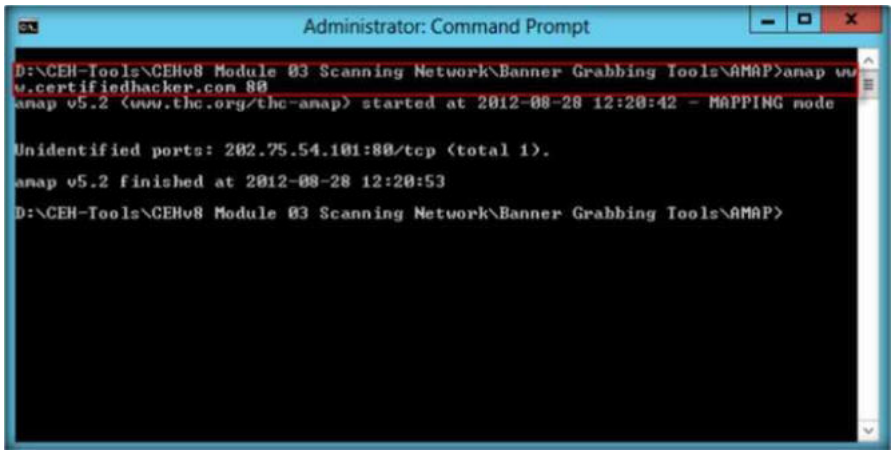


Рисунок 3.1: Amap www.ceitifiedhacker.com с Port 80

2. Видно, что определённые прикладные протоколы работают для введенного имени хоста и 80 порта.
3. Используйте IP адрес для проверки приложений на порту.
4. В командной строке введите IP своего локального Windows Server 2008 amap 10.0.0.4 75-81 и нажмите enter.
5. Попытайтесь просканировать различные веб-сайты используя различные диапазоны amap www.certifiedliacker.com 1-200.

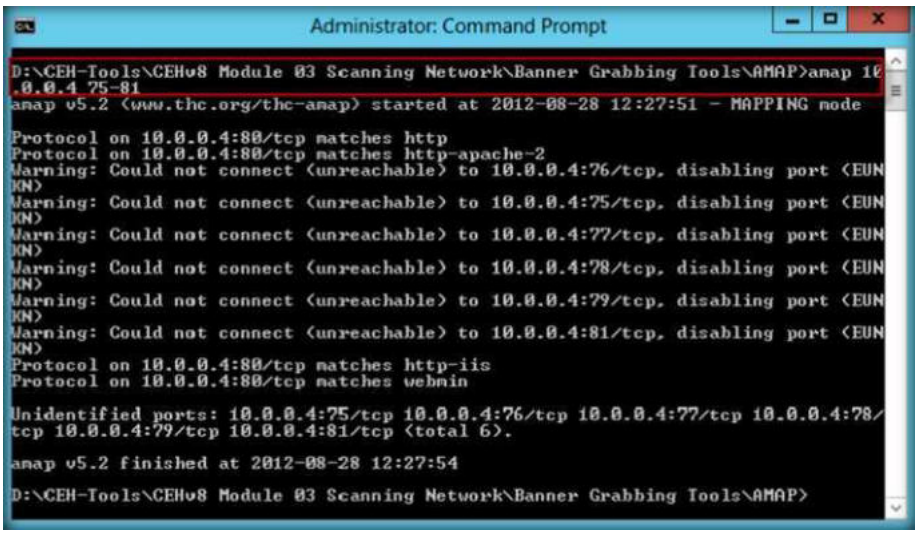


Рисунок 3.2: Amap с IP в диапозоне 75-81

Анализ практической работы

Запишите все IP адреса, открытые порты и их приложения и протоколы открытые в практической.

Средства	Собранная информация
Amap	Открытый порт: 80
	Севрвера: – http-apach-2; – http-iis; – webmin.
	Порты: – 10.0.0.4:75/tcp. – 10.0.0.4:76/tcp. – 10.0.0.4:77/tcp. – 10.0.0.4:78/tcp. – 10.0.0.4:79/tcp. – 10.0.0.4:81/tcp.

Вопросы

1. Выполните команду amap для имени хоста с портом отличным от 80.
2. Проанализируйте, как amap получает приложения с разных машин.
3. Используйте различные опции amap и проанализируйте результаты.

Практическое занятие №4. Контроль TCP/IP с помощью CurrPorts Tool

Цели работы

Целью является помочь студенту определить и перечислить все порты TCP/IP и UDP.

Вам необходимо:

1. Отсканировать систему на открытые TCP/IP и UDP порты.
2. Собрать информацию об открытых портах и процессах.
3. Перечислить все существующие IP адреса.
4. Закрыть все нежелательные соединения TCP уничтожить процесс, который открыл порт

Средства для выполнения практической работы

Вам необходимо:

1. CurrPorts.
2. Загрузить можно по ссылке http: //www.nirsoft.net/utils/cports.html.
3. Скриншоты могут отличаться.
4. Windows Server 2012.
5. Права администратора CurrPorts tool.

Краткие теоретические сведения Представление о контроле TCP/IP

Контроль TCP/IP портов проверяет есть ли многократное использование IP подключений. Сканирует порты TCP/IP для получения списка всех открытых портов и также выводит все IP на экран.

Постановка задачи

Запустите CurrPorts, который покажет процессы, порты, IP и их статусы.

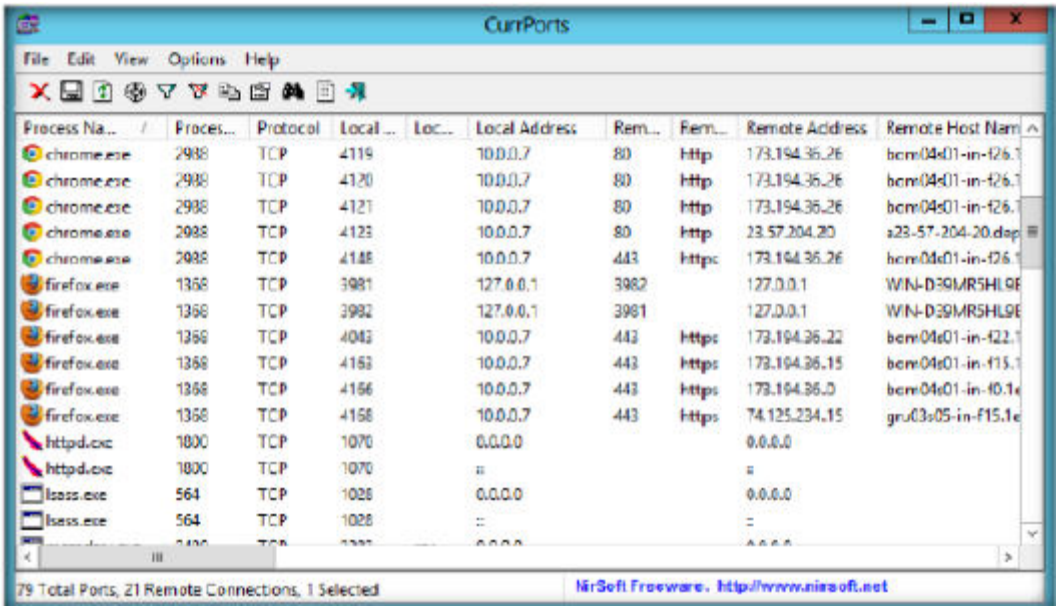


Рисунок 4.1: CurrPorts

2. CurrPorts причислит все процессы и их ID, протоколы, локальный и удаленный порты.

3. Чтобы просмотреть все как HTML, нажмите View - HTML Reports - All Items.

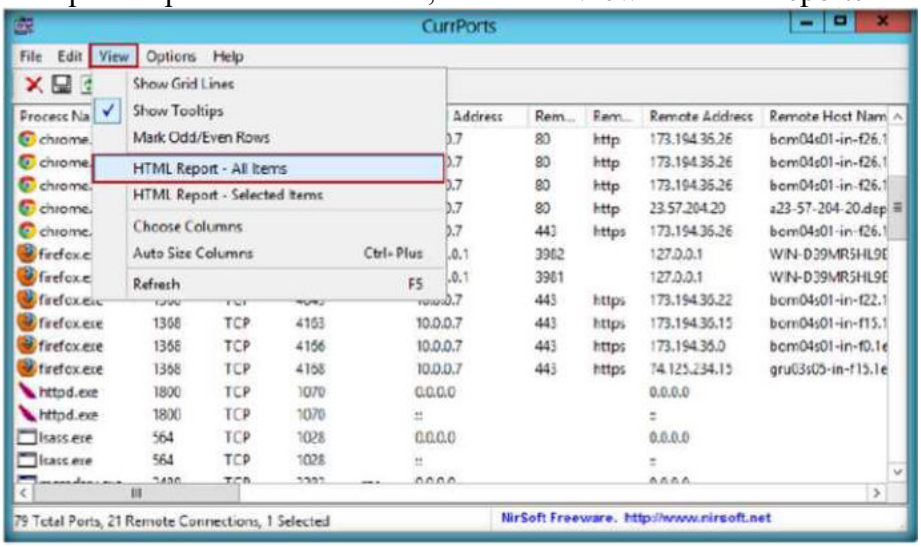
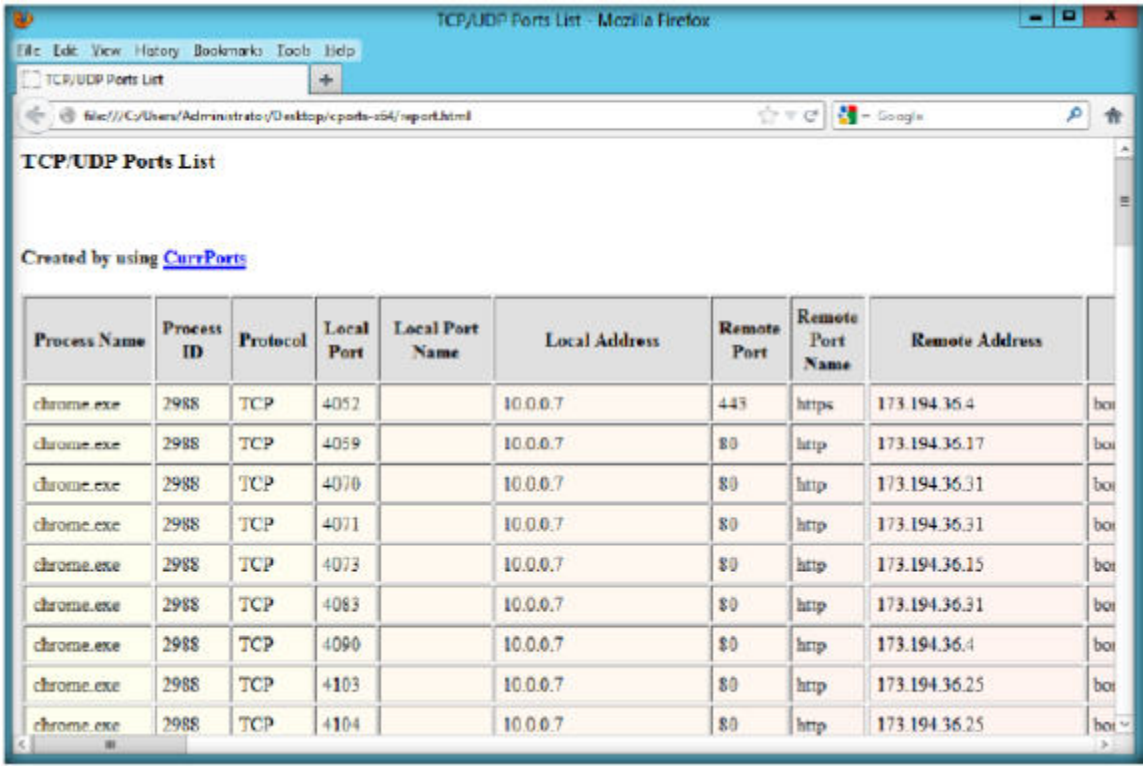


Рисунок 4.2: HTML Report - All Items

4. The HTML Report автоматически откроется в стандартном браузере.



Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address
chrome.exe	2988	TCP	4052		10.0.0.7	443	https	173.194.36.4
chrome.exe	2988	TCP	4059		10.0.0.7	80	http	173.194.36.17
chrome.exe	2988	TCP	4070		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4071		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4073		10.0.0.7	80	http	173.194.36.15
chrome.exe	2988	TCP	4083		10.0.0.7	80	http	173.194.36.31
chrome.exe	2988	TCP	4090		10.0.0.7	80	http	173.194.36.4
chrome.exe	2988	TCP	4103		10.0.0.7	80	http	173.194.36.25
chrome.exe	2988	TCP	4104		10.0.0.7	80	http	173.194.36.25

Рисунок 4.3: CurrPorts Report - All Items

5. Для сохранения нажмите, File - Save Page As...Ctrl+S.

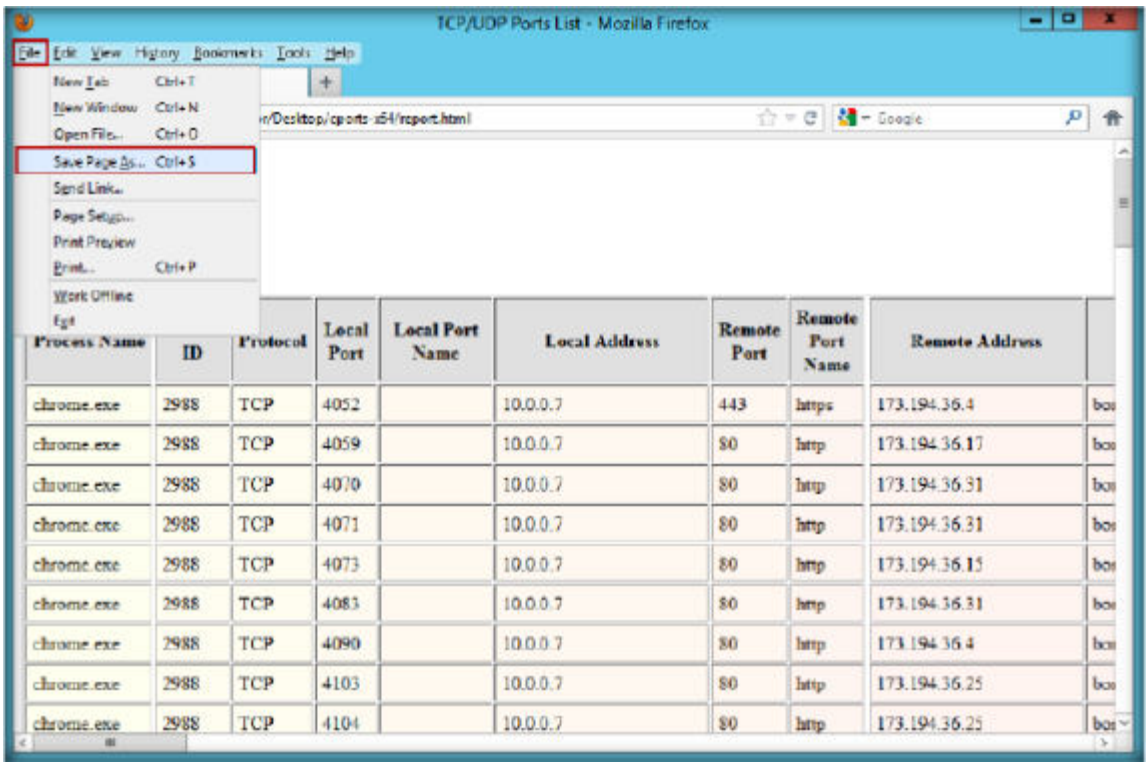


Рисунок 4.4: Сохранение CurrPorts Report - All Items

6. Для просмотра только выбранного отчета, нажмите View - HTML Reports - Selected Items

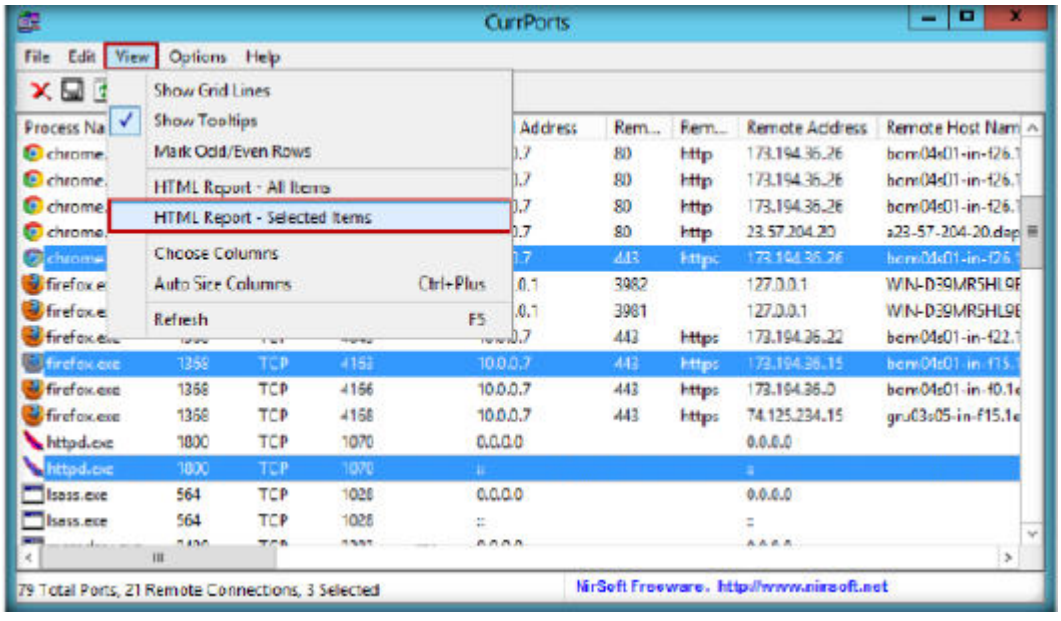


Рисунок 4.5: CurrPorts с HTML Report - Selected Items

6. Также используется стандартный браузер.

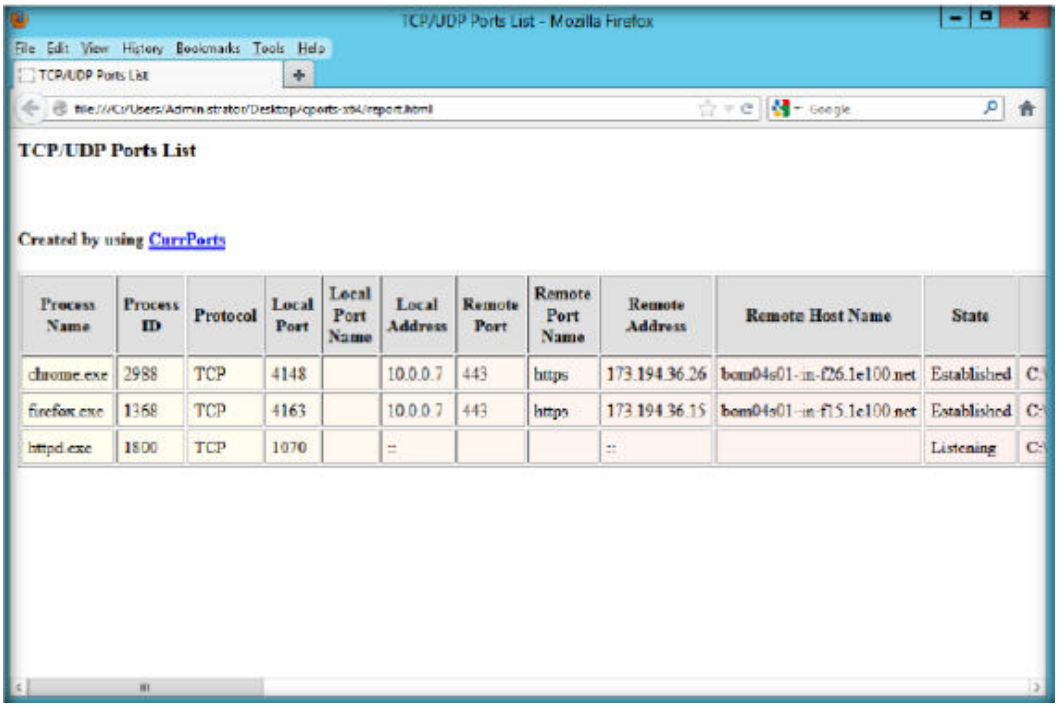


Рисунок 4.6: CurrPorts с HTML Report - Selected Items

8. Для сохранения, нажмите File - Save Page As...Ctrl+S

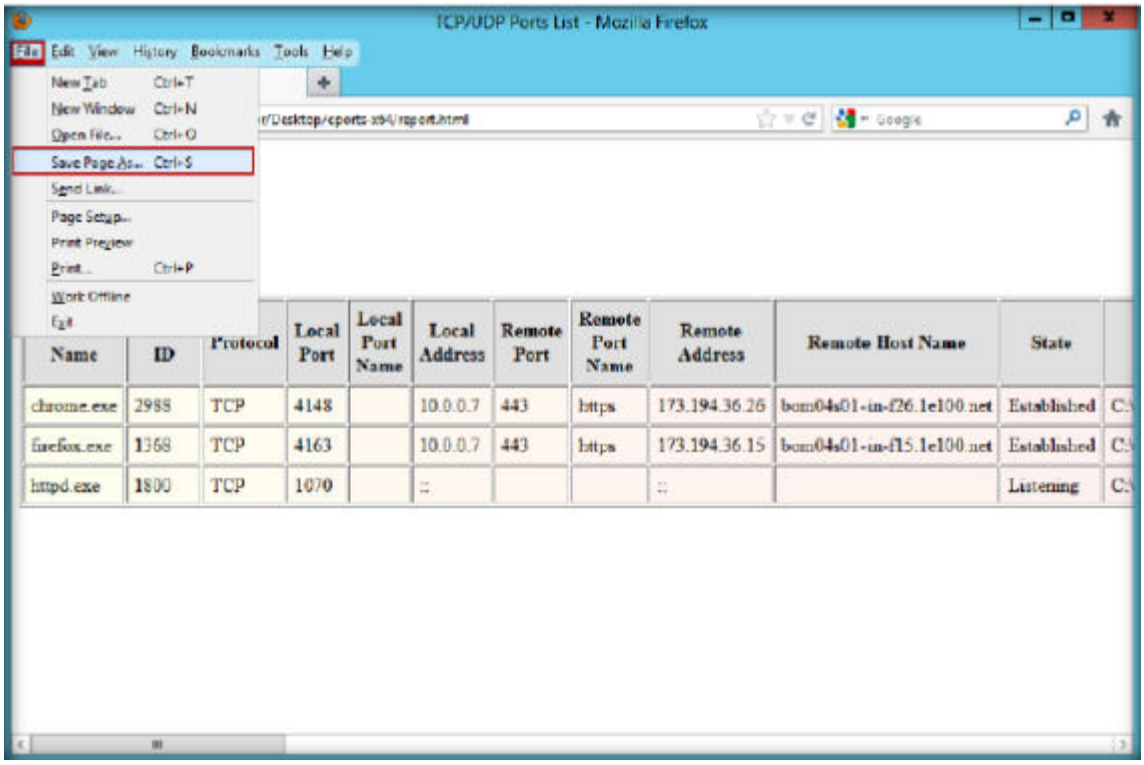


Рисунок 4.7: Сохранение CurrPorts с HTML Report - Selected Items

9. Для просмотра свойств порта, выберете порт и нажмите File -> Properties.

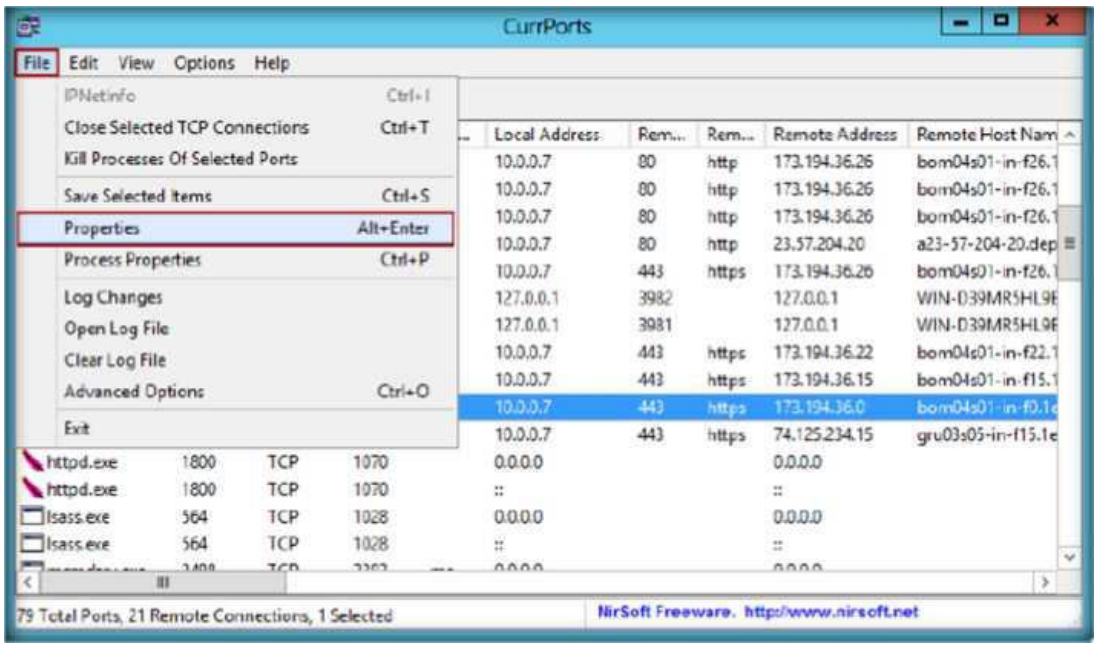


Рисунок 4.8: Выбранный порт

10. В итоге можно просмотреть все свойства выбранного порта.
11. Нажмите ок.

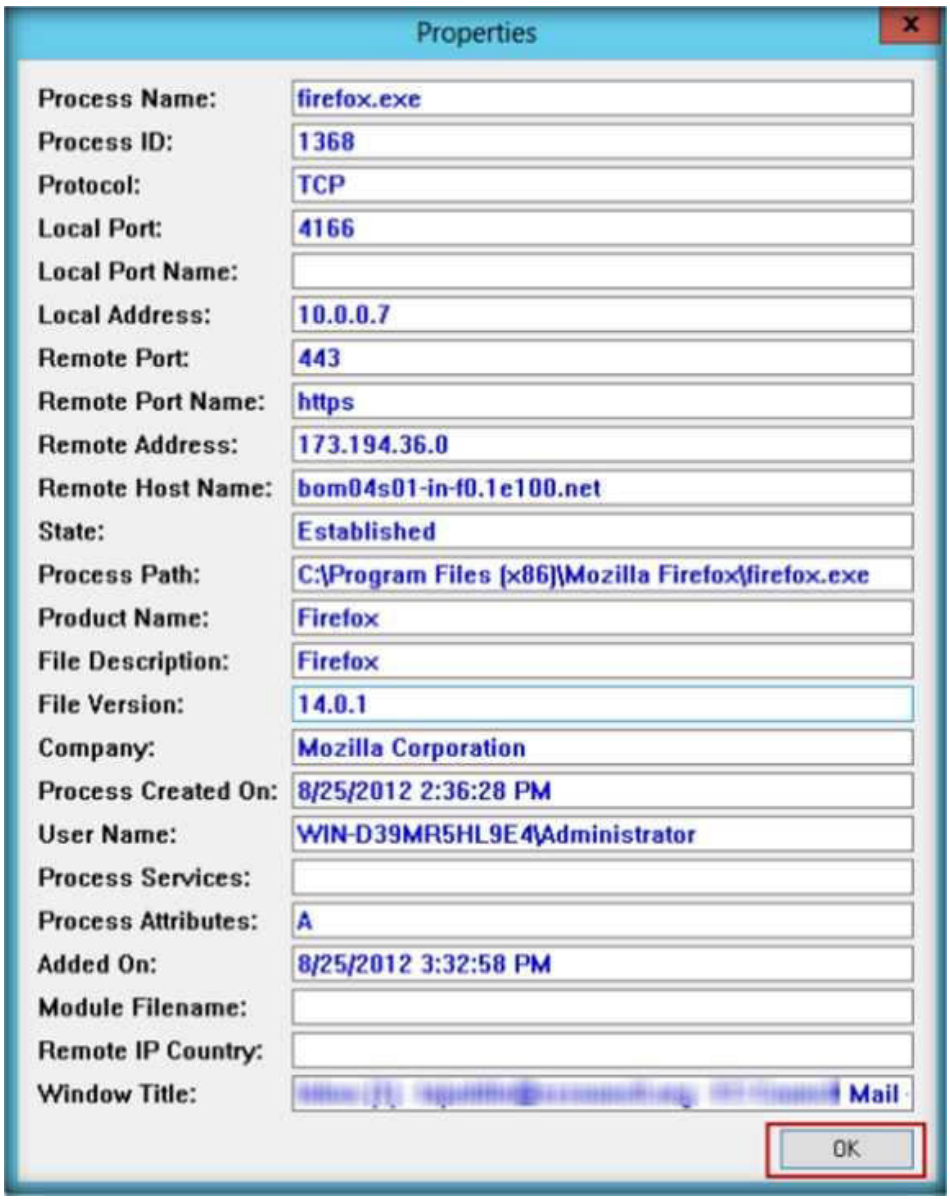


Рисунок 4.9: Свойства порта

12. Для того чтобы закрыть выбранное TCP соединение, нажмите File - Close Selected TCP Connections (или Ctrl+T).

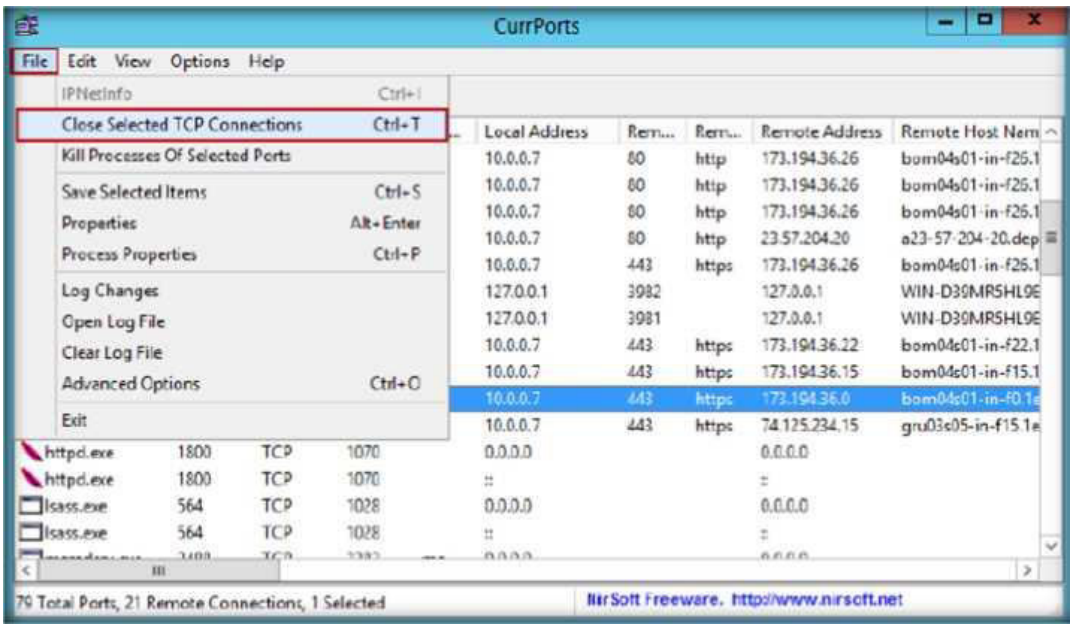


Рисунок 4.10: Закрыть соединение

13. Для уничтожение процесса, открывшего порт, нажмите File -> Kill Processes of Selected Ports

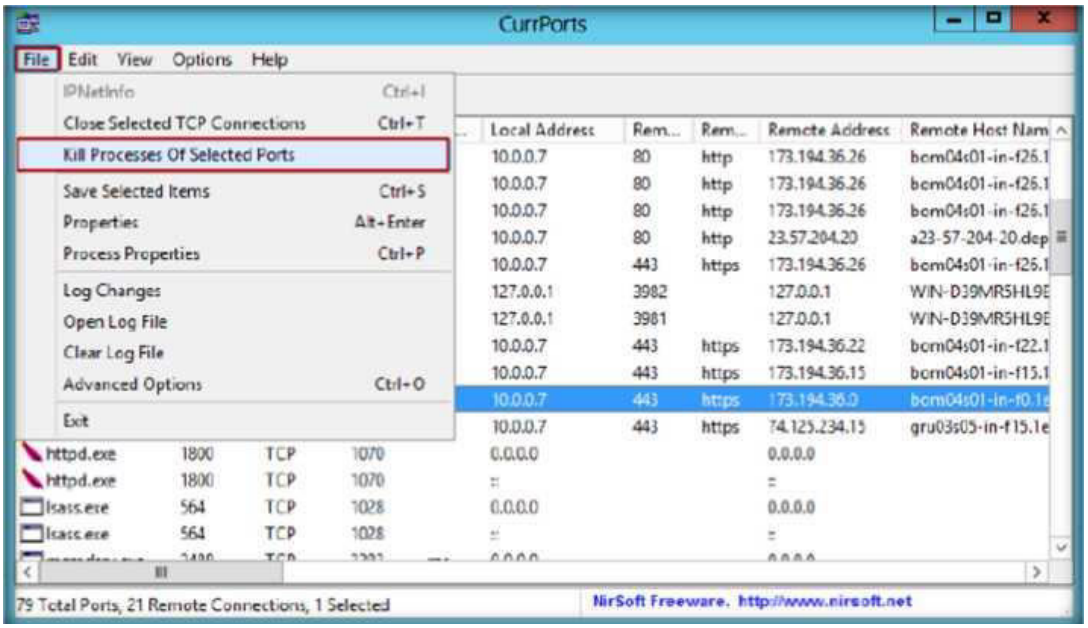


Рисунок 4.11: Закрытие процесса

14. Для выходы, нажмите File - Exit.

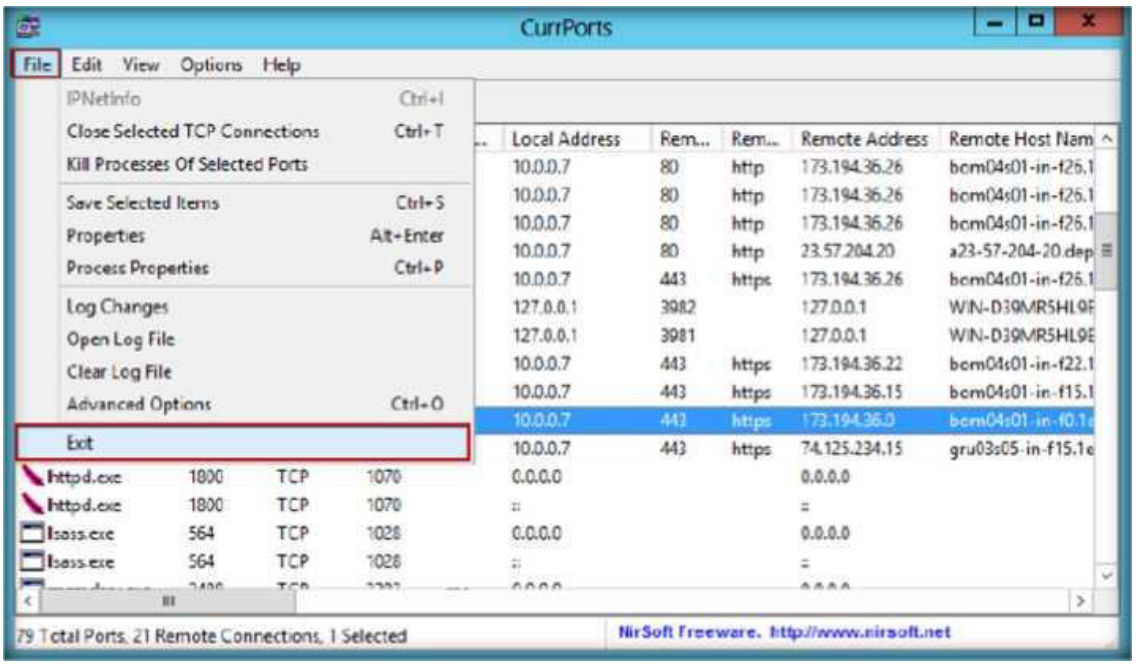


FIGURE 4.12: Выход

Анализ практической работы

Запишите все IP адреса, открытые порты, приложение и протоколы открытые в практической.

Средства	**Собранная информация**
CurrPorts	Специализация: Сеть для сканирования открытых
	Отчет: – Process Name – Process ID – Protocol – Local Port – Local Address – Remote Port – Remote Port Name – Remote Address – Remote Host Name

Вопросы

1. Проанализируйте результаты программы, создав фильтр на порт 80 и UDP 53.
2. Проанализируйте результаты создав фильтр выводящие только открытые порты.
3. Определите что использовать в CurrPorts, для следующих проблемах:
    a. неопознанные приложения.
    b. нет удаленного адреса.
    c. неизвестно государство.

Практическое занятие №5. Сканирование сети на уязвимостей с помощью LanGuard 2012

Цели работы

Целью практической является помочь студенту провести сканирование системы для выявления уязвимостей.

Вам необходимо:

1) Выполнить сканирование.
2) Контролировать сеть.
3) Обнаружить уязвимые порты.
4) Идентифицировать уязвимости системы обеспечения безопасности.
5) Корректировать систему обеспечения безопасности.

Средства для выполнения практической работы

Вам необходимо:

1) GFI Languard.
2) Загрузить можно по ссылке http://www.gfj.com/lannetscan.
3) Скриншоты могут отличаться.
4) Windows 2012 Server как хост.
5) Windows Server 2008 - виртуальная машина.
6) Microsoft .NET Framework 2.0.
7) Права администратора GFI LANguard Network Security Scanner.
8) Регистрация на сайте http://www.gfi.com/lannetscan для получения ключа.
9) Код активации, который придет на почту после регистрации.

Краткие теоретические сведения

Представление о сканировании сети

Как администратор, Вы часто должны иметь дело отдельно с проблемами, связанными с управлением исправлениями и сетевым контролем. Ваша обязанность обеспечить анализ рисков и поддержать безопасное и совместимое сетевое состояние.

Сканирования безопасности или аудиты позволяют Вам идентифицировать и оценить возможные риски в сети. Контролирующие операции подразумевают любой тип проверки выполненного во время аудита сетевой безопасности. Они включают открытые проверки порта, получение недостающих патчей Microsoft, информацию о службе и пользователе и т.д.

Постановка задачи

Следуя шагам мастера установки установите GFI LANguard network scanner на хост машину.

1. Нажмите Пуск.

Рисунок 5.1: Рабочий стол

2. Запустите GFI LANguard.

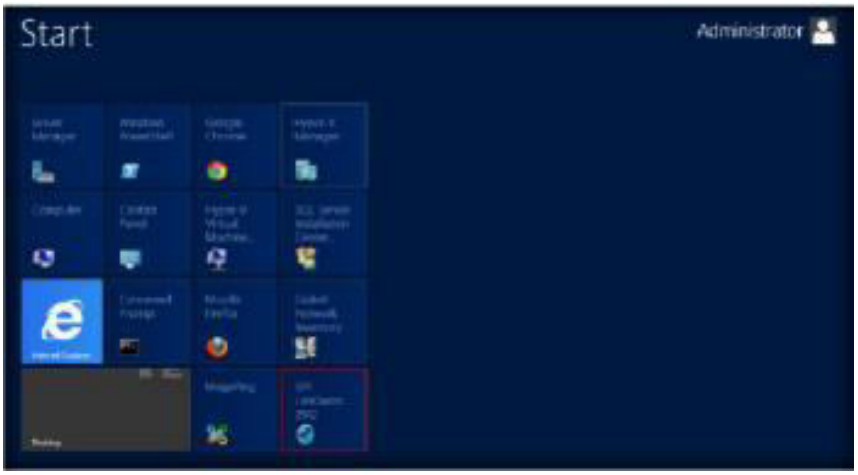


Рисунок 5.2 Windows Server 2012 – Приложения

3. Главное окно GFI LanGuard 2012.

Рисунок 5.3: The GFI LANguard

4. Нажмите запустить сканирование GFI LANguard.

Рисунок 5.4: The GFI LANguard

5. Откроется новое окно сканирования.
   - В Scan Target, выберите localhost.
   - В Profile option, выберите Full Scan.
   - В Credentials option, выберите currently logged on user.
6. Нажмите Scan.

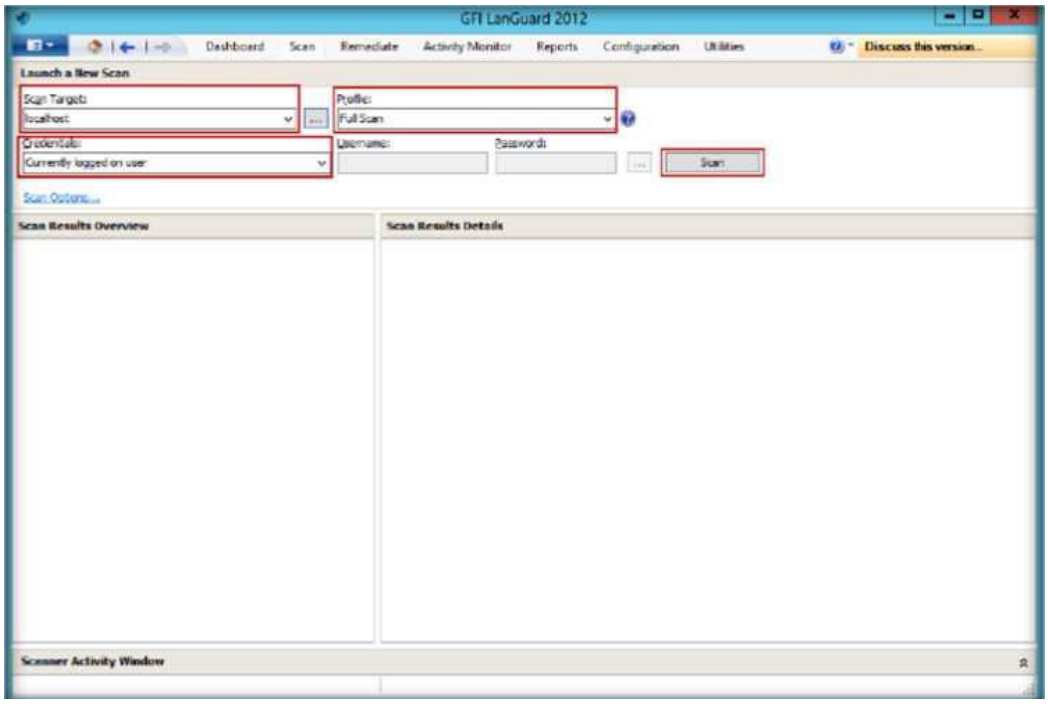


Рисунок 5.5: Настройки

7. Сканирование запустилось и оно займёт какое то время, которое указанно ниже.

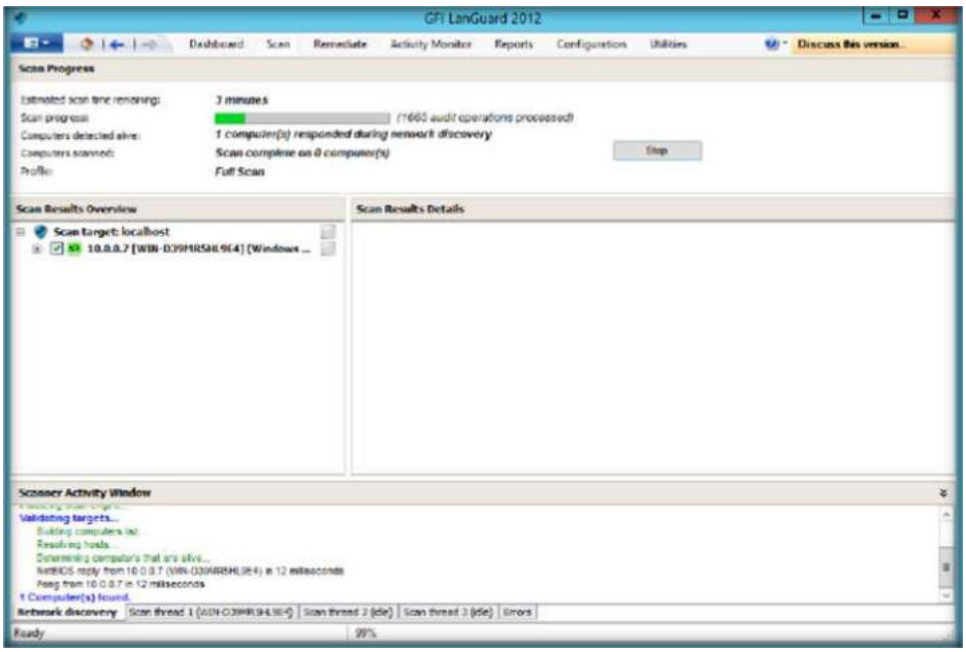


Рисунок 5.6: The GFI LanGuard

8. После завершения сканирование, вы увидите результат.

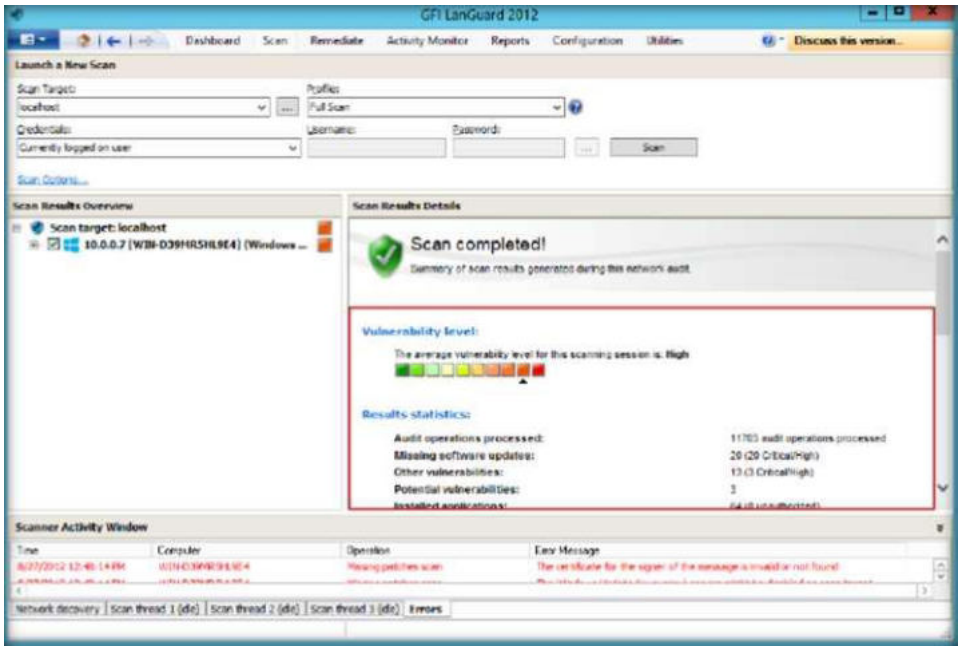


Рисунок 5.7: The GFI LanGuard

9. Чтобы просмотреть результат сканирования щелкните по IP адресу.
10. Нажмите Vulnerability Assessment, это покажет оценку уязвимостей и аудит По и сети.

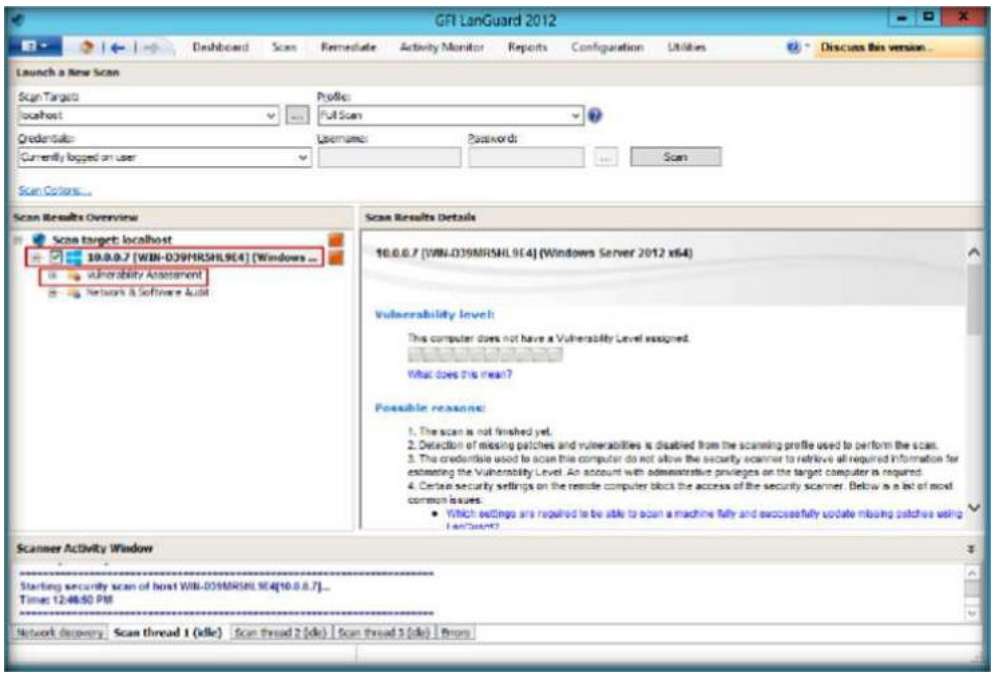


Рисунок 5.8: Vulnerability Assessment

11. Это покажет все индикаторы Vulnerability Assessment по категориям.

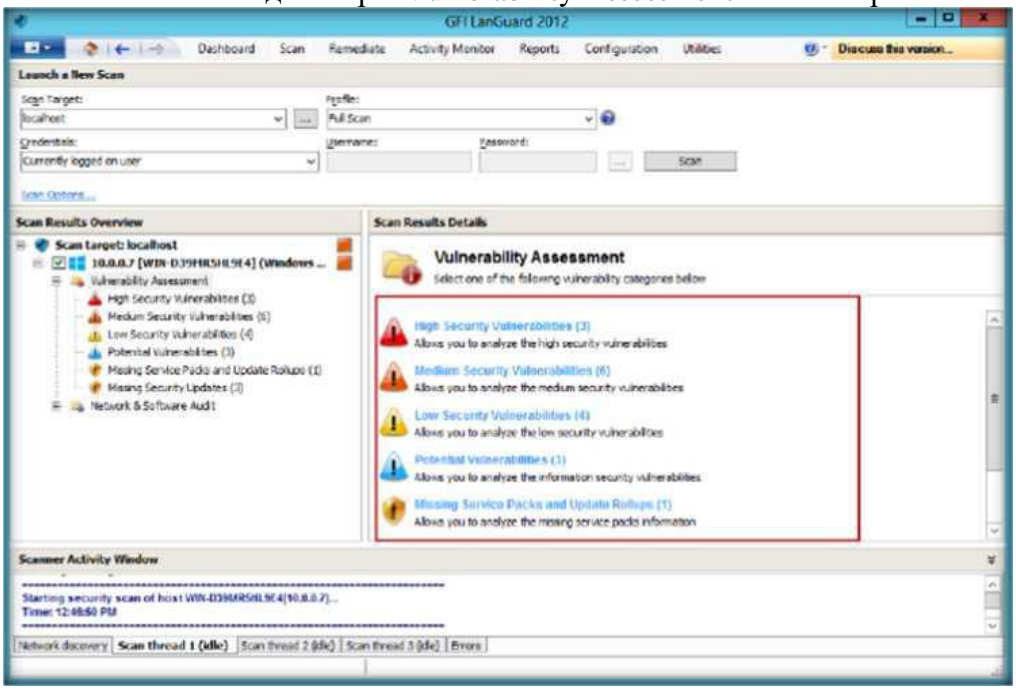


Рисунок 5.9: Категории Vulnerability Assessment

12. Нажмите Network & Software Audit и потом System Patching Status, который покажет все системные исправления.

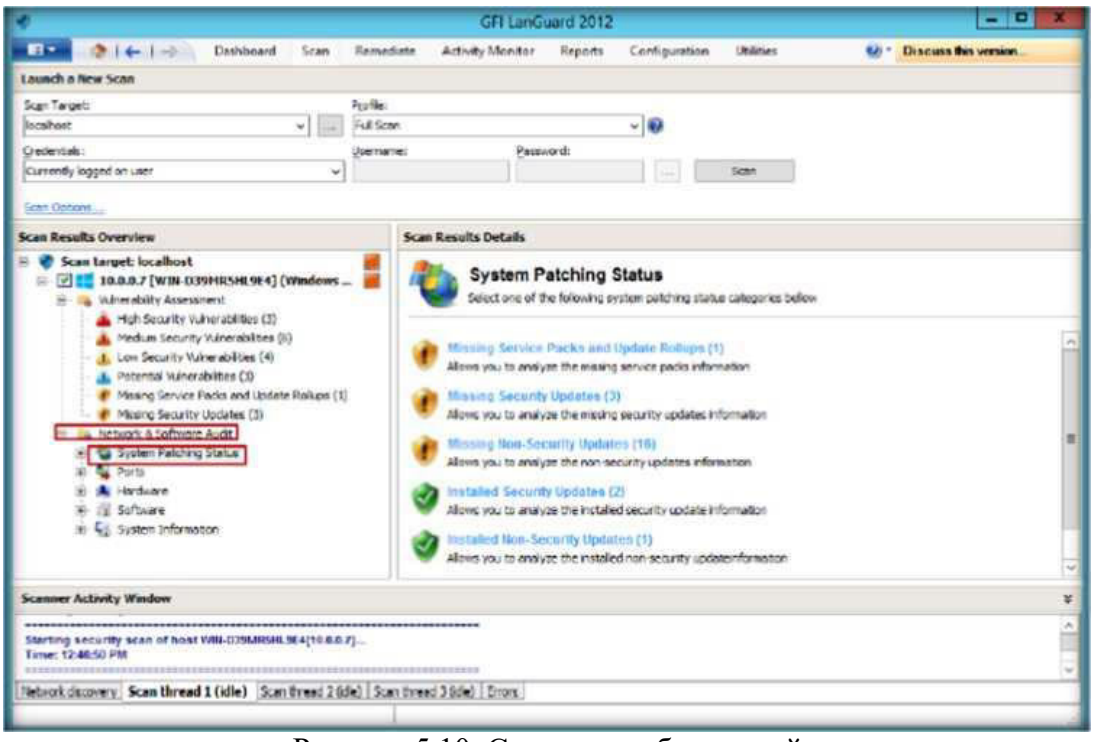


Рисунок 5.10: Состояние обновлений

13. Нажмите Ports, затем Open TCP Ports.

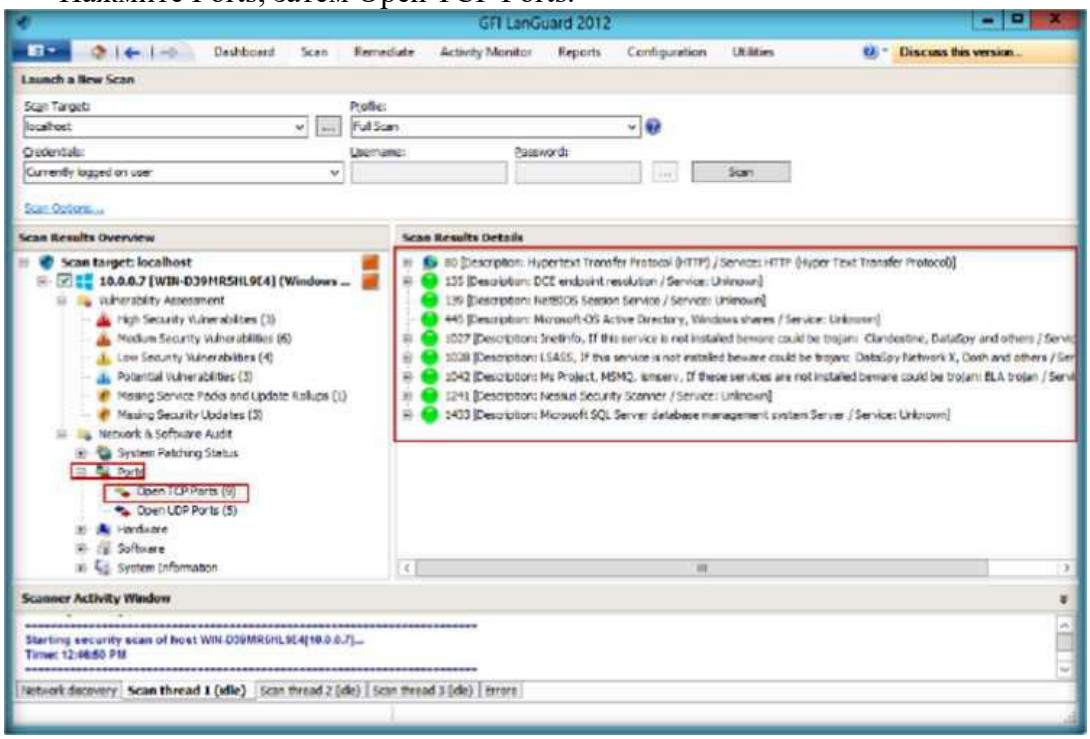


Рисунок 5.11: TCP/UDP Порты

14. Нажмите System Information, которая покажет всю системную информацию.
15. Нажмите Password Policy.

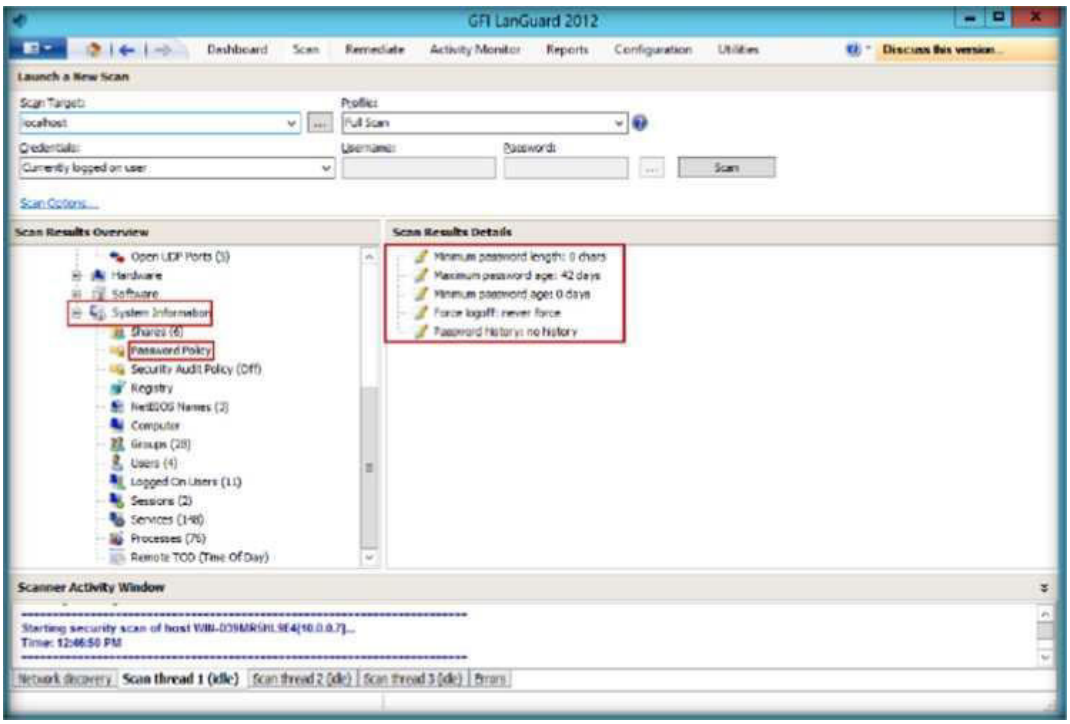


Рисунок 5.12: Password Policy

16. Нажмите Groups, которая покажет все группы в системе.

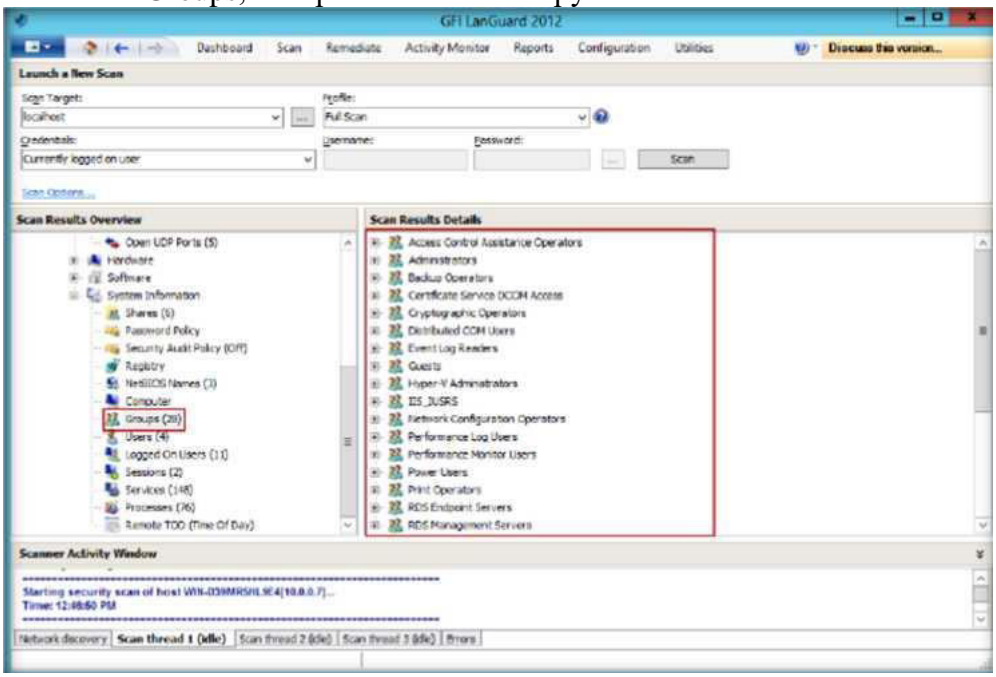


Рисунок 5.13: Информация о группах Groups

17. Нажмите Dashboard tab, которая покажет всю информацию сети.

Рисунок 5.14: Отчет состояния сети

Анализ практической работы

Запишите все результаты, угрозы и уязвимости обнаруженные во время сканирования проведенного в практической.

Средства	Собранная информация
The GFI LANguard	Уровень уязвимостей
	Оценка уязвимостей
	Состояние системного исправления
	Детали сканирования открытых портов TCP
	Детали результатов сканирования для политики паролей
	Вся сеть: – Уровень уязвимостей – Датчики безопасности – Уязвимые компьютеры – Состояние агента – Тенденция уязвимостей в течении времени – Распределение уязвимостей

Вопросы

1. Проанализируйте как GFI LANguard защищает против червей.
2. При каких обстоятельствах GFI LANguard вывод диалог во время патча.
3. Вы можете изменить сообщение, выведенное на экран, когда GFI LANguard выполняет административные задачи? Если да, то как?

Практическое занятие №6. Аудит сети с помощью Nmap

Цели работы

Целью практической является помощь студентам в изучении и понимании управления службами и обновлениями, расписанием сетевых задач, мониторингом служб.

Вам необходимо:

1) Сканировать TCP и UDP порты.
2) Проанализировать детали узлов и их топологию.
3) Определить типы пакетных фильтров.
4) Записать и сохранить все отчеты сканирования.
5) Сравнить результаты для подозрительных потов.

Средства для выполнения практической работы

To perform the lab, you need:

1) Nmap.
2) Загрузить можно по ссылке http://nmap.org.
3) Скриншоты могут отличаться.
4) Windows Server 2012 как хост.
5) Windows Server 2008 как виртуальную машину.
6) Браузер с интернетом.
7) Права администратора для запуска Nmap tool.

Краткие теоретические сведения Представление о сканировании сети

Сетевые адреса сканируются для того чтобы определить:

1) Какие версии приложений и служб предлагают узлы.
2) Какие ОС они используют.
3) Какие пакетные фильтры или брандмауэры они используют и многие другие.

Постановка задачи

Следуя указаниям мастера установки, поставьте Nmap на хост машину. (Window Server 2012).

1. Нажмите Пуск.

Рисунок 6.1: Windows Server 2012 – Рабочий стол

2. Нажмите Nmap-Zenmap GUI и откройте Zenmap.

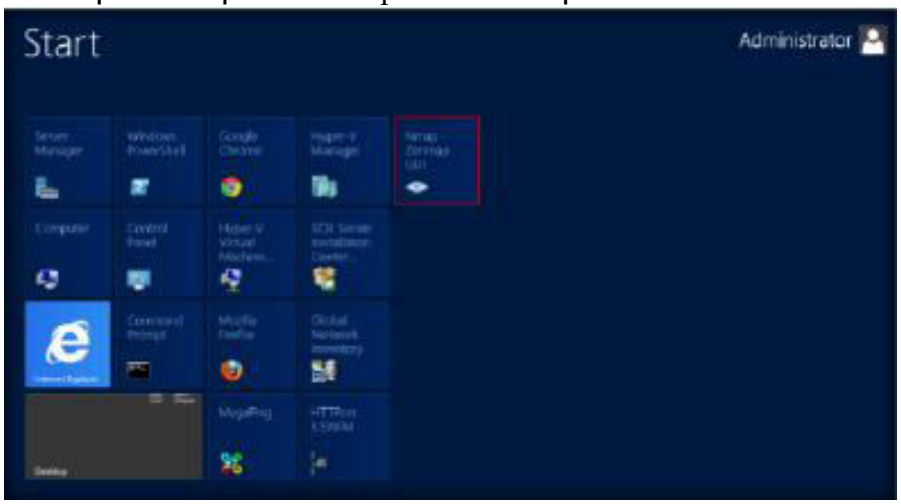


Рисунок 6.2 Windows Server 2012 – Приложения

3. Nmap - Zenmap GUI окно.

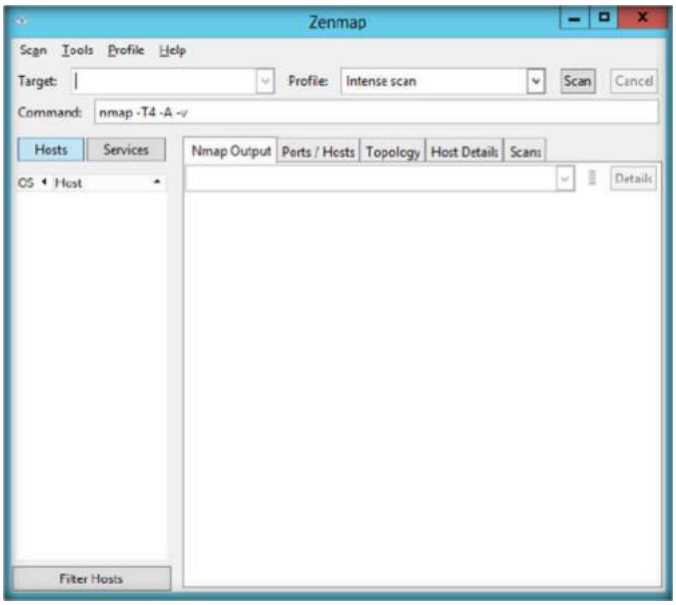


Рисунок 6.3: The Zenmap

4. Введите IP (10.0.0.4) виртуальной машины.
5. IP может отличаться в зависимости от настройки вашей виртуальной машины.
6. Выберите тип профиля, который хотите отсканировать - Intense Scan.
7. Нажмите сканирование.

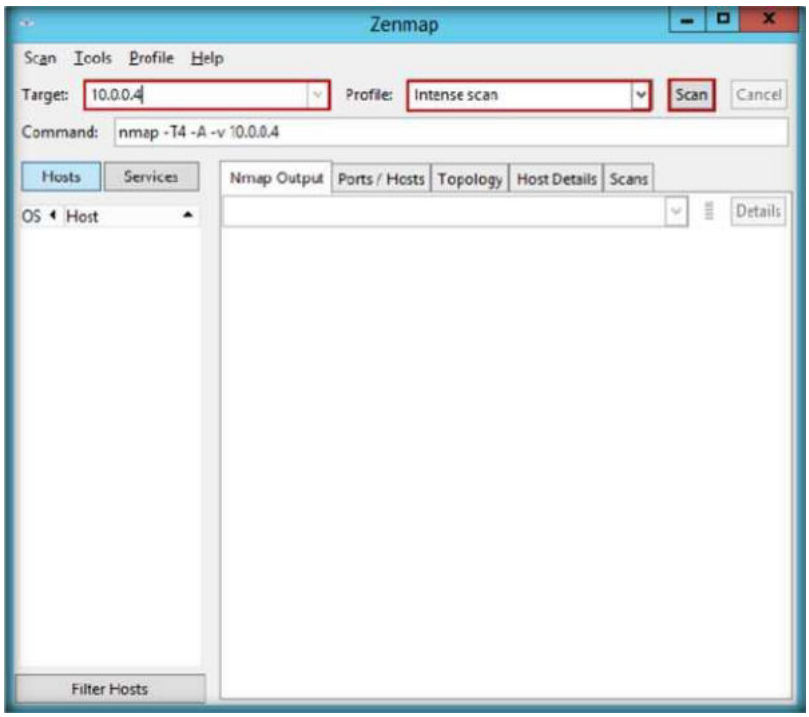


Рисунок 6.4: настройка цели в The Zenmap

8. Nmap сканирует указанный IP и выводит результаты во вкладке Nmap Output.

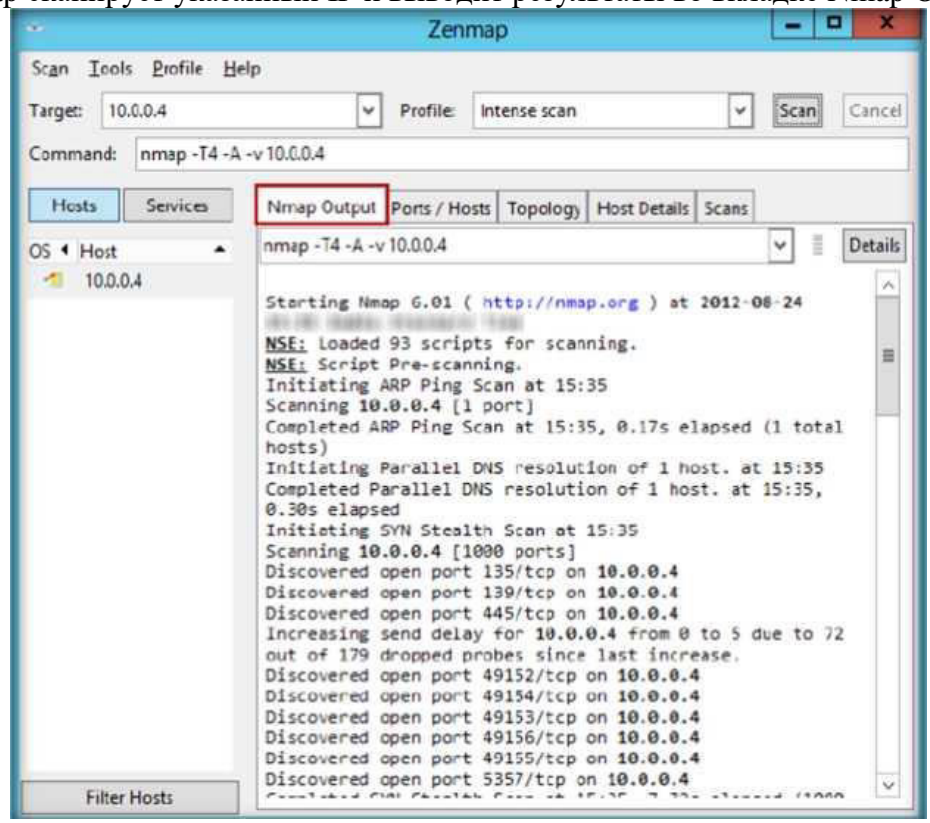


Рисунок 6.5: Nmap Output

9. После сканирования Nmap выводит результаты.

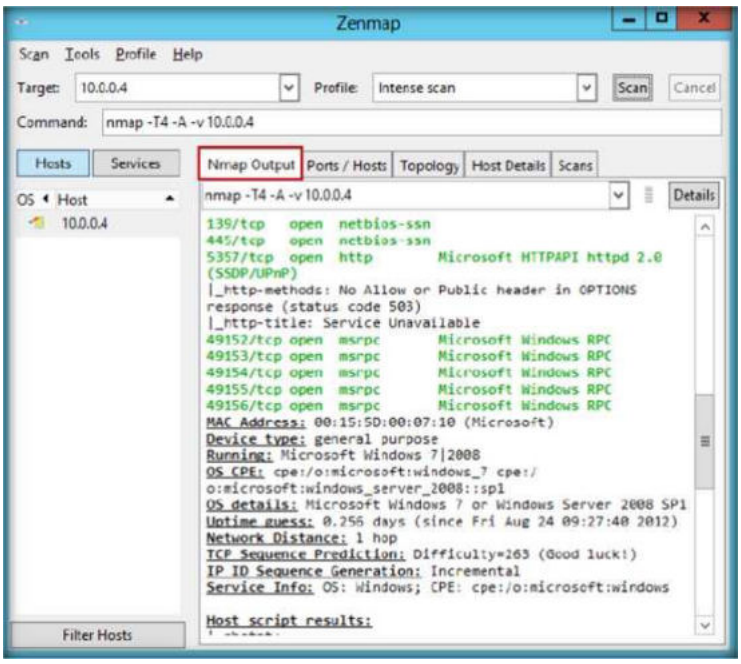


Рисунок 6.6: Nmap Output

10. Нажмите Ports/Hosts чтобы получить больше информации о сканировании.
11. Nmap также показывает порты, протоколы, службы и версии.

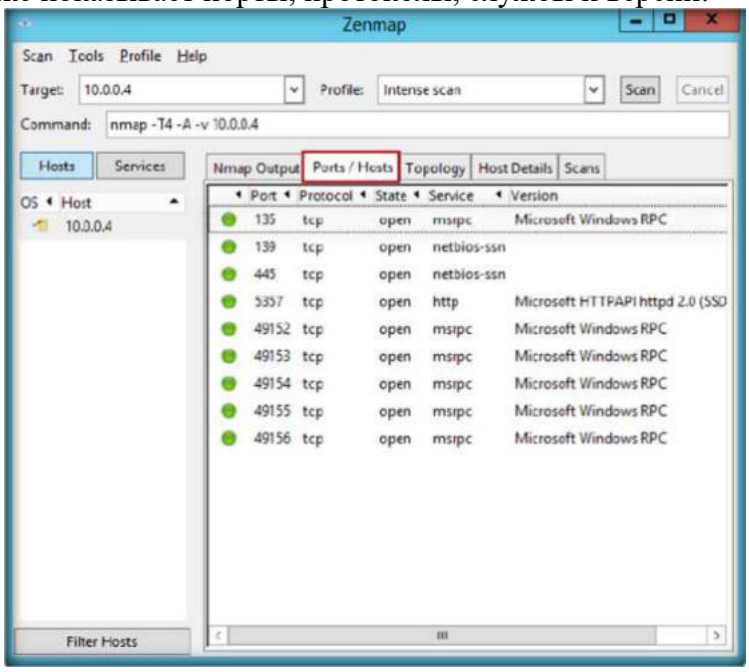


Рисунок 6.7: Ports/Hosts

12. Нажмите вкладку Topology чтобы просмотреть топологию выбранного IP.

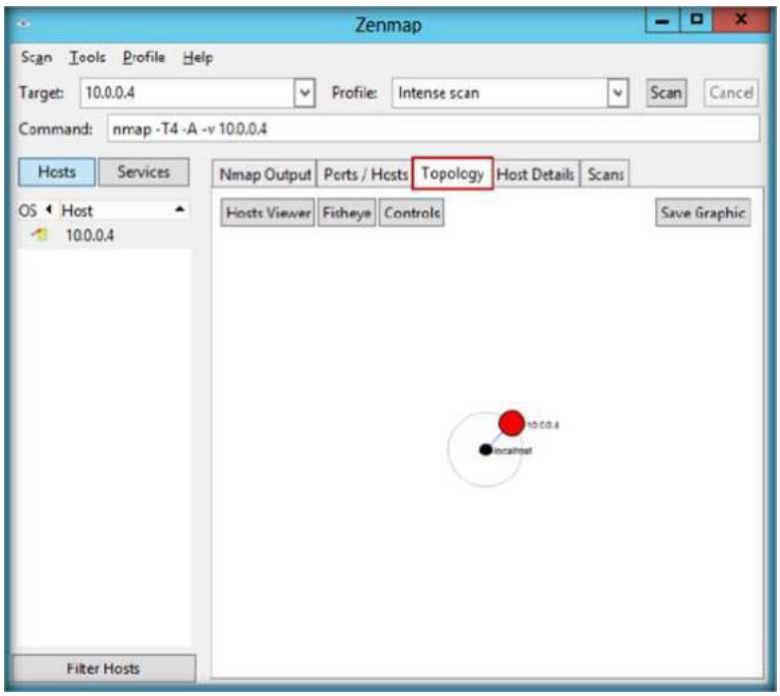


Рисунок 6.8: Topology

13. Нажмите Host Details чтобы узнать детали все узлов, обнаруженных во время сканирования профиля.

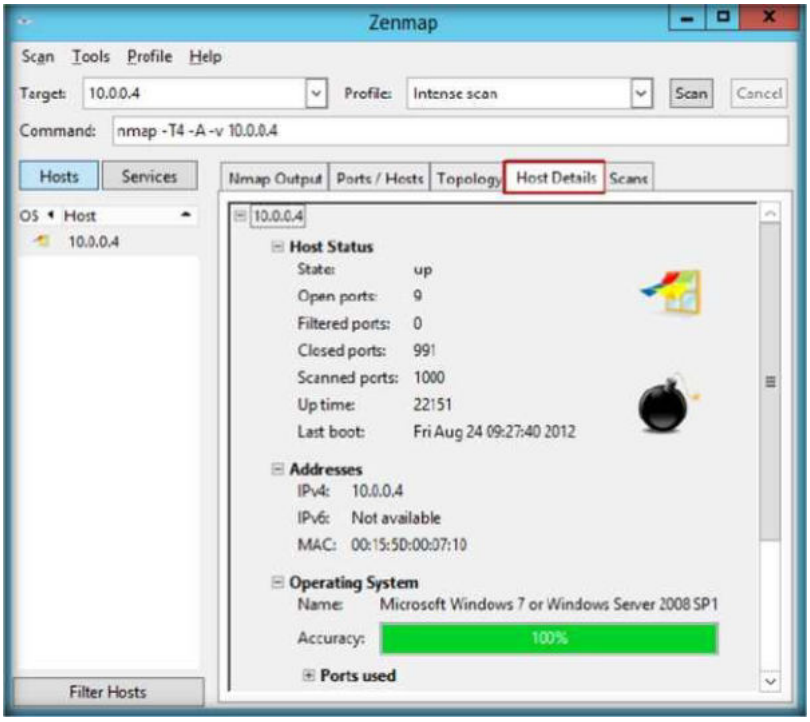


Рисунок 6.9: Host Details

14. Нажмите Scans чтобы отсканировать детали для выбранных IP адресов.

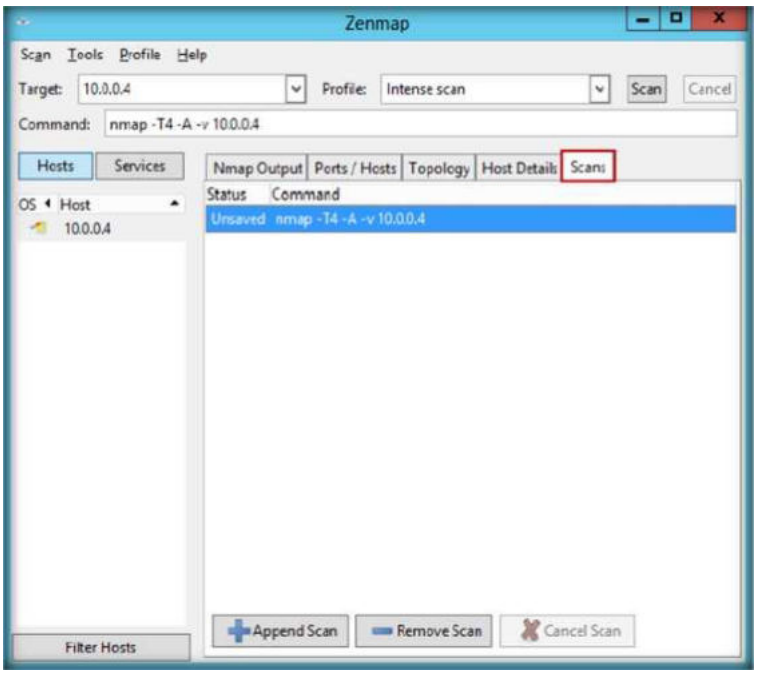


Рисунок 6.10: Scan

15. Теперь нажмите вкладку Services, которая покажет список доступных служб.
16. Нажмите службу http для перечисления всех адресов, имен узлов, портов и их состояний.

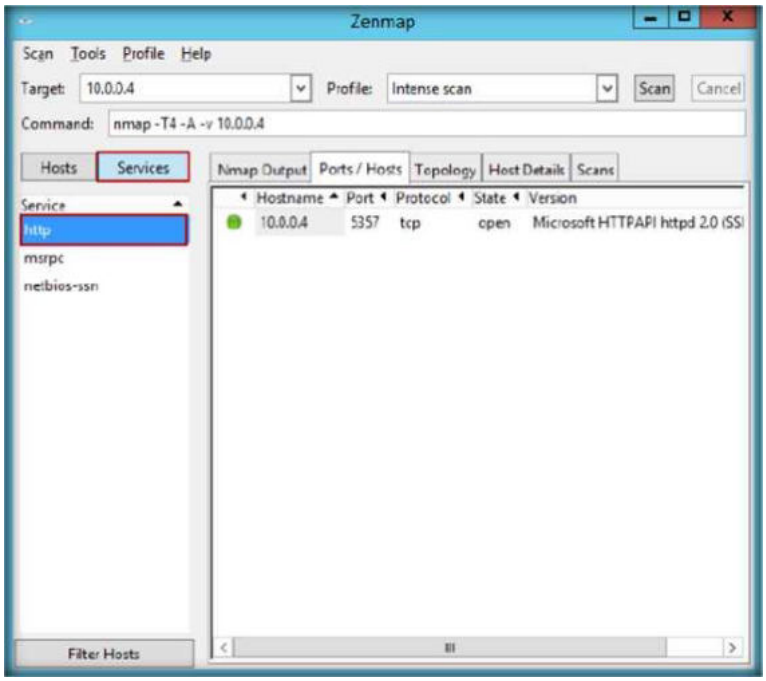


Рисунок 6.11: Services option

17. Нажмите msrpc для перечисления всех Microsoft Windows RPC.

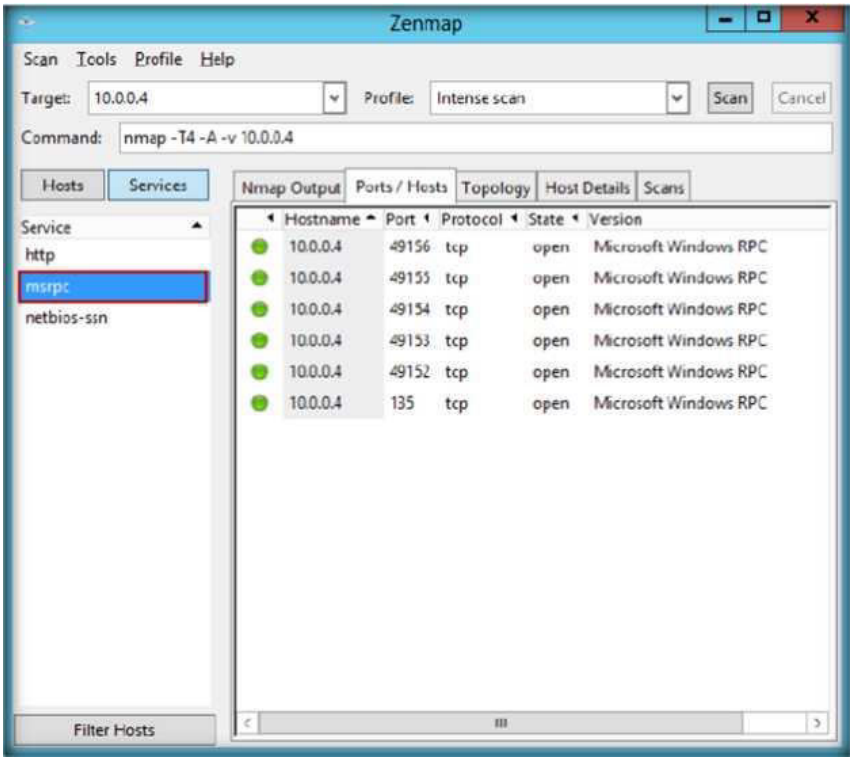


Рисунок 6.12 msrpc

18. Нажмите netbios-ssn для перечисления всех имен NetBIOS.

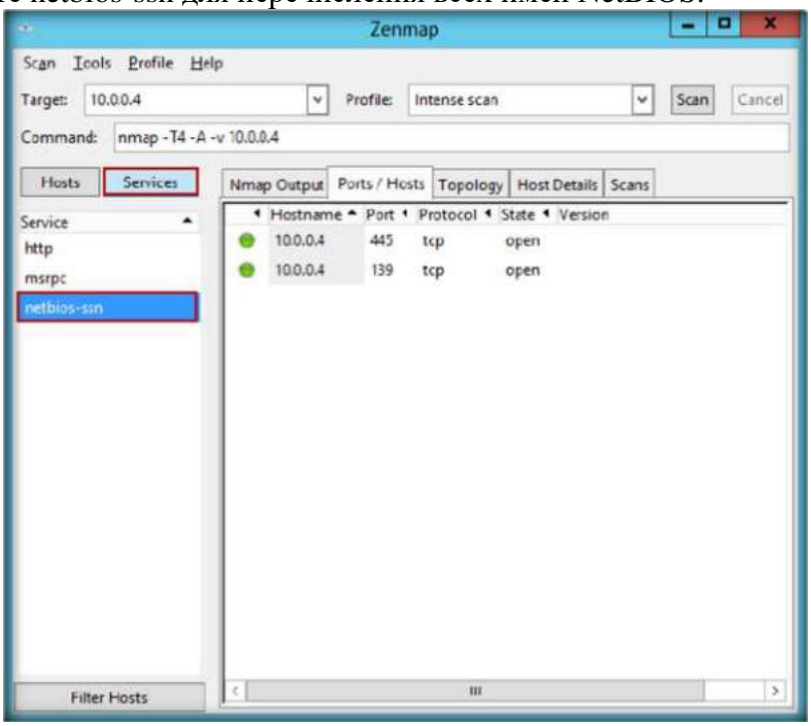


Рисунок 6.13: netbios-ssn

19. Xmas сканирование отправляет TCP удаленному устройству с URG, ACK, RST, SYN, and набором флагов FIN. FIN сканирует только OS TCP/IP разработанным согласно RFC 793. Текущая версия Microsoft Windows не поддерживает это.

20. Теперь, для выполнения Xmas сканирвоания, Вам необходимо создать новый специализация. Click Profile - New Profile or команду

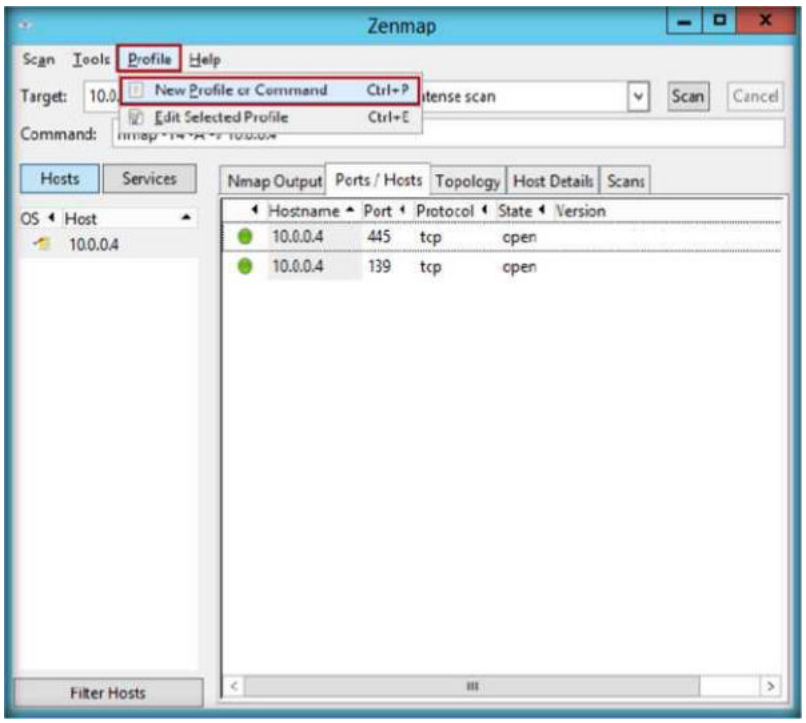


Рисунок 6.14: The Zenmap New Profile

21. В Profile, введите Xmas Scan в имя профиля.

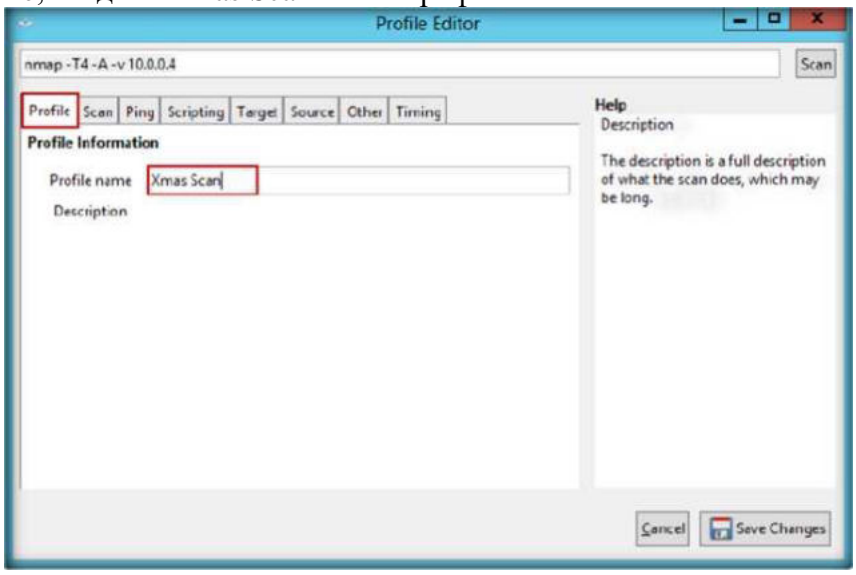


Рисунок 6.15: Редактор профиля

22. Нажмите вкладку Scan и выберите Xmas Tree сканирование (-sX).

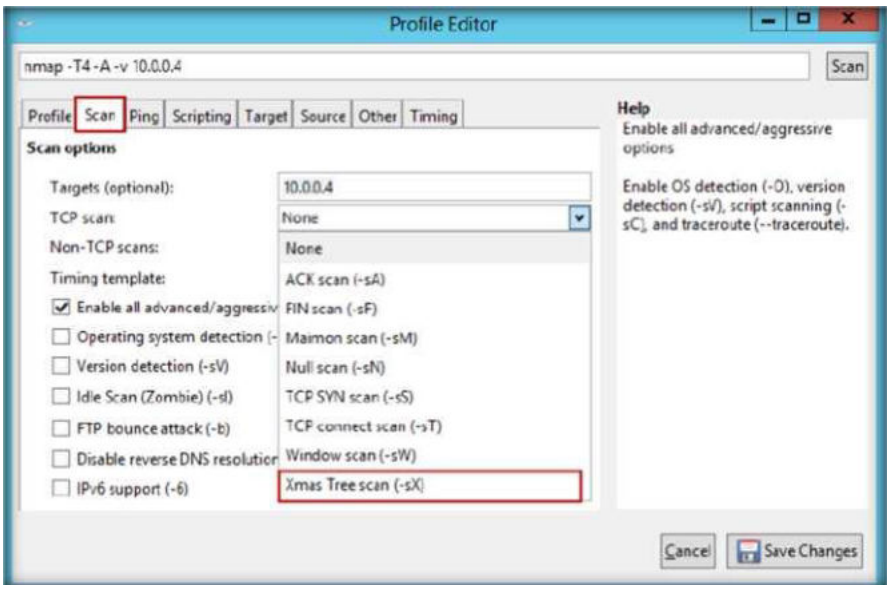


Рисунок 6.16: Scan

23. Выберите None в Non-TCP сканировании, далее выберите Aggressive (- T4) и нажмите сохранить изменения.

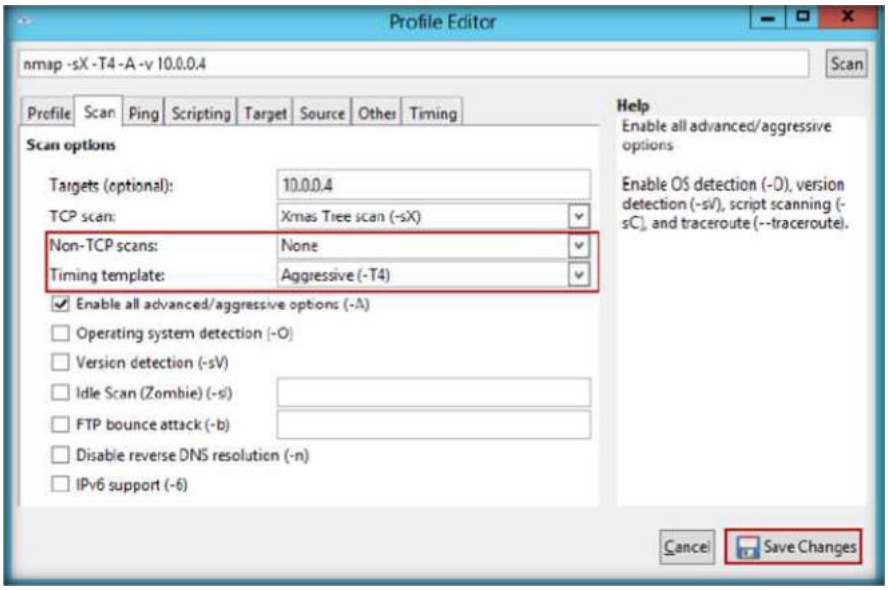


Рисунок 6.17: Scan t

24. Введите IP адрес цели и тип сканирования Xmas. Нажмите сканировать.

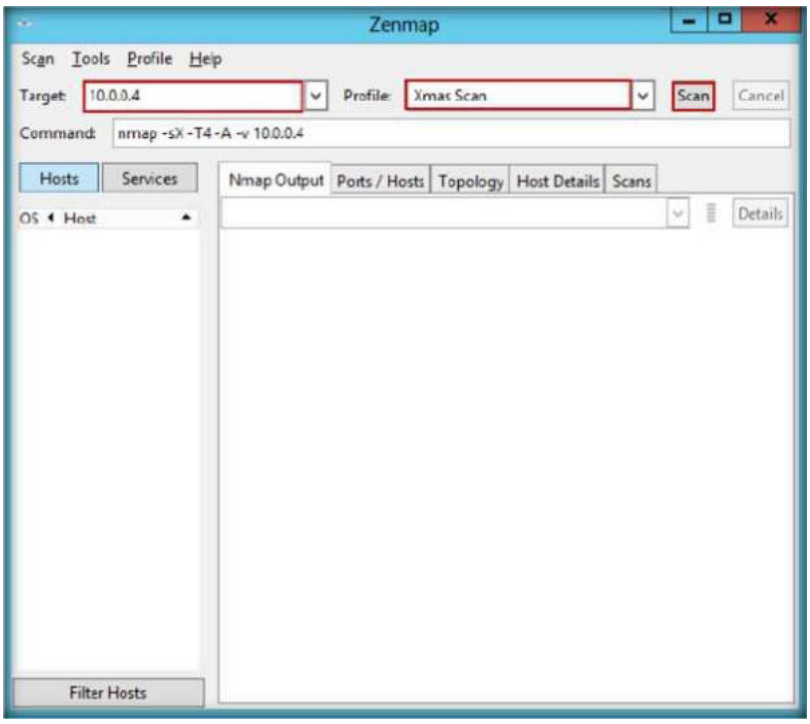


Рисунок 6.18: Настройки сканирования

25. Nmap сканирует IP адрес и выводит на экран результаты.

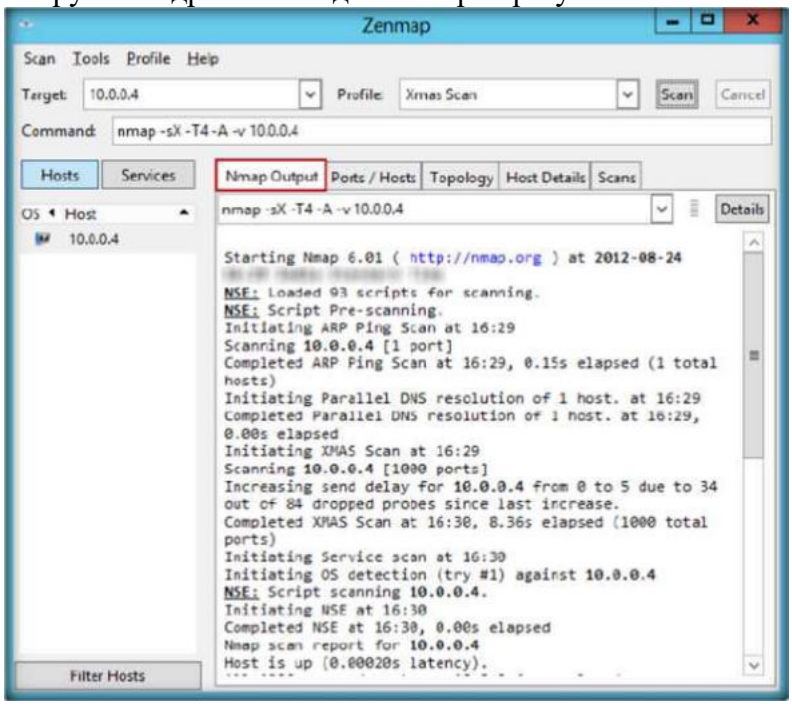


Рисунок 6.19: Результаты

26. Нажмите вкладку Services, чтобы увидеть все доступные службы.

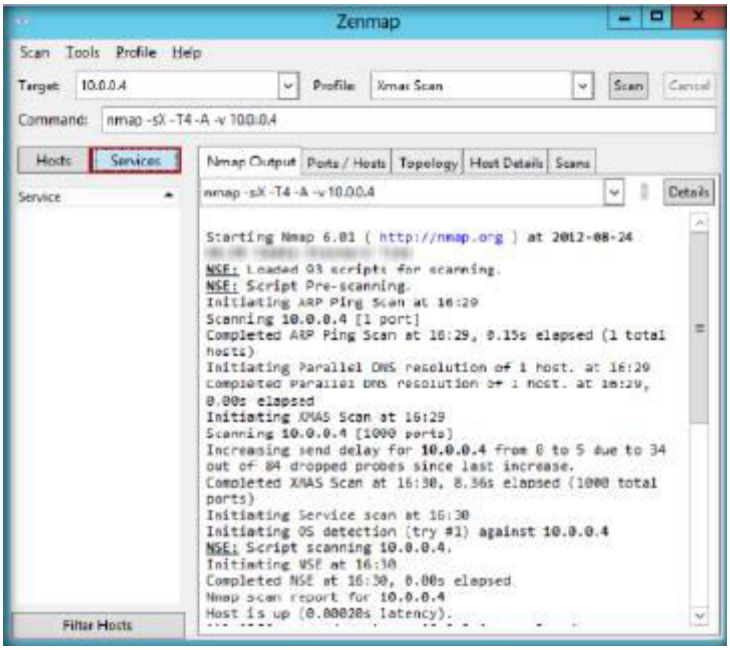


Рисунок 6.20: Services

27. Null сканирование работает только если реализация TCP/IP ОС разработана согласно стандарту RFC 793. Атакующий при этом передает кадр TCP без флагов.

28. Чтобы выполнить нулевое сканирование для выбранного IP, создайте новый специализация. Click Profile -> New Profile или

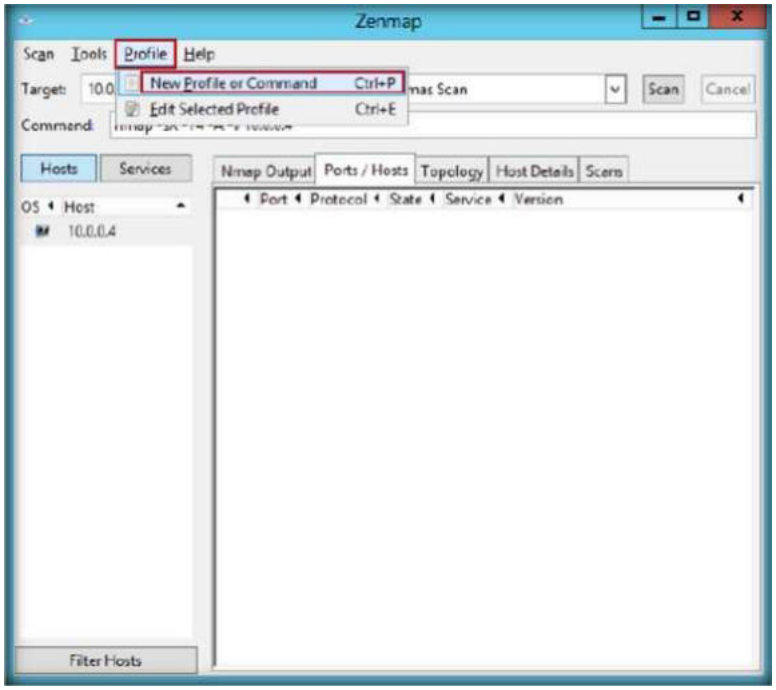


Рисунок 6.21: New Profile

29. Во вкладке Profile, введите имя Null Scan.

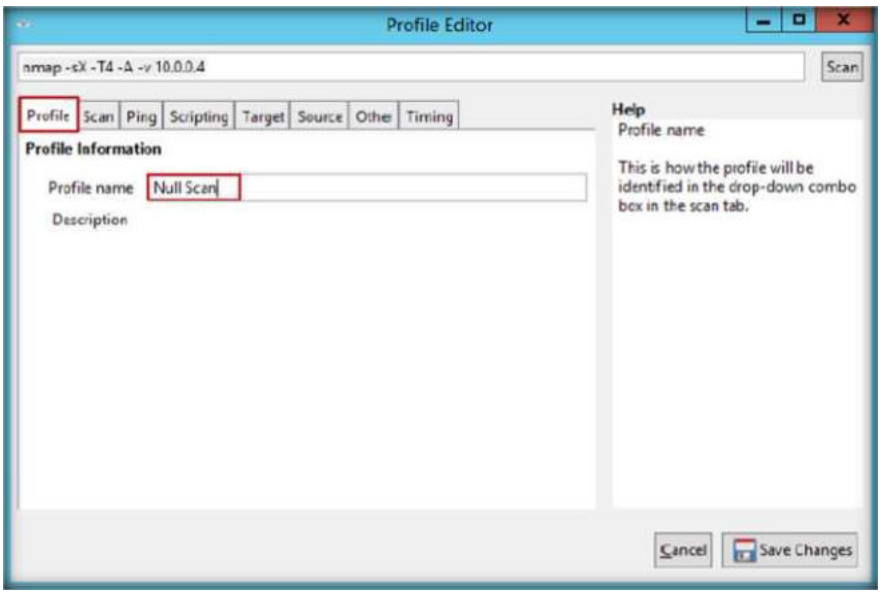


Рисунок 6.22: Profile

30. Нажмите вкладку Scan. Теперь выберете Null Scan (-sN) из выпадающего списка.

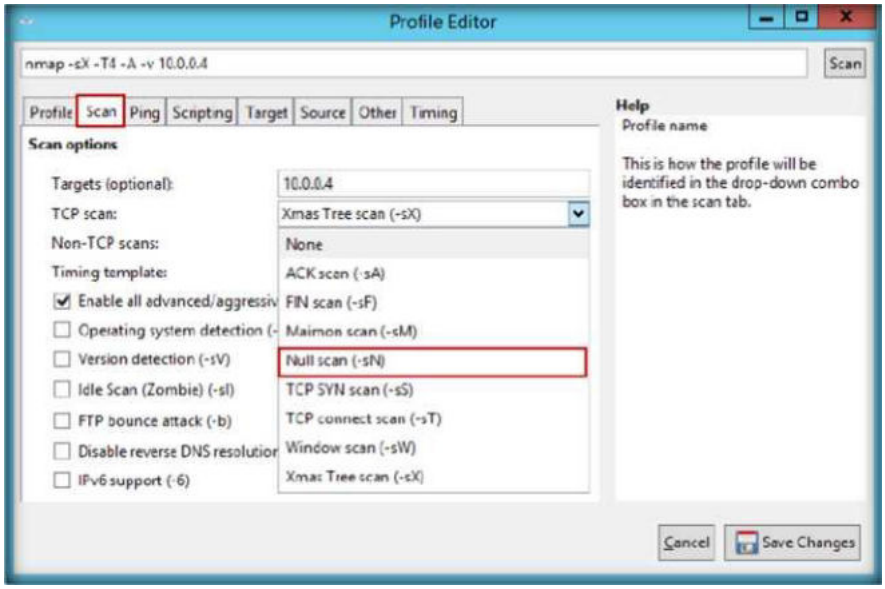


Рисунок 6.23: Profile

31. Выберите None из Non-TCP сканирования и Aggressive (-T4).
32. Нажмите сохранить изменения.

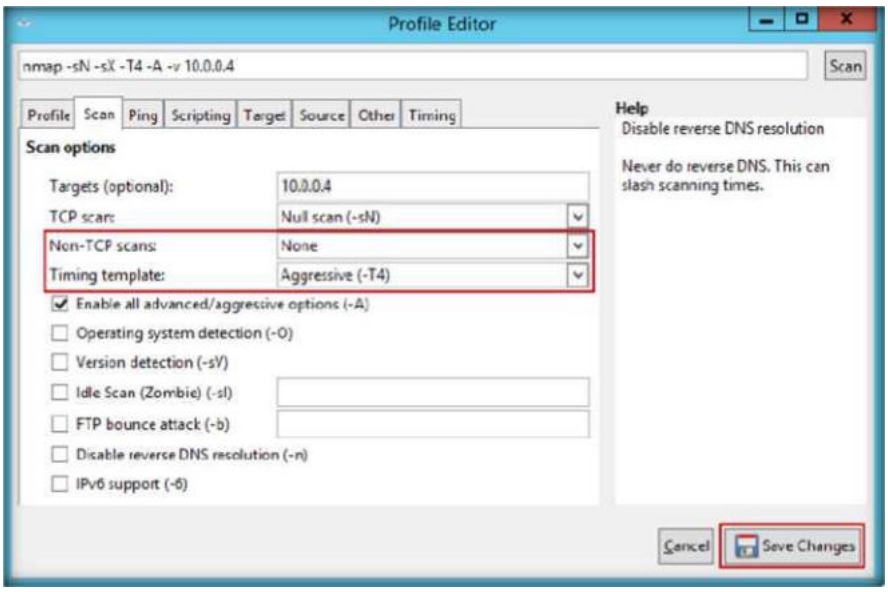


Рисунок 6.24: Profile

33. В главном окне введите IP цели и выберете нулевой специализация затем нажмите Сканировать.

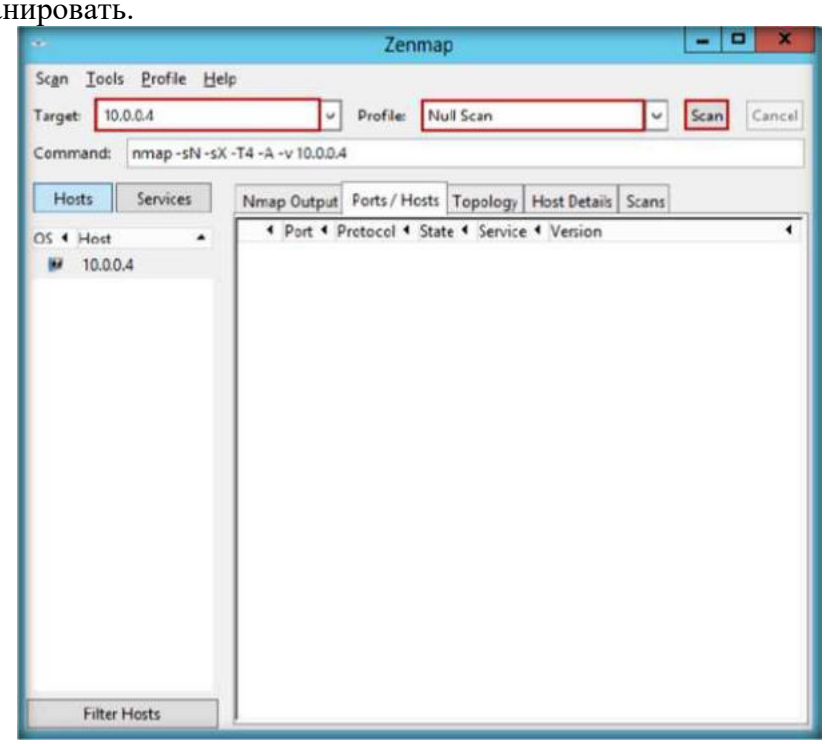


Рисунок 6.25: Настройка сканирования.

34. Nmap сканирует выбранный IP и выводит результаты.

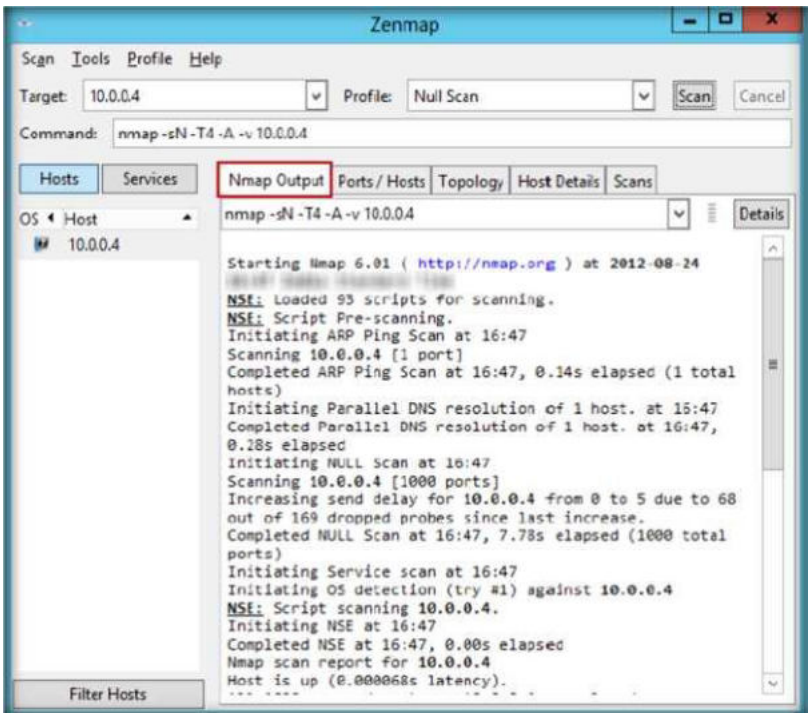


Рисунок 6.26: Nmap Output

35. Щелкните по вкладке Host Details, чтобы просмотреть детали узла..

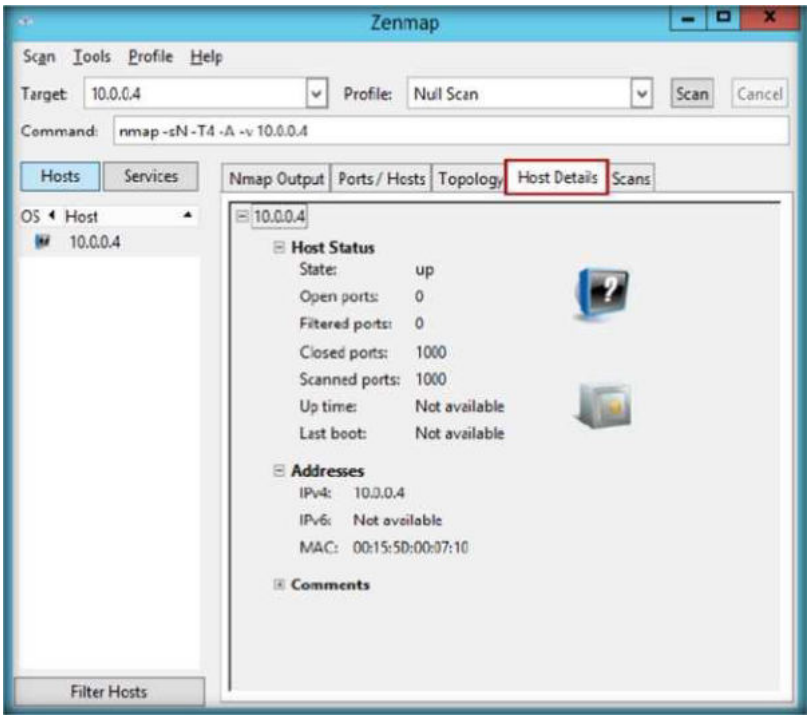


Рисунок 6.27: Host Details

36. Атакующий отправляет текстовый пакет ACK со случайным порядковым номером. Ни один ответ не означает что порт фильтруется..

37. Для использования ACK Flag сканирования IP, создайте новый Profile -> New Profile или Ctrl+P.

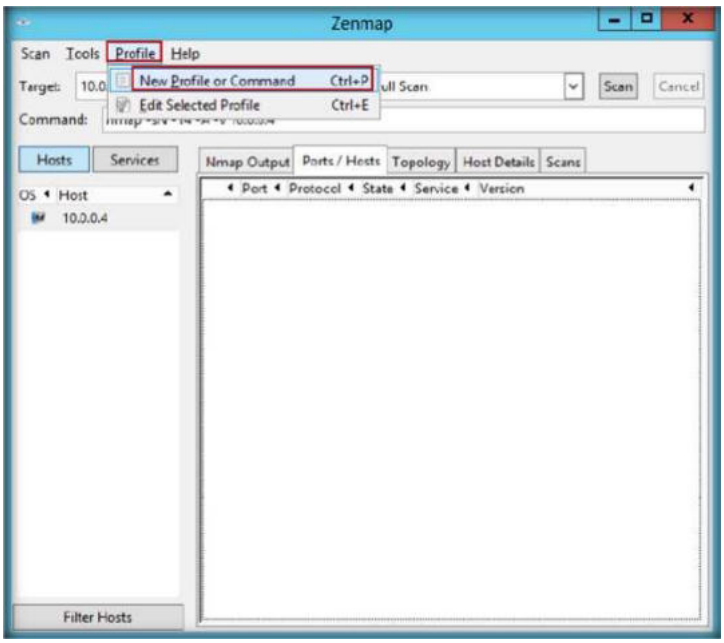


Рисунок 6.28: New Profile.

38. В профиле введите имя ACK Flag Scan.

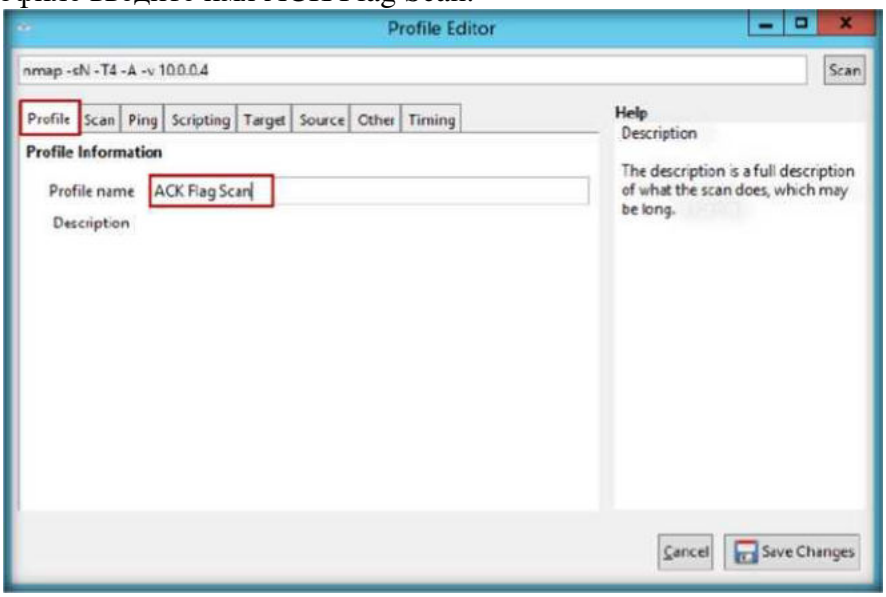


Рисунок 6.29: Profile

39. Чтобы выбрать параметры для сканирования ACK, щелкните по вкладке Scan, выберите сканирование ACK (-sA).

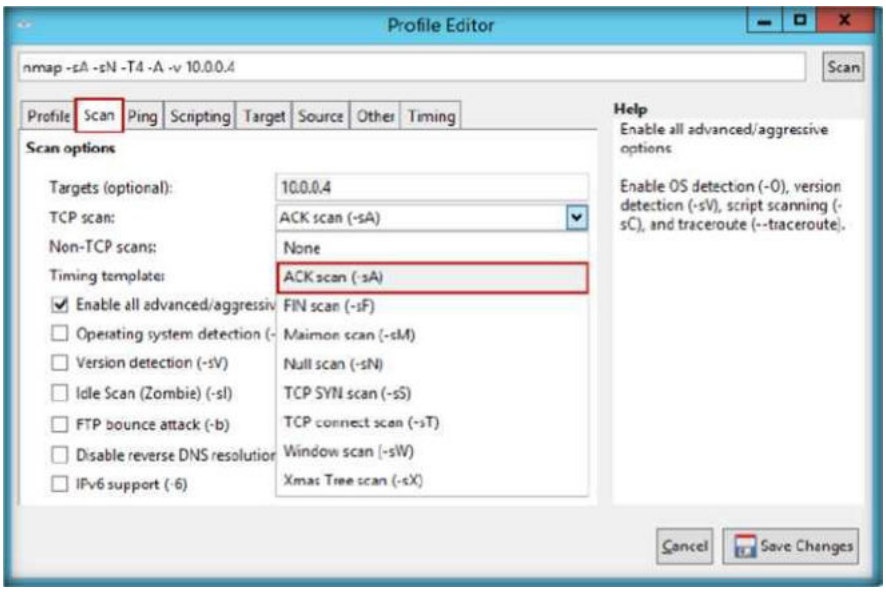


Рисунок 6.30: Scan

40. Щёлкните по вкладке Ping и выберите IPProto (-PO) probe и нажмите сохранить.

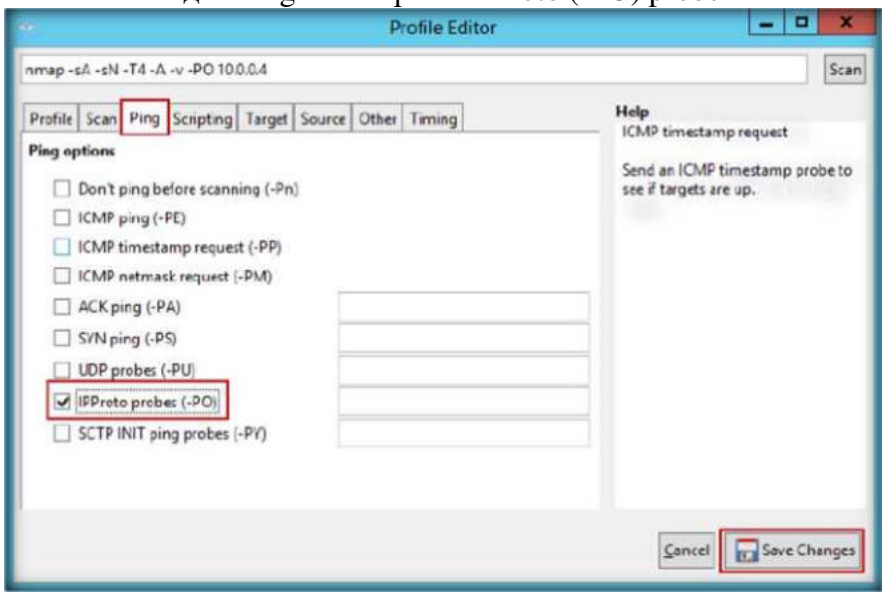


Рисунок 6.31: Ping

41. В главном окне программы введите IP цели (10.0.0.3), выберите сканирование ACK Flag Scan из профиля и нажмите Сканировать.

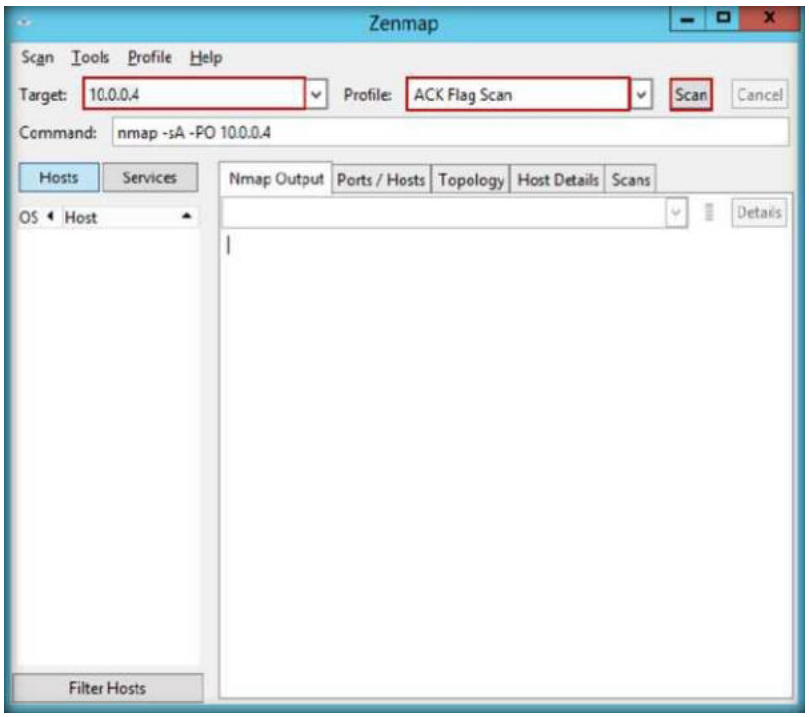


Рисунок 6.32: Настройка сканирования

42. Nmap сканирует целевой IP адрес и выводит результат на экран.

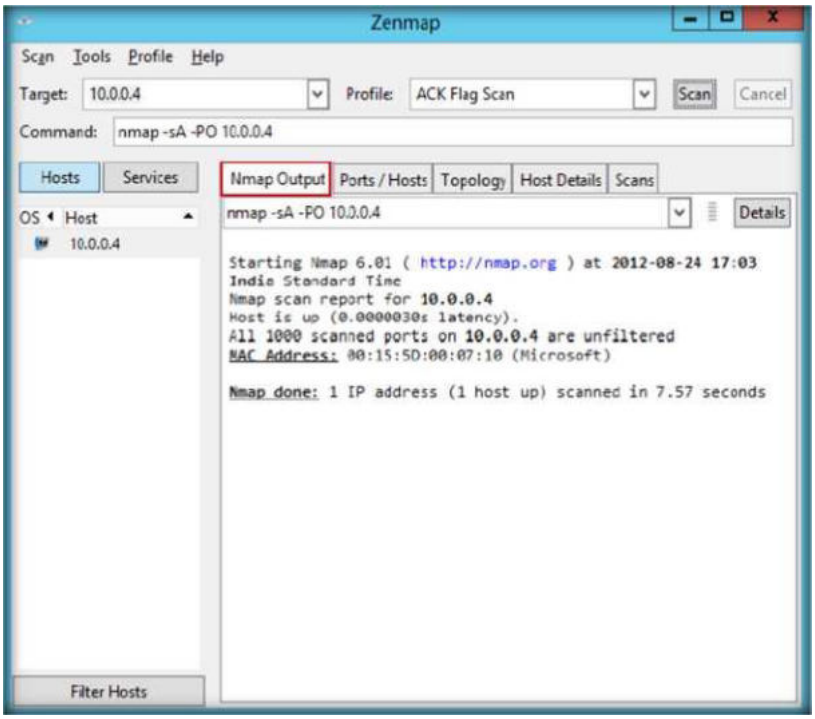


Рисунок 6.33: Nmap Output

43. Чтобы рассмотреть больше деталей нажмите Host Details.

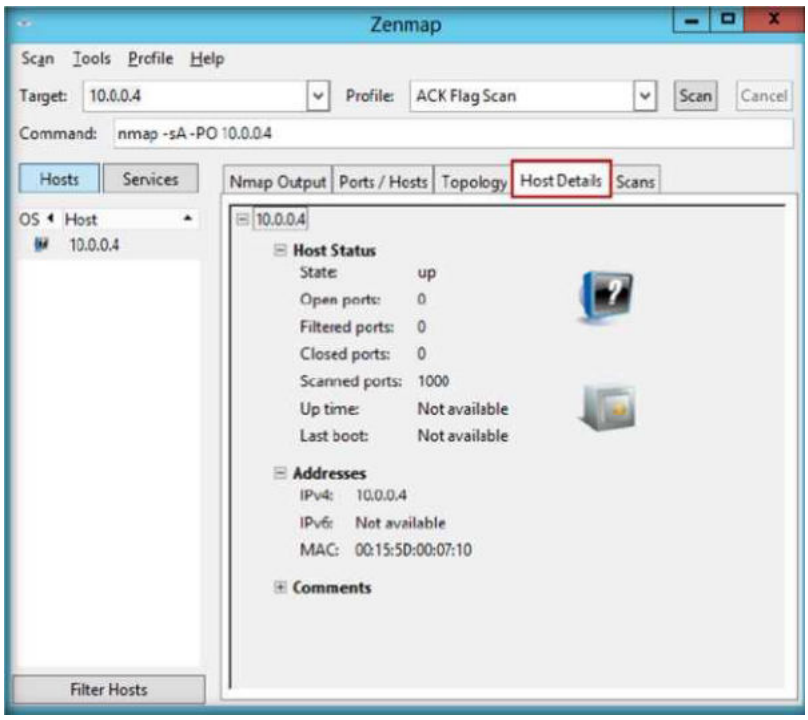


Рисунок 6.34: Host Details

Анализ практической работы

Запишите все IP адреса, открытые и закрытые порты, службы и протоколы, которые вы обнаружили во время лабораторной.

Средства	Собранная информация
Nmap	Типы сканирования: – Intense scan – Xmas scan – Null scan – ACK Flag scan
	Детали Intense сканирования - Nmap Output – ARP Ping Scan - 1 host – Parallel DNS resolution of 1 host – SYN Stealth Scan • Discovered open port on 10.0.0.4 o 135/tcp, 139/tcp, 445/tcp, ... – MAC Address – Operating System Details – Uptime Guess – Network Distance – TCP Sequence Prediction – IP ID Sequence Generation – Service Info

Вопросы

1. Проанализируйте и оцените результаты сканируя с помощью:
    a. Stealth Scan (Half-open Scan)
    b. nmap -P
2. Выполните обратное TCP Flag Scanning and проанализируйте узлы и службы для целевой машины в сети.

Практическое занятие №7. Сканирование сети с помощью NetScan Tools Pro

Цели работы

Целью работы является диагностика, контроль и обнаружение всех устройств в сети.
Вам необходимо:

1) Обнаружить IPv4/IPv6 адрес, имя хоста, имя узла, email и URLs.
2) Определить локальный порт.

Средства для выполнения практической работы

Вам нужно:

1) NetScan Tools Pro.
2) Его можно загрузить по ссылке http://www.netscantools. com/nstpromain.html.
3) Скриншоты могут отличаться.
4) Windows Server 2012.
5) Права администратора.

Краткие теоретические сведения Представление о сканировании сети

Сетевое сканирование – процесс исследования сети, для обеспечения контроля данных или устройств в сети. Сетевое сканирование можно использовать снаружи сети для определения уязвимостей.

NetScan Tool Pro выполняет:

1) Контроль доступности сетевых устройств.
2) Уведомляет IP адреса, узлы, домены и порты.

Постановка задачи

Установите NetScan Tool Pro в Window Server 2012.

1. Нажмите Пуск.

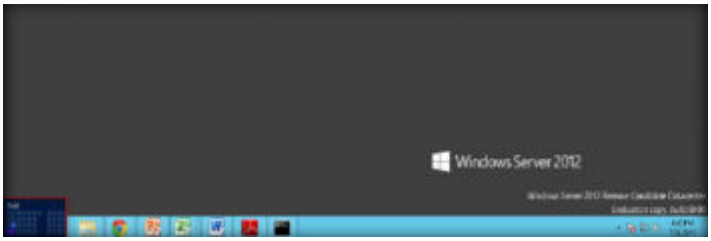


Рисунок 7.1: Windows Server 2012 – Рабочий стол

2. Нажмите NetScan Tool Pro.

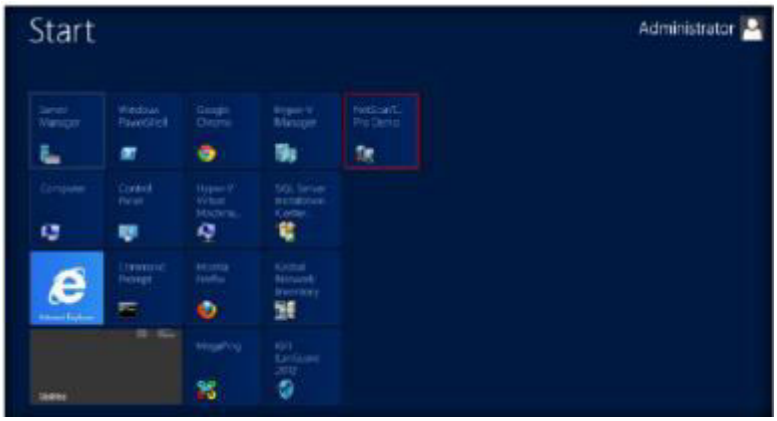


Рисунок 7.2 Windows Server 2012 – Приложения

3. Если вы используете демо-версию NetScan Tools Pro, тогда нажмите начать Demo.
4. Откройте или создайте окно New Result Database-NetScanTools Pro, введите имя новой БД
5. Расположение каталога по умолчанию, нажмите продолжить.

Рисунок 7.3: NetScan Tools Pro

6. Главное окно The NetScan Tools Pro представлено на рисунке.

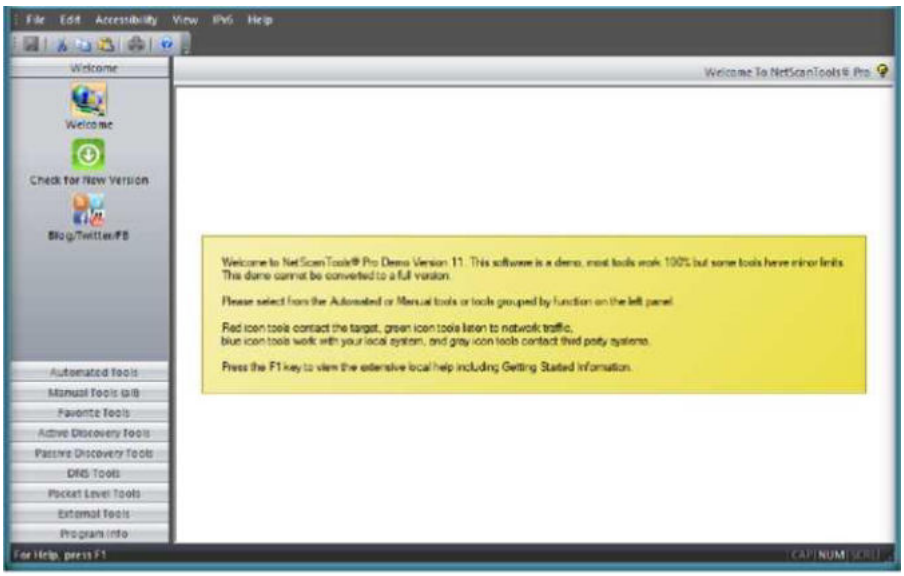


Рисунок 7.4: NetScan Tools Pro

7. Выберите Manual Tools (all) слева и нажмите ARP Ping.
8. Нажмите OK.

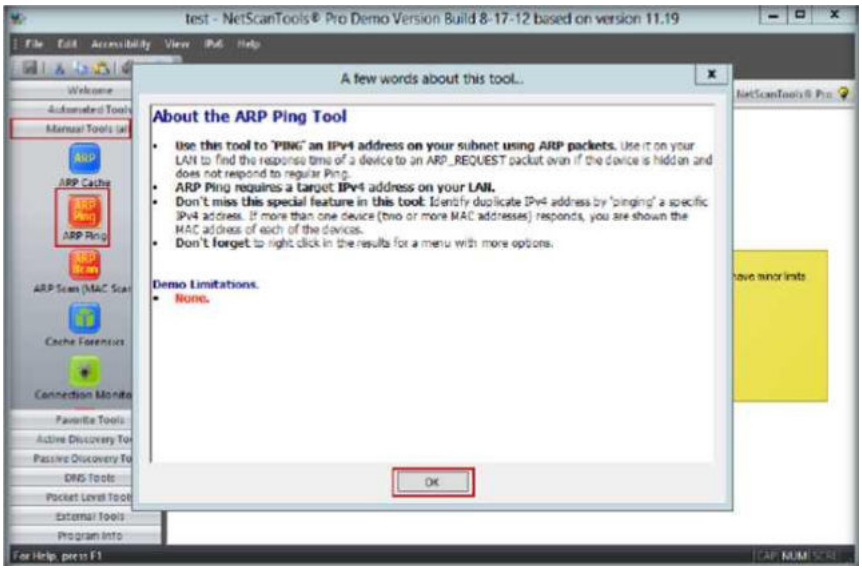


Рисунок 7.5: Опции

9. Выберите Send Broadcast ARP, затем переключатель Unicast ARP, введите IP адрес IPv4 Address, и нажмите Send Arp.

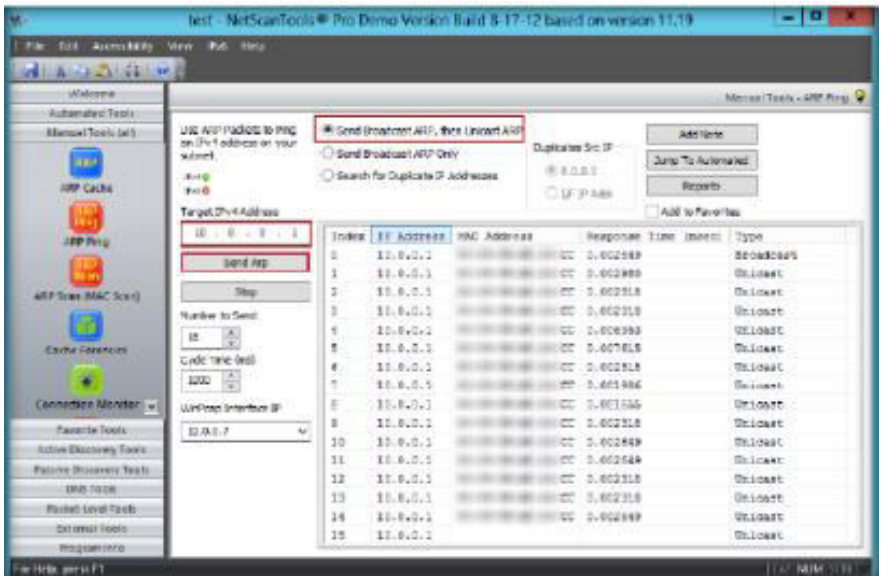


Рисунок 7.6: Результат ARP Ping

10. Нажмите ARP Scan (MAC Scan) слева. Откроется окно с информацией. Нажмите OK.

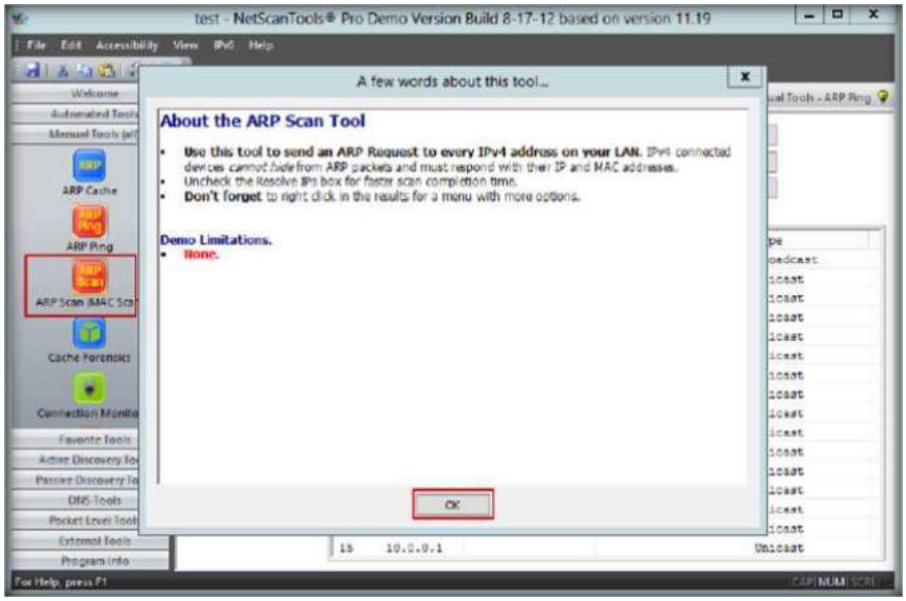


Рисунок 7.7: ARP Scan (MAC Scan)

11. Введите диапазон IPv4адреса.
12. Нажмите Do Arp Scan.

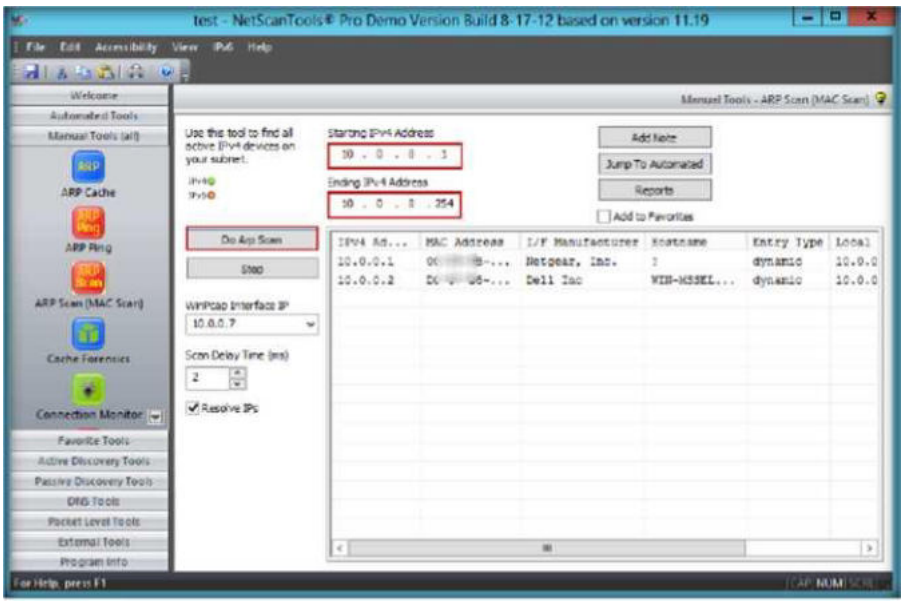


Рисунок 7.8 Результат ARP Scan (MAC Scan)

13. Нажмите DHCP Server Discovery слева, откроется окно с информацией о DHCP Server Discovery Tool. Нажмите OK.

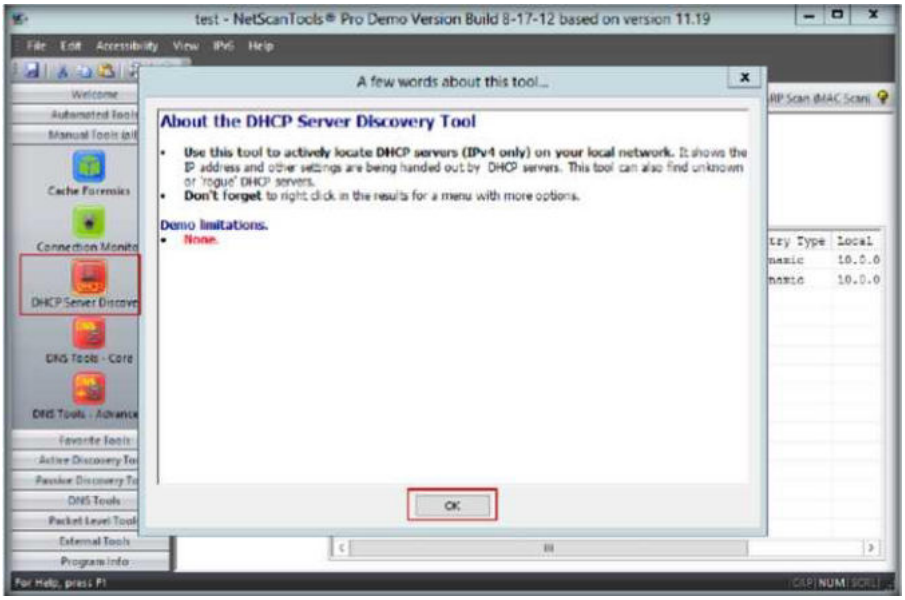


Рисунок 7.9: DHCP Server Discovery Tool

14. Выберете все опции Discover и нажмите Discover DHCP Servers.

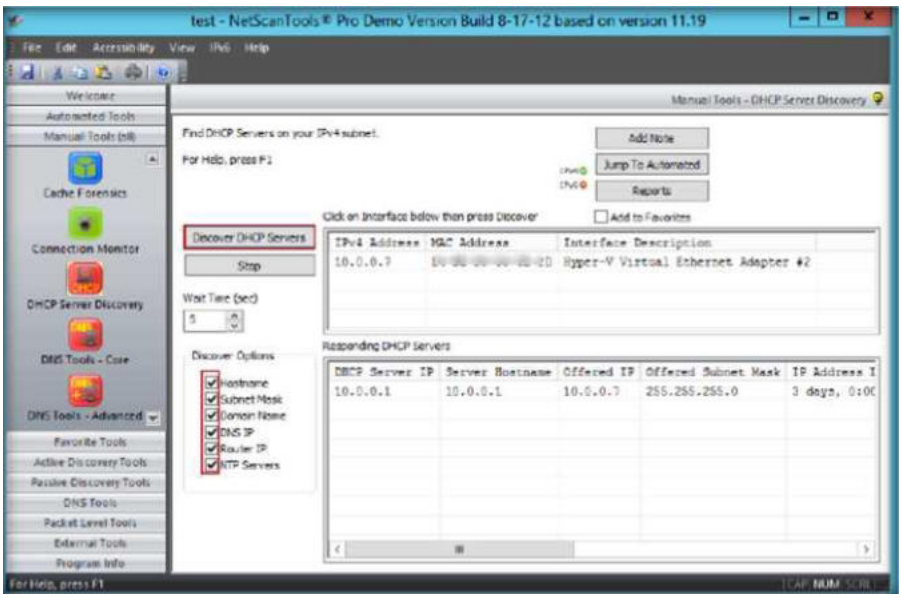


Рисунок 7.10: Результат DHCP Server Discovery

15. Нажмите Ping сканер. Появится окно с информацией о Ping Scanner tool. Нажмите OK.

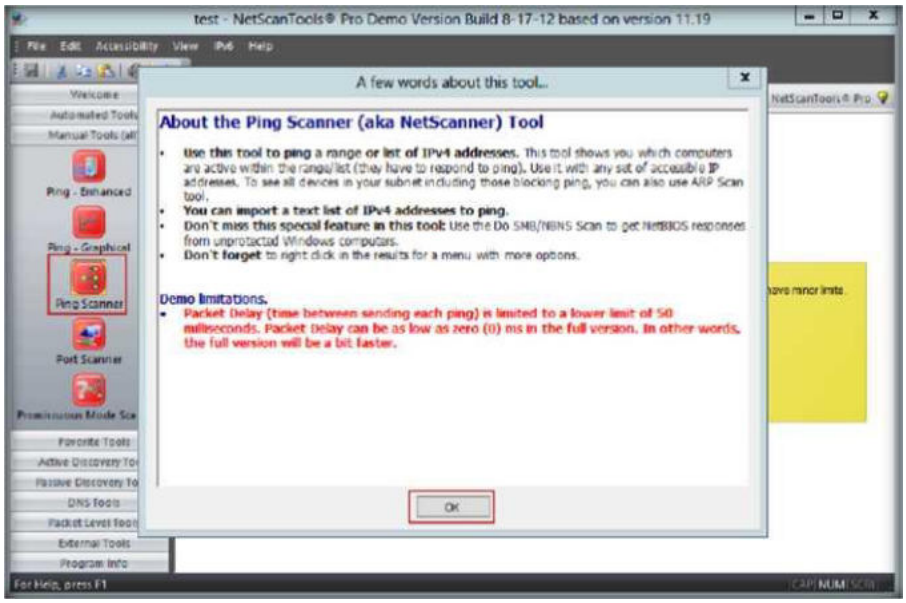


Рисунок 7.11: Ping scanner

16. Выберете переключатель Use Default System DNS, и введите диапазон IP в полях Start IP и End IP.

17. Нажмите Start.

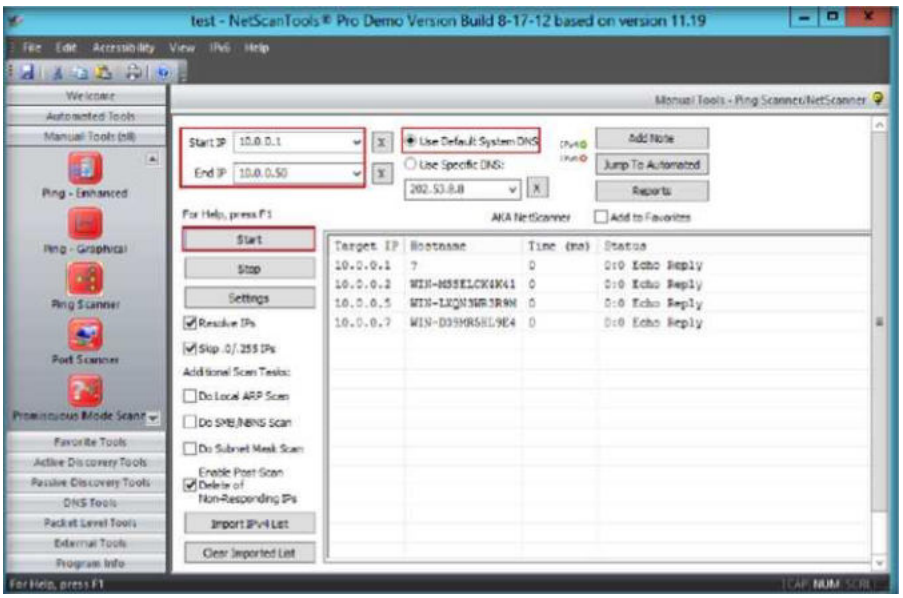


Рисунок 7.12: Результат

18. Нажмите Port scanner. Появится окно с информацией о port scanner tool. Нажмите OK.

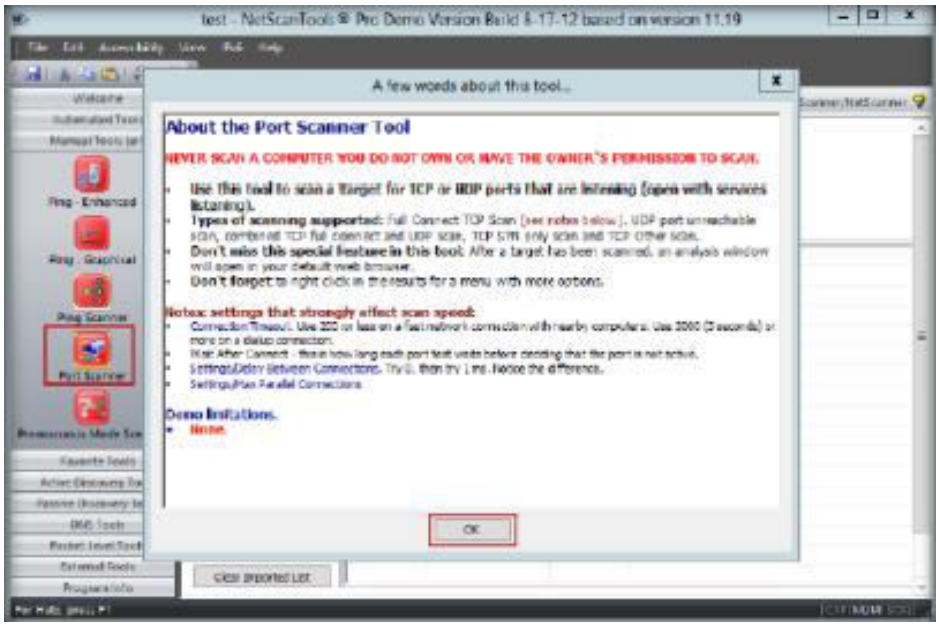


Рисунок 7.13: Port scanner

19. Введите IP адрес и выберете переключатель TCP Ports only.
20. Нажмите Scan Range of Ports.

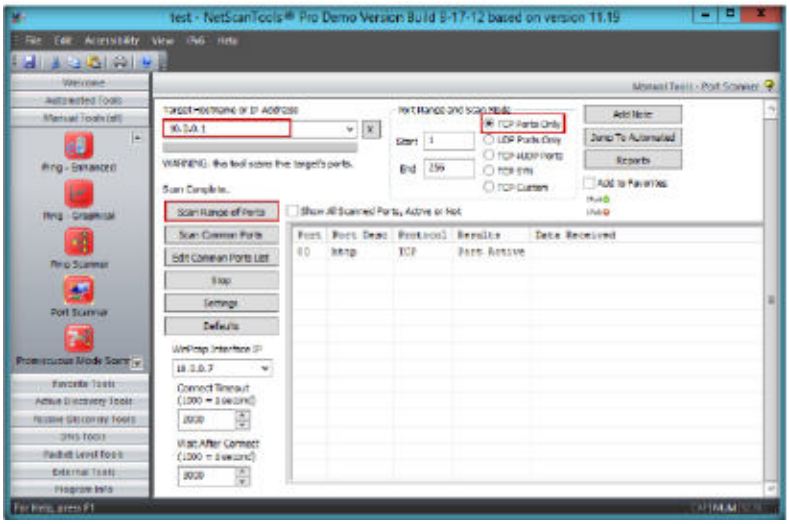


Рисунок 7.14: Результат Port scanner

Анализ практической работы
Запишите все IP адреса, порты, службы и протоколы, которые вы обнаружили.

Средства	Собранная информация
NetScan Tools pro	Результаты ARP Scan: – IPv4 Address – MAC Address – I/F Manufacturer – Hostname – Entry Type – Local Address
	Информация о серверах Discovered DHCP: – IPv4 Address: 10.0.0.7 – Interface Description: Hyper-V Virtual Ethernet Adapter #2 – DHCP Server IP: 10.0.0.1 – Server Hostname: 10.0.0.1 – Offered IP: 10.0.0.7 – Offered Subnet Mask: 255.255.255.0

Вопросы

1. Инструменты NetScan Tools Pro поддерживают прокси-серверы или брандмауэры?

Практическое занятие №8. Чертеж диаграмм сети с помощью LANSurveyor

Цели работы

Цель этой практической состоит в обнаружении и построении топологии сети.
Вам необходимо:

1) Нарисовать карту вашей сети.
2) Создать отчет, который включает все ваши перключатели и концентраторы

Средства для выполнения практической работы

1) LANSurveyor.
2) Можно загрузить по ссылку http: // www.solarwinds.com/
3) Скриншоты могут отличаться.
4) Windows Server 2012.
5) Браузер с интернетом.
6) Права администратора для запуска LANSurveyor tool.

Краткие теоретические сведения

Представление о LANSurveyor

SolarWinds LAN автоматически находит вашу сеть и производит ее построение в виде графика, которое можно экспортировать в Visio. Программа автоматически обнаруживает изменения и изменяет топологию.

Постановка задачи

Установите LANSurveyor в Windows Server 2012.

1. Нажмите Пуск

Рисунок 8.1: Windows Server 2012 – Рабочий стол

2. Заупстите LANSurvyor.

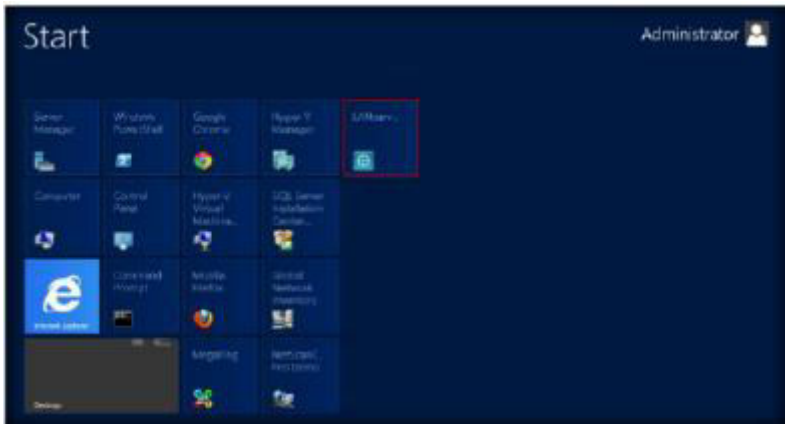


Рисунок 8.2 Windows Server 2012 – Приложения

3. Рассмотрите ограничение программы, а затем нажмите продолжить.

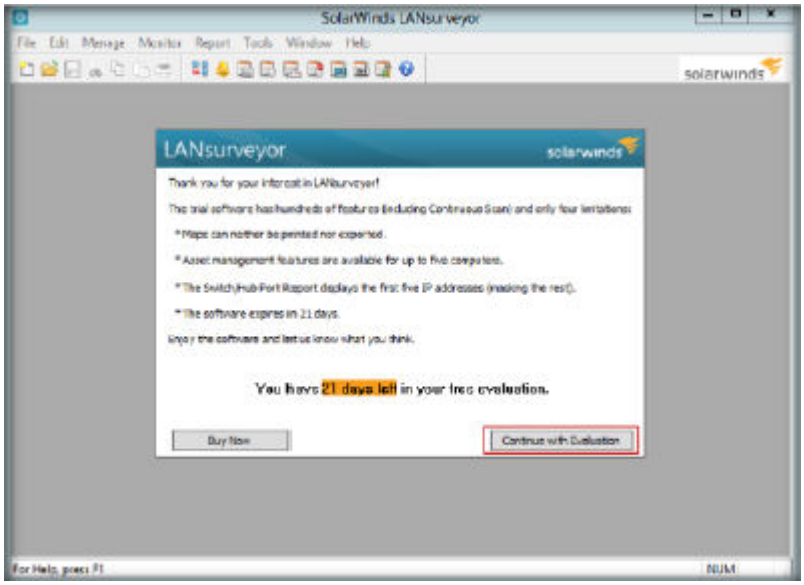


Рисунок 8.3: Ограничения LANSurveyor

4. Далее нажмите Старт.

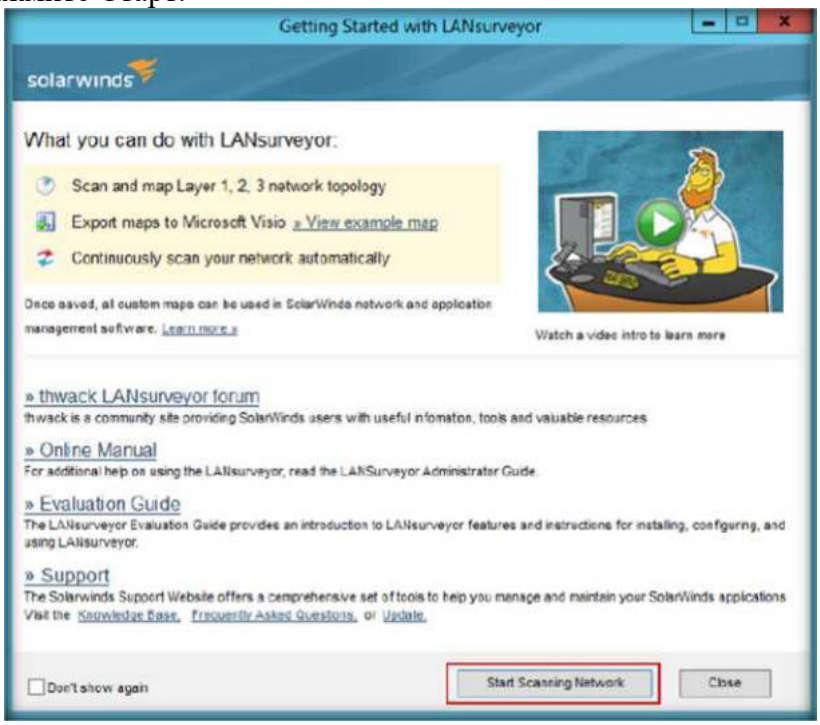


Рисунок 8.4: Начало

5. Появится окно, в котором необходимо ввести начальный и конечный IP адрес, затем нажать Старт.

Рисунок 8.5: Новая карта

6. Введенные IP будут отображаться как на следующем рисунке.

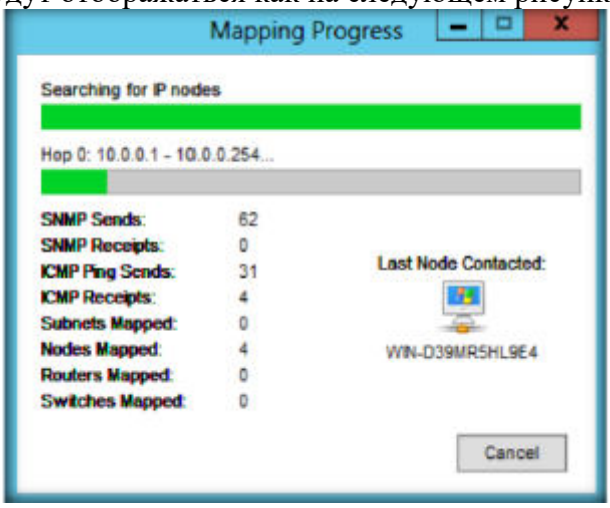


Рисунок 8.6: Прогресс построения

7. LANsurveyor выводит на экран вашу карту сети.

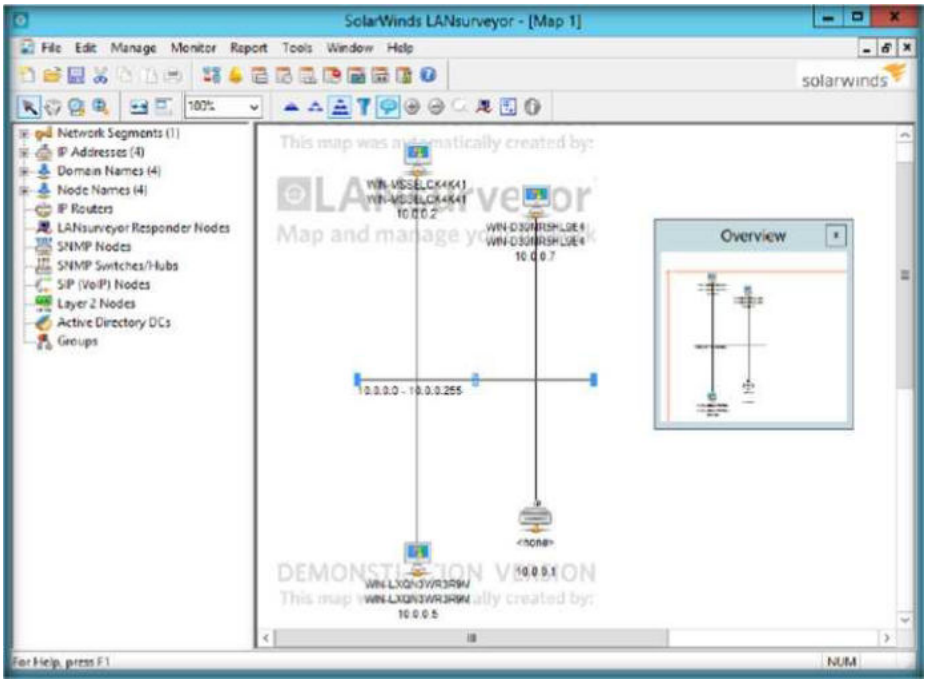


Рисунок 8.7: Карта сети

Анализ практической работы

Запишите все IP адреса, доменные имена, имена узлов и узлы SNMP, которые вы обнаружили.

Средства	Собранная информация
LANSurveyor	IP адрес: 10.0.0.1 -10.0.0.254
	IP Nodes Details:IPv4 Address: – SNMP Send - 62 – ICMP Ping Send - 31 – ICMP Receipts - 4 – Nodes Mapped - 4
	Детали сети: – IP Address - 4 – Domain Names - 4 – Node Names - 4

Вопросы

1. Могут ли быть обнаружены точки беспроводного соединения?

Практическое занятие №9. Отображение сети с помощью Friendly Pinger

Цели работы

Целью практической является обнаружение и схематическое изображение топологии сети.

Вам необходимо:

1) Изучить сеть.
2) Изобразить топологию сети.
3) Обнаружить новые устройства и модификации сети.
4) Выполнить управление запасами для аппаратных и программных активов.

Средства для выполнения практической работы

Вам необходимо:

1) Friendly Pinger.
2) Можно загрузит по ссылке http://www.kilievich.com/fpinger /dowidoad.htm.
3) Скриншоты могут отличаться.
4) Windows Server 2012.
5) Браузер с интернетом.
6) Права администратора для Friendly Pinger tool.

Краткие теоретические сведения Представление о построении сети

Сетевое отображение - исследование физической связи сетей. Сетевое отображение часто выполняется, чтобы проследить работу серверов и операционных систем сетей. Этот метод обнаруживает новые устройства и модификации, сделанные в топологии сети. Вы можете выполнять управление запасами для аппаратных и программных активов.

Friendly Pinger выполняет:

1) Контроль доступных сетевых устройств.
2) Уведомляет если какой либо сервер отключается.
3) Ping всех устройств.
4) Аудит всех компонентов сети.

Постановка задачи

1. Установите Friendly Pinger в Windows Server 2012.
2. Зайдите в Пуск.

Рисунок 9.1: Windows Server 2012 – Рабочий стол

3. Запустите Friendly Pinger.

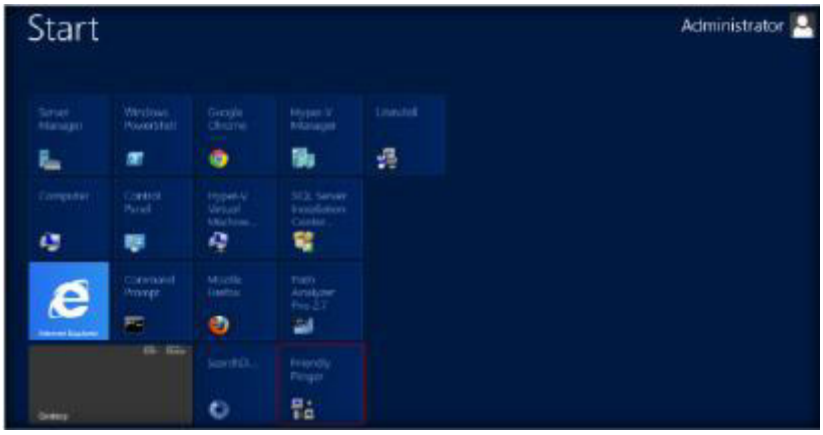


Рисунок 9.2: Windows Server 2012 – Приложения

4. The Friendly Pinger откроется и выдаст онлайн запрос.
5. Нажмите No.

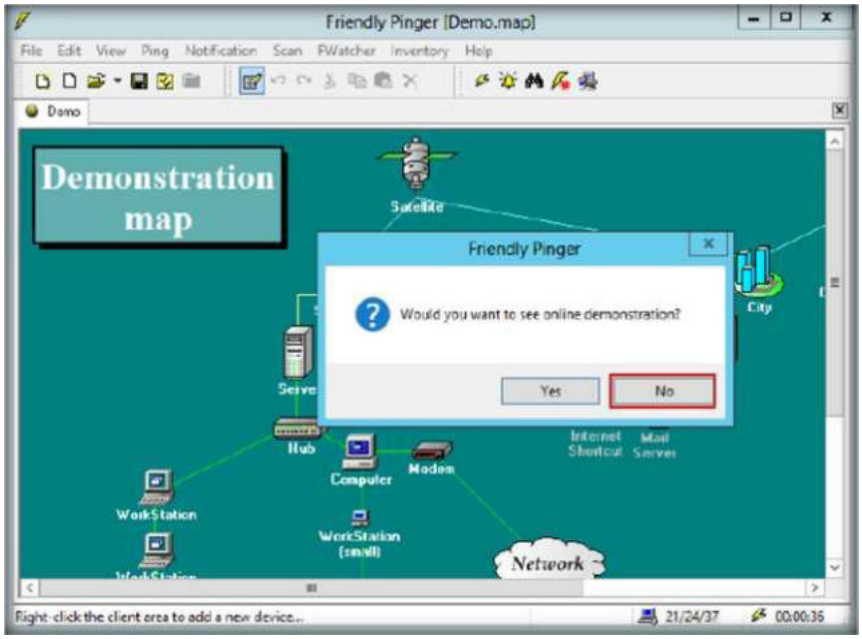


Рисунок 9.3: FPinger

6. Выберите File - Wizard.

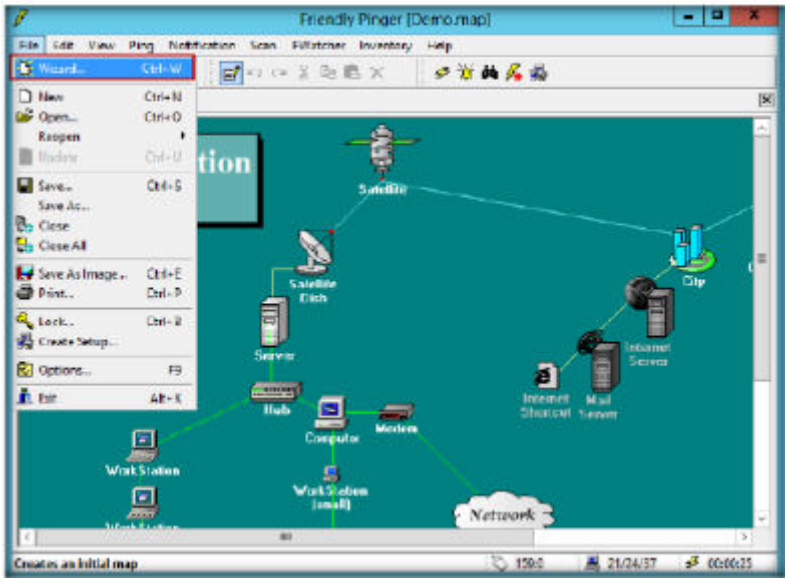


Рисунок 9.4: FPinger

7. Чтобы создать начальное отображение сети, заполните диапозон адресов как на рисунке и нажмите Next.

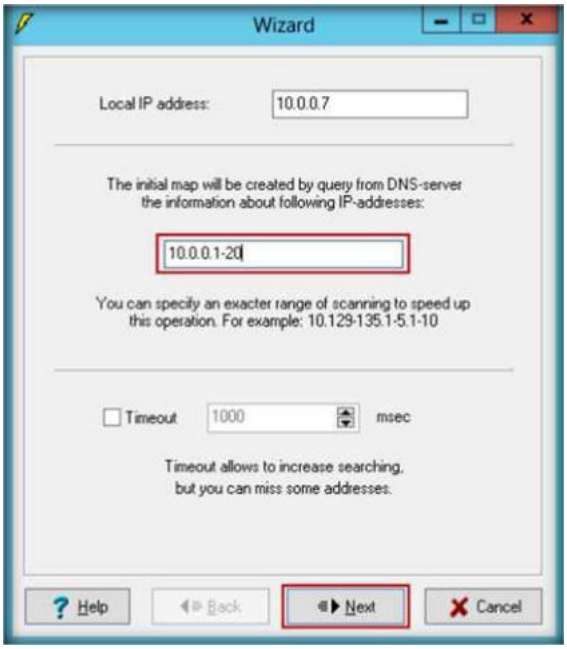


Рисунок 9.5: Настройка

8. Затем мастер начнет сканировать сеть и перечислять IP адреса.
9. Нажмите Next.

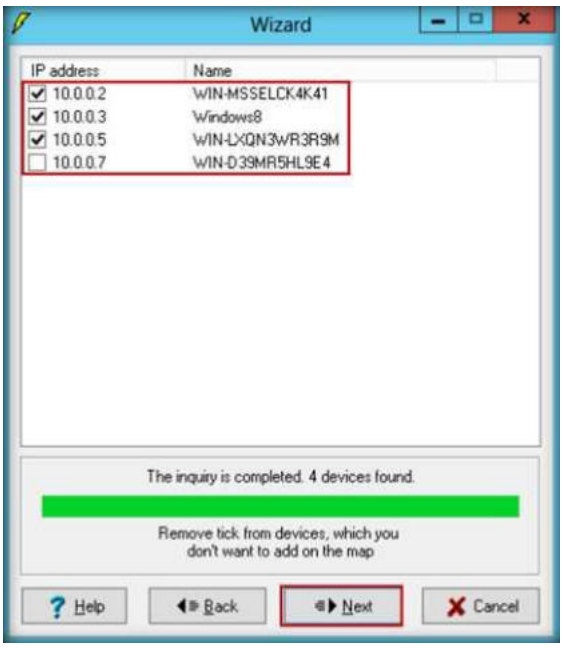


Рисунок 9.6: Результат сканирования

10. Установите опции по умолчанию как на рисунке и нажмите Next.

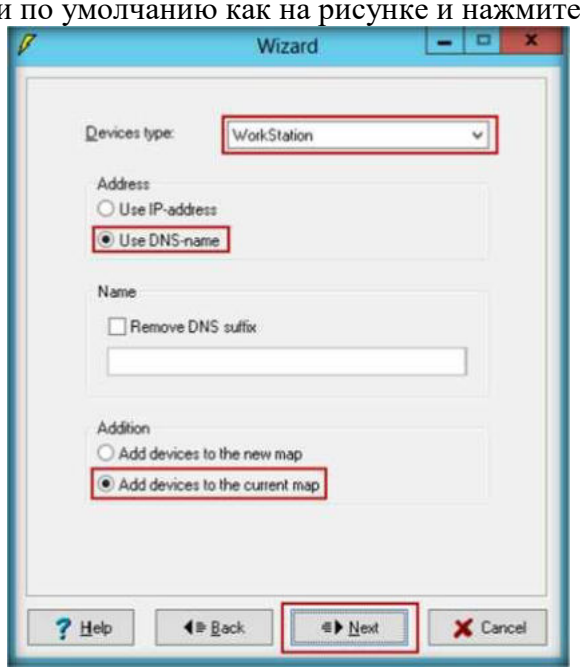


Рисунок 9.7: Опции

11. Затем программа будет отображать сетевую карту в окне, как на рисунке.

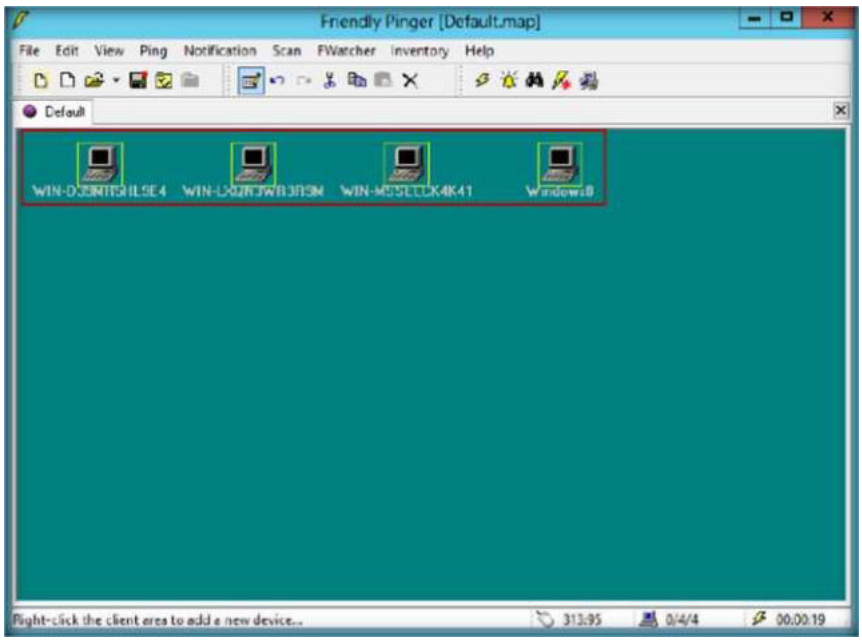


Рисунок 9.8: Сетевая карта

12. Чтобы отсканировать выбранный компьютер сети, выберете его и нажмите Scan.

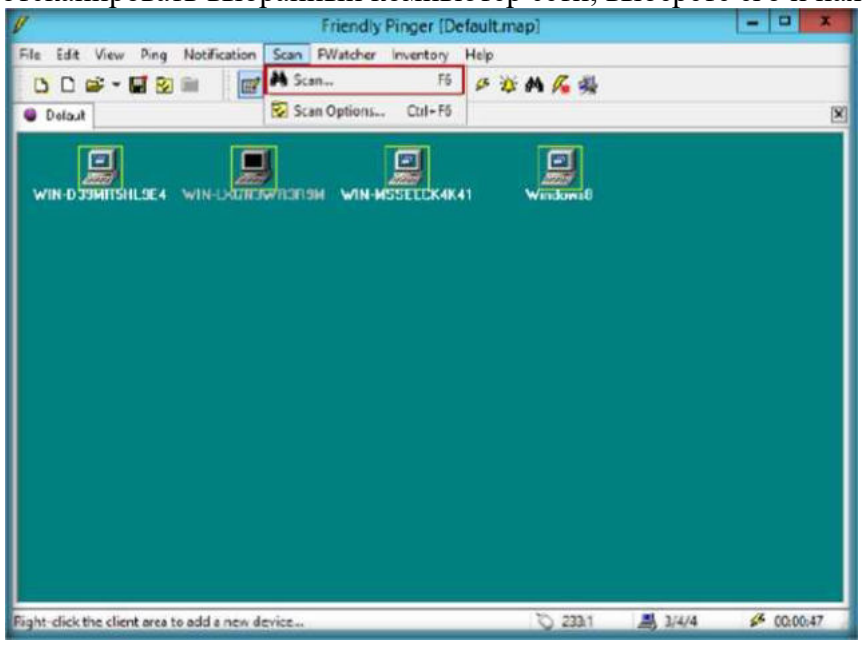


Рисунок 9.9: Сканирование компьютера

13. В результате появятся детали сканирования.

Рисунок 9.10: Результат сканирования

14. Нажмите Inventor, чтобы просмотреть детали конфигурации выбранного компьютера.

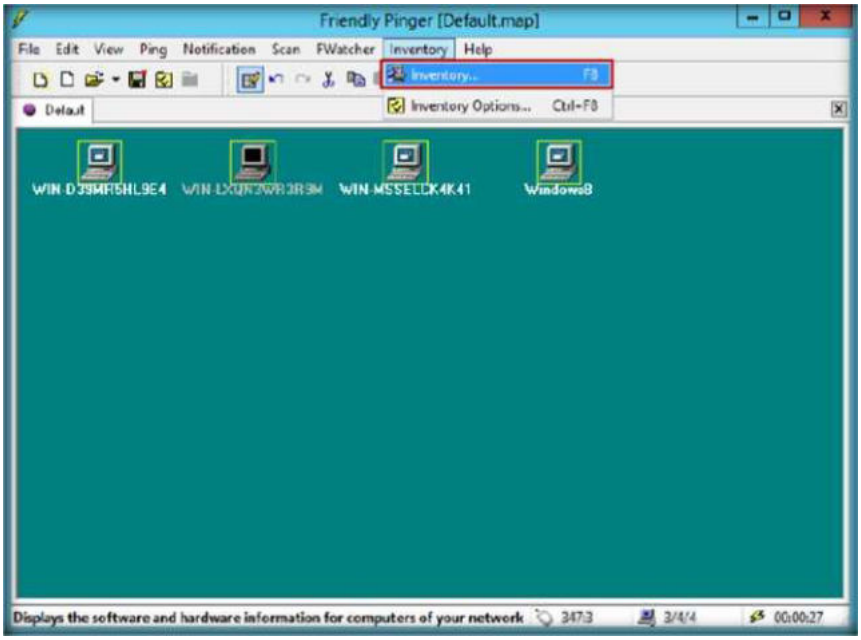


Рисунок 9.11: Конфигурация

15. Вкладка General показывает общие сведения.

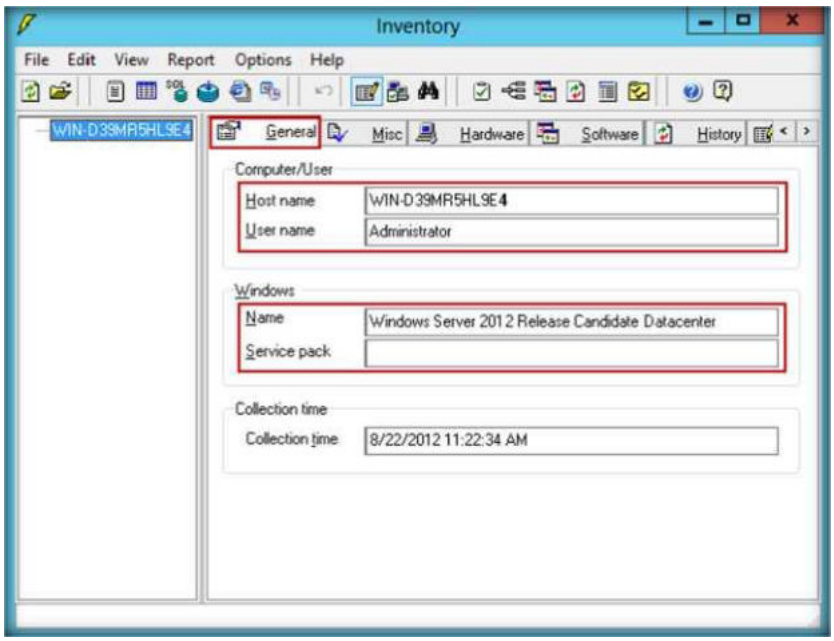


Рисунок 9.12: General

16. Вкладка Misc показывает различные сетевые адреса.

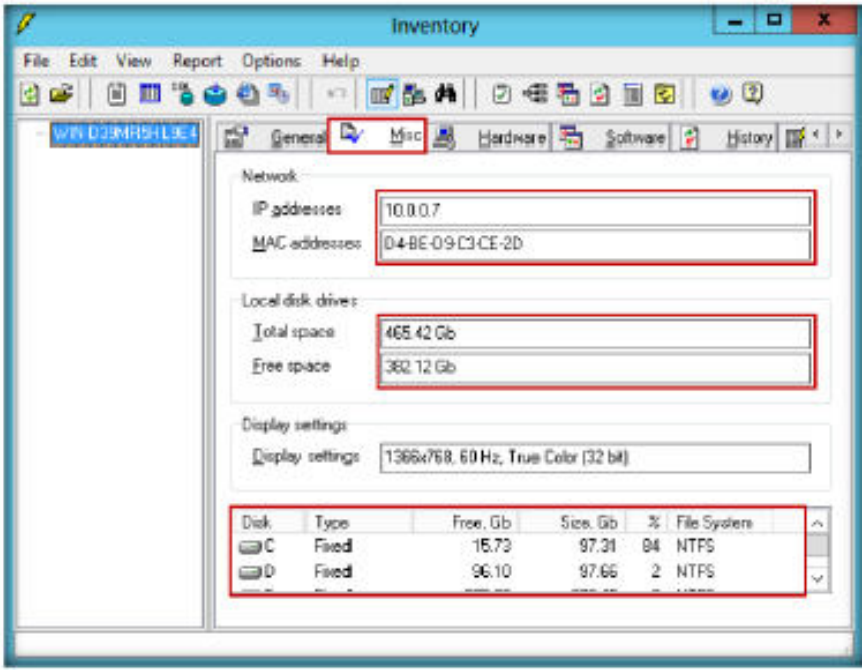


Рисунок 9.13: Misc

17. Вкладка Hardware показывает аппаратные компонентные детали.

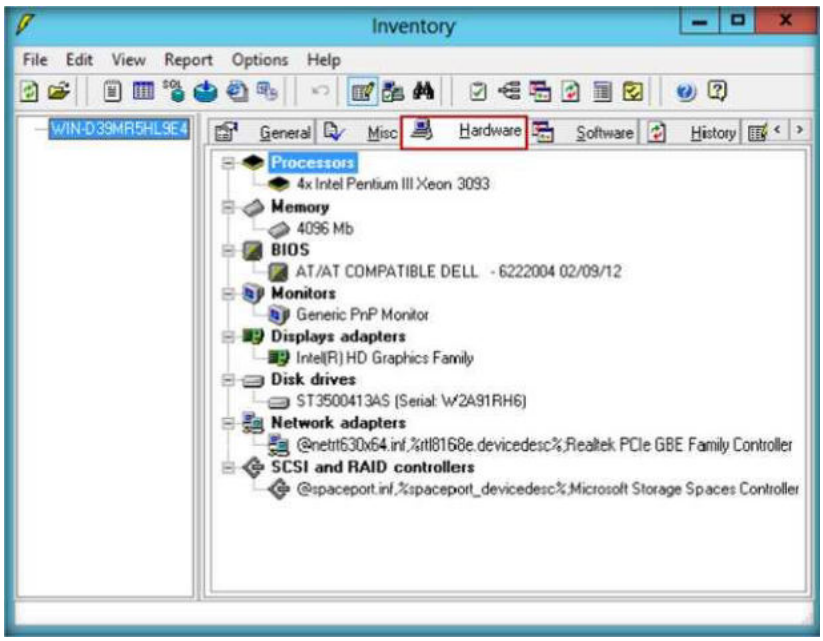


Рисунок 9.14: Hardware

18. Вкладка Software показывает установленное ПО.

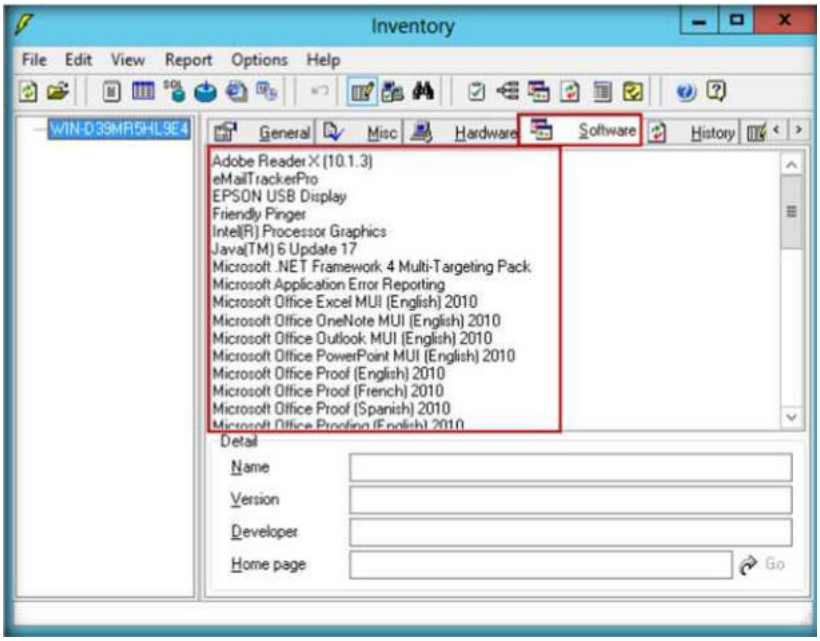


Рисунок 9.15: Software

Анализ практической работы

Запишите все IP -адреса, протоколы и порты, которые вы обнаружили работе.

Средства	Собранная информация
FriendlyPinger	IP адреса: 10.0.0.1 -10.0.0.20
	Найденные IP адреса: – 10.0.0.2 – 10.0.0.3 – 10.0.0.5 – 10.0.0.7
	Детали по 10.0.0.7: – Computer name – Operating system – IP Address – MAC address – File system – Size of disk – Hardware information – Software information

Вопросы

1. FPinger поддерживает брандмауэры и прокси-сервера?
2. Исследуйте язык программирования используемый в FPinger.

Практическое занятие №10. Сканирование сети с помощью Nessus Tool

Цели работы

Целью работы является сканирование сети и получение навыков использования Nessus. Вы научитесь:

1) Использовать Nessus.
2) Сканировать сеть на уязвимости.

Средства для выполнения практической работы

Вам необходимо:

1) Nessus.
2) Можно загрузить по ссылке http:/www.Tenable.com/prodncts /nessus/ nessnsdownload- agreement/
3) Скриншоты могут отличаться.
4) Windows Server 2012.
5) Браузер с выходом в интернет.
6) Права администратора для запуска Nessus tool.

Краткие теоретические сведения Представление о Nessus Tool

Nessus помогает студентам изучать, понимать, и определять уязвимости и слабые места системы и сети, чтобы знать, как можно использовать систему. Сетевые уязвимости могут быть и топологией сети и уязвимостями ОС, открытыми портами и рабочими службами, приложением и ошибками конфигурации службы.

Постановка задачи

1. Установить Nessus.
2. Открыть файл - щёлкните Run.

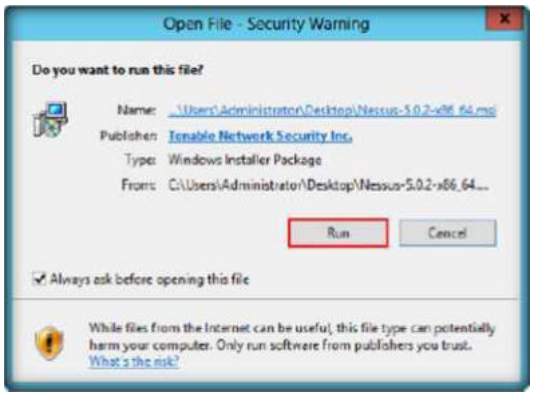


Рисунок 10.1: Установка

3. Запустится помощник установки. Нажмите Next.

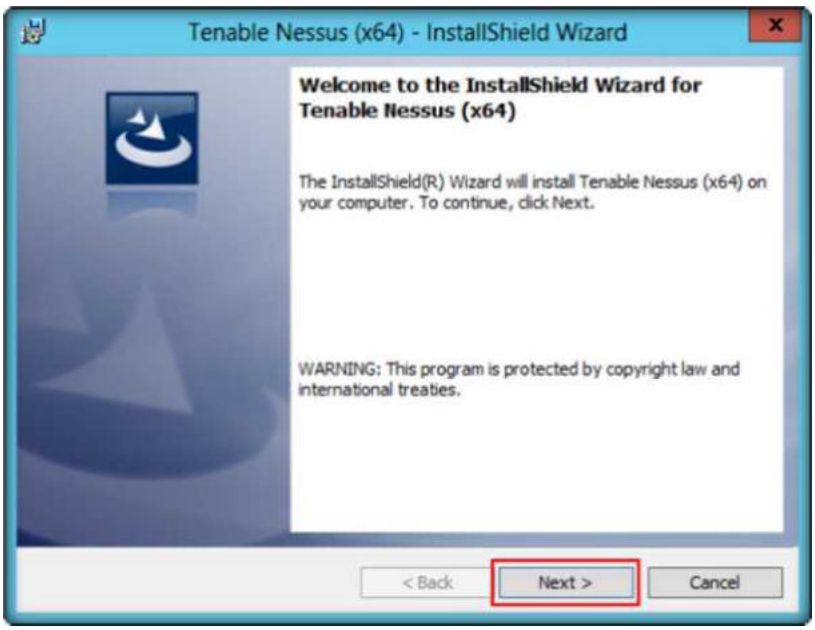


Рисунок 10.2: Установка

4. Примите лицензионно соглашение.
5. Выберите что согласны и нажмите Next.

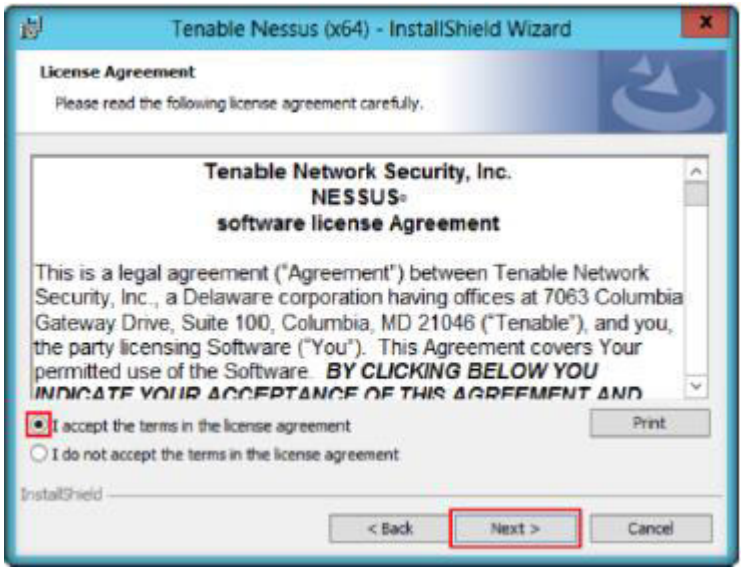


Рисунок 10.3: Install Wizard

6. Выберете путь установки и нажмите Next.

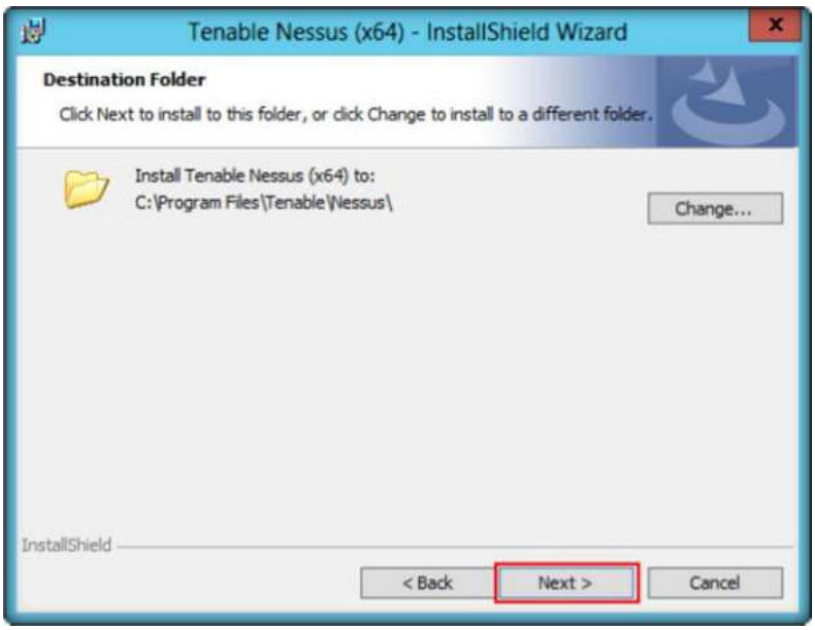


Рисунок 10.4: Install Wizard

7. Выберете тип установки – полная установка или выборочная.

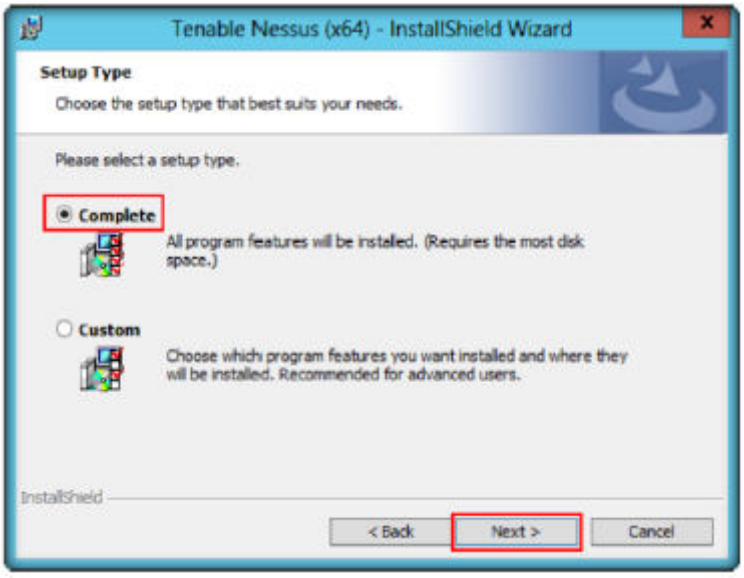


Рисунок 10.5: Install Wizard

8. Нажмите установить

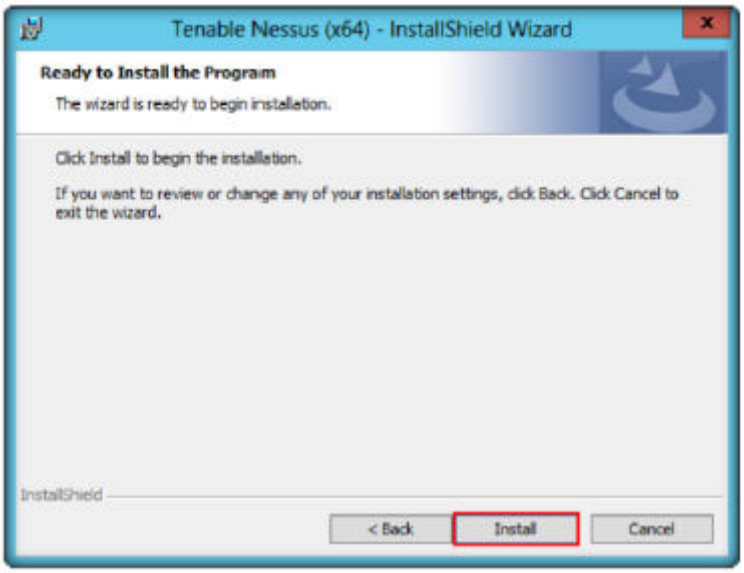


Рисунок 10.6: Install Wizard

9. После установки нажмите Finish.

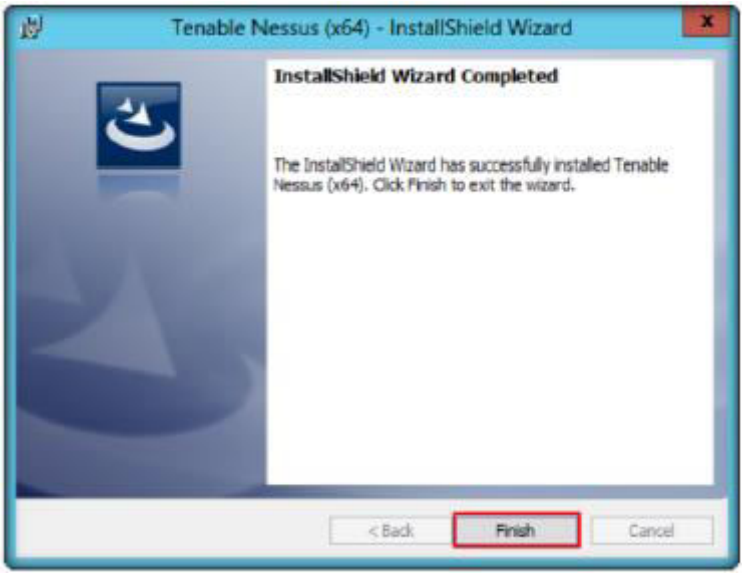


Рисунок 10.7: Install Shield

10. Главные каталоги Nessus показаны в таблице.

Nessus Home Directory	Nessus Sub-Directories	Purpose
Windows		
\Program Files\Tenable\Nessus	\conf	Configuration files
	\data	Stylesheet templates
	\nessus\plugins	Nessus plugins
	\nessus\users\<username>\kbs	User knowledgebase saved on disk
	\nessus\logs	Nessus log files

ТАБЛИЦА 10.1: Главные каталоги Nessus

11. После установки Nessus открывается в Вашем браузере по умолчанию.
12. Появится экран Welcome to Nessus, щелкните по ссылке, чтобы соединиться через SSL

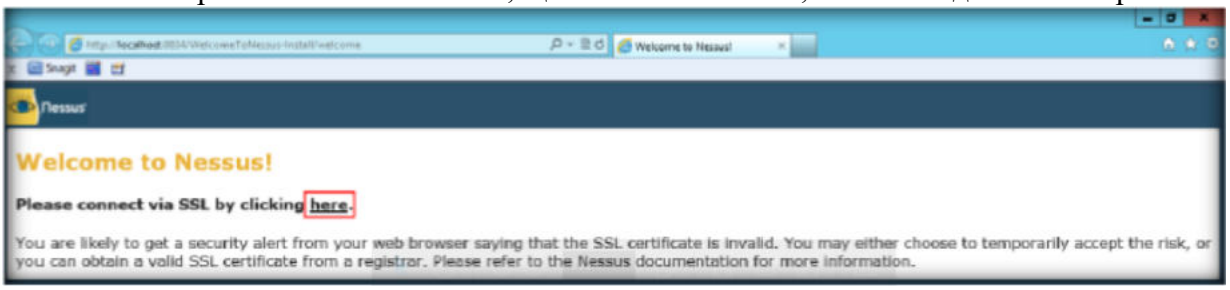


РИСУНОК 10.8: Сертификация SSL Nessus

13. Нажмите "OK", если появляется следующее предупреждение системы безопасности

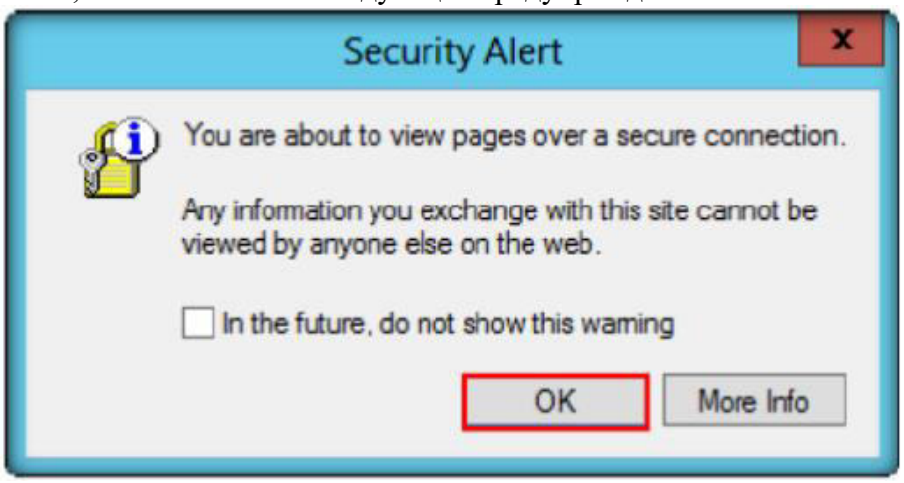


РИСУНОК 10.9: Предупреждение системы безопасности Internet Explorer

14. Нажмите “Continue to this website” («Продолжить соединение к этому веб-сайту» (не рекомендуется))

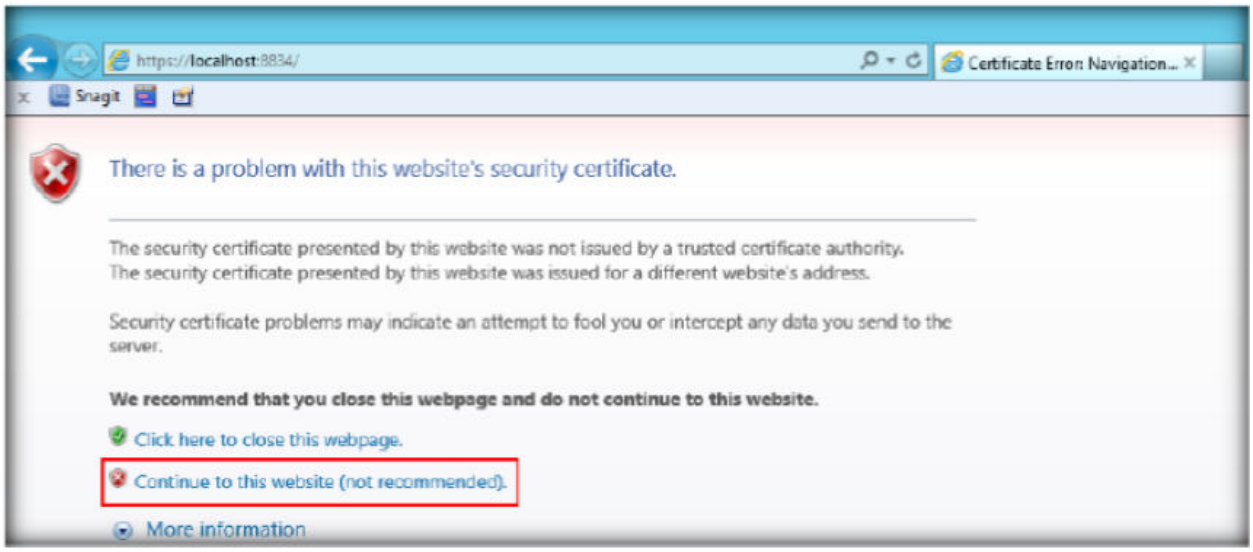


РИСУНОК 10.10: Сертификат безопасности веб-сайта Internet Explorer

15. Нажмите «OK» , если появится следующее Предупреждении системы безопасности.

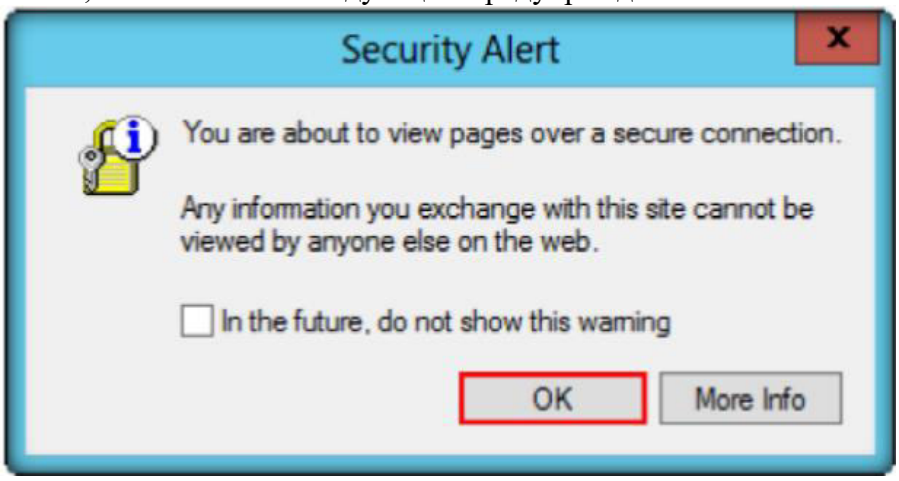


РИСУНОК 10.11: Предупреждение системы безопасности Internet Explorer

16. Появится окно «Спасибо за установку Nessus». Щелкните по кнопке «Get Started», чтобы запустить приложение.

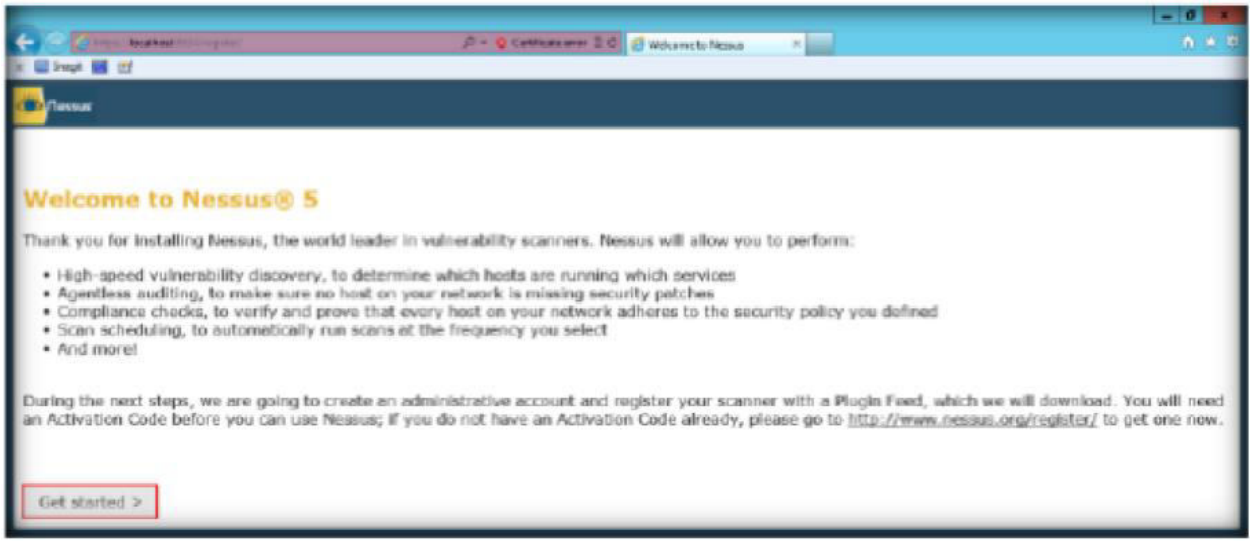


РИСУНОК 10.11: Начало работы Nessus

17. В первоначальной учетной записи введите учетные данные и нажмите Next> (Далее).

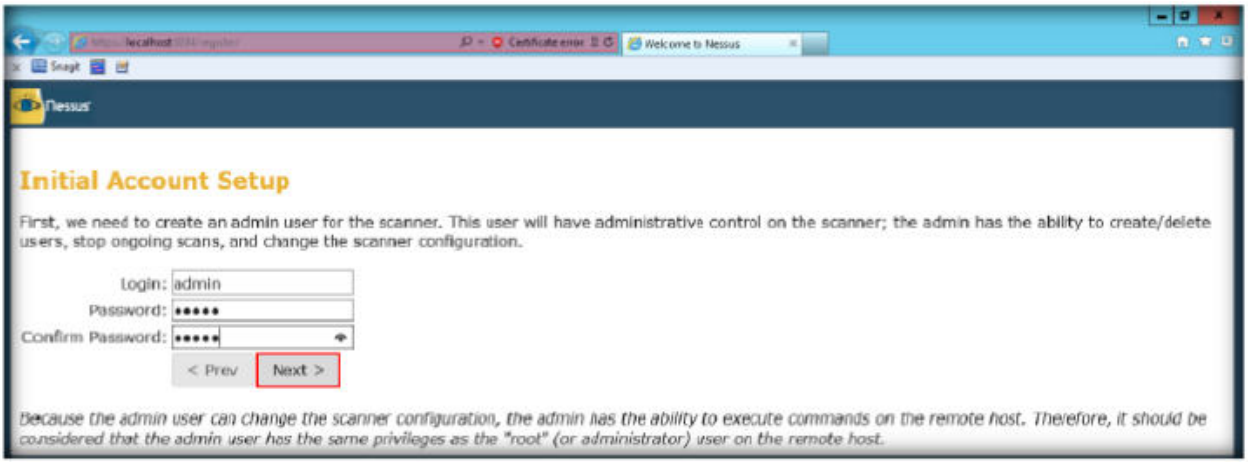


РИСУНОК 10.12: Учетная запись Nessus

18. В «Plugin Feed Registration» (сменной регистрации канала) Вы должны ввести код активации. Чтобы получить код активации, нажмите ссылку http://www.nessus.org/register/.
19. Нажмите значок «Using Nessus at Home» и Вы получите код активации.

РИСУНОК 10.13: Получение кода активации Nessus

20. В «Nessus for Home» примите соглашение, нажав кнопку «Agree», как показано ниже на рисунке.

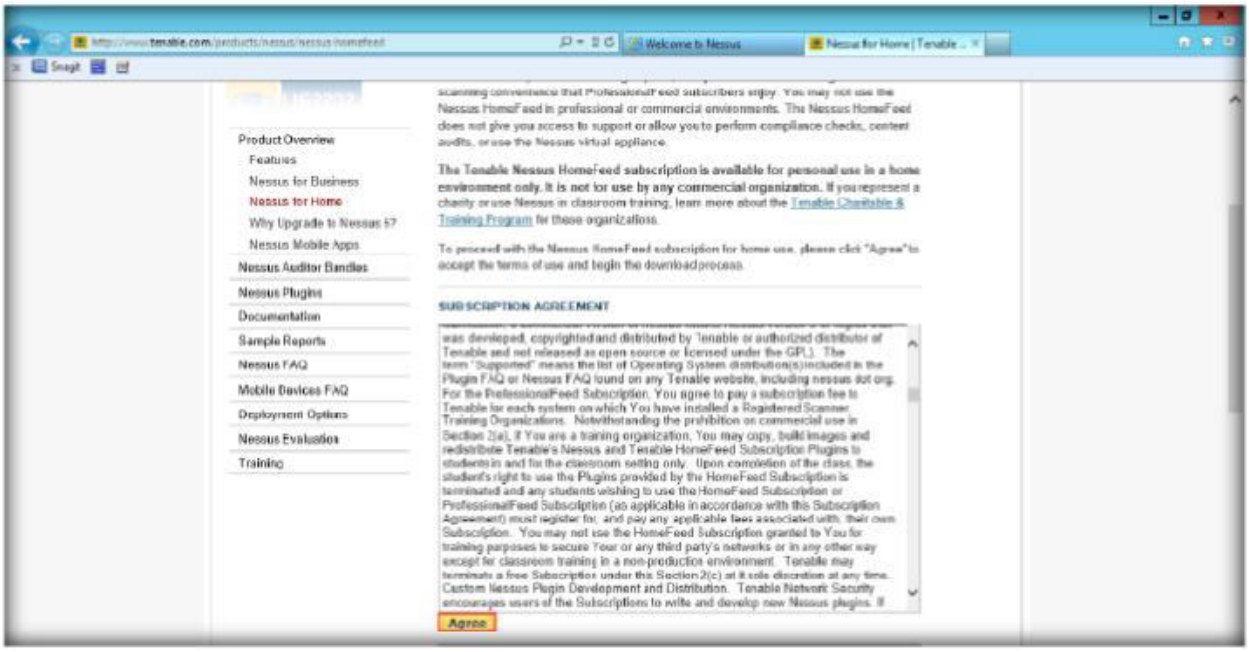


РИСУНОК 10.14: Соглашение о подписке Nessus

21. Заполните раздел «Register a HomeFeed», чтобы получить код активации, и нажмите «Register».

РИСУНОК 10.15: Регистрация

22. В подтверждение успешной регистрации появится окно «Thank You for Registering!».

РИСУНОК 10.16: Завершенная регистрация Nessus

23. Теперь войдите на свою электронную почту, указанную Вами во время регистрации, для получения кода активации, как показано ниже на снимке экрана.

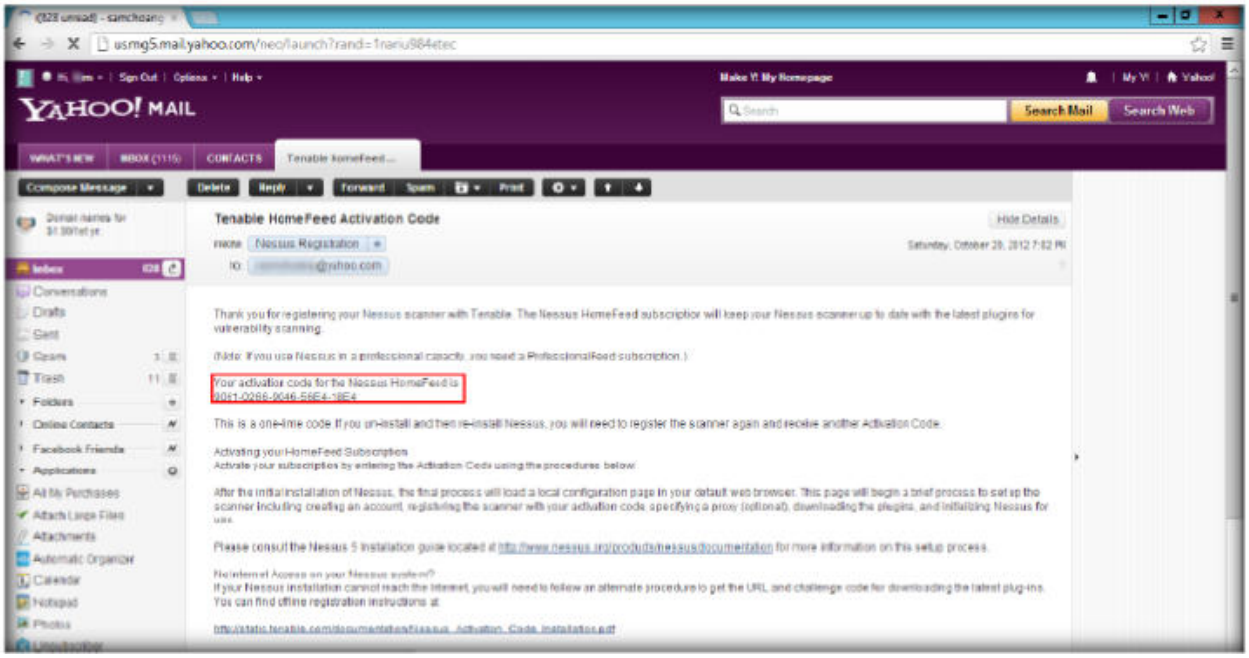


РИСУНОК 10.17: Получение кода активации

24. Теперь введите код активации, полученный Вами на почте, и нажмите «Next» (Далее).

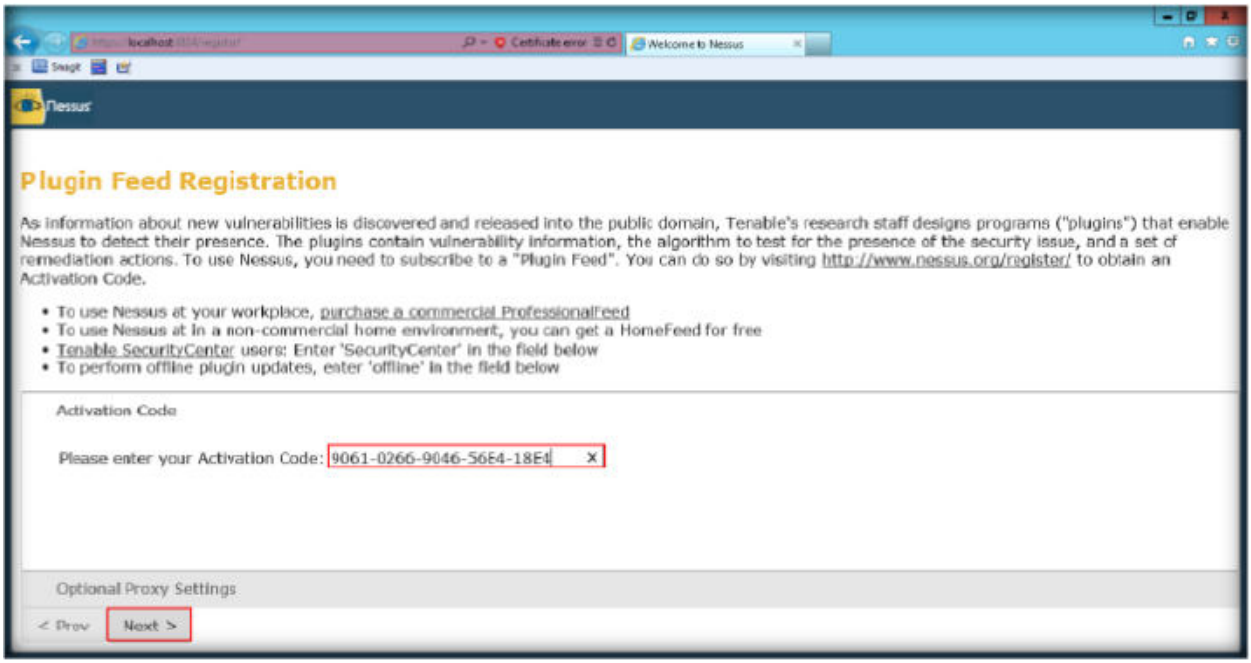


РИСУНОК 10.18: Введение кода активации в Nessus

25. Появится окно «Registering…».

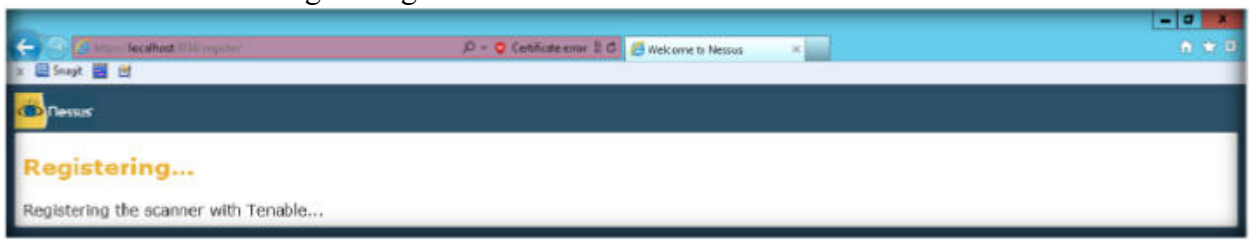


РИСУНОК 10.19: Nessus регистрирует код активации

26. После успешной регистрации нажмите «Next: Download plugins >», чтобы загрузить плагины Nessus.

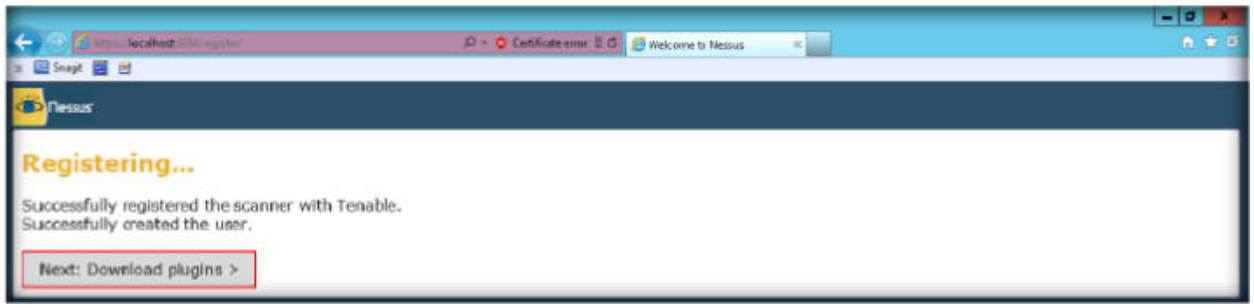


РИСУНОК 10.20: Загрузка плагинов Nessus

27. Nessus выберет плагины и установит их. Это займет время.

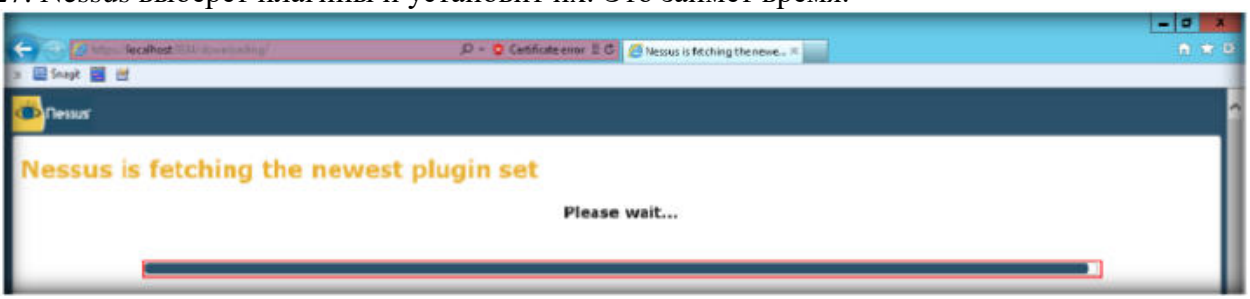


РИСУНОК 10.21: Nessus выбирает и устанавливает плагины

28. Появится страница «Nessus Log In». Введите имя пользователя и пароль, данные во время регистрации, и нажмите «Log In» (вход в систему).

РИСУНОК 10.22: Окно «Nessus Log In»

29. Появится окно «Nessus HomeFeed». Нажмите "OK".

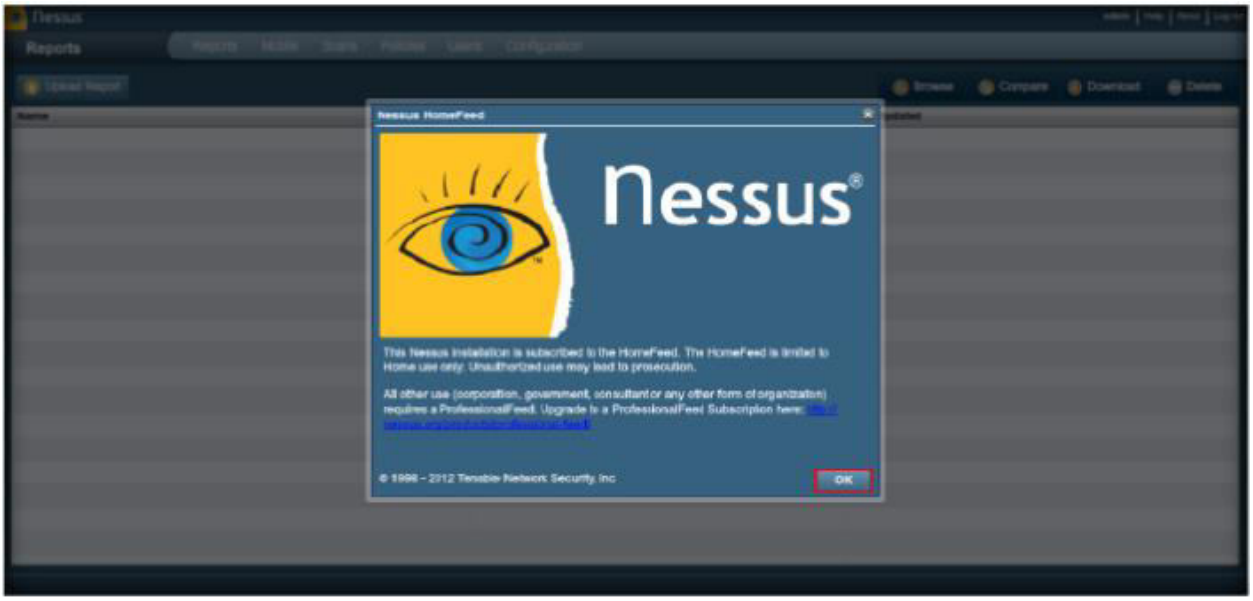


РИСУНОК 10.23: Подписка Nessus HomeFeed

30. После того, как Вы успешно войдете в систему, появится окно «Nessus Daemon», как показано в следующем снимке экрана.

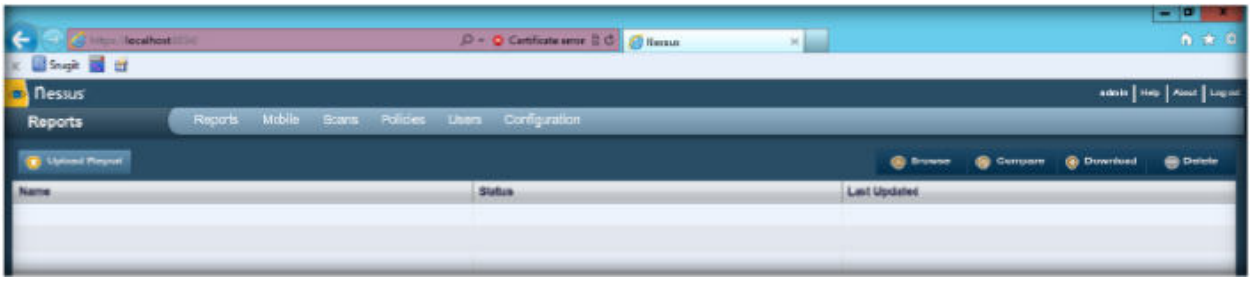


РИСУНОК 10.24: Основная страница Nessus

31. Если у Вас есть «Administrator Role» (Роль Администратора), Вы увидите вкладку «Users» (пользователи), которая перечислит всех пользователей, их роли и последние входы в систему.

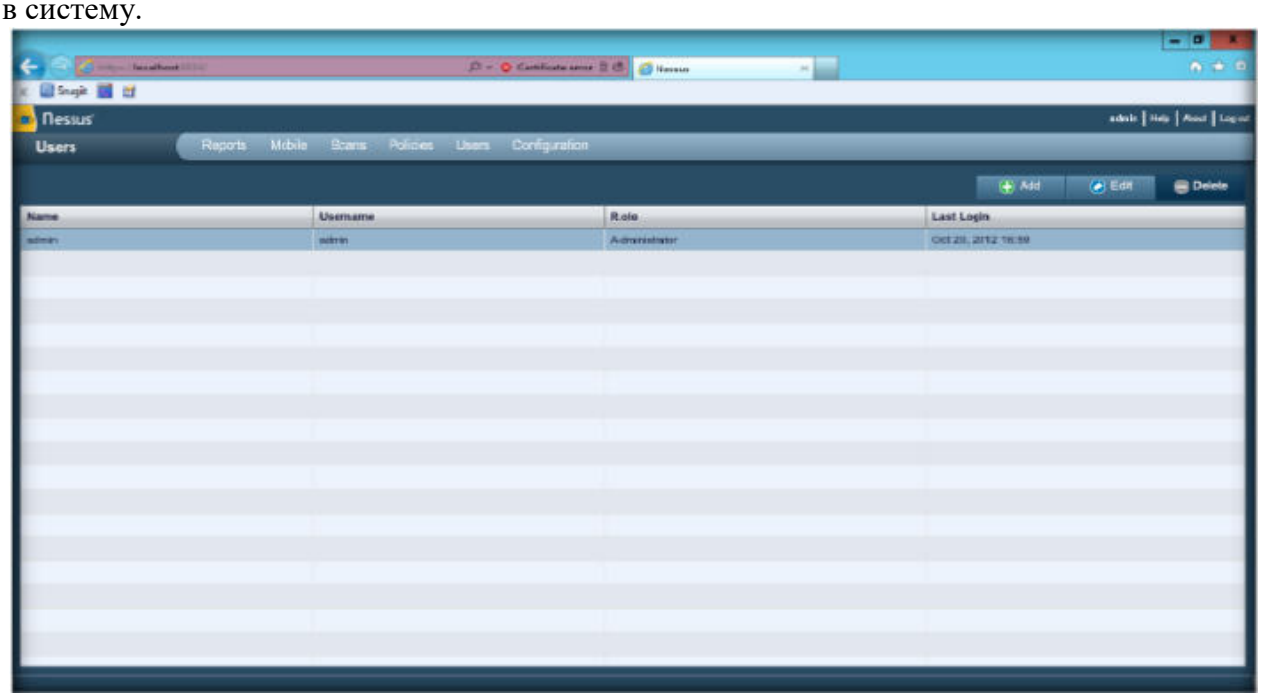


РИСУНОК 10.25: Окно администратора Nessus

32. Чтобы добавить новую политику, нажмите Policies → Add Policy. Заполните разделы «General policy» (Общей политики), а именно «Basic» (Основной), «Scan» (Сканирование), «Network Congestion» (Перегрузка сети), «Port Scanners» (Сканеры Порта), «Port Scan Options» (Опции Сканирования портов) и «Performance» (Производительность).

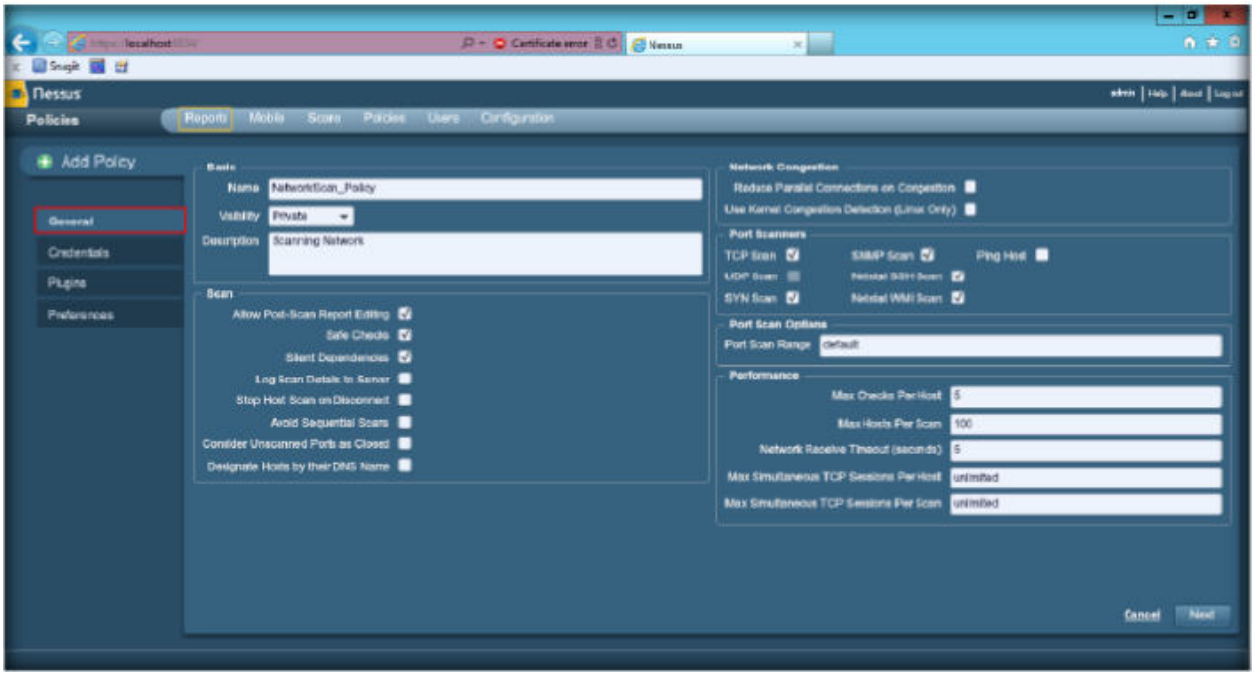


РИСУНОК 10.26: Добавление политики

33. Чтобы сконфигурировать учетные данные новой политики, щелкните по вкладке «Credentials», показанной на левой панели “Add Policy» (Добавление политики).

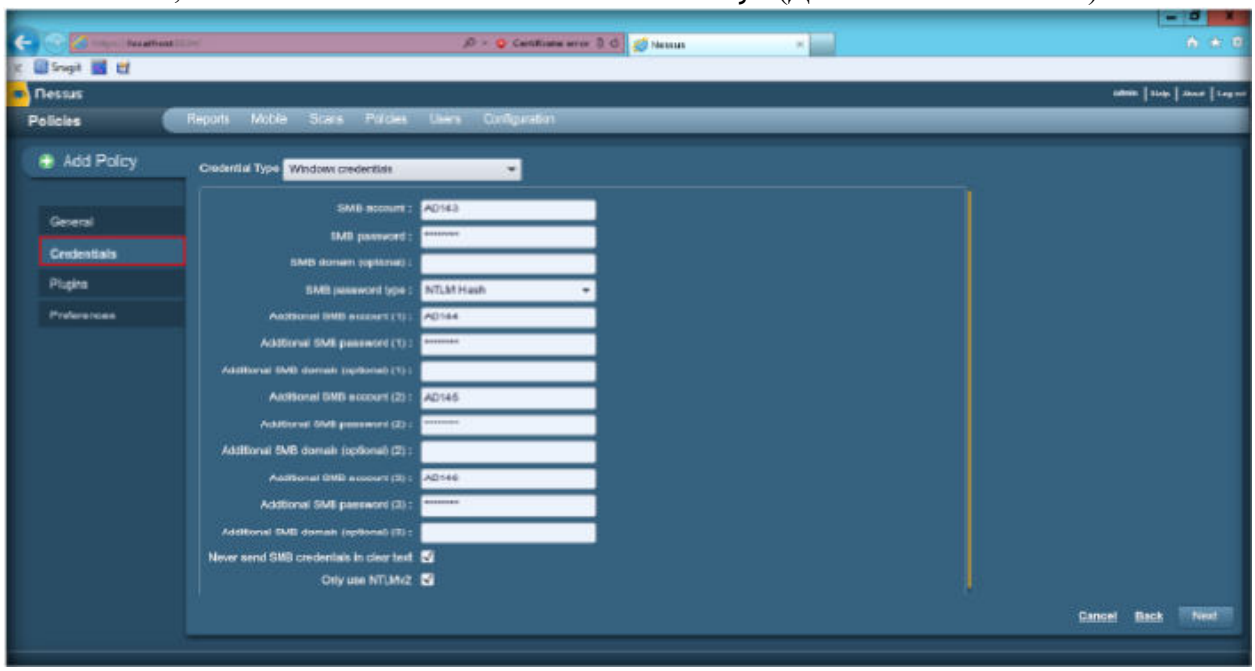


РИСУНОК 10.27: Добавление политики и урегулирование учетных данных

34. Чтобы выбрать необходимые плагины, щелкните по вкладке «Plugins» на левой панели “Add Policy» (Добавление политики).

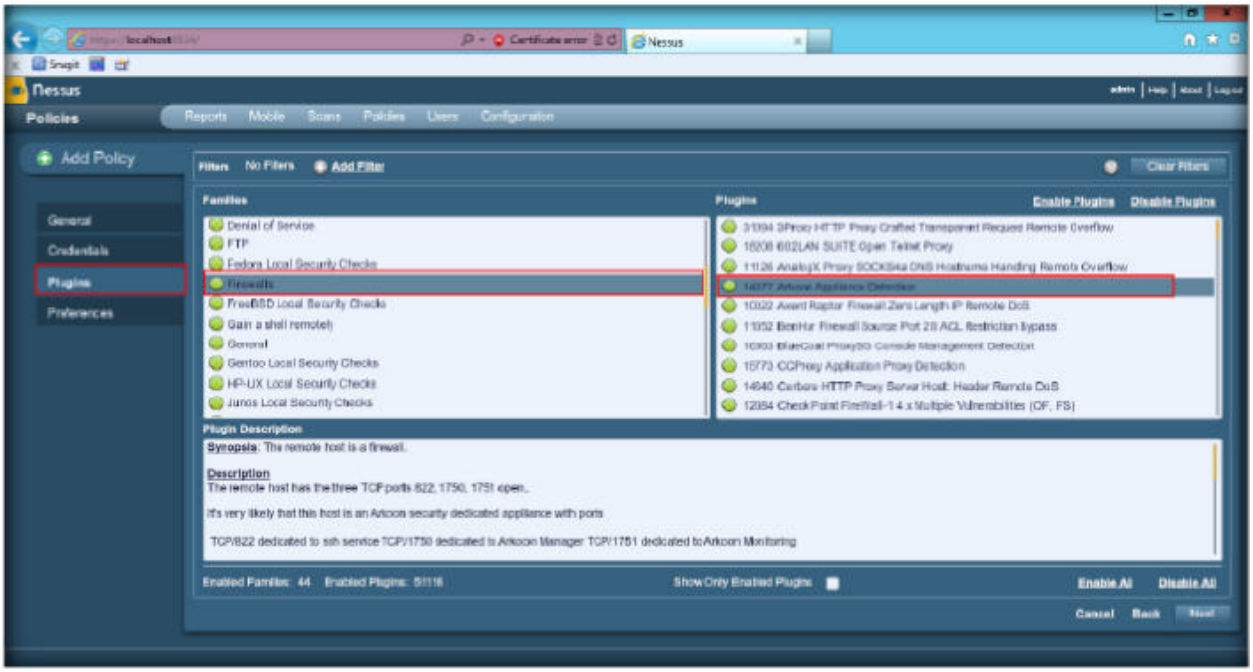


РИСУНОК 10.28: Добавление политики и выбор Plugins

35. Чтобы сконфигурировать предпочтения, щелкните по вкладке «Preferences» на левой панели “Add Policy» (Добавление политики).
36. В поле «Plugin» выберите параметры настройки «Database» (базы данных) из выпадающего списка.
37. Введите необходимые данные для входа в систему.
38. Введите Database SID: 4587, чтобы использовать Database port: 124, и выберите тип автора Oracle: SYSDBA.
39. Нажмите «Submit» (подтвердить).

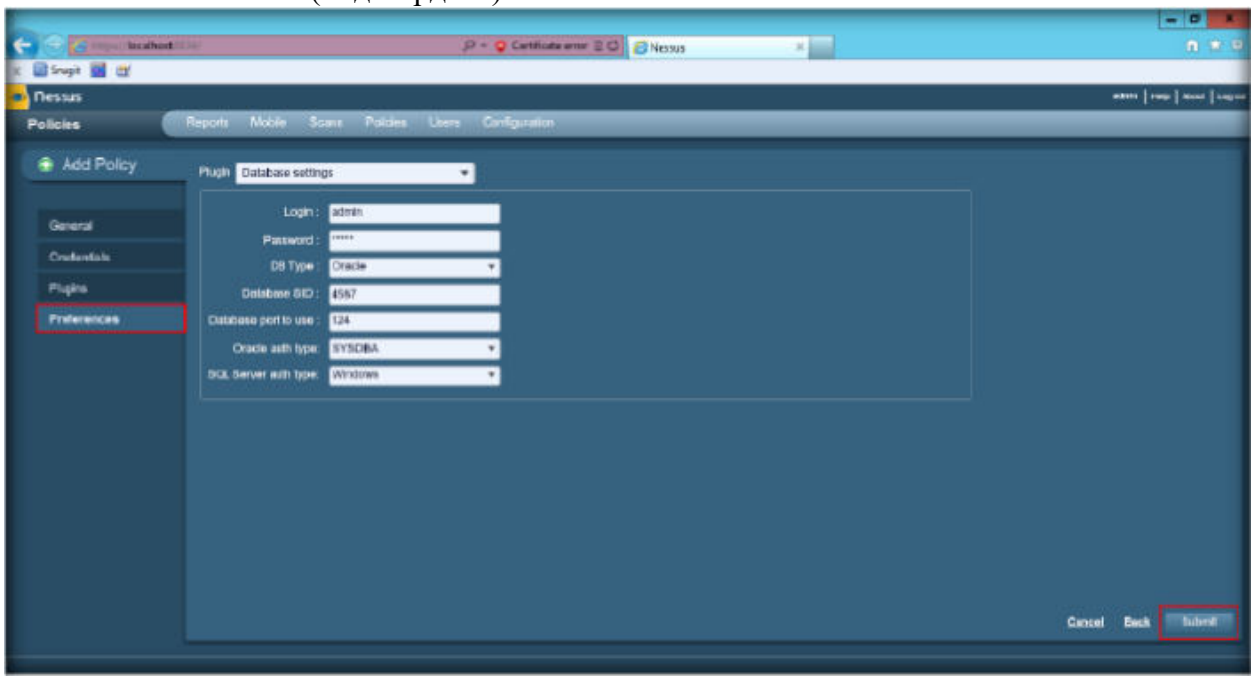


РИСУНОК 10.29: Добавление политики и урегулирование предпочтений

40. Политика сообщения “NetworkScan_Policy” была успешно добавлена на дисплей, как показано на снимке экрана ниже.

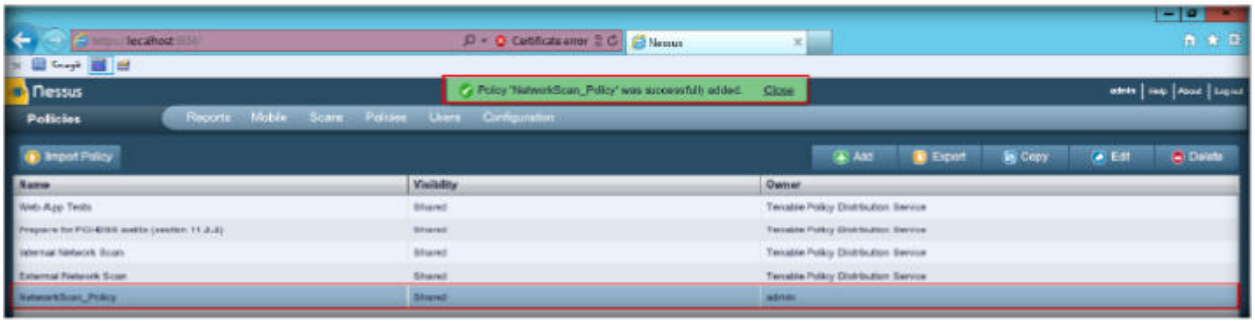


РИСУНОК 10.30: Политика NetworkScan

41. Теперь, нажмите Scans → Add (добавить), чтобы открыть окно «Add Scan».
42. Введите «field Name» (имя поля), «Type» (Тип), «Policy» (политику) и «Scan Target» (Цель Сканирования).
43. В «Scan Targets» (Целях Сканирования) введите IP-адрес своей сети. В этой лабораторной работе мы сканируем 10.0.0.2.
44. Нажмите «Launch Scan» в правом нижнем углу окна.

Примечание: IP-адреса могут отличаться по Вашей среде лабораторной работы.

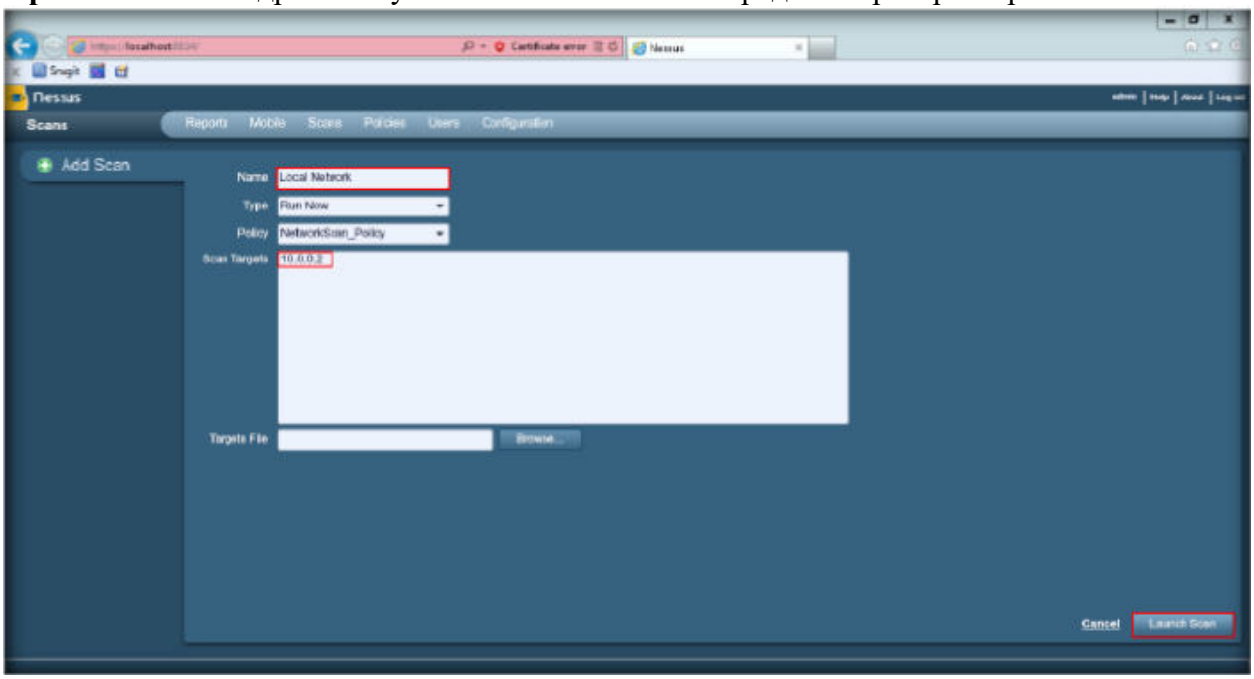


РИСУНОК 10.31: Добавление сканирования

45. Сканирование запускается и начинает сканировать сеть.

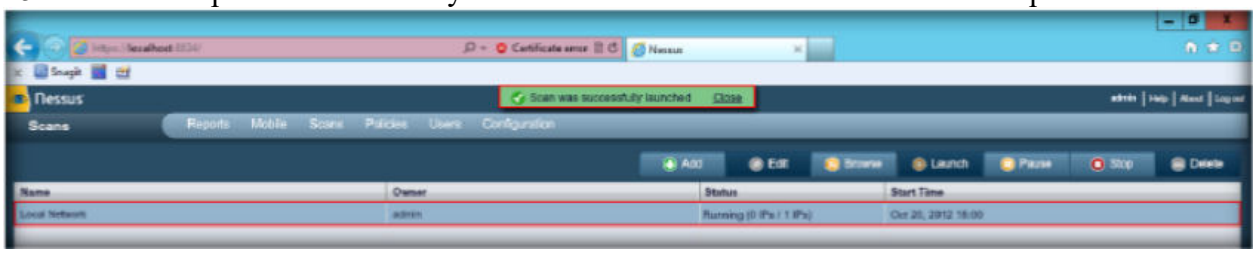


РИСУНОК 10.32: Сканирование

46. После того, как сканирование завершится, щелкните по вкладке «Reports» (отчеты).

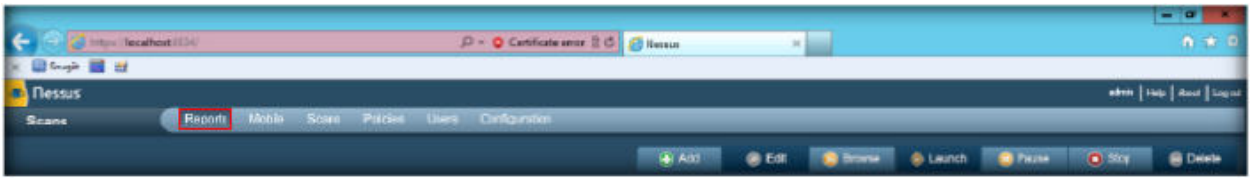


РИСУНОК 10.33: вкладка Nessus «Reports»

47. Дважды щелкните по «Local Network», чтобы просмотреть подробный отчет сканирования.

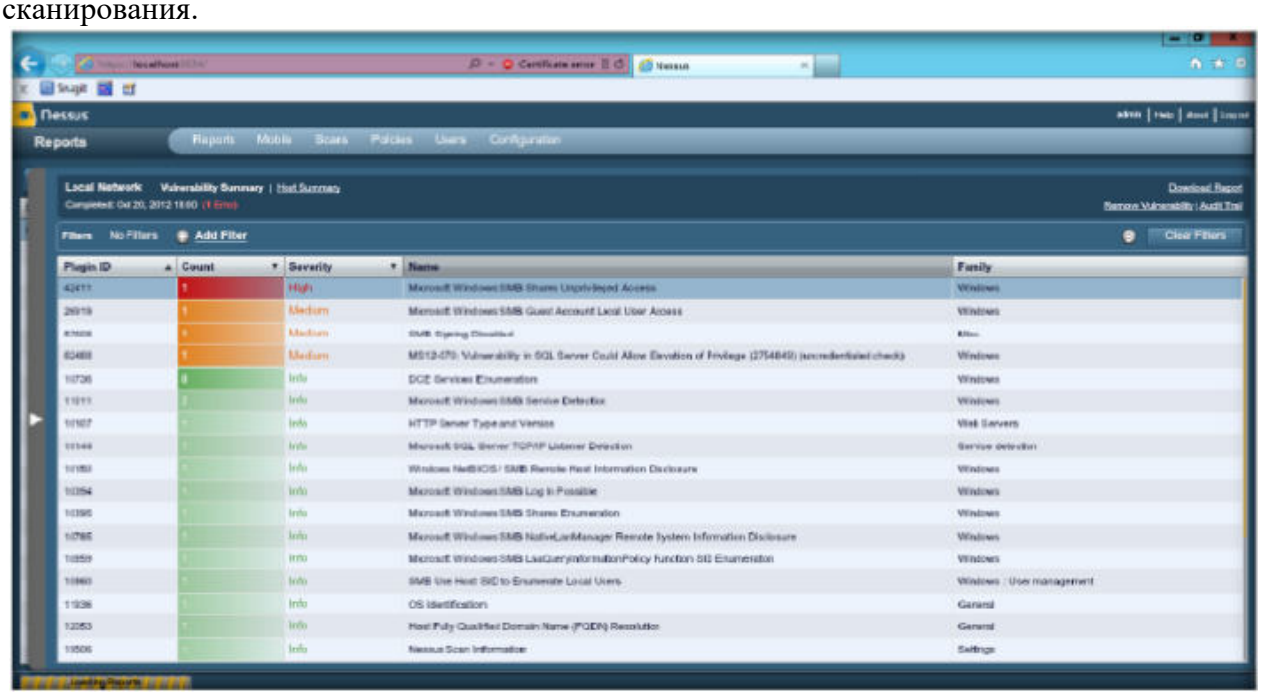


РИСУНОК 10.34: Отчет сканирования

48. Дважды щелкните по любому результату и Вы получите более подробное резюме, описание, уровень безопасности и решение.

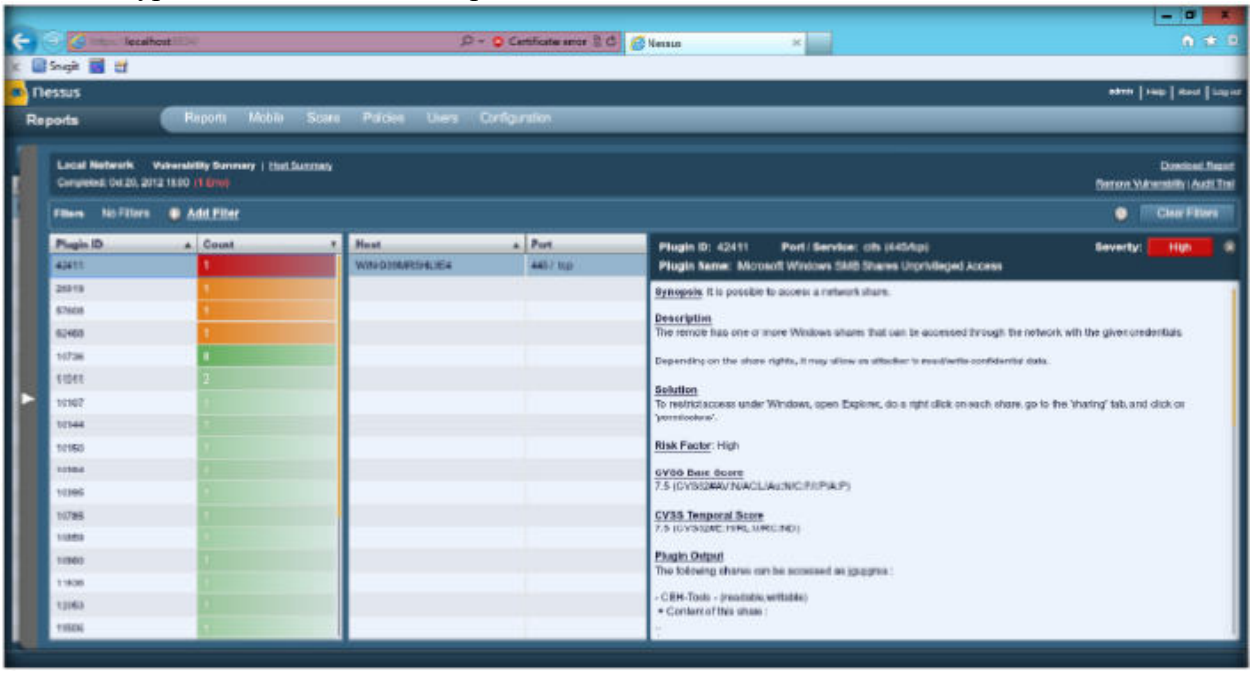


РИСУНОК 10.35: Отчет сканирования

49. Нажмите кнопку «Download Report» на левой панели.
50. Вы можете загрузить доступные отчеты с расширением **.nessus** с помощью выпадающего списка.

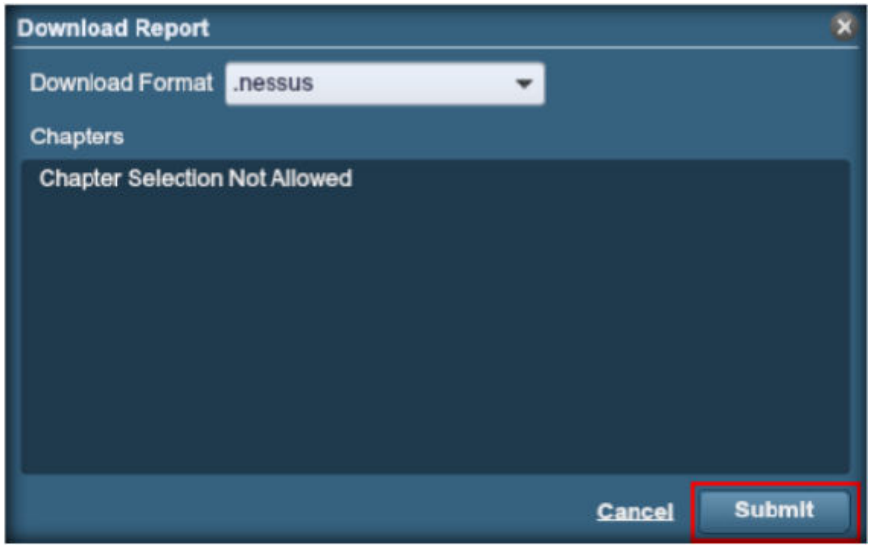


РИСУНОК 10.36: Отчет загрузки с расширением .nessus

51. Теперь, нажмите «Log out» (выйти из системы).
52. В Диспетчере серверов Nessus нажмите «Stop Nessus Server».

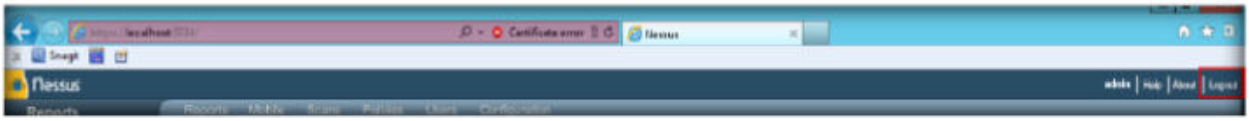


РИСУНОК 10.37: Выход из системы Nessus

Анализ лабораторной работы
Результаты по данной лабораторной работе представлены в таблице ниже.

Инструмент / Утилита	Собранная информация / Достигнутые цели
Nessus	**Целевая машина сканирования:** локальный узел
	Выполненная политика сканирования: сетевая политика сканирования
	Целевой IP-адрес: 10.0.0.2
	Результат: Локальные уязвимости узла

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы
1. Оцените платформы ОС, для которых у Nessus есть сборки. Работает ли Nessus с центром обеспечения безопасности?
2. Как лицензия Nessus работает в среде VM (Виртуальной машины)?

Практическое занятие №11. Контроль сканирования при помощи Global Network Inventory

Цели работы

Эта практическая работа покажет Вам, как могут быть отсканированы сети и как использовать инструмент *Global Network Inventory*.

Она научит Вас как:

- Использовать инструмент Global Network Inventory

Средства практической работы

Чтобы выполнить лабораториную работу Вам необходимо:

- *Global Network Inventory* располагается в **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner**
- Вы можете также загрузить последнюю версию ***Global Network Inventory*** по этой ссылке http://www.magnetosoft.com/products/global network inventory/gn i_features.htm/
- Если Вы решите загрузить последнюю версию, то снимки экрана, показанные в лабораторной работе, могут отличаться.
- Компьютер с Windows Server 2012 как атакующий (хост-машина)
- Другой компьютер с Windows Server 2008 как жертва (виртуальная машина)
- Веб-браузер с доступом к Интернету
- Выполните шаги мастера по установке ***Global Network Inventory***
- Административные привилегии для пользования инструментами

Краткие теоретические сведения

Обзор *Global Network Inventory*

Global Network Inventory - один из инструментов для контроля безопасности и тестирования брандмауэров и сетей. Он также используется для неактивного сканирования.

Задания по лабораторной работе

1. Запустите Меню "Пуск", наведя курсор мыши в нижний левый угол рабочего стола.

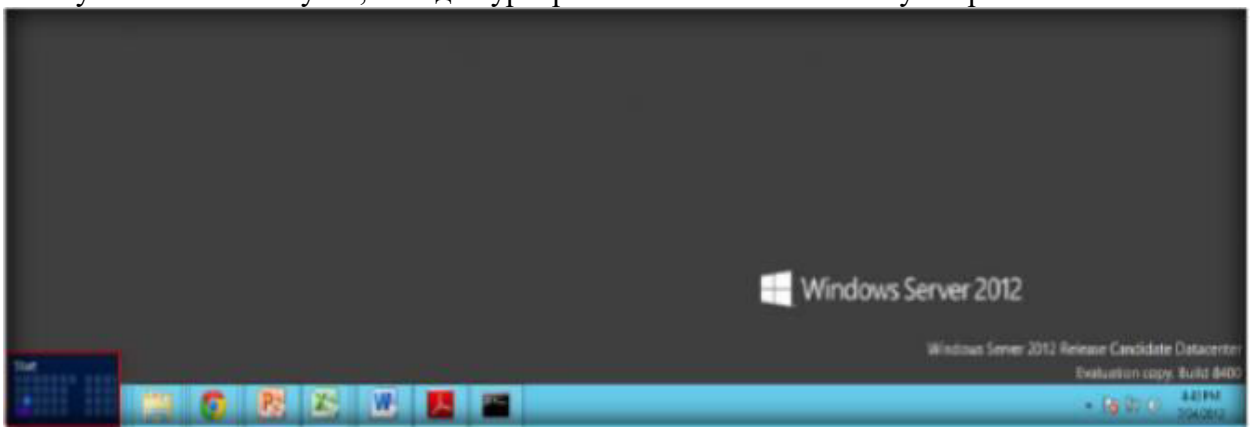


РИСУНОК 11.1: Windows Server 2012 – Рабочий стол

2. Щелкните по «Global Network Inventory» чтобы открыть его.

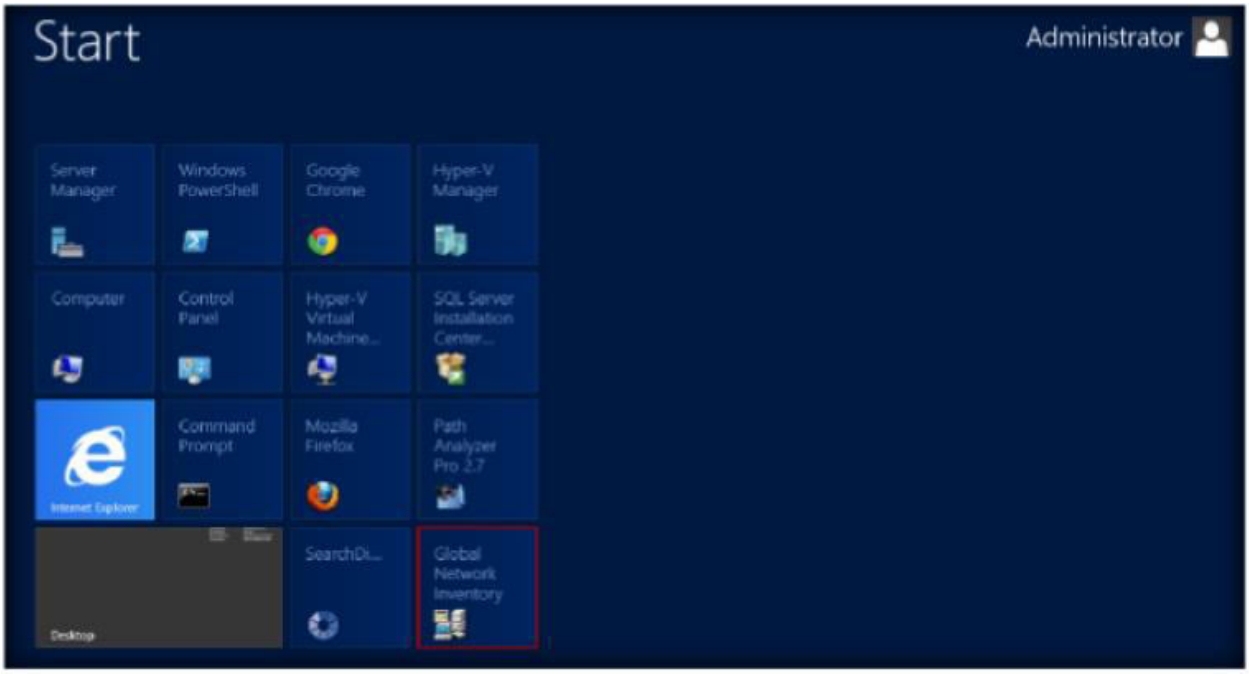


РИСУНОК 112: Windows Server 2012 - приложения

3. Появится окно Global Network Inventory как показано на снимке экрана ниже.
4. Также появится окно «Tip of Day». Нажмите «Close».

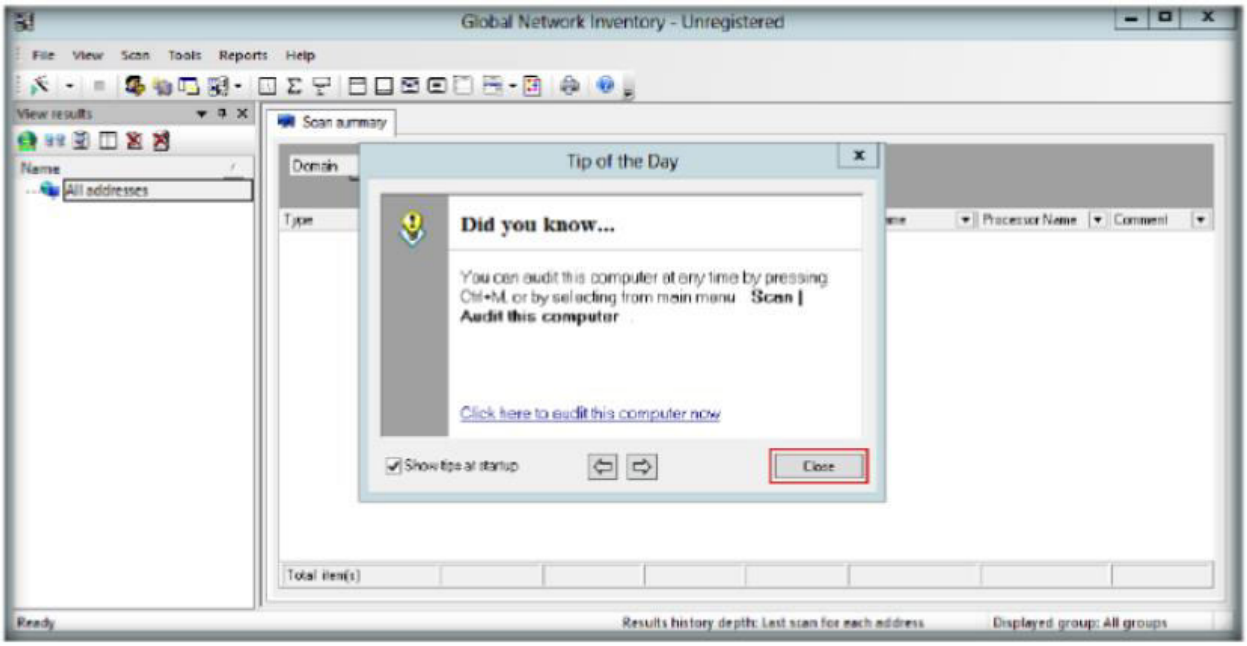


РИСУНОК 113: главное окно Global Network Inventory

5. Включите виртуальную машину Windows Server 2008 от менеджера Hyper-V.

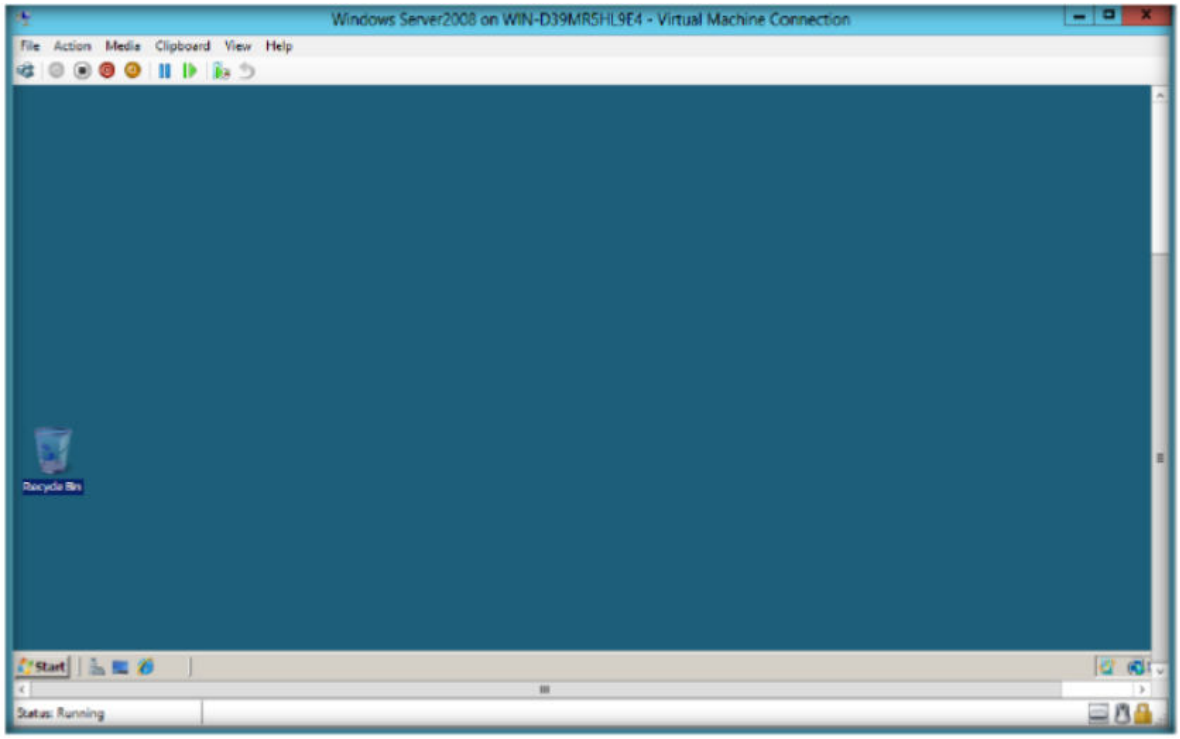


РИСУНОК 11.4: Виртуальная машина Windows 2008

6. Теперь переключитесь назад на машину Windows Server 2012, и появится новое окно «Audit Wizard». Нажмите «Next» (или на панели инструментов выберите вкладку «Scan» и нажмите мастер аудита «Launch»).

РИСУНОК 11.5: Мастер Global Network Inventory

7. Выберите «IP range scan» (диапазон сканирования IP) и затем нажмите «Next» (Далее) в «Audit Scan Mode wizard» (Контрольном мастере режима сканирования).

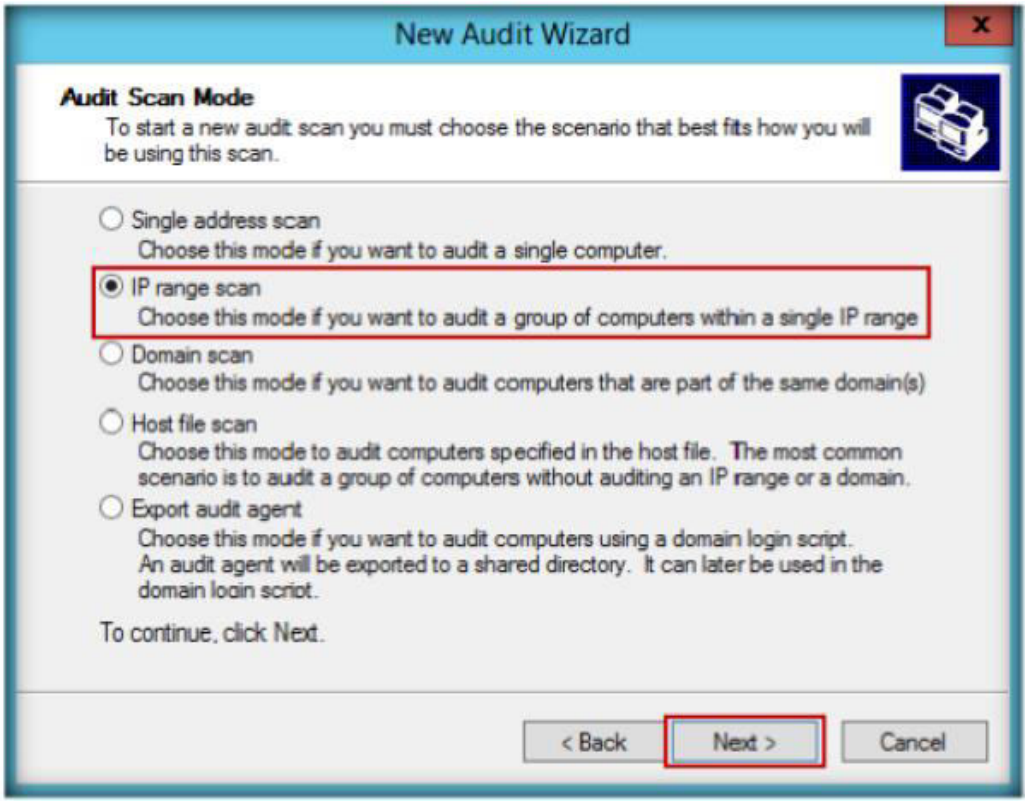


РИСУНОК 11.6: Режим сканирования аудита Global Network Inventory

8. Установите диапазон сканирования IP. Нажмите «Next» (Далее) в Range Scan wizard (мастере сканирования диапазона IP).

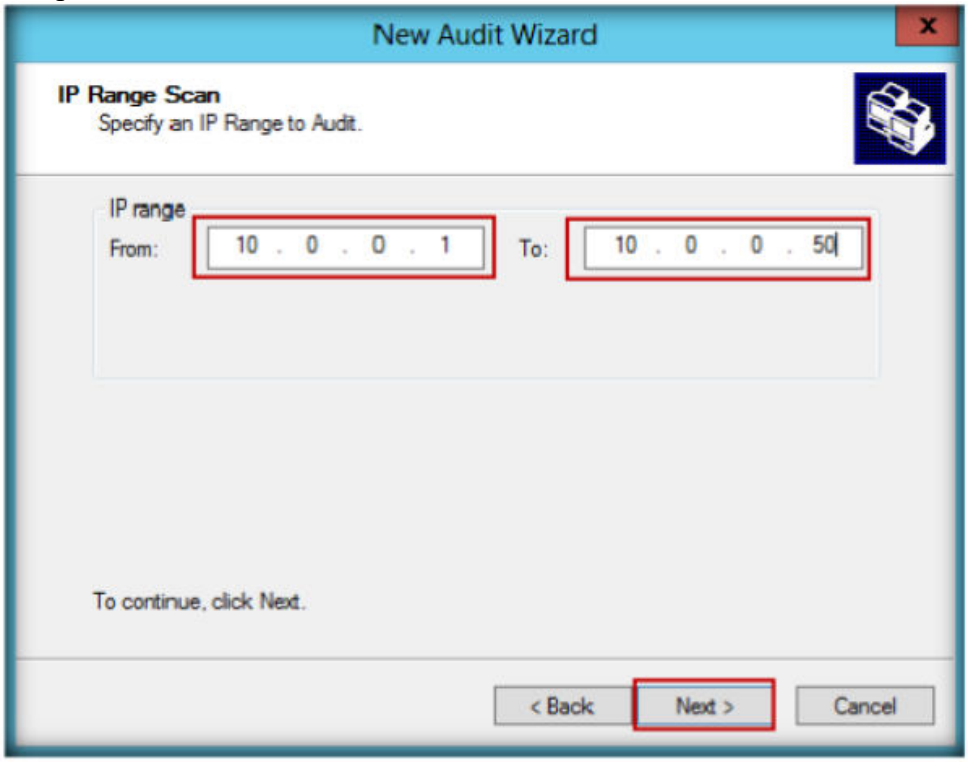
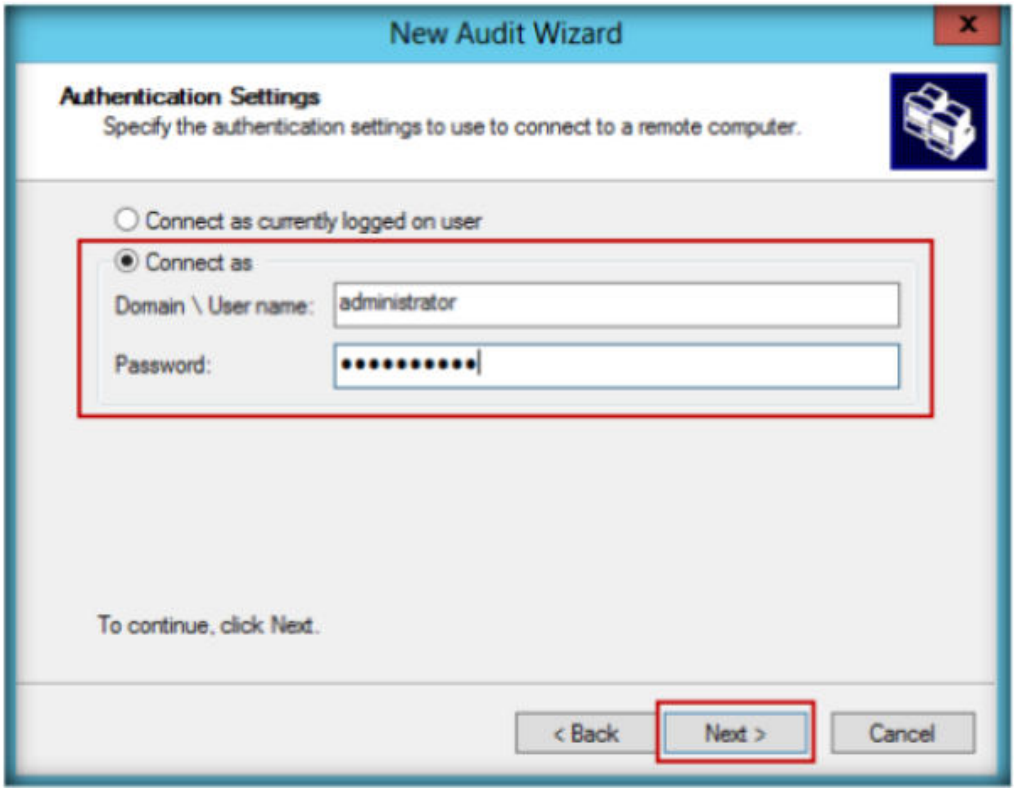


РИСУНОК 11.7: Установление диапазона сканирования IP

9. В мастере «Authentication Settings» выберите «Connect as», заполните важные учетные данные своей Виртуальной машины Windows Server 2008 и нажмите «Next».



Глобальная переменная РИСУНКА 11.8 Настройка сетевых параметров аутентификации Global Network Inventory

10. Установите параметры по умолчанию и нажимают кнопку «Finish», чтобы завершить работу с мастером.

РИСУНОК 11.9: Финал работы с мастером Global Network Inventory

11. На экран выводится прогресс сканирования.

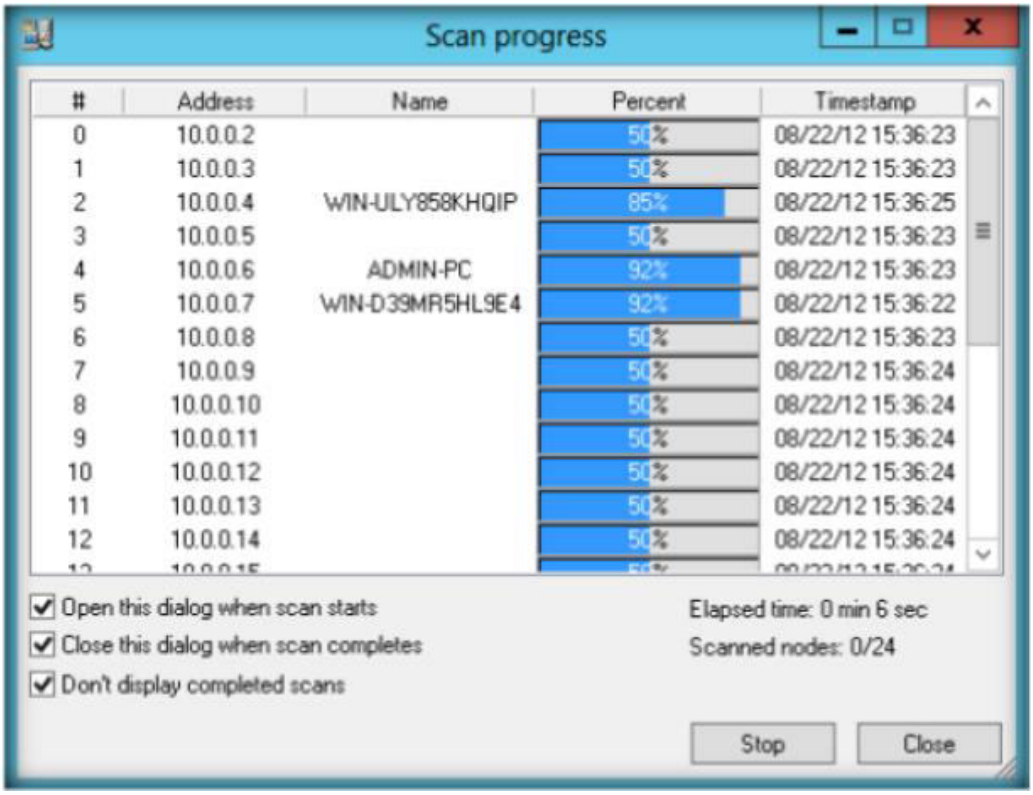


РИСУНОК 11.10: Процесс сканирования Global Network Inventory

12. После завершения сканирования, можно просмотреть результаты, как показано ниже на снимке экрана.

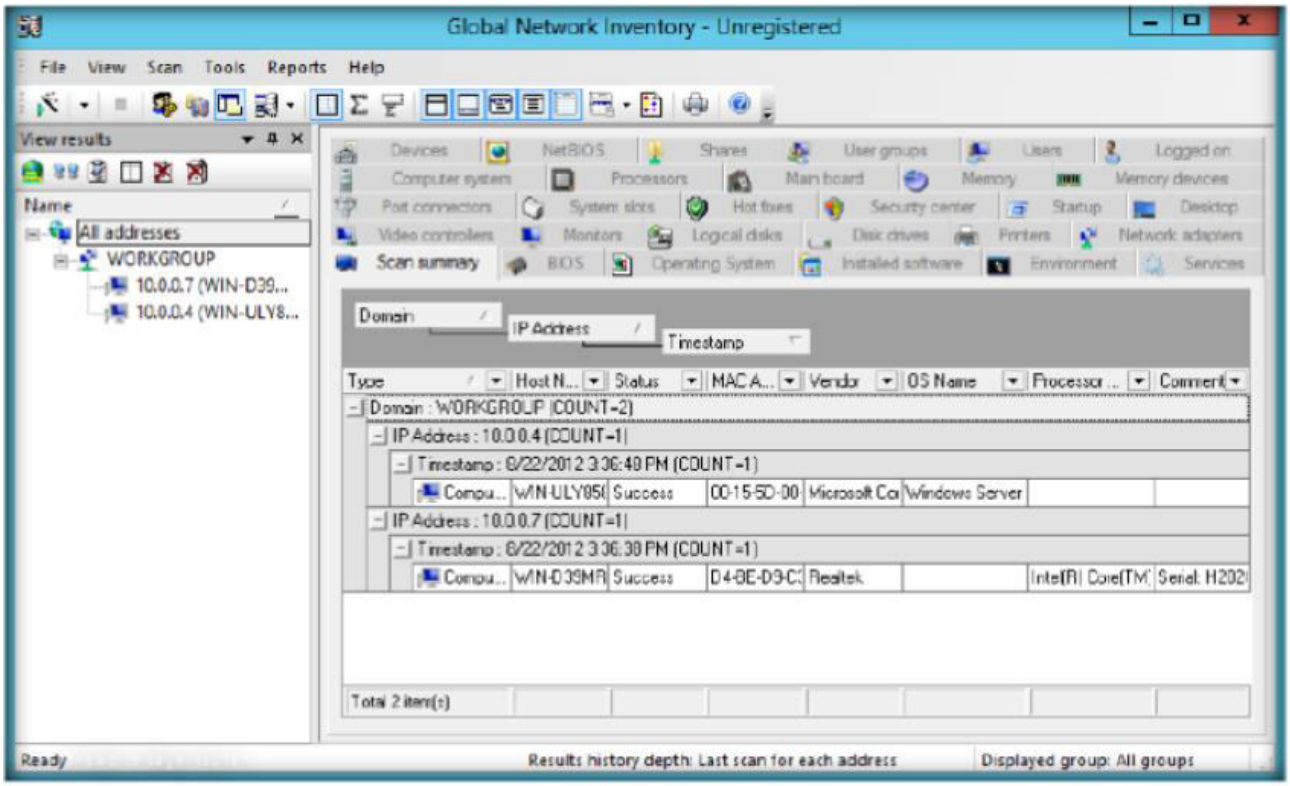


РИСУНОК 11.11: Результаты сканирования Global Network Inventory

13. Теперь выберите Windows Server 2008 из «view results» (результатов представления), чтобы просмотреть отдельные результаты.

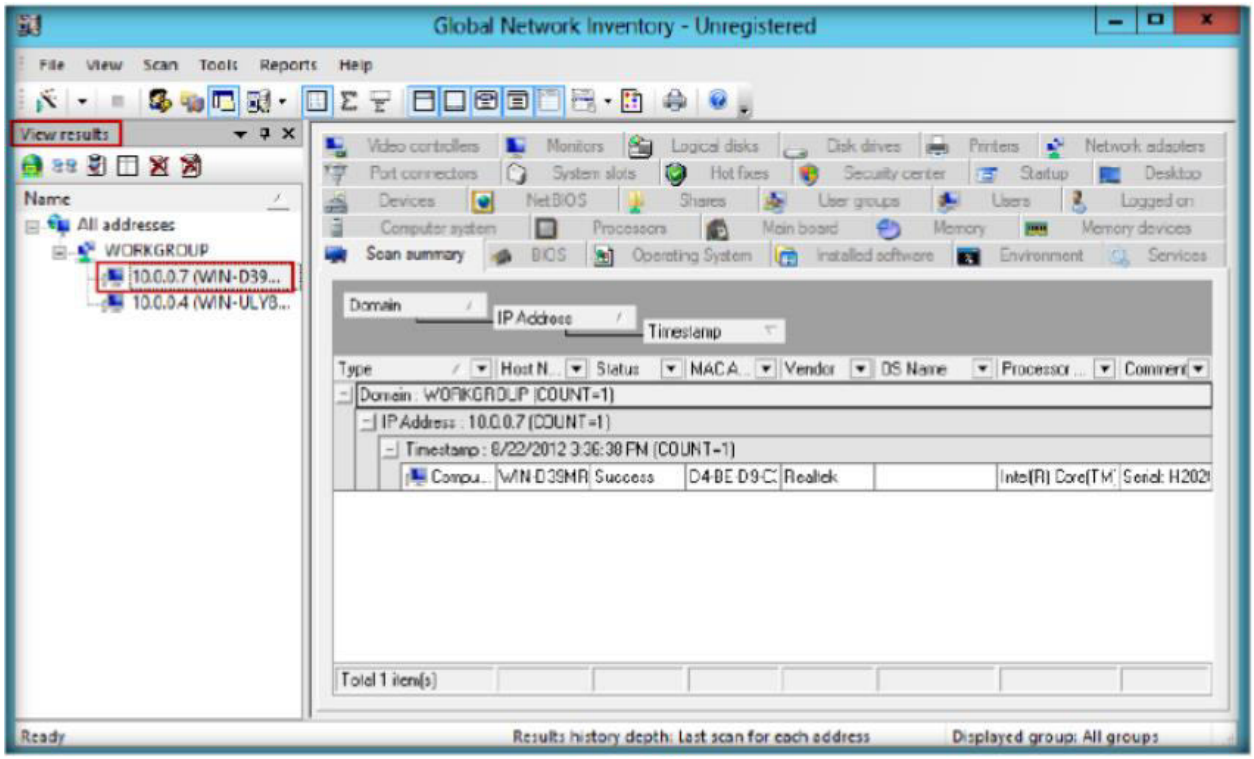


РИСУНОК 11.12 Индивидуальные результаты Windows Server 2008

14. Раздел «Scan Summary» дает Вам краткий обзор машин, которые были отсканированы.

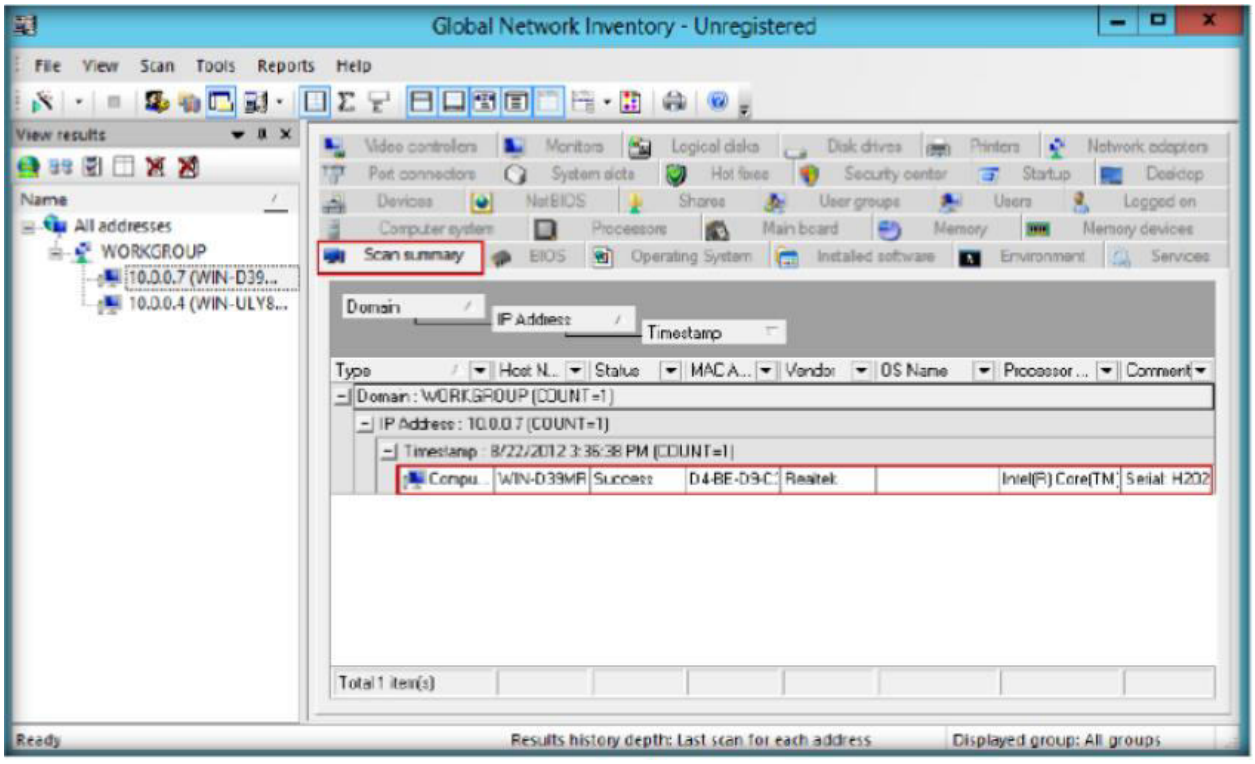


РИСУНОК 11.13: Вкладка «Scan Summary»

15. Раздел «BIOS» сообщает подробности параметров настройки BIOS.

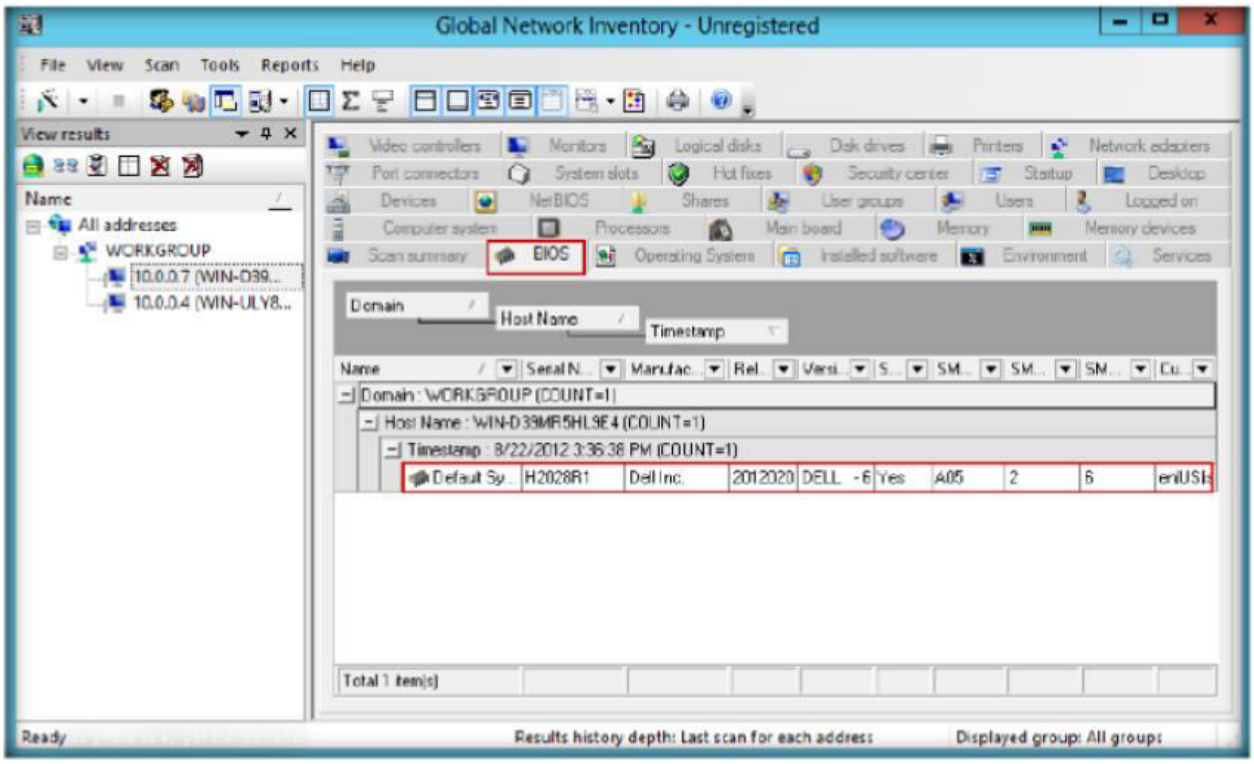


РИСУНОК 11.14: Вкладка «BIOS»

16. Вкладка «Memory» суммирует память в Вашей отсканированной машине.

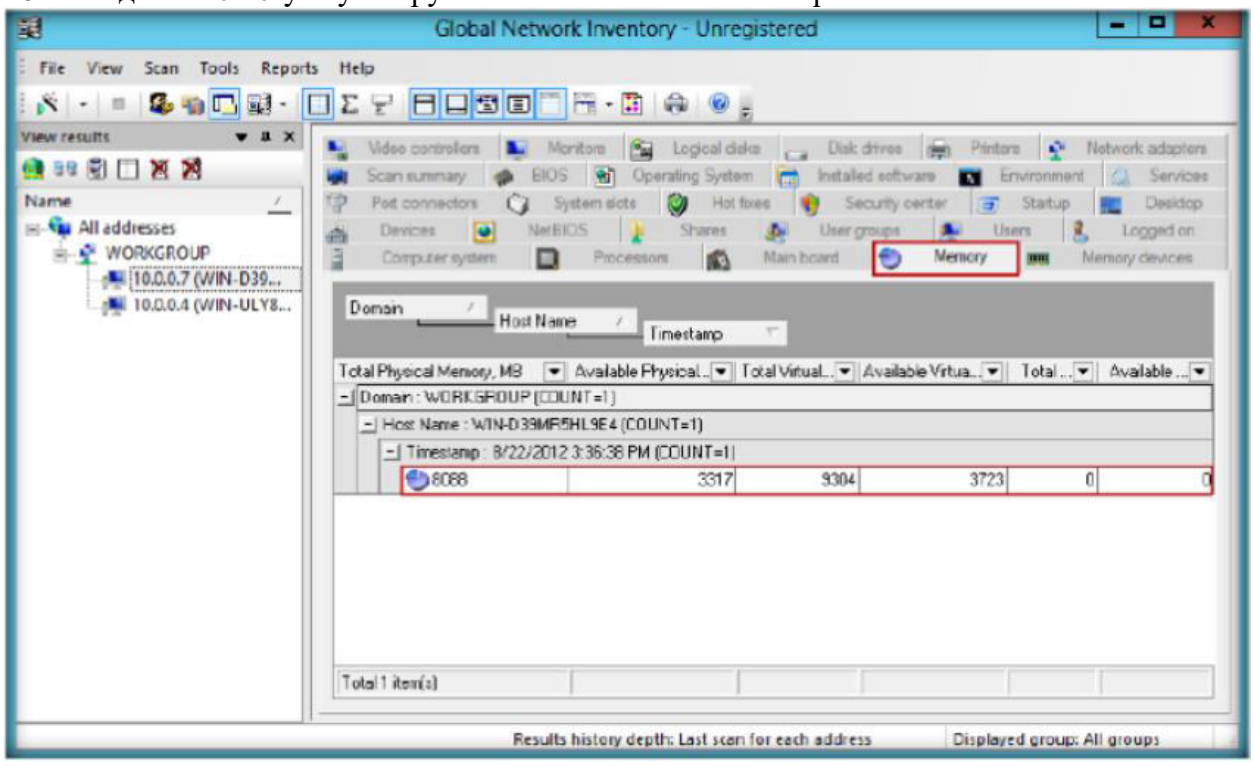


РИСУНОК 11.15: Вкладка «Memory»

17. В разделе «NetBIOS» можно просмотреть дополнительные детали.

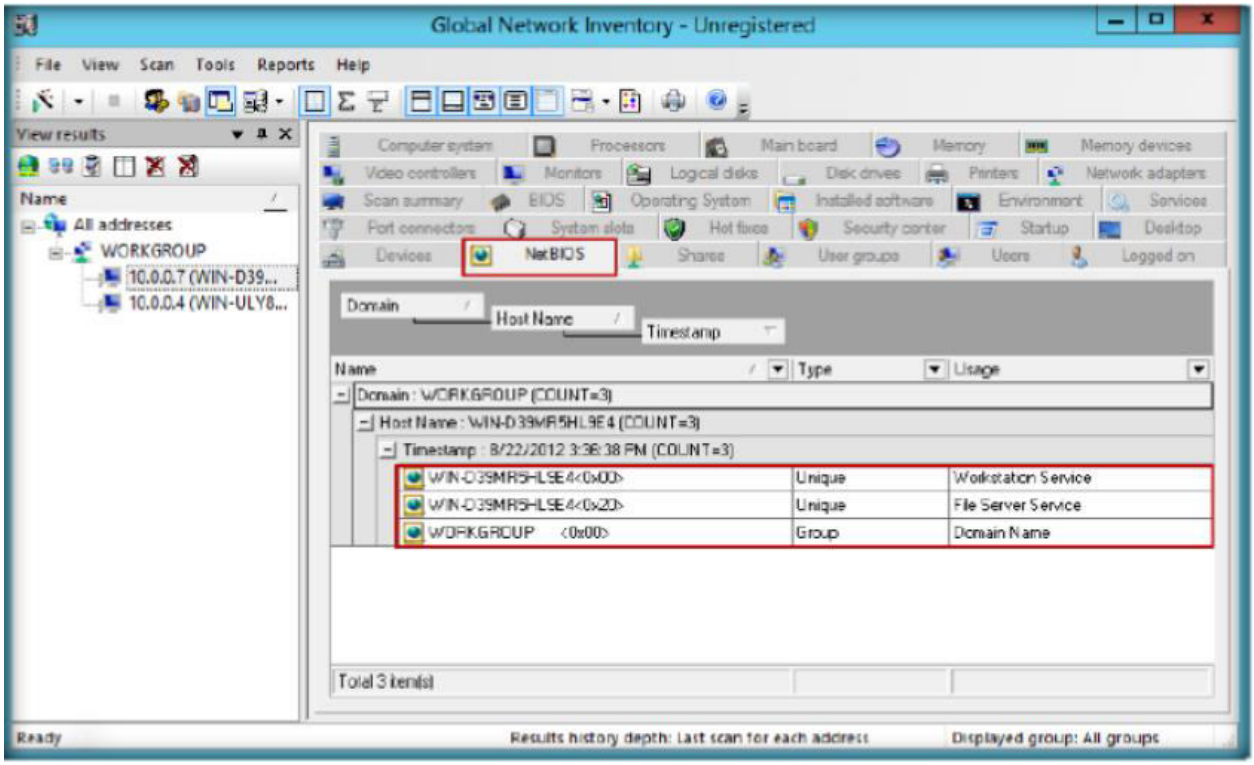


РИСУНОК 11:16: Вкладка «NetBIOS»

18. Вкладка «User Groups» показывает детали учетной записи пользователя с рабочей группой.

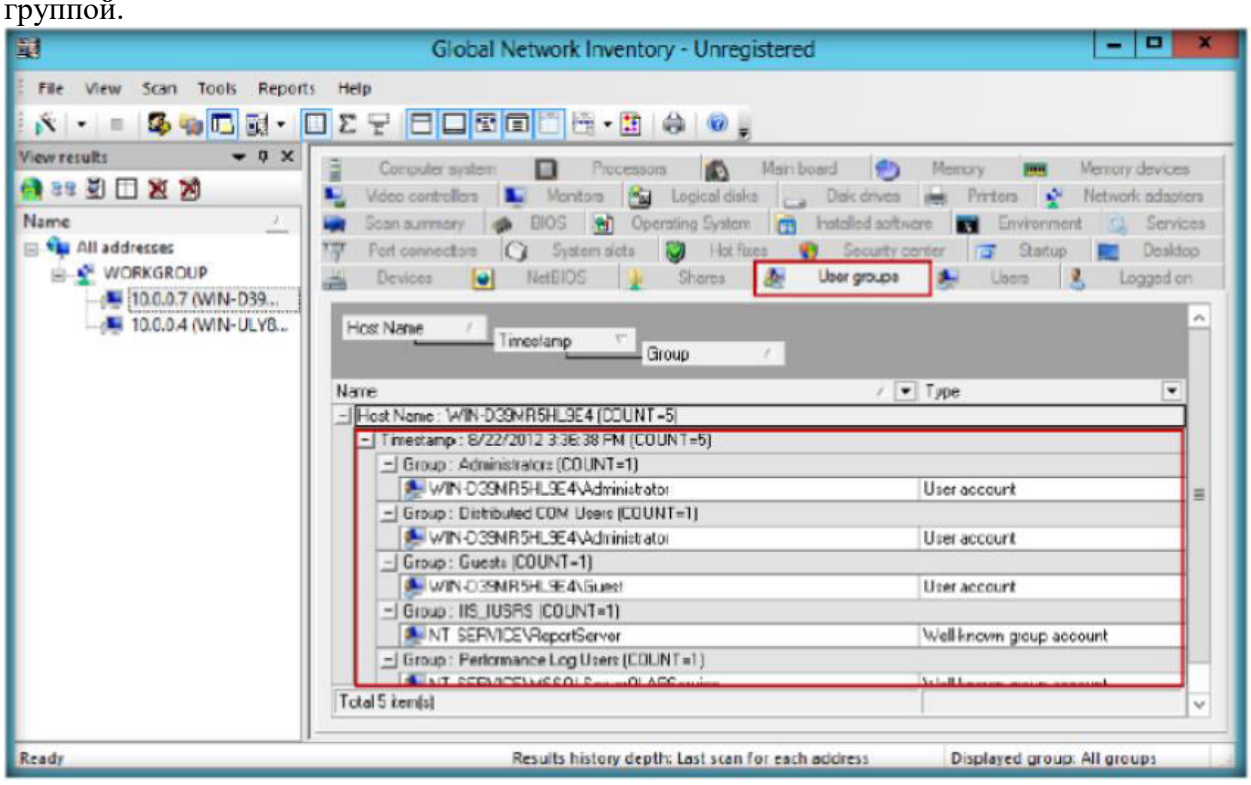


РИСУНОК 11.17: Вкладка «User Groups»

19. Вкладка «Logged on» подробно показывает, кто входил в систему и детали машины.

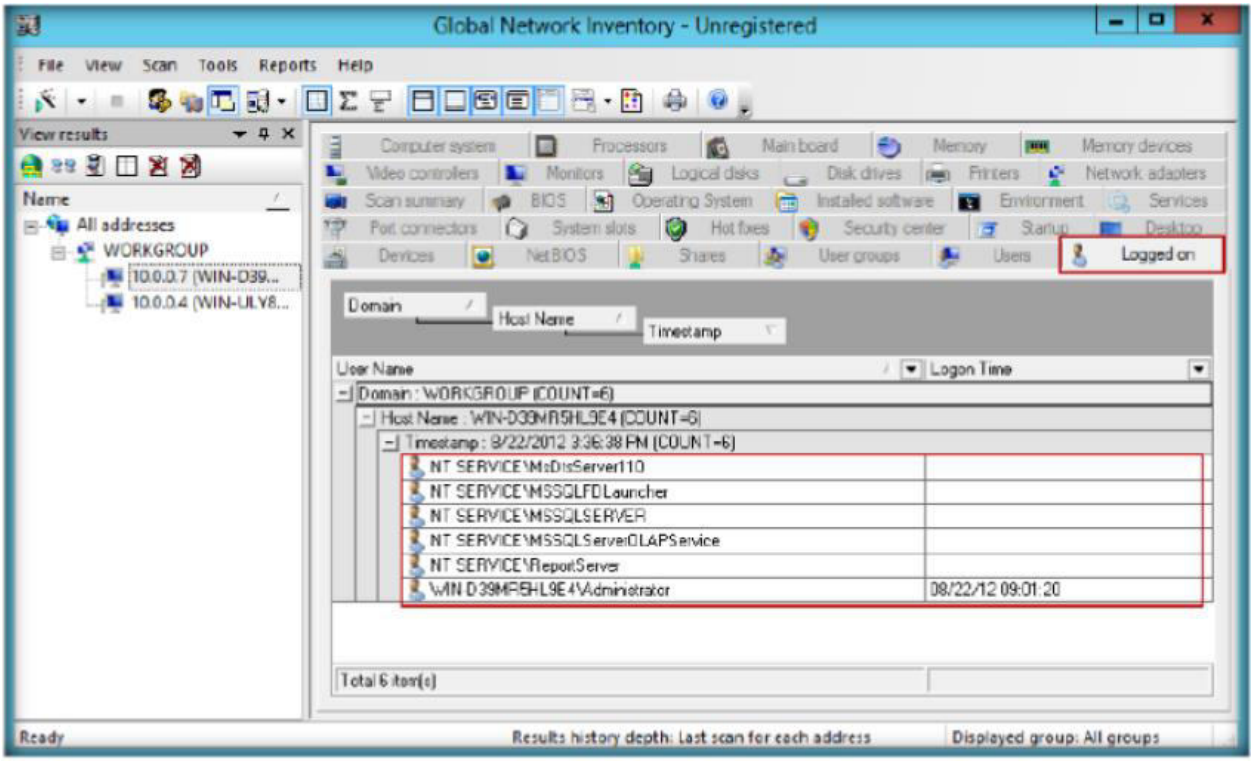


РИСУНОК 11.18: Вкладка «Logged on»

20. Раздел «Port connectors» показывает порты, соединенные в сети.

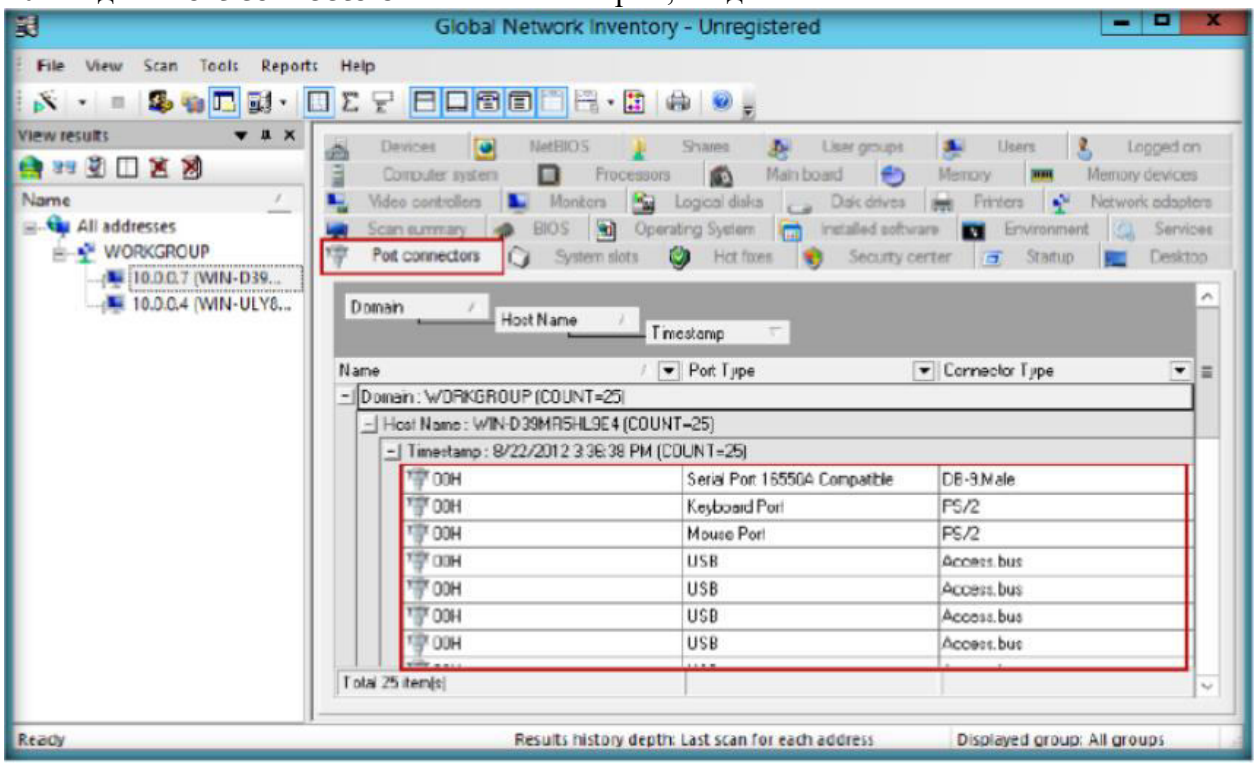


РИСУНОК 11.19: Раздел «Port connectors»

21. Раздел «Service» показывает детали служб, установленных в машине.

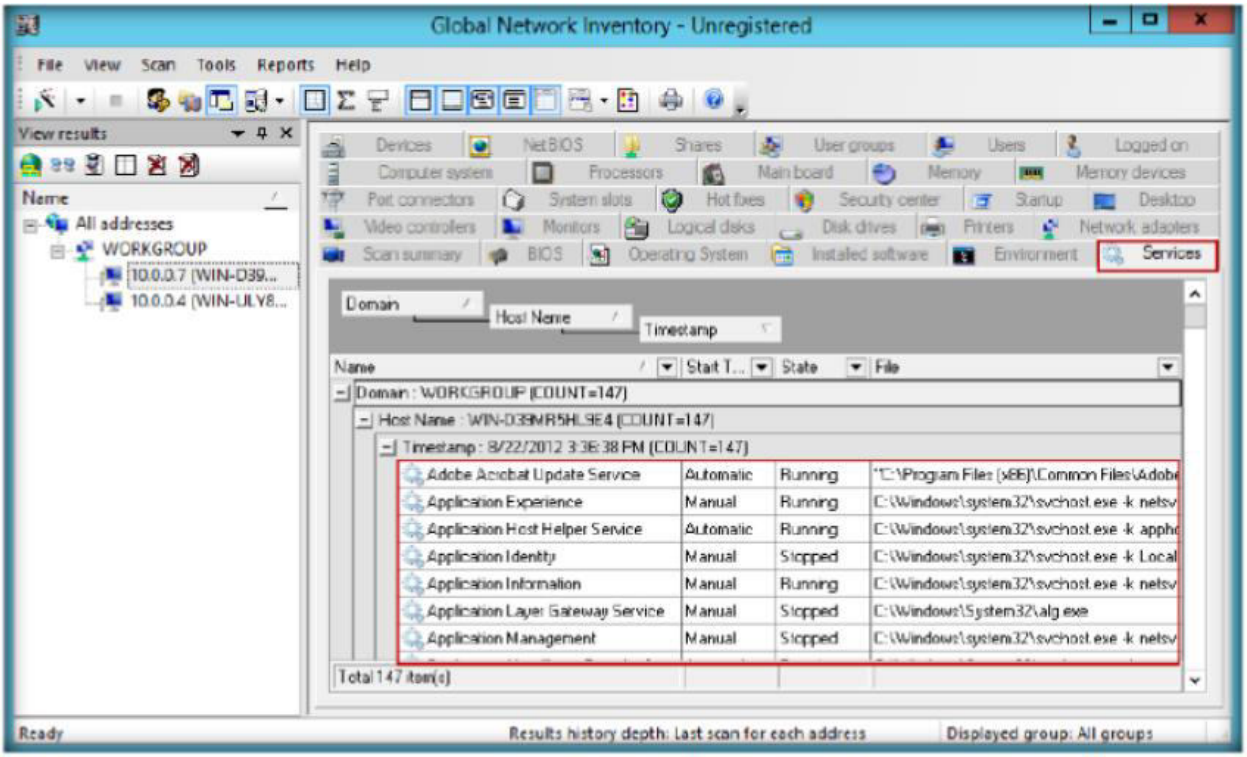


РИСУНОК 11.20: Раздел «Service»

22. Раздел «Network Adapters» показывает IP адаптера и тип адаптера.

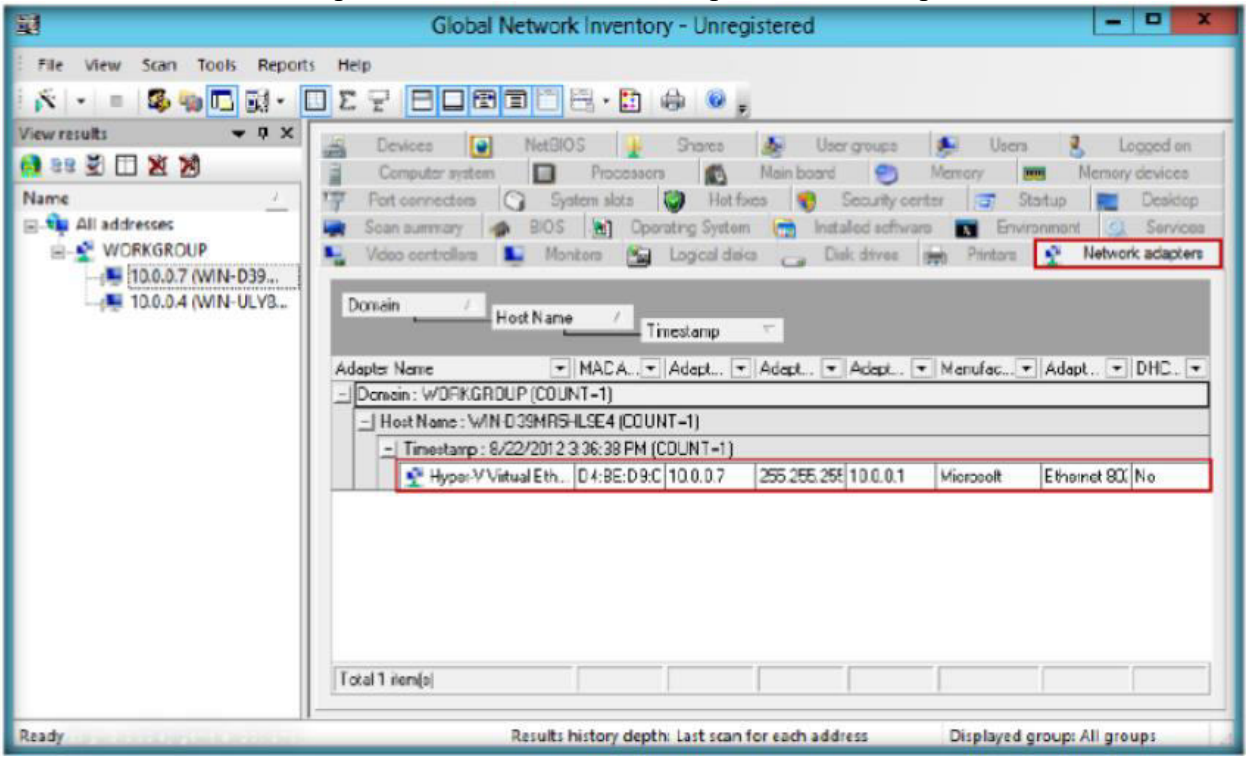


РИСУНОК 11.21: Раздел «Network Adapters»

Анализ практической работы

Запишите все IP-адреса, порты и приложения запуска и протоколы, которые Вы обнаружили во время выполнения лабораторной работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
Global Network Inventory	**Диапазон сканирования IP:** 10.0.0.1 — 10.0.0.50
	Отсканированный IP-адрес: 10.0.0.7,10.0.0.4
	Результат: ✓ Сводка сканирования ✓ BIOS ✓ Память ✓ NetBIOS ✓ UserGroup ✓ Зарегистрированный ✓ Соединитель порта ✓ Службы ✓ Сетевой адаптер

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы

1. Может ли Global Network Inventory контролировать удаленные компьютеры и сетевые устройства, и если да, как?
2. Как можно экспортировать Global Network agent (Глобальный Сетевой агент) в совместно используемый сетевой каталог?

Анонимный просмотр с помощью Proxy Switcher

Цели работы

Эта практическая работы покажет Вам, как могут быть отсканированы сети и как использовать Proxy Switcher. Она научит Вас как:

- Скрыть свой IP-адрес от веб-сайтов, которые Вы посещали
- Переключить прокси-сервер для улучшенного анонимного перемещения

Средства лабораторной работы

Чтобы выполнить лабораторную работу, Вам необходимо:

- Proxy Switcher расположен в **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- Вы можете также загрузить последнюю версию Proxy Switcher по этой ссылке http://www.proxyswitcher.com/
- Если Вы решите загрузить последнюю версию, то снимки экрана, показанные в лабораторной работе, могут отличаться
- Компьютер с Windows Server 2012
- Веб-браузер с доступом к Интернету
- Выполните шаги мастера установки, чтобы установить Proxy Switcher
- Административные привилегии для пользования инструментами

Краткие теоретические сведения

Обзор Proxy Switcher

Proxy Switcher позволяет Вам автоматически выполнять действия на основе

обнаруженного сетевого соединения. Proxy Switcher идет с некоторыми действиями по умолчанию, например, устанавливает параметры настройки по доверенности для Internet Explorer, Firefox и Opera.

Постановка задачи

1. Установите Proxy Workbench в Windows Server 2012 (хост-машина)
2. Proxy Workbench расположен в **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
3. Выполните шаги мастера установки и установите его на всех платформах операционной системы Windows.
4. Эта Практическое занятие будет выполняться в среде лаборатории CEH - на Windows Server 2012, Windows Server 2008 и Windows 7
5. Откройте браузер Firefox в своем Windows Server 2012, перейдите к «Tools» и нажмите «Options» в строке меню.

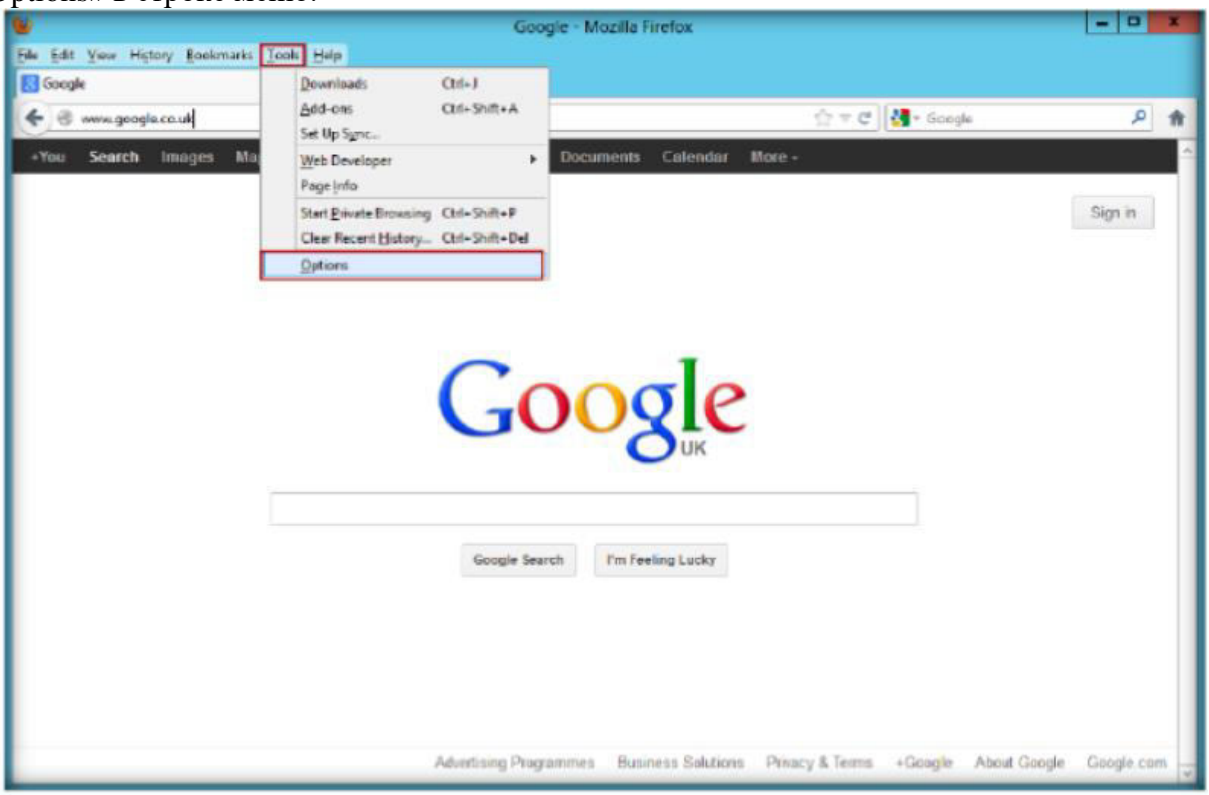


РИСУНОК 12.1: Вкладка «Options» в Firefox

6. Перейдите к «Advanced profile» (Усовершенствованному профилю) в мастере опций Firefox, и выберите вкладку «Network», и затем нажмите «Settings».

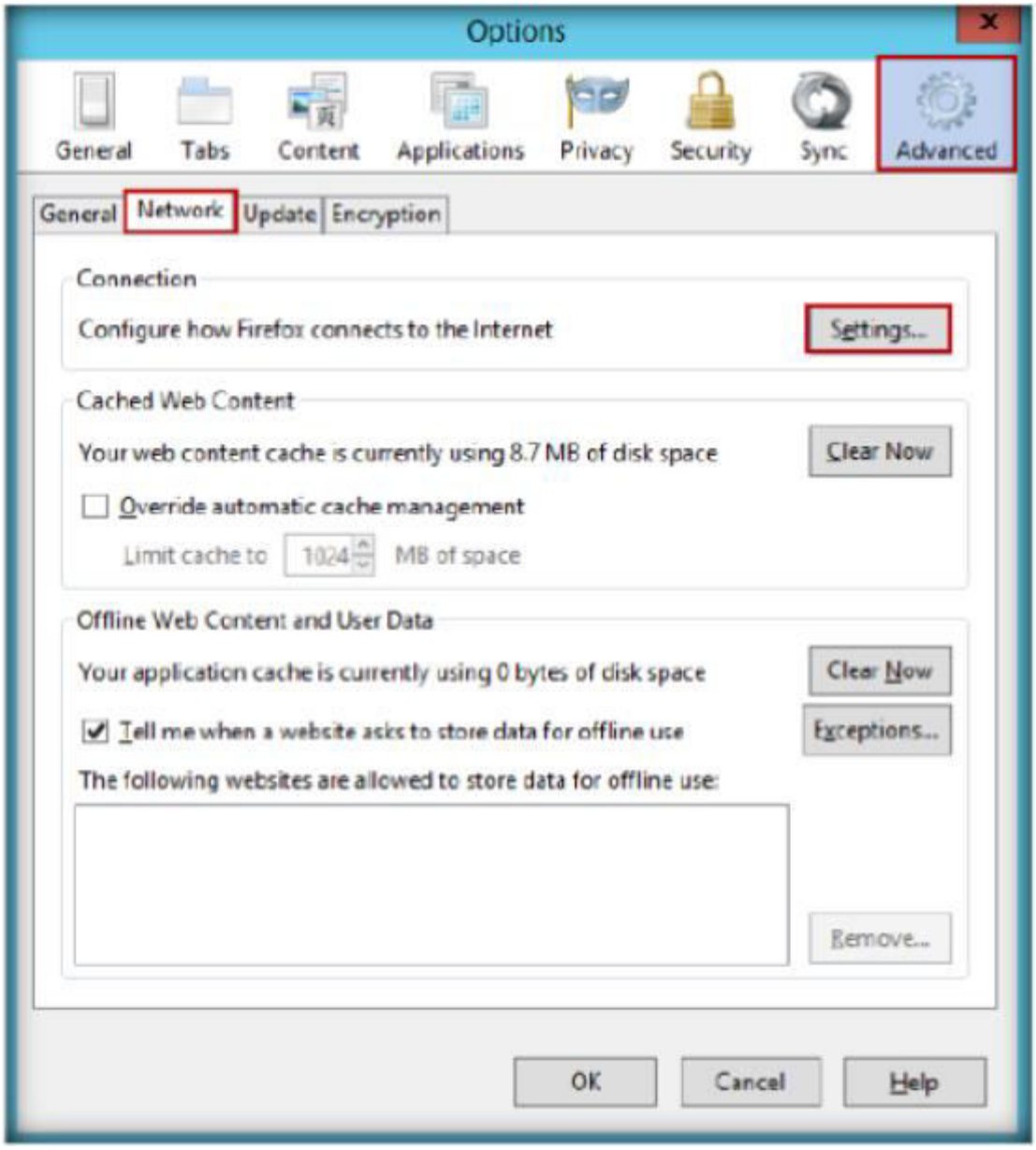


РИСУНОК 12.2: Параметры настройки сети в Firefox

7. Выберите «Use System proxy settings» (Используйте Системный переключатель параметров настройки прокси) и нажмите "OK".

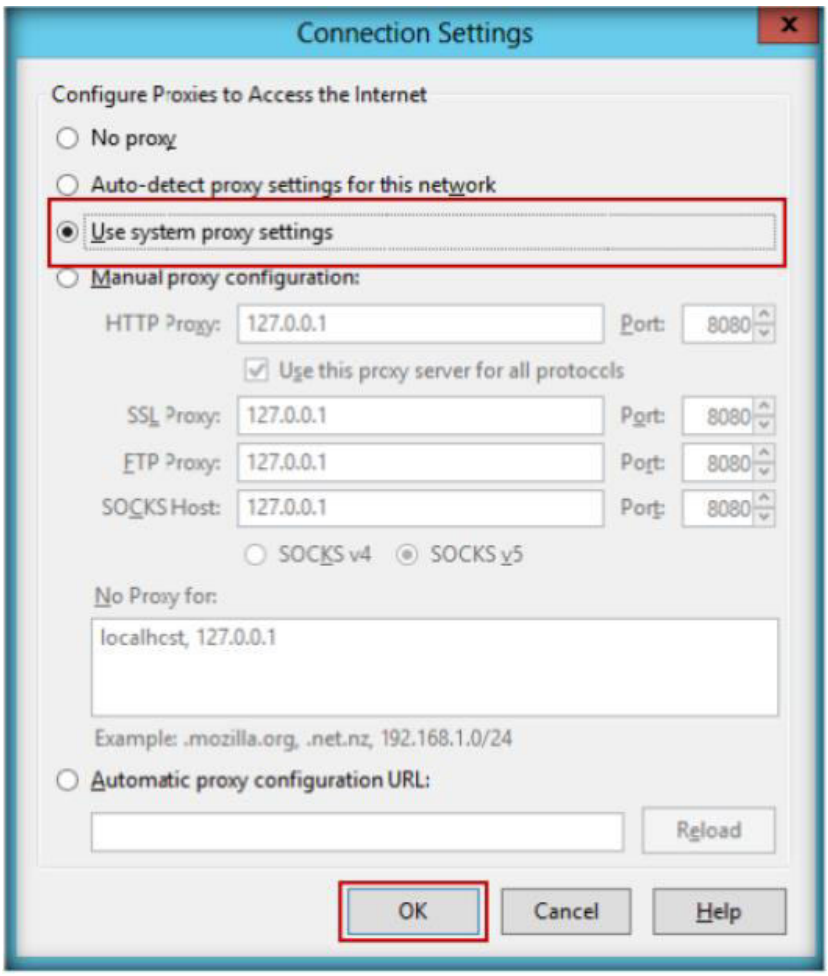


РИСУНОК 12.3: Настройки подключения Firefox

8. Теперь, чтобы установить Proxy Switcher Standard, выполните шаги мастера установки.
9. Чтобы запустить Proxy Switcher Standard, перейдите к Меню "Пуск", наведя курсор мыши в нижний левый угол рабочего стола.

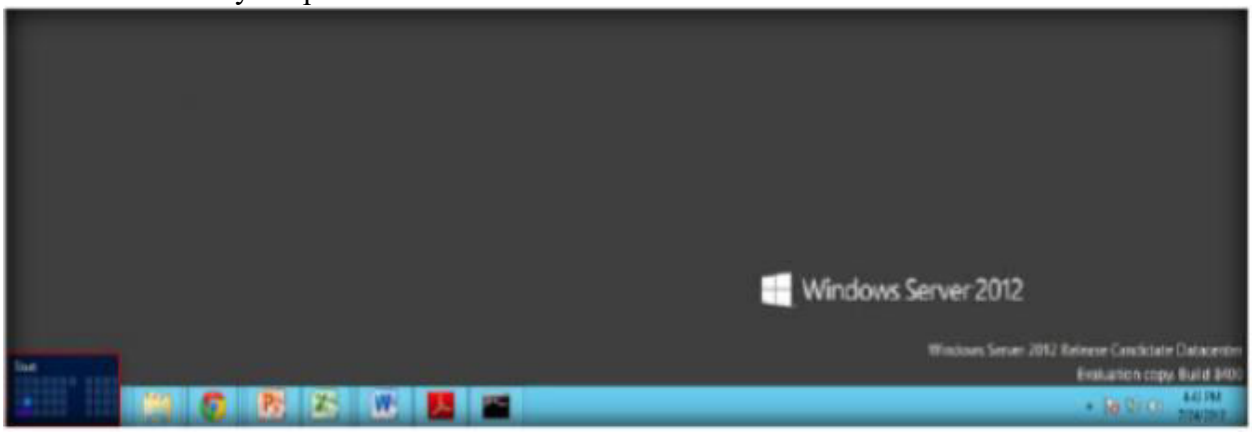


РИСУНОК 12.4: Windows Server 2012 – Рабочий стол

10. Щелкните по приложению Proxy Switcher Standard, чтобы открыть окно Proxy Switcher ИЛИ нажмите Proxy Switcher из списка значков.

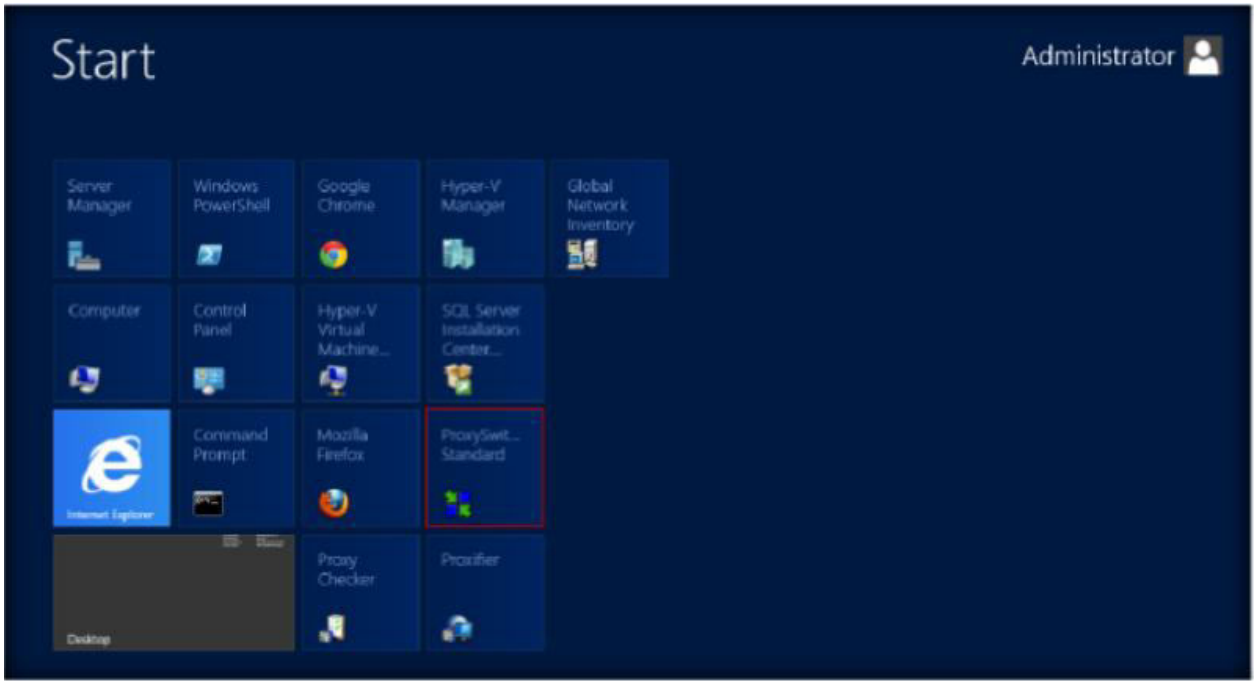


РИСУНОК 12.5: Windows Server 2012 - приложения

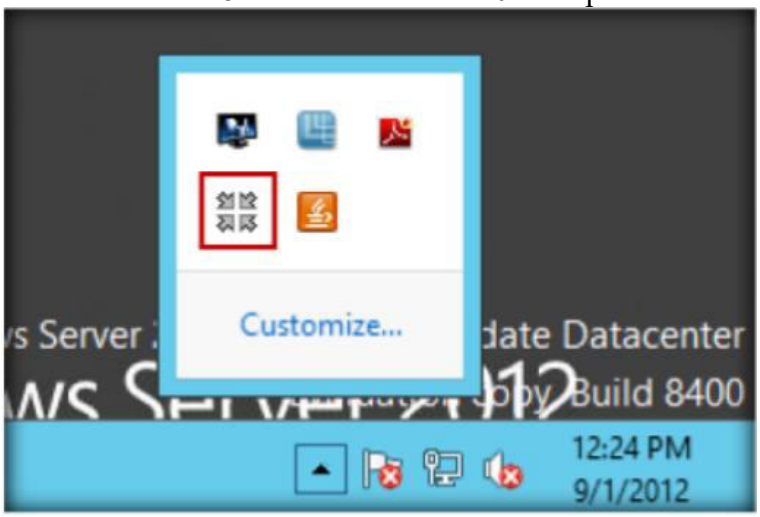


РИСУНОК 12.6: Выберите Proxy Switcher

11. Мастер Proxy List появится, как показано ниже на снимке экрана. Нажмите «Next».

РИСУНОК 12.7: Мастер Proxy List

12. Выберите «Find New Server, Rescan Server, Recheck Dead» из общего перечня и нажмите кнопку «Finish».

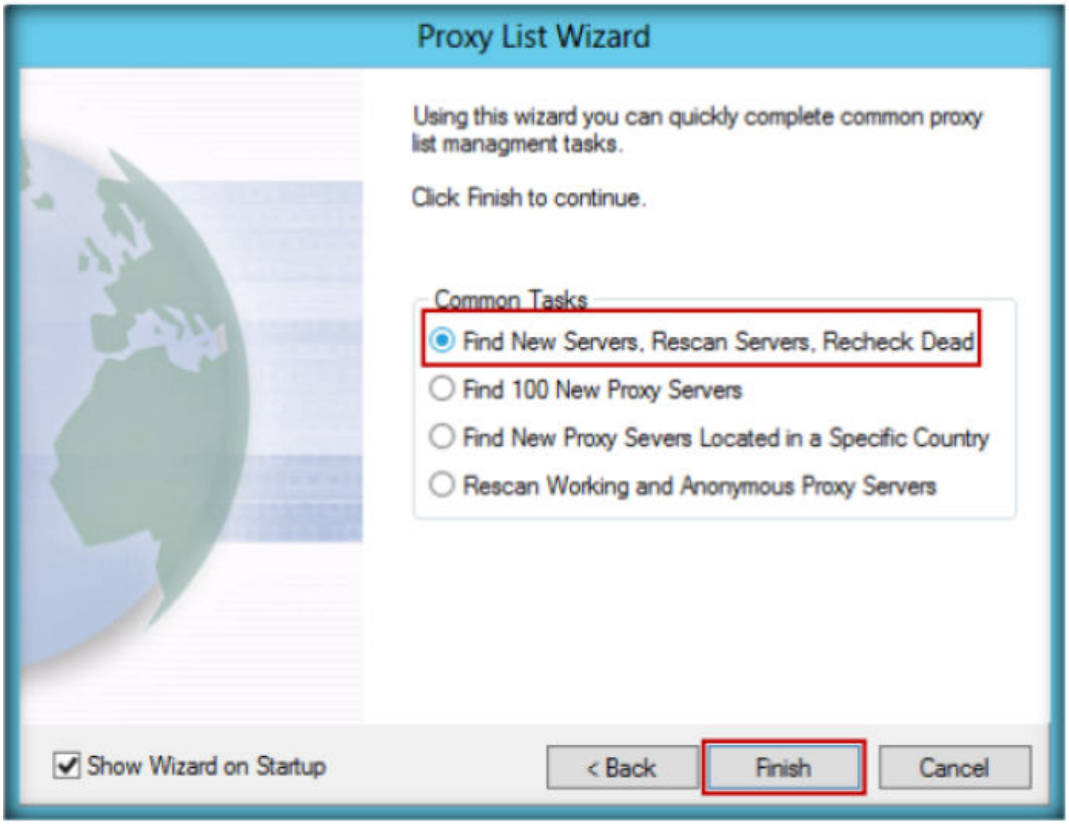


РИСУНОК 12.8: Выбор общих задач

13. Список загруженных прокси-серверов покажется на левой панели.

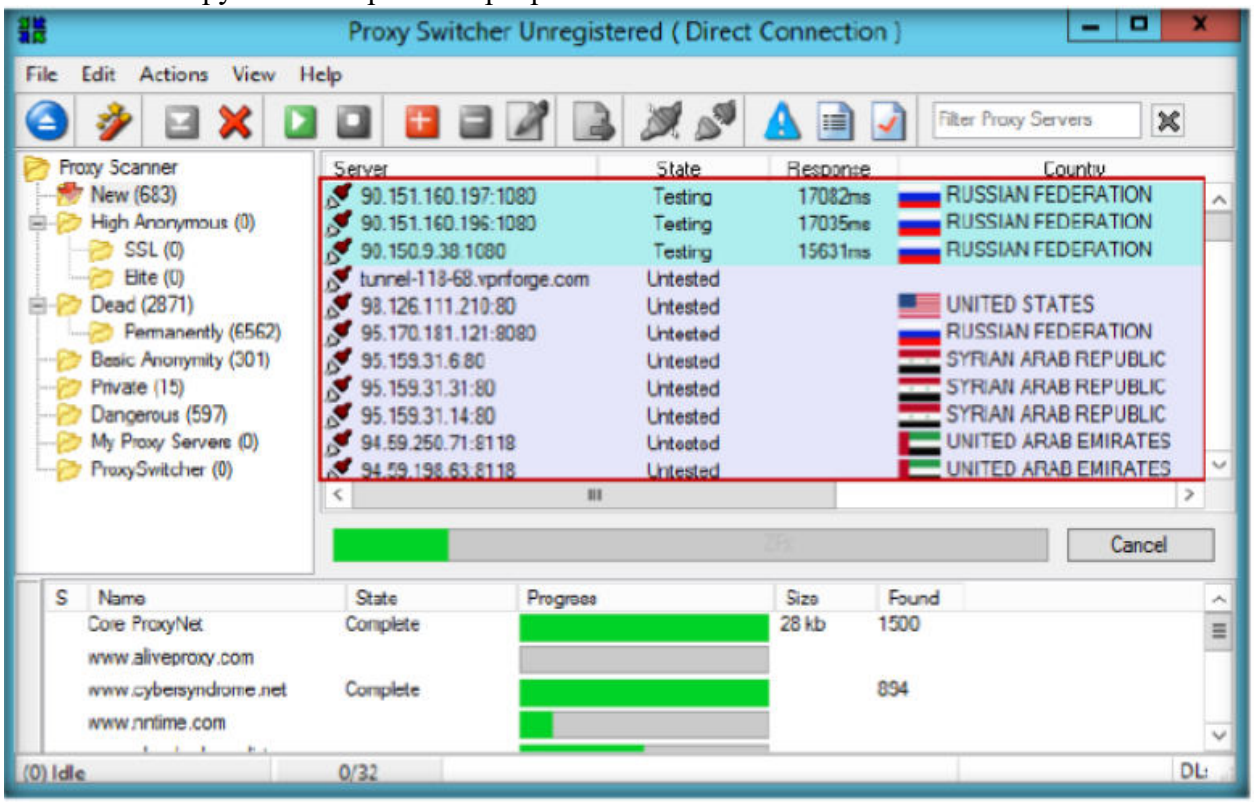


РИСУНОК 12.9: Список загруженного Прокси-сервера

14. Чтобы прекратить загрузку прокси-сервера нажмите  .

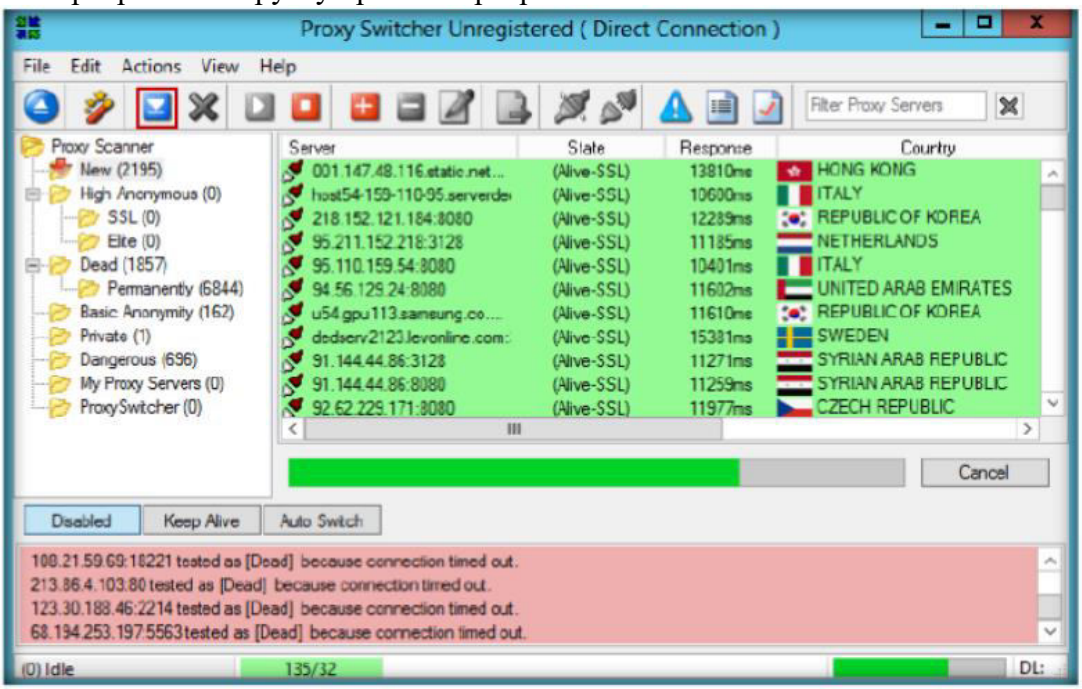


РИСУНОК 12.10: остановка загрузки прокси-сервера

15. Нажмите «Basic Anonymity» на основной панели. Покажется список загруженных прокси-серверов.

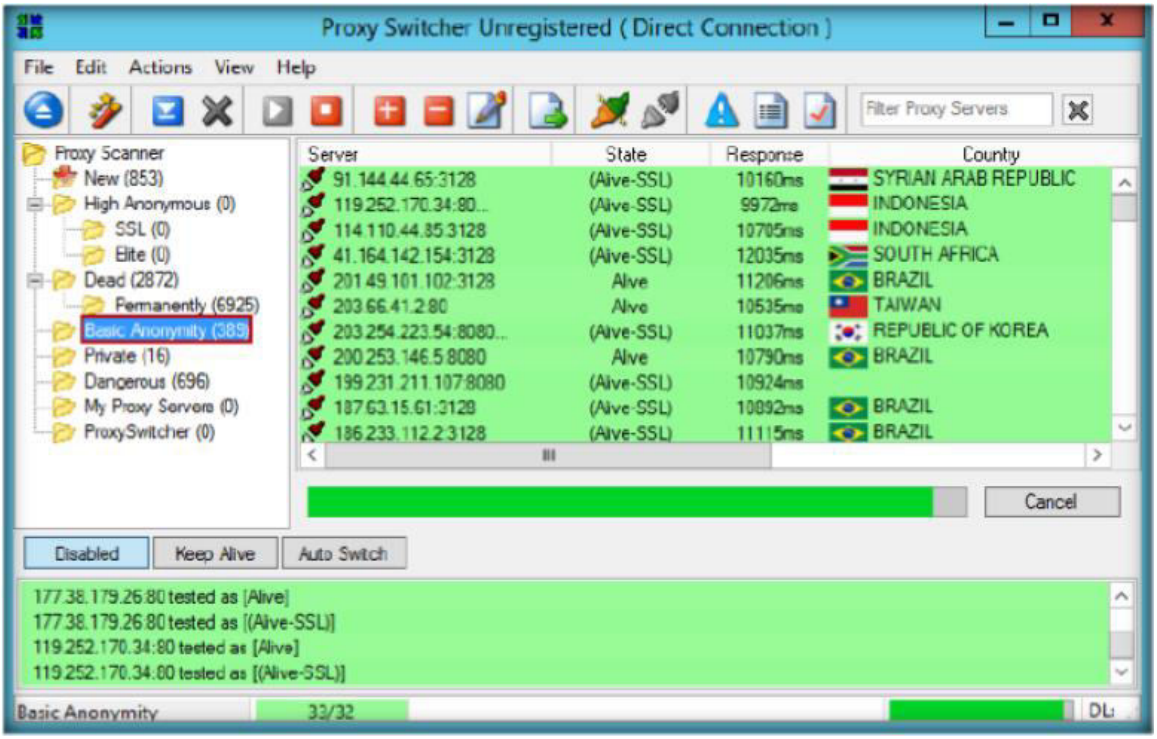


РИСУНОК 1211: Выбор загруженного Прокси-сервера

16. Выберите один IP-адрес Прокси-сервера на основной панели и щелкните  иконку.

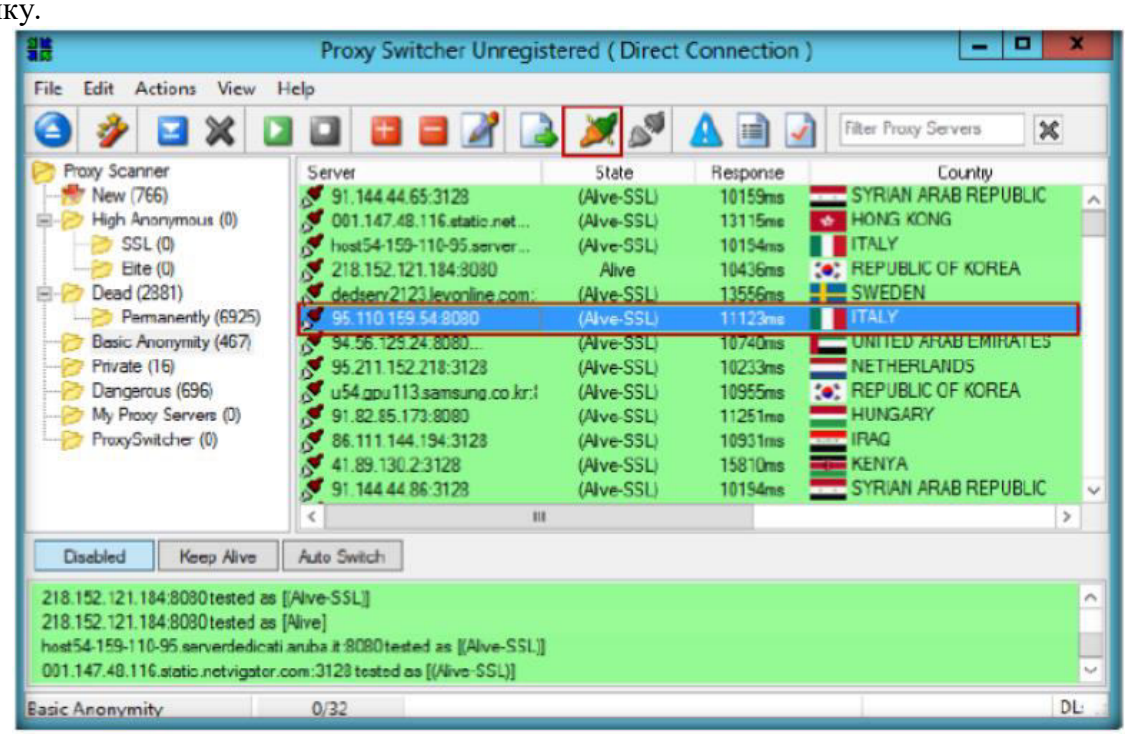


РИСУНОК 12.12: Выбор прокси-сервера

17. Выбранный прокси-сервер соединится, и он покажет следующий значок соединения.

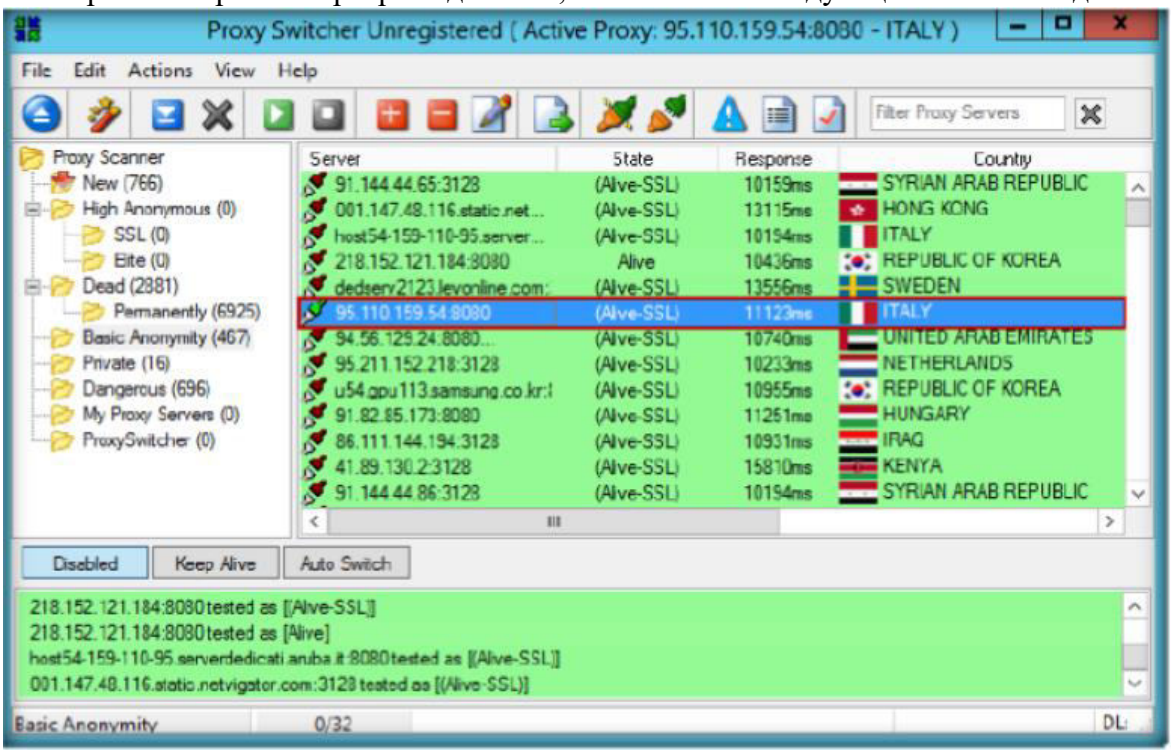


РИСУНОК 12.13: Успешное соединение выбранного прокси-сервера

18. Перейдите к веб-браузеру (Firefox) и введите следующий URL http://www.pioxyswitchei.com/check.php, чтобы проверить соединение выбранного прокси-сервера. Если соединение успешно, тогда у Вас будет так, как показано ниже на снимке экрана.

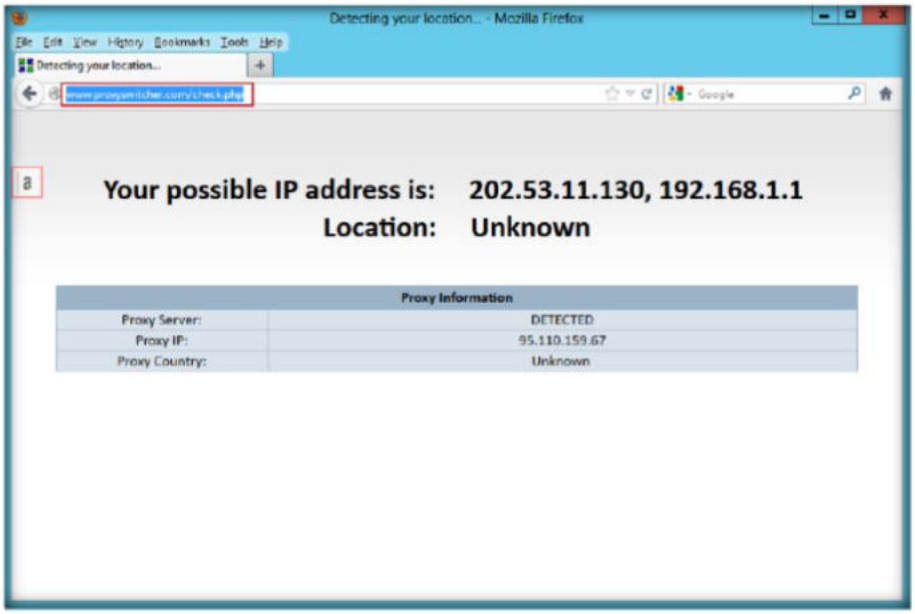


РИСУНОК 12.14: Обнаруженный прокси-сервер

19. Откройте другую вкладку в веб-браузере и перемещайтесь, анонимно используя этот прокси.

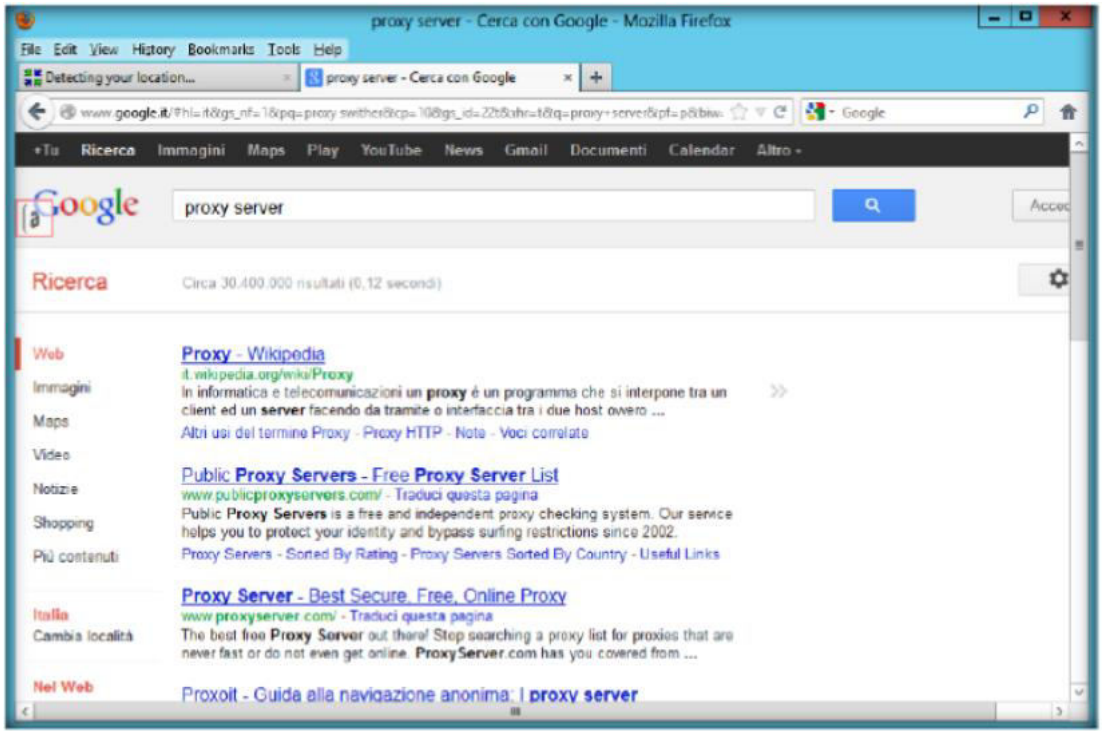


РИСУНОК 12.14: Перемещение используя прокси-сервер

Анализ практической работы

Запишите все IP-адреса прокси-серверов и связь, которую Вы обнаружили во время выполнения лабораторной работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
Proxy Switcher	**Сервер:** Список доступных прокси-серверов
	Выбранный IP-адрес прокси-сервера: 95.110.159.54
	Выбранное название страны по доверенности: ИТАЛИЯ
	Конечный IP-адрес прокси-сервера: 95.110.159.67

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ **ПРАКТИЧЕСКОЙ** РАБОТЕ.

Вопросы

1. Какие технологии используются для Proxy Switcher?
2. Почему у Proxy Switcher исходный код не открытый?

Практическое занятие №13. Объединение в цепочку с помощью Proxy Workbench

Цели работы

Эта практическая работа покажет Вам, как могут быть отсканированы сети и как использовать Proxy Workbench. Она научит вас как:

- Пользоваться инструментом Proxy Workbench
- Объединить в цепь хост-машину Windows и Виртуальные машины

Средства лабораторной работы

Чтобы выполнить лабораторную работу, Вам небходимо:

- Proxy Workbench расположен в **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**
- Вы можете также загрузить последнюю версию Proxy Workbench по этой ссылке http://proxyworkbench.com
- Если Вы решаете загрузить последнюю версию, то снимки экрана, показанные в лабораторной работе могут отличаться
- Компьютер с Windows Server 2012 как атакующий (хост-машина)
- Другой компьютер с Window Server 2008 и Windows 7 как жертва (виртуальная машина)
- Веб-браузер с доступом к Интернету
- Выполните шаги мастера установки, чтобы установить Proxy Workbench
- Административные привилегии для пользования инструментами

Краткие теоретические сведения

Обзор Proxy Workbench

Proxy Workbench - прокси-сервер, который выводит на экран данные в режиме реального времени. Даже данные текущие между веб-браузером и веб-сервером, анализируя FTP в пассивных и активных режимах.

Постановка задачи

1. Установите Proxy Workbench на всех платформах операционной системы Windows (Windows Server 2012, Windows Server 2008 и Windows 7)

2. Proxy Workbench расположены в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench

3. Вы можете также загрузить последнюю версию Инструментальных средств по доверенности по этой ссылке http://proxyworkbench.com

4. Выполните шаги мастера установки и установите его на всех платформах операционной системы Windows

5. Эта Практическое занятие будет выполняться в среде лаборатории CEH - на Windows 2012, Windows Server 2008 и Windows 7

6. Откройте браузер Firefox в своем Windows Server 2012, и перейдите к «Tools» (Инструментам) и щелкните по «Options» (опциям).

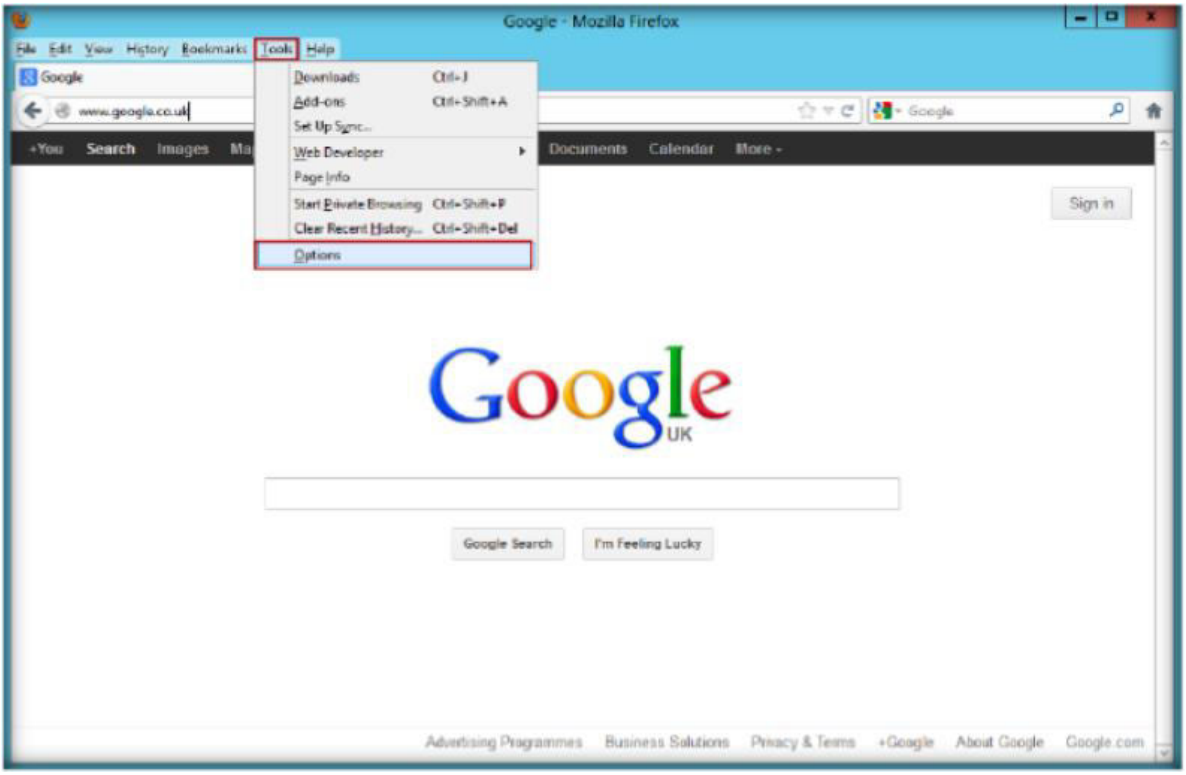


РИСУНОК 13.1: Вкладка «Options» в Firefox

7. Перейдите к «Advanced profile» (Усовершенствованному профилю) в мастере опций Firefox, и выберите вкладку «Network», и затем нажмите «Settings».

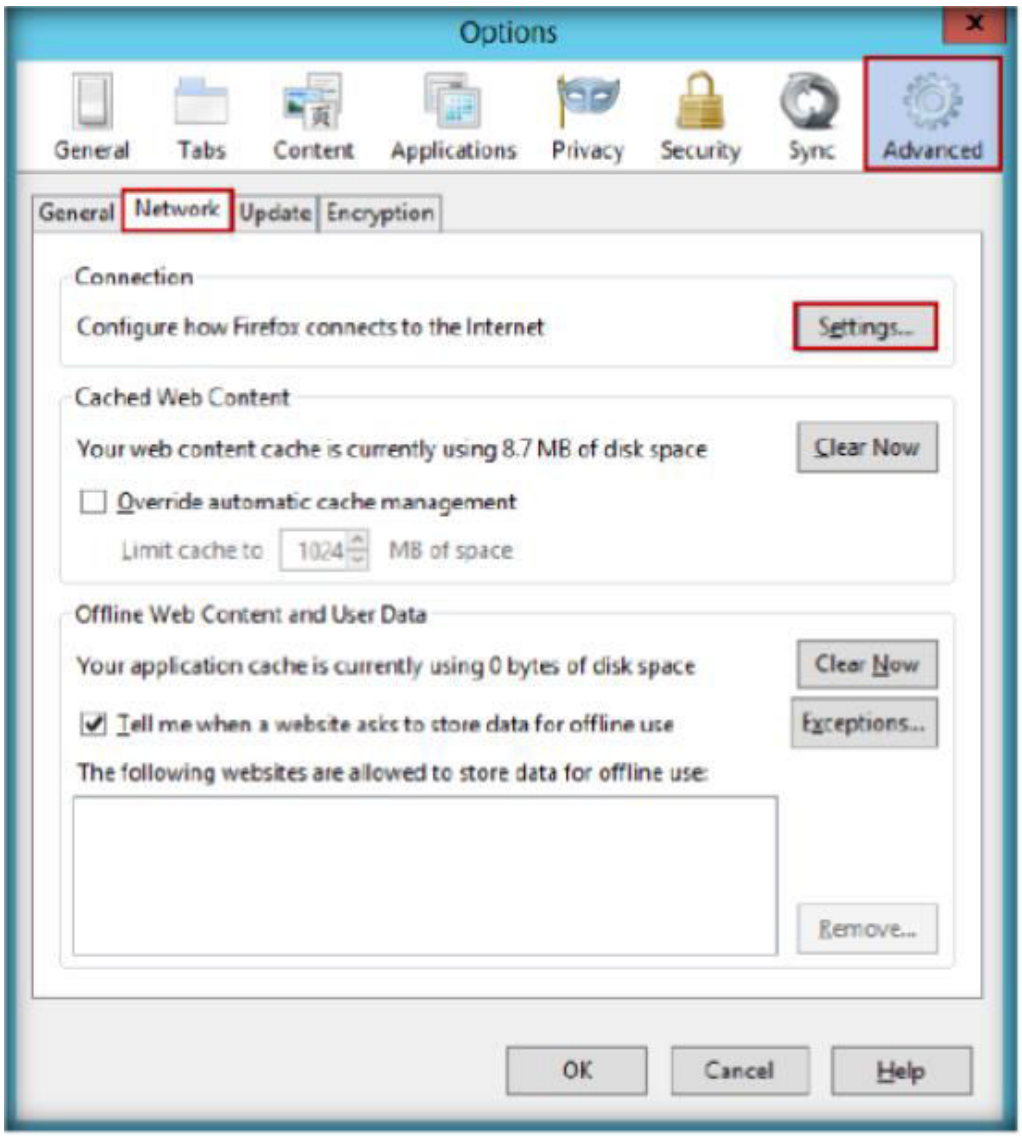


РИСУНОК 13.2Параметры настройки сети Firefox

8. Проверьте ручную конфигурацию по доверенности в мастере настроек подключения.

9. Введите HTTP прокси как 127.0.0.1 и введите значение порта 8080, проверьте опцию «Use this proxy server for all protocols» (использовать этот прокси-сервер для всех протоколов) и нажмите "OK".

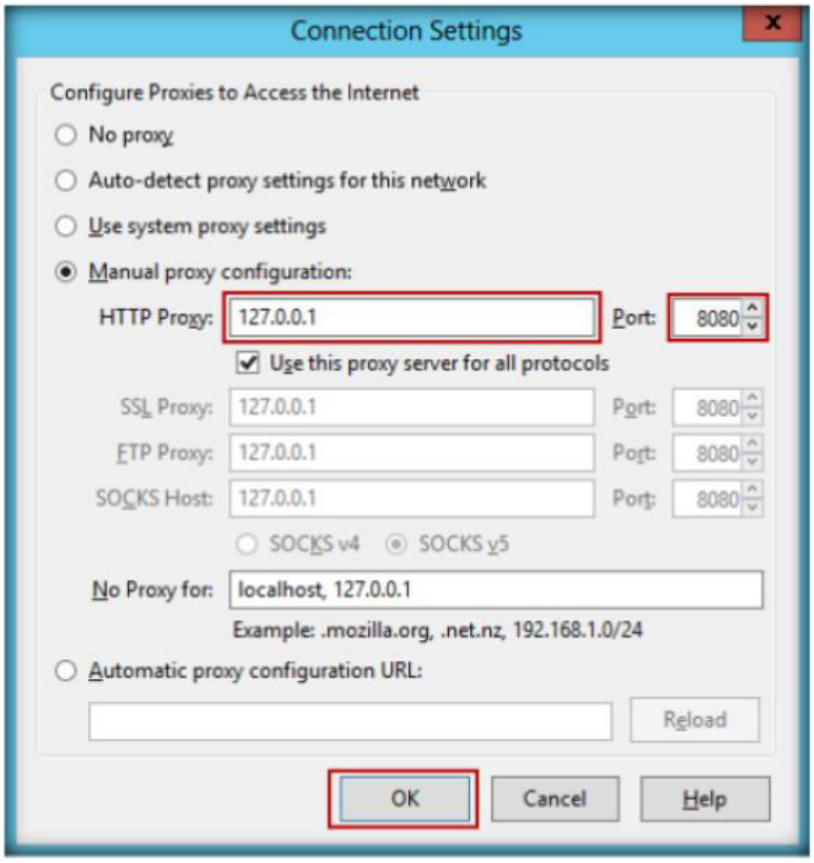


РИСУНОК 13.3: Настройки подключения Firefox

10. Если Вы встретитесь с ошибкой порта, игнорируйте ее.
11. Запустите Меню "Пуск".

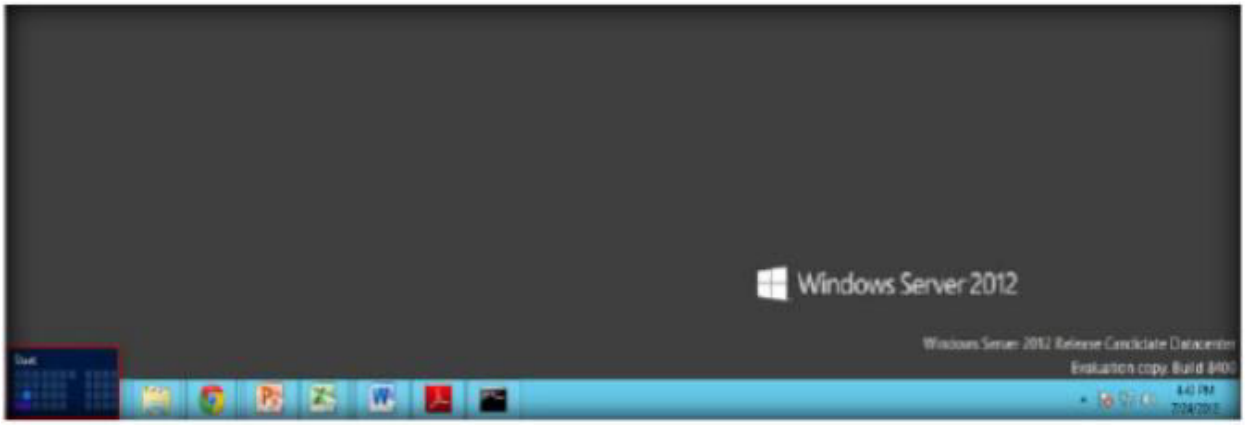


РИСУНОК 13.4: Windows Server 2012 – Рабочий стол

12. Щелкните по приложению Proxy Workbench, чтобы открыть окно Proxy Workbench.

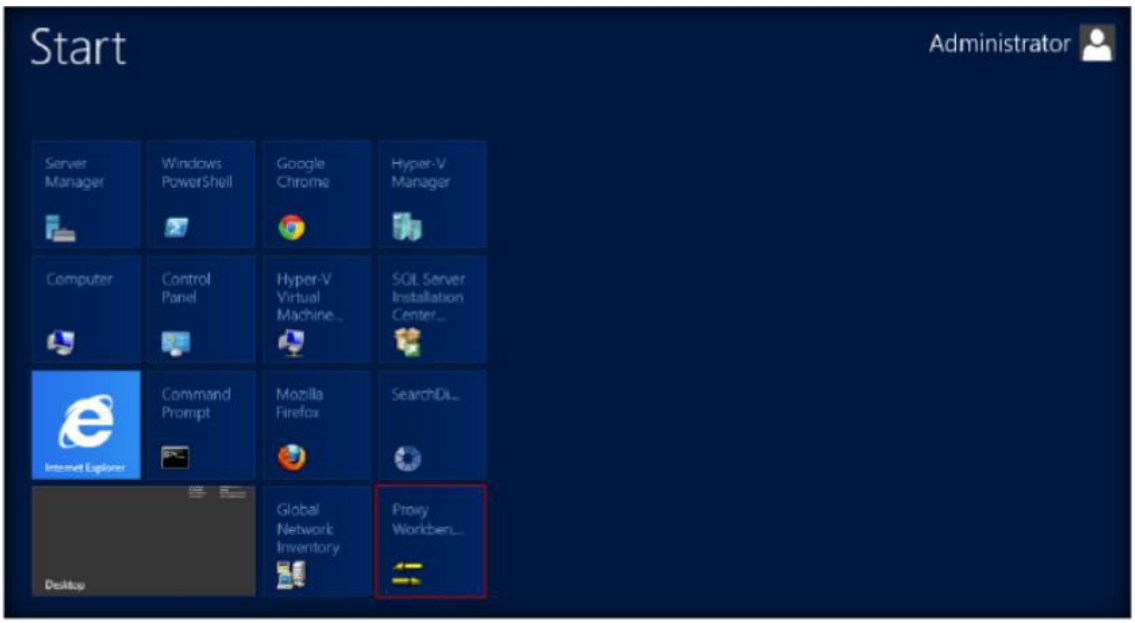


РИСУНОК 13.5: Windows Server 2012 - приложения

13. Появляется главное окно Proxy Workbench.

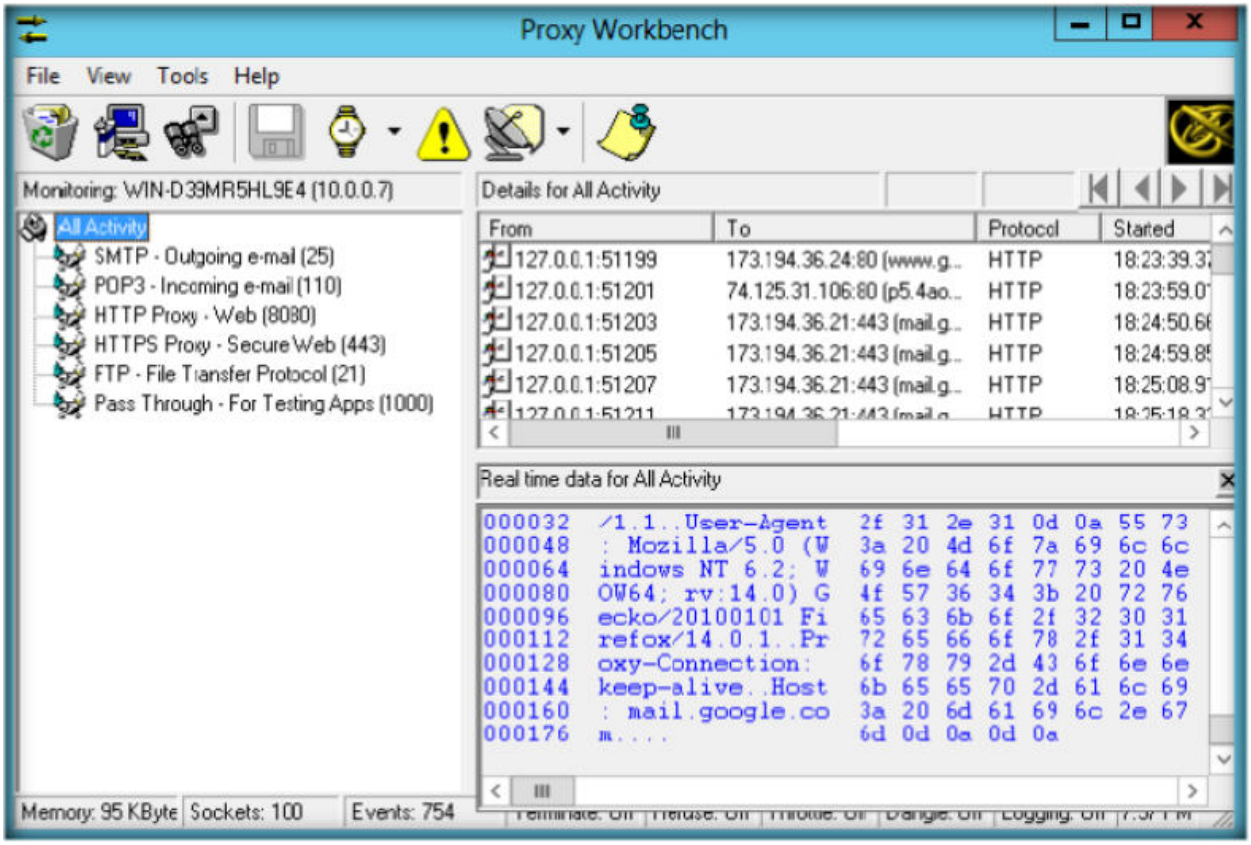


РИСУНОК 13.6: Главное окно Proxy Workbench

14. Перейдите к «Tools» на панели инструментов и выберите «Configure Ports».

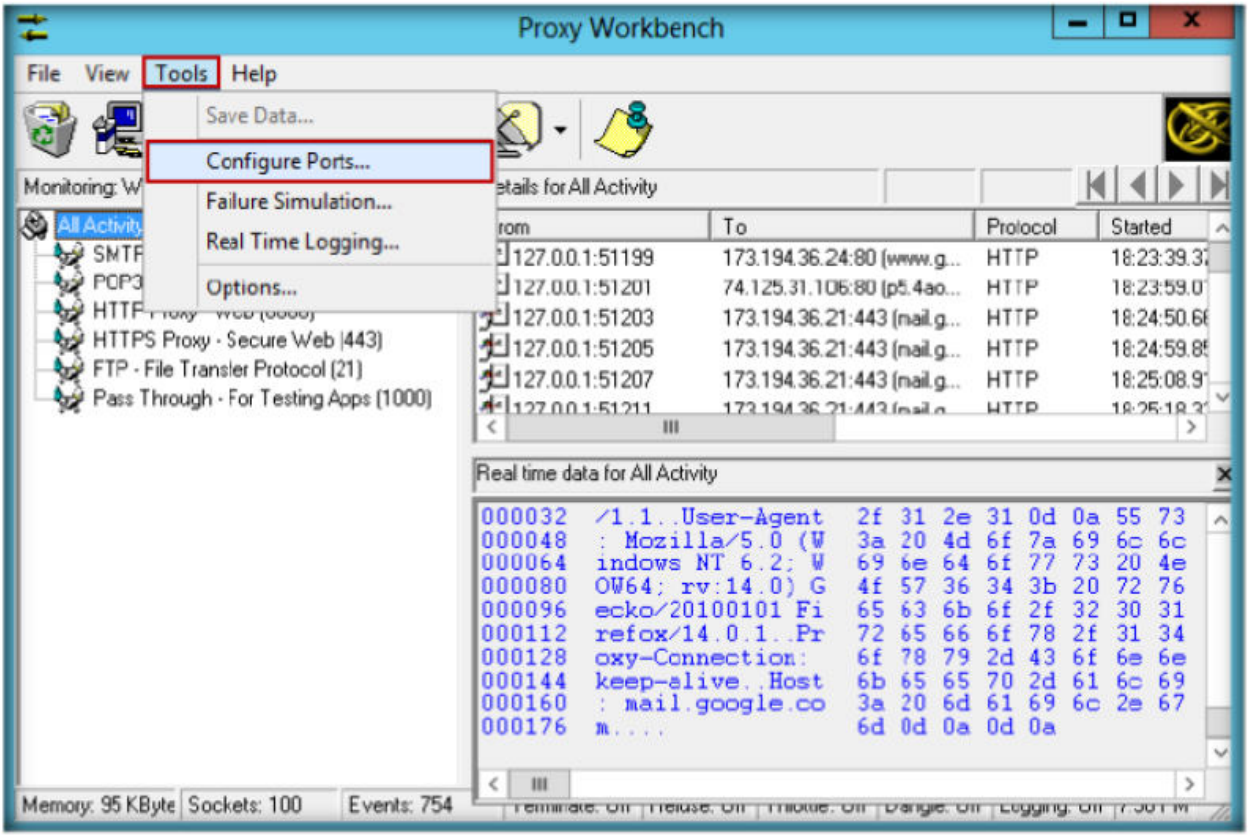


РИСУНОК 13.7: Опция «Configure Ports»

15. В мастере конфигурации Proxy Workbench выберите 8080 HTTP Proxy - сеть на левой панели портов.
16. Выберите HTTP в правой области протокола, присвоенного портировать 8080 и нажмите «Configure HTTP for port 8080».

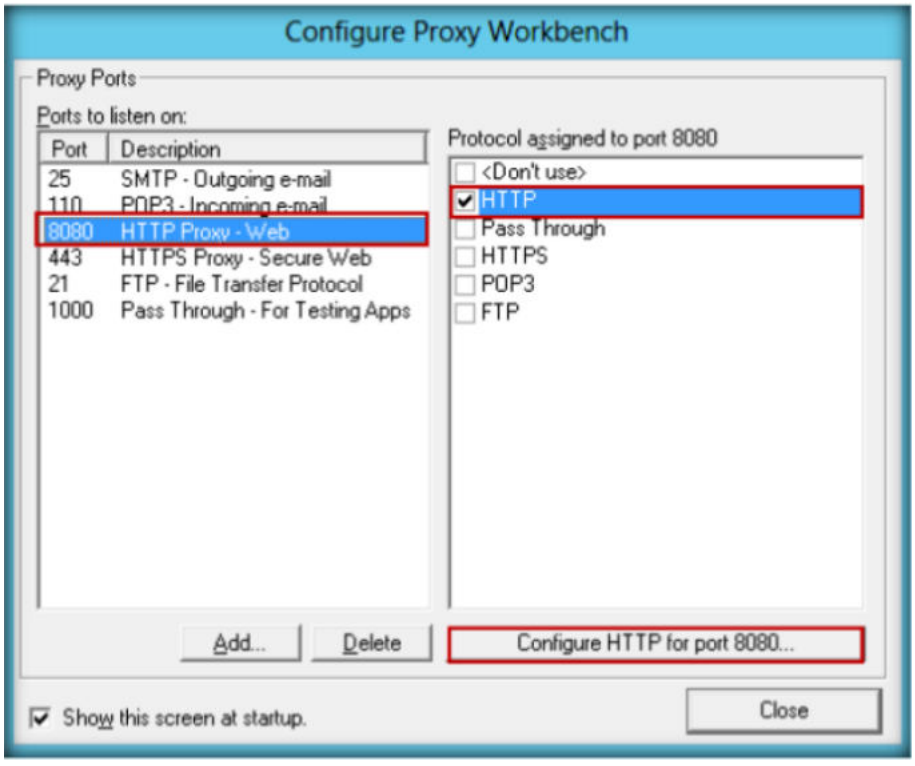


РИСУНОК 13.8: HTTP для порта 8080 в Proxy Workbench

17. Появится окно свойств HTTP. Теперь проверьте подключение через другой прокси, введите свой IP-адрес виртуальной машины Windows Server 2003 в прокси-сервер, введите 8080 в порту и затем нажмите "OK".

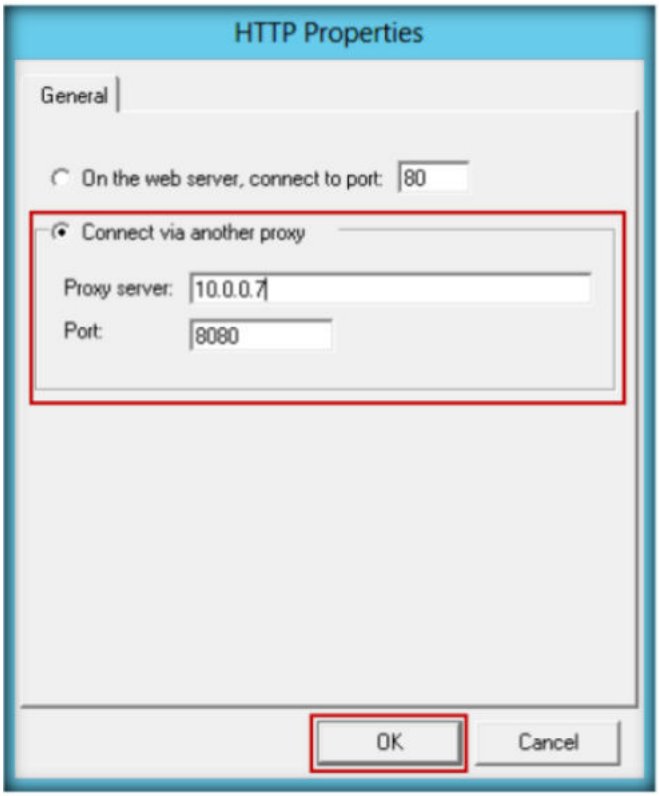


РИСУНОК 13.9: HTTP для порта 8080 в Proxy Workbench

18. Нажмите «Close» в мастере конфигурации Proxy Workbench после завершения настройки параметров конфигурации.

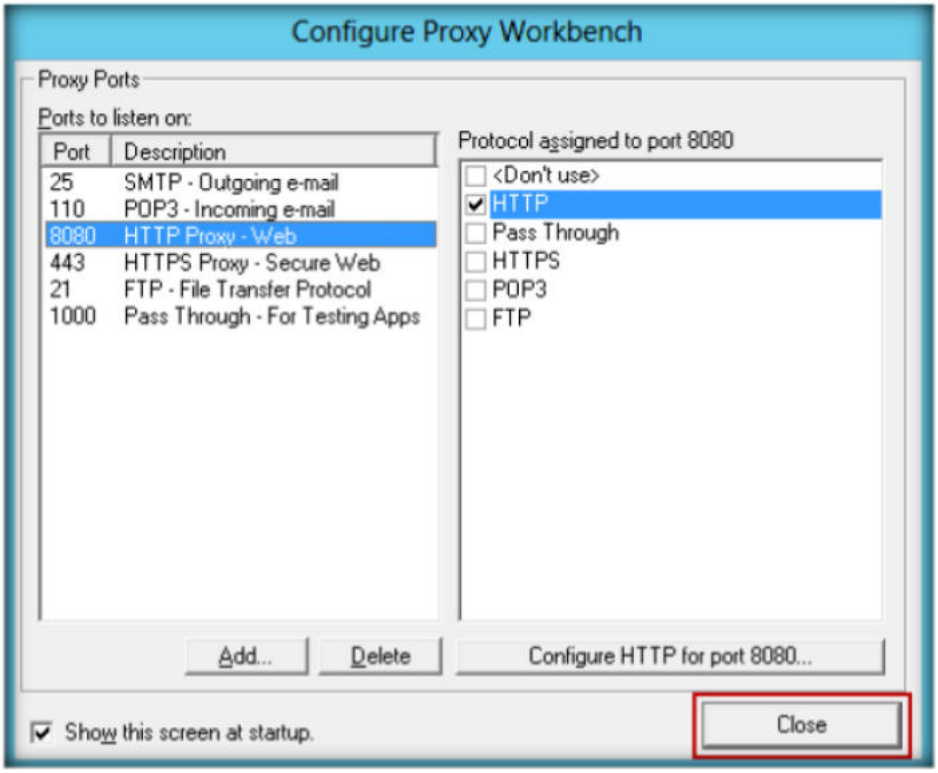


РИСУНОК 13.10: Сконфигурированный прокси Proxy Workbench

19. Повторите шаги конфигурации Proxy Workbench от шага 11 до шага 15 в виртуальных машинах Windows Server 2008.
20. В типе Windows Server 2008 года IP-адрес виртуальной машины Windows 7.
21. Откройте браузер Firefox в Windows Server 2008 и просмотрите веб-страницы.
22. Proxy Workbench генерируют трафик. Он будет сгенерирован как показано в Windows Server 2008
23. Проверьте «**To**» столбец. Он показывает передачу трафика к 10.0.0.3 (виртуальная машина Windows Server 2008).

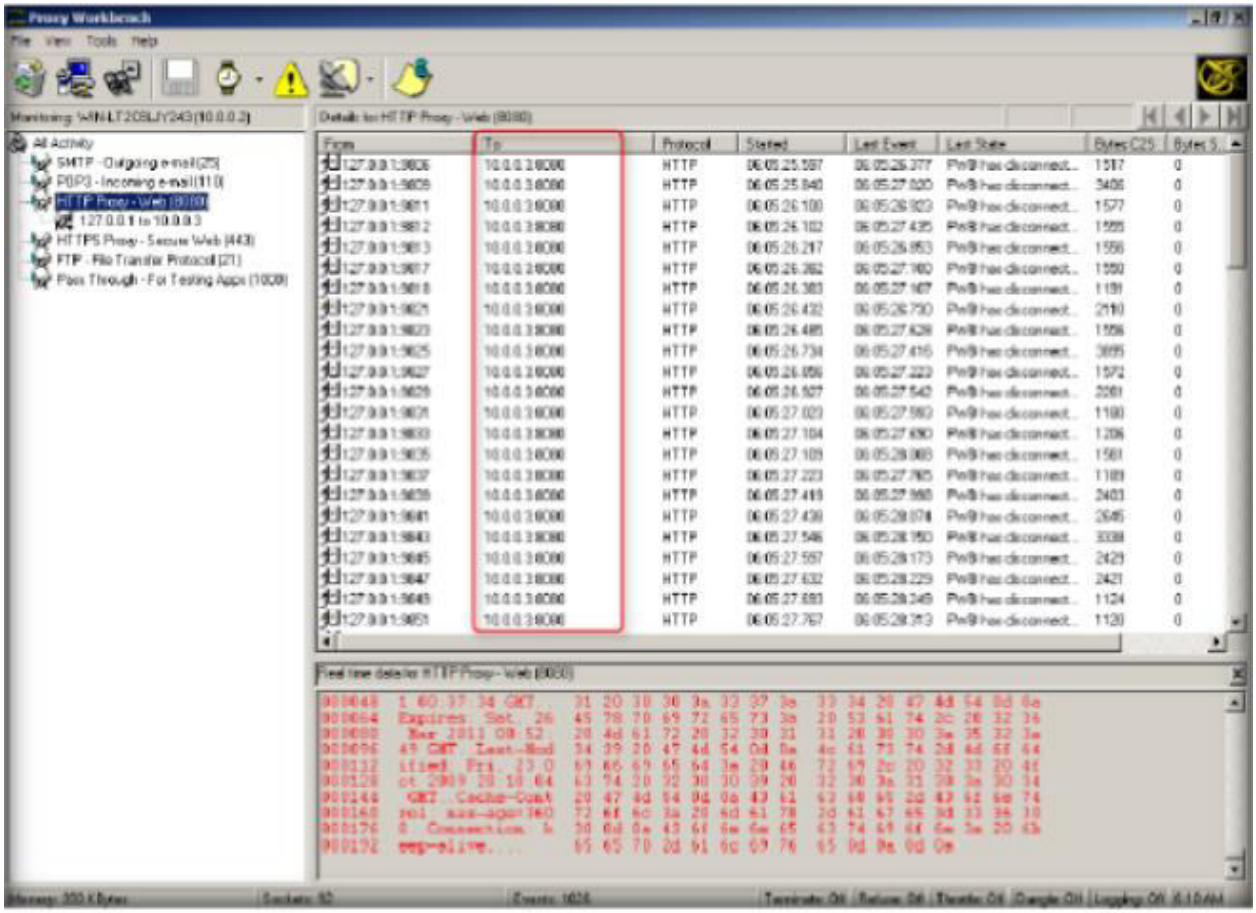


РИСУНОК 13.11: Proxy Workbench генерирует трафик в хост-машине Windows Server 2012

24. Теперь войдите в систему Виртуальной машины Windows Server 2008 и проверьте столбец «**To**». Он показывает передачу трафика к 10.0.0.7 (Виртуальная машина Windows 7).

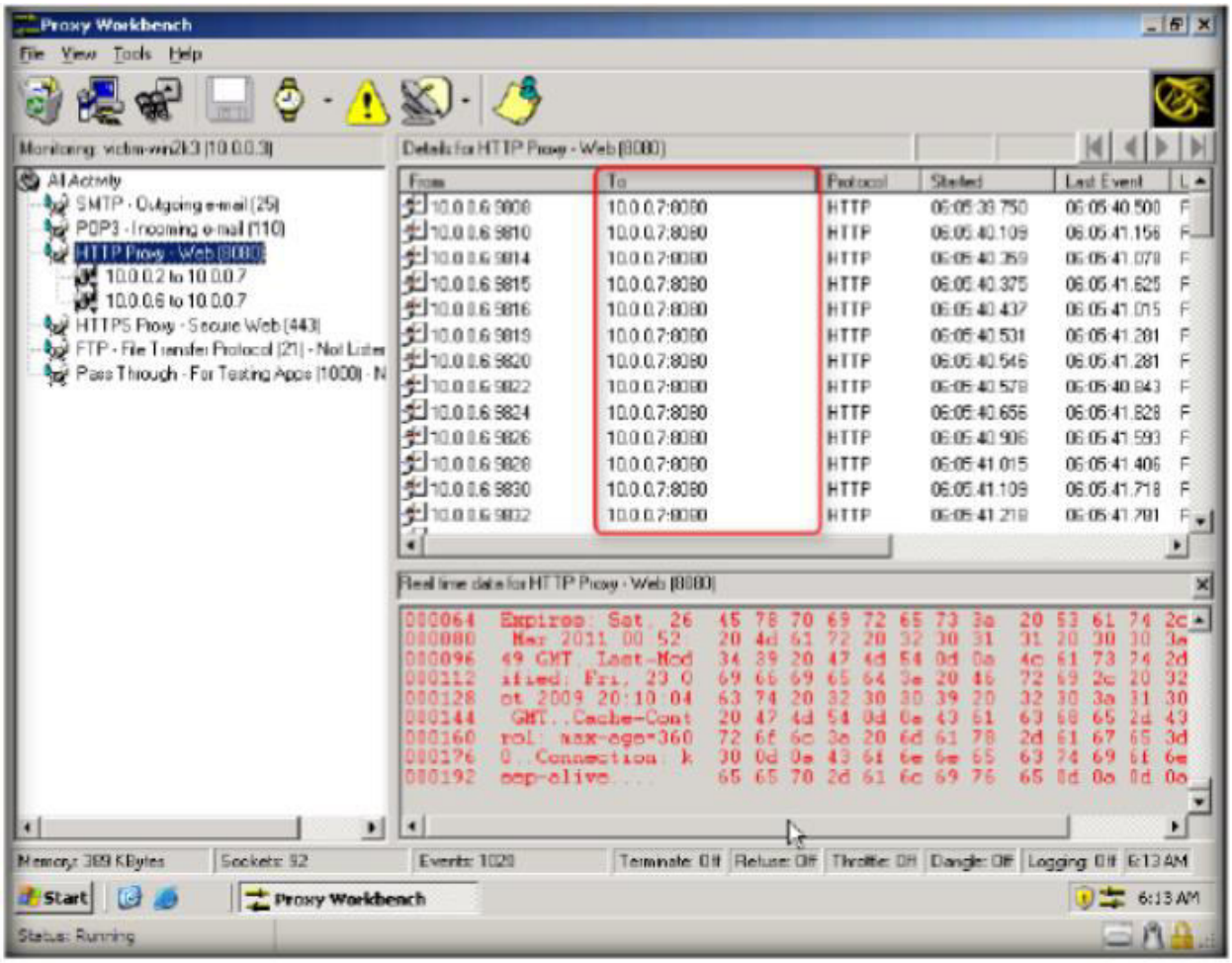


РИСУНОК 13.12 Proxy Workbench генерирует трафик в виртуальной машине Windows Server 2003

25. Выберите «Select On the web server, connect to port 80» в виртуальной машине Windows 7 и нажмите "OK".

РИСУНОК 13.13: Свойства конфигурирования HTTP в Windows 7

26. Теперь проверим трафик в 10.0.0.7 (Виртуальная машина Windows 7). Столбец “**TO**” показывает трафик, генерируемый от различных веб-сайтов, просмотренных в Windows Server 2008.

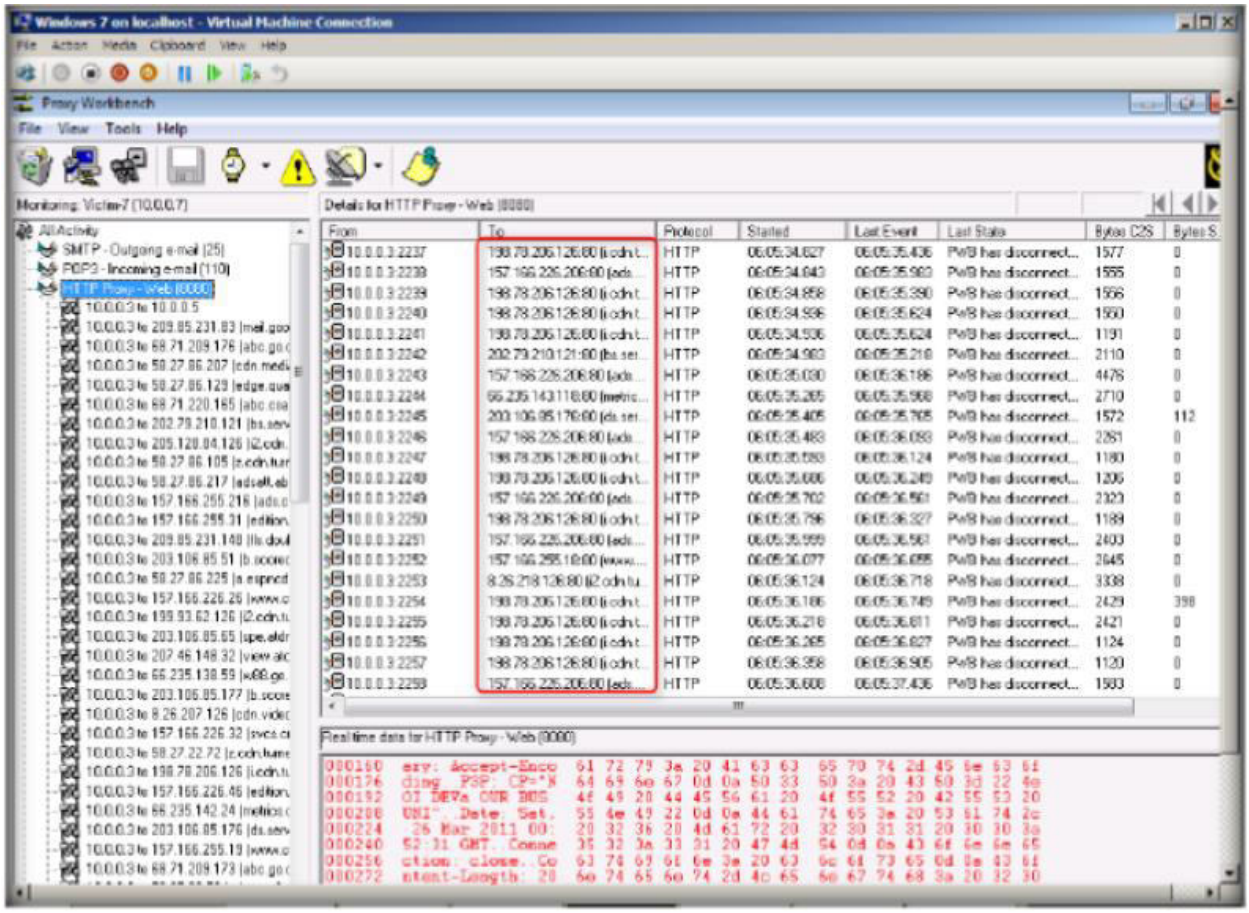


РИСУНОК 13.14: Proxy Workbench генерирует трафик в виртуальной машине Windows 7

Анализ практической работы

Запишите все IP-адреса, порты, приложения запуска и протоколы, которые Вы обнаружили во время выполнения практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
Proxy Workbench	**Используемый прокси-сервер:** 10.0.0.7
	Отсканированный порт: 8080
	Результат: Трафик, полученный в виртуальных машинах windows 7 (10.0.0.7)

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы

1. Исследуйте завершение отказа, соединения и отказ.
2. Как запись в журнал в реальном времени записывает все в Proxy Workbench?

Практическое занятие №14. Туннелирование HTTP с помощью HTTPort

Цели работы

Эта Практическое занятие покажет Вам, как могут быть отсканированы сети и как пользоваться HTTPort и HTTHost

Средства лабораторной работы

Для выполнения лабораторной работы Вам нужен инструмент HTTPort: • HTTPort расположен в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort

- Вы можете также загрузить последнюю версию HTTPort по ссылке http://www.targeted.org/
- Если Вы решите загрузить последнюю версию, то снимки экрана, показанные в лабораторной работе могут отличаться от тех, что получите Вы.
- Установите HTTHost на виртуальную машину Windows Server 2008
- Установите HTTPort на хост-машину Windows Server 2012
- Выполните шаги мастера установки и установите его.
- Требуются административные привилегии чтобы пользоваться данным инструментом
- Эта Практическое занятие не сможет выполняться, если удаленный сервер фильтрует/блокирует HTTP, туннелирующий пакеты

Краткие теоретические сведения Обзор HTTPort

HTTPort создает прозрачный туннель через прокси-сервер или брандмауэр. HTTPort позволяет использовать все виды интернет-программного обеспечения из-за прокси. Это обходит прокси HTTP и HTTP, брандмауэры и прозрачные акселераторы

Постановка задачи

1. Прежде чем пользоваться инструментом, Вы должны остановить службы IIS Admin Service и World Wide Web Publishing на виртуальной машине Windows Server 2008
2. Перейдите к «Administrative Privileges» (Административным привилегиям) → «Services» (Службы) → «IIS Admin Service» (Администраторская Служба IIS), щелкните правой кнопкой и щелкните «Stop».

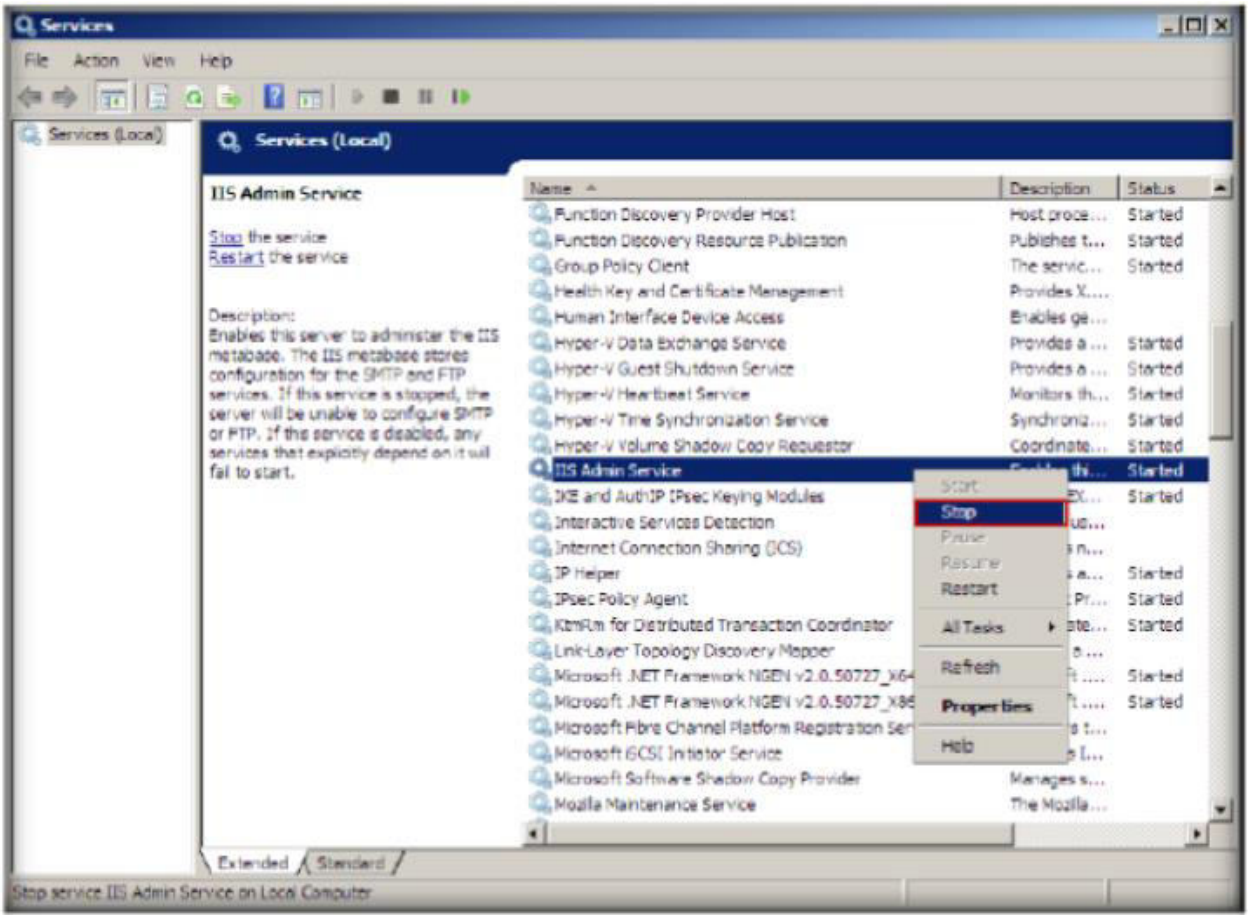


РИСУНОК 14.1: Остановка администраторской службы IIS в Windows Server 2008

3. Перейдите к «Administrative Privileges» (Административным привилегиям) → «Services» (Службы) → «World Wide Web Publishing Services», щелкните правой кнопкой и нажмите по опции «Stop».

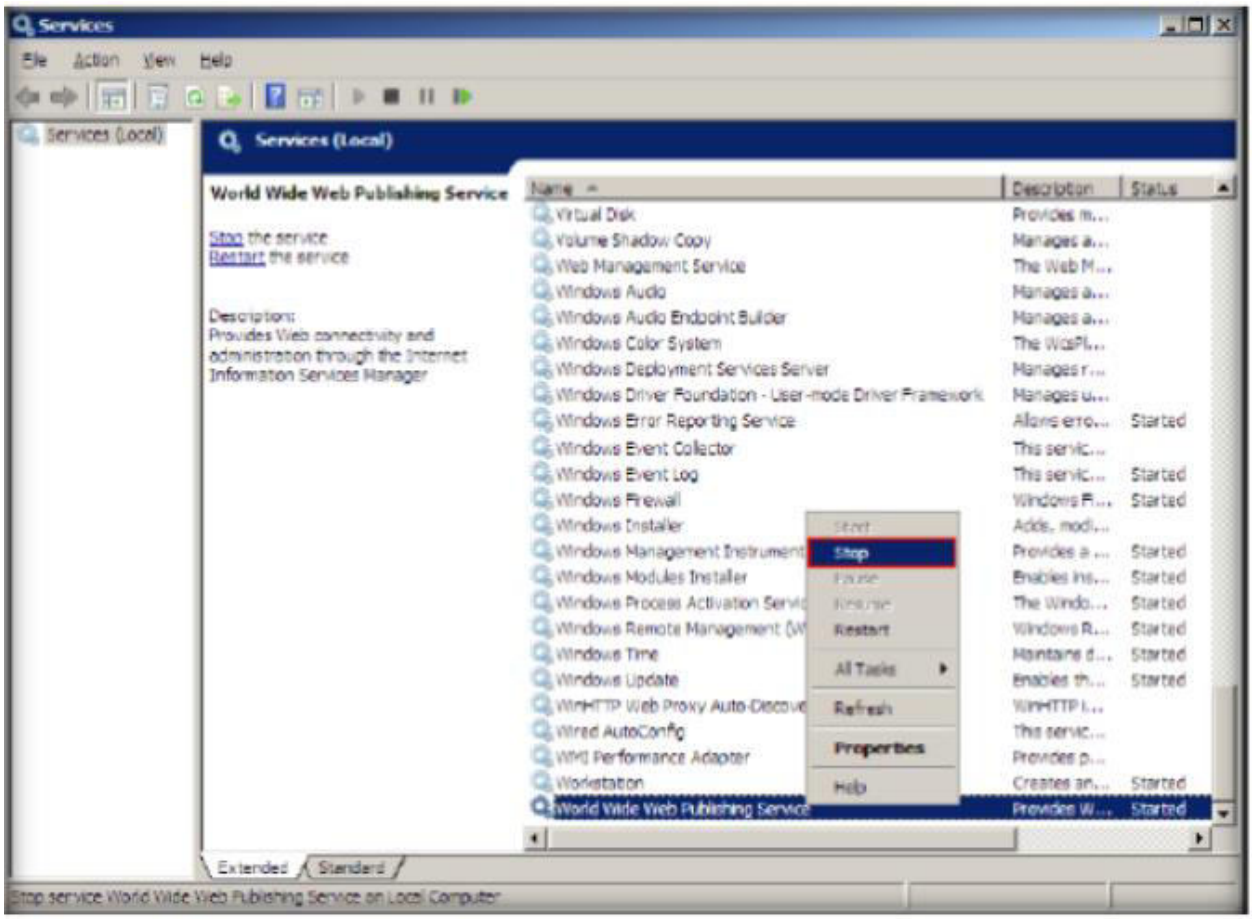


РИСУНОК 14.2: Остановка служб всемирной паутины в Windows Server 2008

4. Откройте Mapped Network Drive “CEH-Tools" Z:\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTHost.
5. Откройте папку HTTHost и дважды щелкните **htthost.exe.**
6. Откроется мастер HTTHost. Выберите вкладку «Options».
7. На вкладке «Options» устанавливаются все параметры настройки, чтобы принять значение по умолчанию кроме поля «Personal Password», которое должно быть заполнено любым другим паролем. В этой лабораторной работе персональный пароль “ magic ”.
8. Проверьте «Revalidate DNS names» (Подтверждать имена DNS), опцию «Log Connections» и нажмите «Apply».

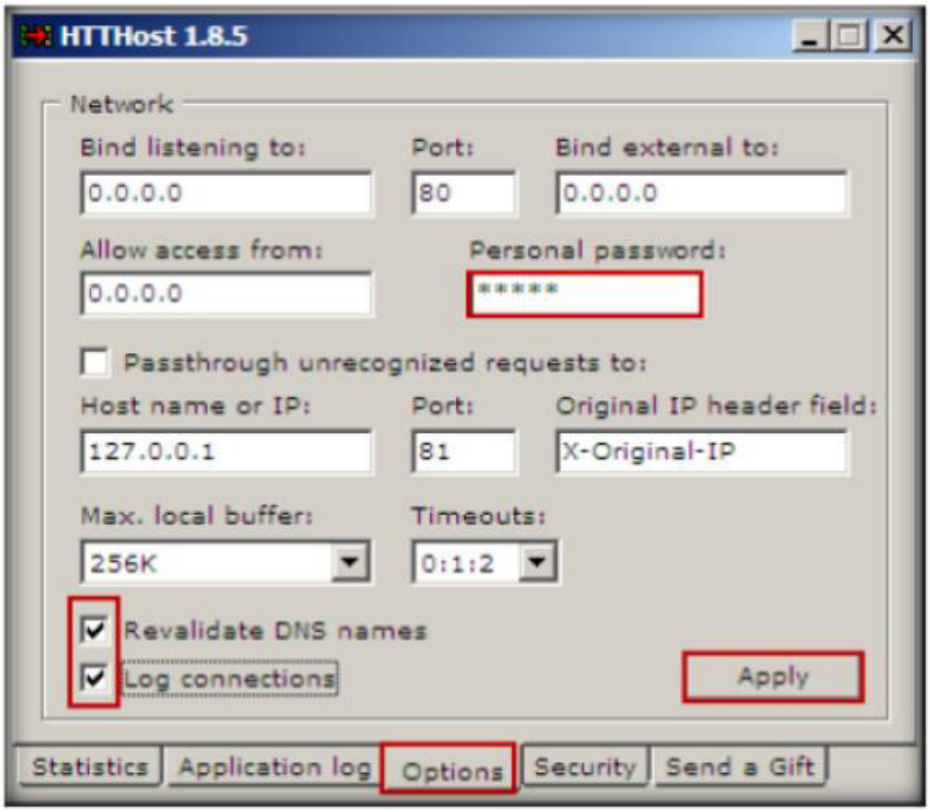


РИСУНОК 14.3: Вкладка «Options» HTTHost

9. Теперь оставьте HTTHost неповрежденным и не выключайте виртуальную машину Windows Server 2008.
10. Переключите Now к хост-машине Windows Server 2012 и установите HTTPort по D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort и двойной щелчок **httport3snfm.exe**
11. Выполните шаги мастера установки.
12. Запустите Меню "Пуск".

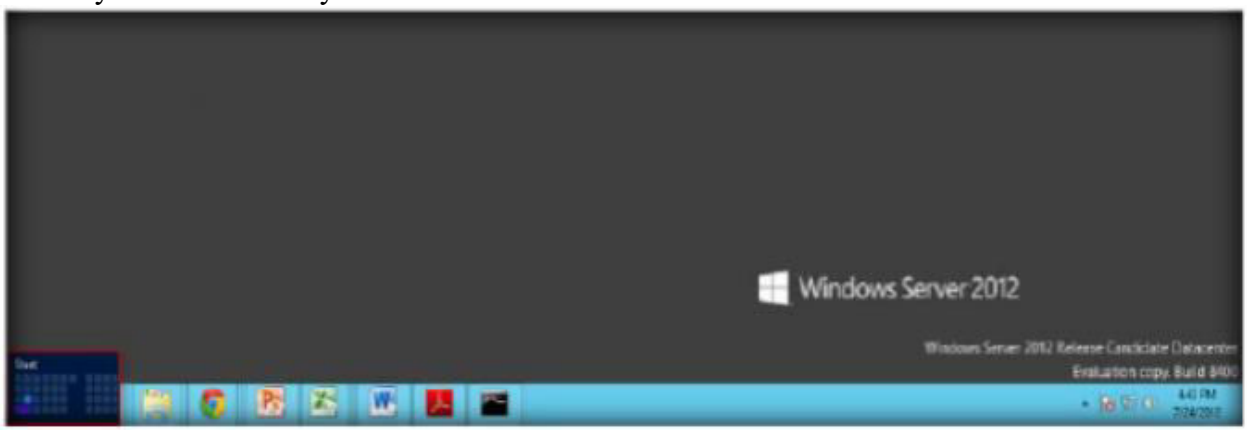


РИСУНОК 14.4: Windows Server 2012 – Рабочий стол

13. Нажмите HTTPort 3.SNFM, чтобы открыть окно HTTPort 3.SNFM.

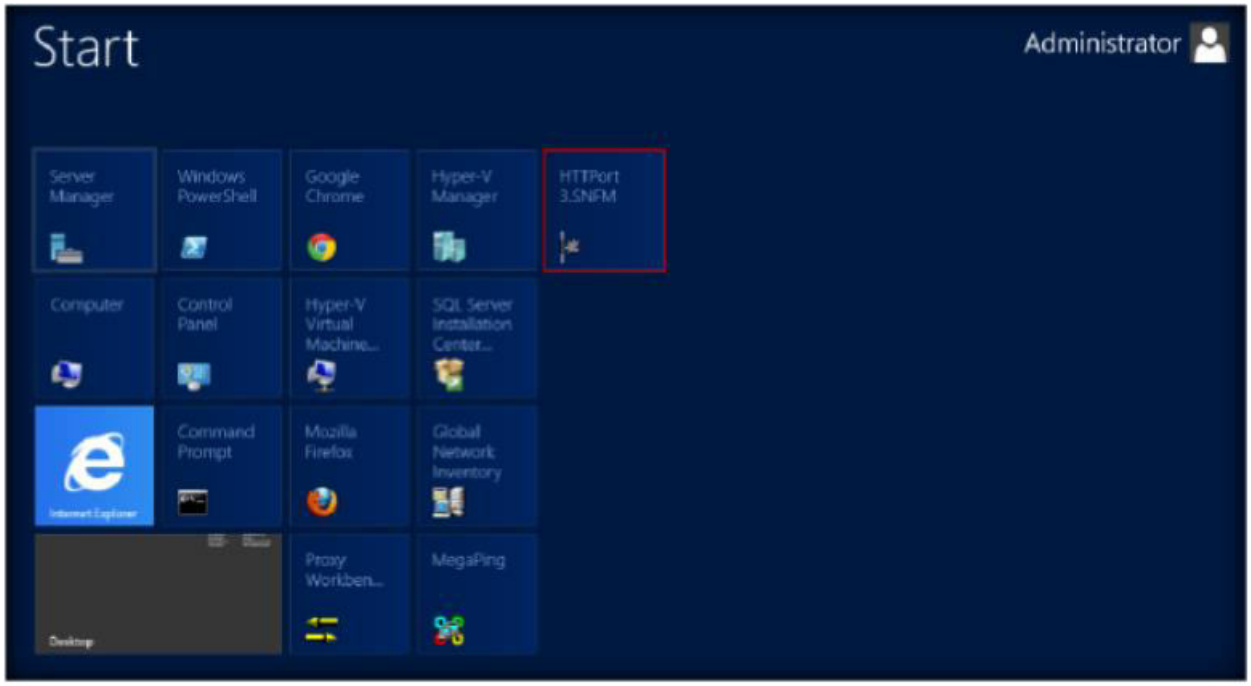


РИСУНОК 14.5: Windows Server 2012 - приложения

14. Появится окно HTTPort 3.SNFM.

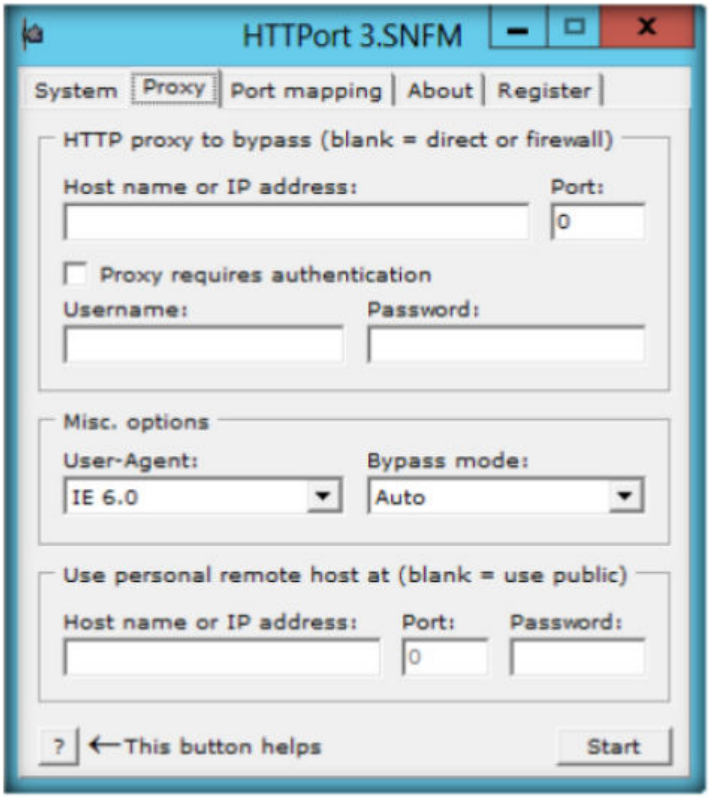


РИСУНОК 14.6: Главное окно HTTPort

15. Выберите вкладку «Proxy» и введите имя хоста или IP-адрес предназначенной машины.
16. Как пример: введите IP-адрес виртуальной машины Windows Server 2008 и введите Номер порта 80.
17. Вы не сможете установить поля Username and Password.
18. В Пользователе в разделе персональный удаленный узел нажмите «start» и затем

остановите и затем вводите предназначенный IP-адрес хост-машины и порт, который должен быть 80.

19. Здесь может использоваться любой пароль. Как пример: введите пароль «magic».

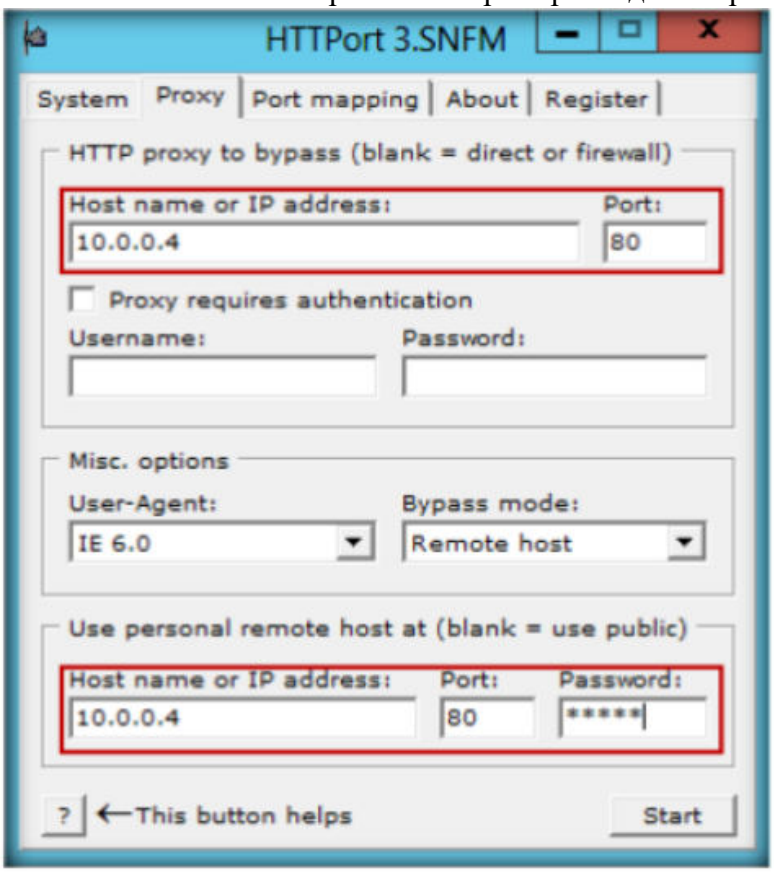


РИСУНОК 14.7: Окно параметров настройки HTTPort Proxy

20. Выберите вкладку «Port Mapping» и нажмите «Add», чтобы создать новое отображение.

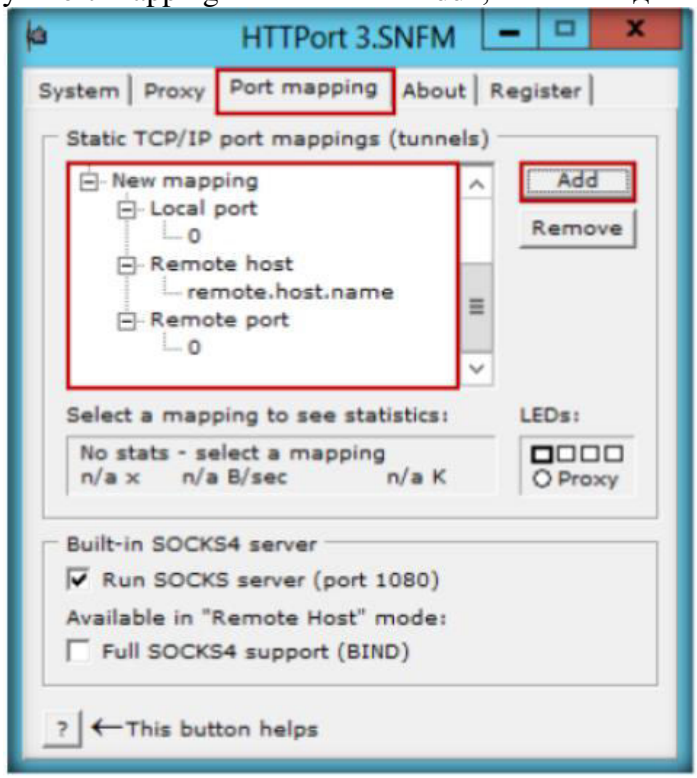


РИСУНОК 14.8: Создание нового отображения HTTPort

21. Выберите «New Mapping Node» и щелкните правой кнопкой по «New Mapping», нажмите «Edit».

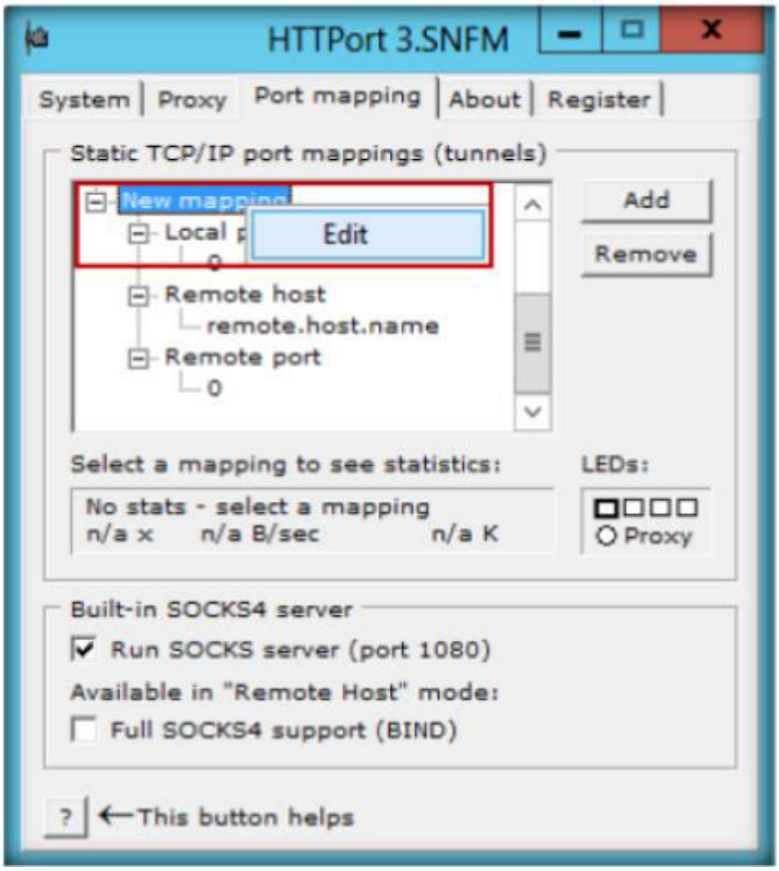


РИСУНОК 14.9: Редактирование HTTPort, чтобы присвоить отображение

22. Переименуйте это как «ftp certified hacker» и выберите узел порта «Local». Щелкните правой кнопкой по «Edit» и введите значение порта 21.
23. Теперь щелкните правой кнопкой по узлу «Remote host», чтобы отредактировать и переименовать его как «ftp.certifiedhacker.com».
24. Теперь щелкните правой кнопкой по узлу «Remote port», чтобы отредактировать и ввести значение порта 21.

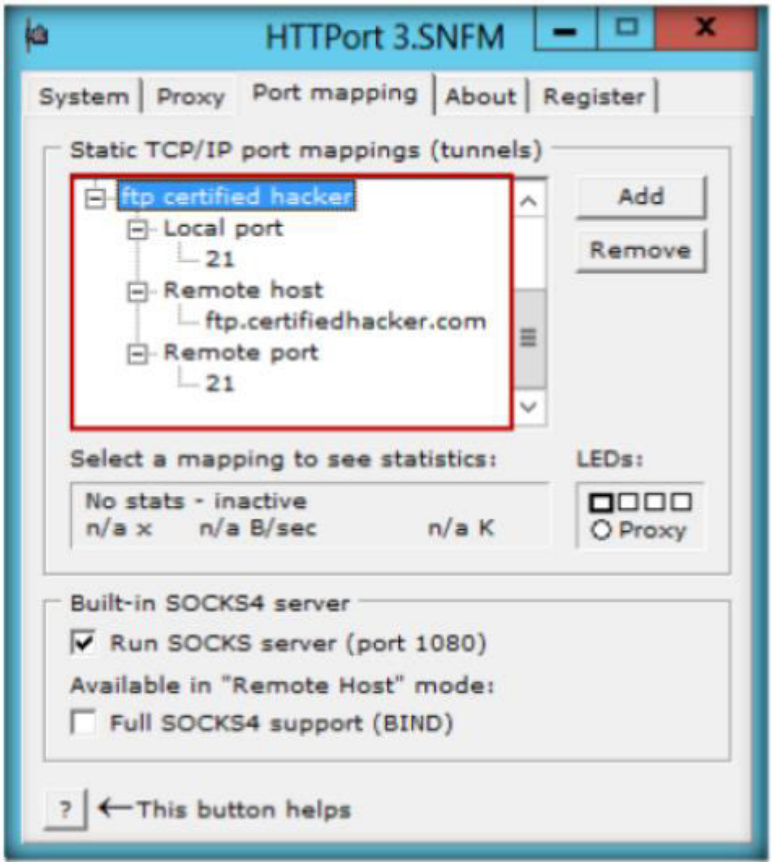


РИСУНОК 14.10: Отображение порта HTTPort Static TCP/IP

25. Нажмите «Start» на вкладке «Proxy» HTTPort, чтобы выполнить туннелирование HTTP.

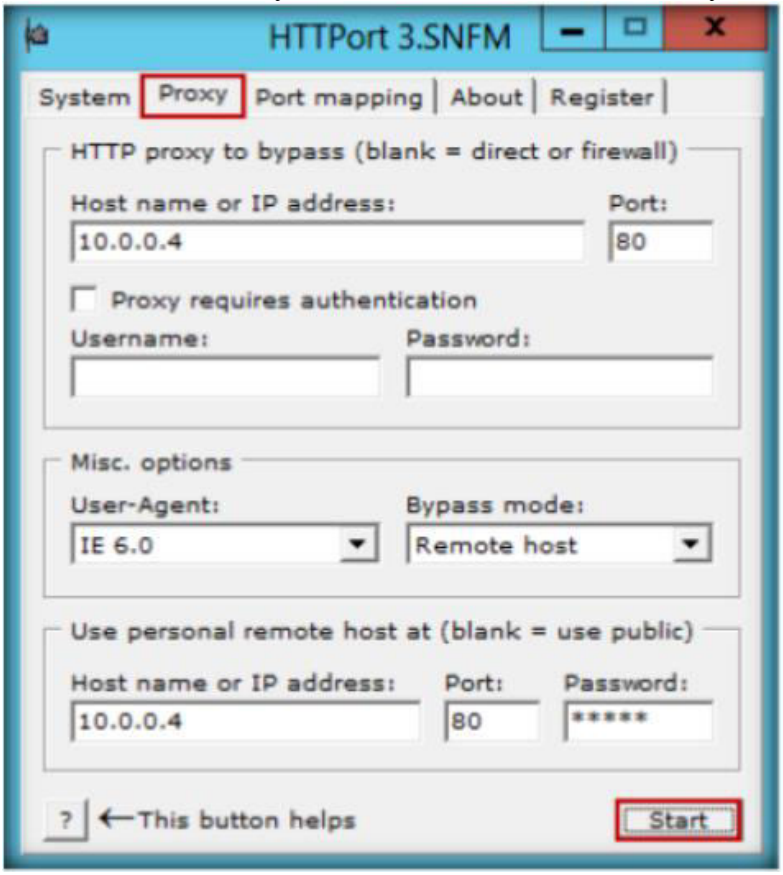


РИСУНОК 14.11: Начало туннелирования

26. Переключите Now виртуальной машины Windows Server 2008 и нажмите «Application log tab».
27. Проверьте последнюю строку если Listener: listening at 0.0.0.0:80. и затем это работает должным образом.

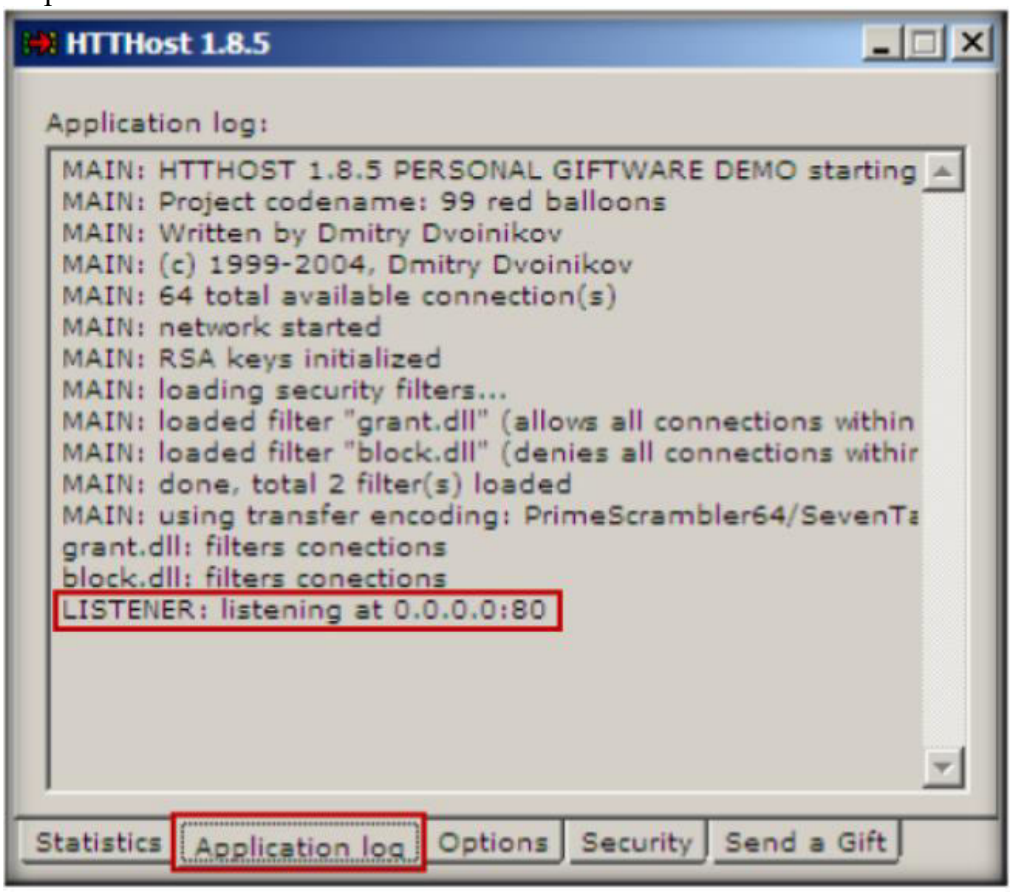


РИСУНОК 14.12 раздел Журнала приложения HTTHost

28. Переключатель Now к хост-машине Windows Server 2012 и включите Брандмауэр Windows.
29. Перейдите к брандмауэру Windows с усовершенствованной безопасностью
30. Выберите «Outbound rules» из левой панели окна и затем нажмите «New Rule» в правой области окна.

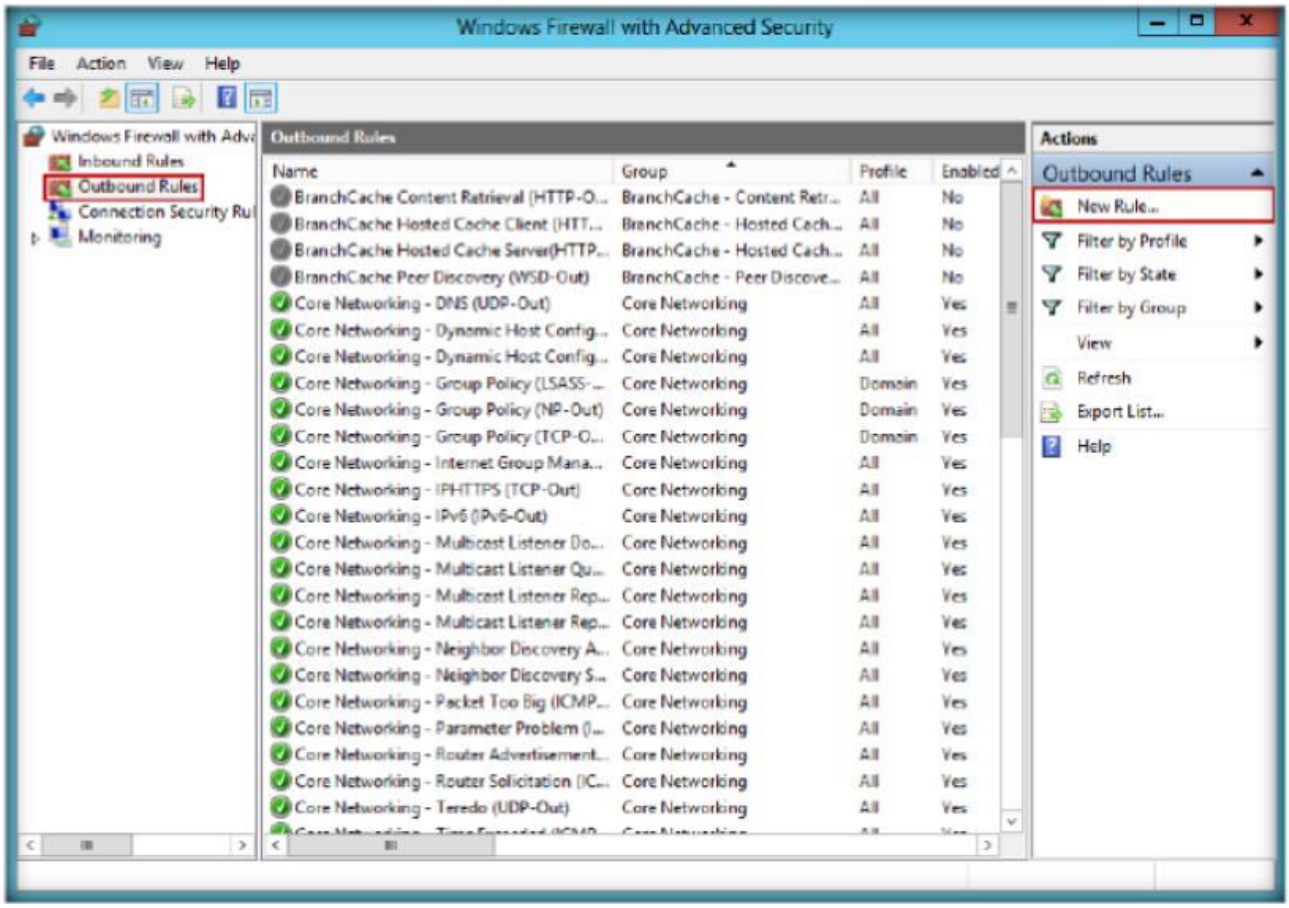


РИСУНОК 14.13: Брандмауэр Windows с окнами Advanced Security в Windows Server 2008

31. В New Outbound Rule Wizard выберите опцию «Port» в разделе «Rule Type» и нажмите Далее.

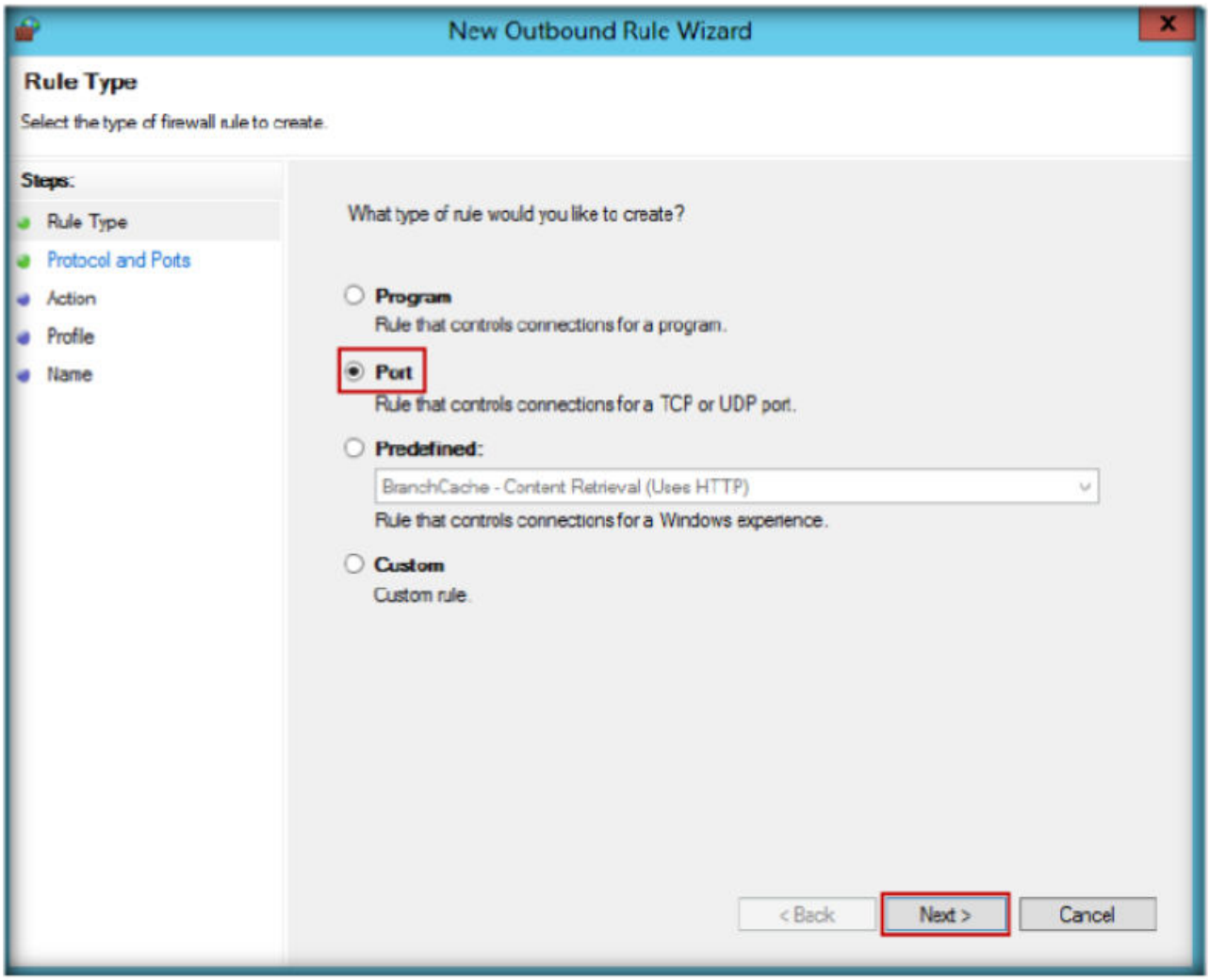


РИСУНОК 14.14: Выбор Rule Type

32. Теперь выберите «All remote ports» в разделе «Protocol и Ports» и нажмите Далее.

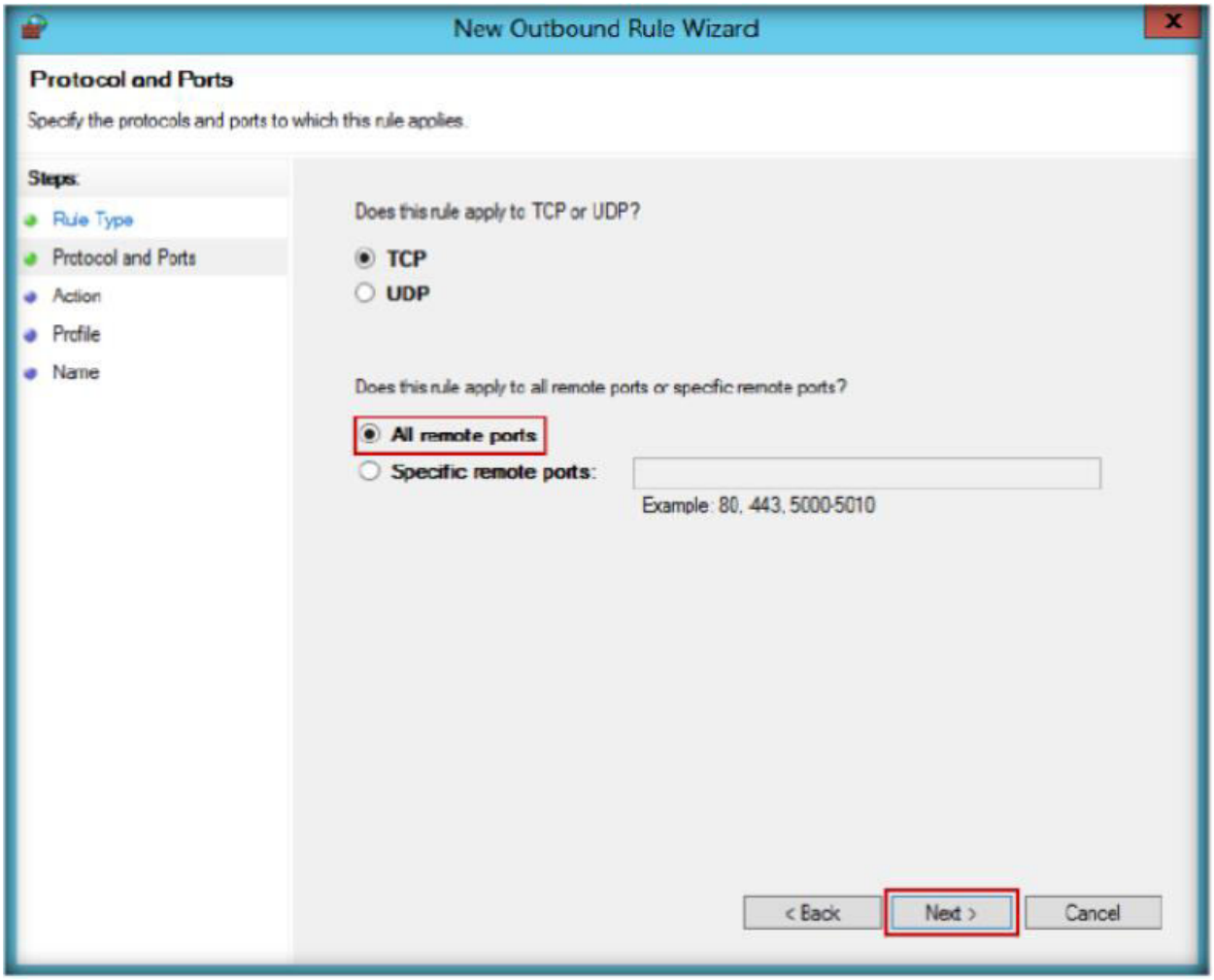


РИСУНОК 14.15: Протоколы присвоения Брандмауэра Windows и Порты

33. В разделе «Action» выберите опцию «Block the connection» и нажмите Далее.

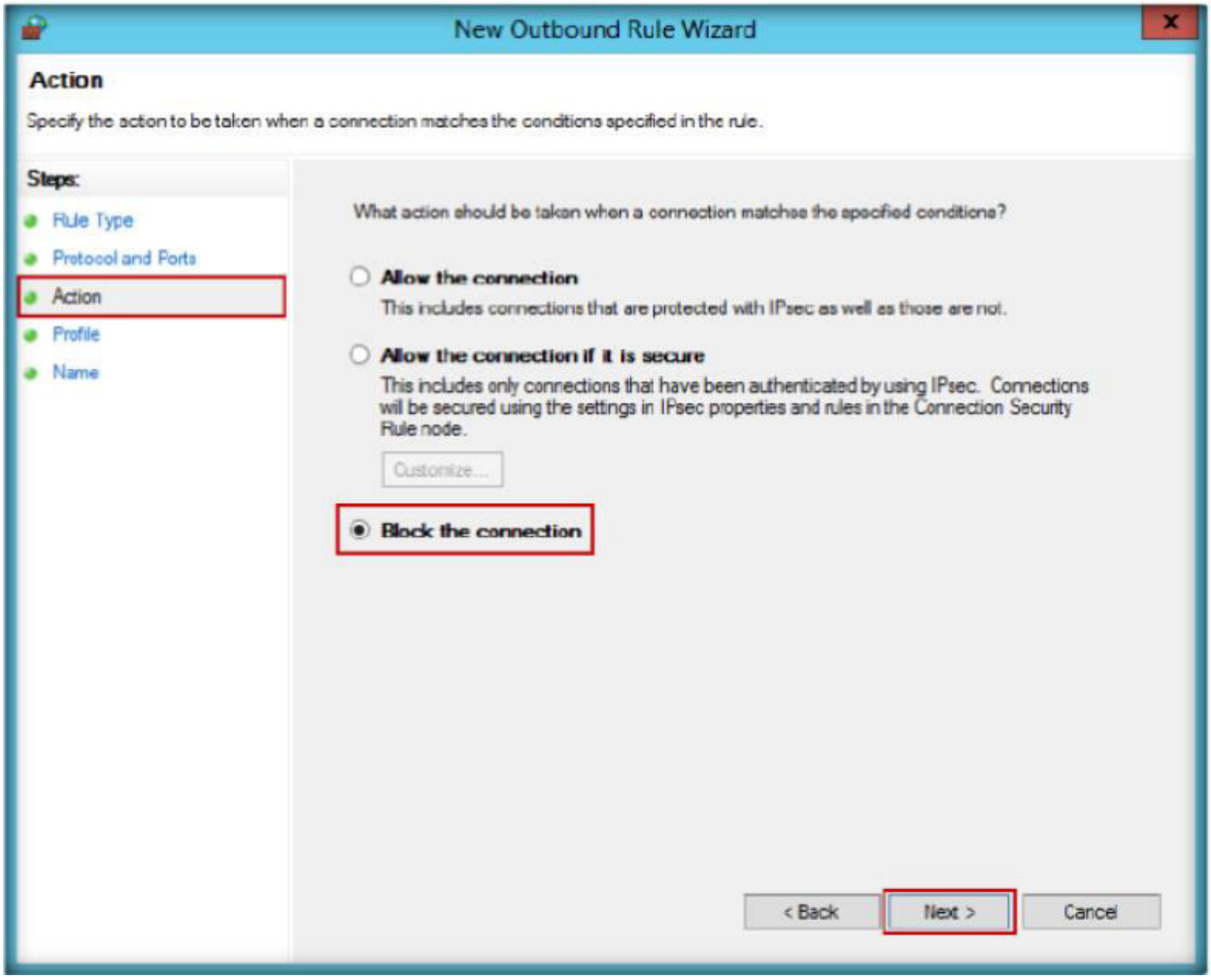


РИСУНОК 14.16: Брандмауэр Windows

34. В разделе «Profile» выберите все три опции и нажмите Далее.

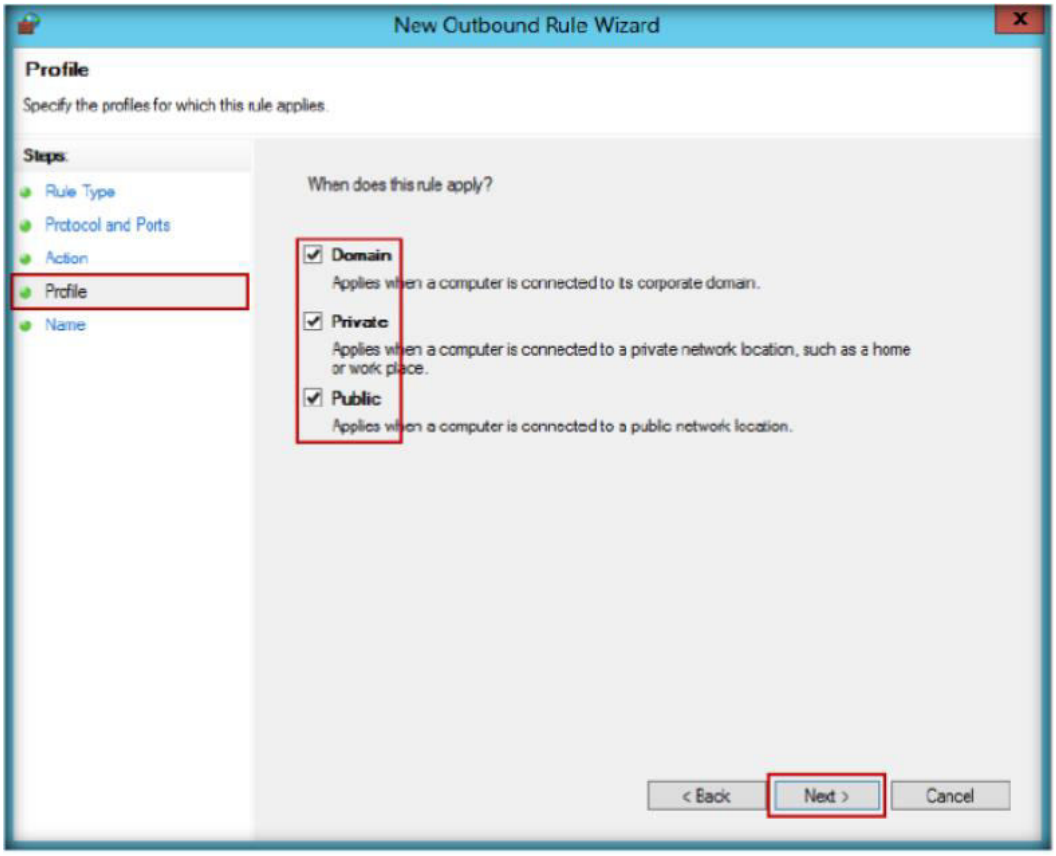


РИСУНОК 14.17: Параметры настройки профиля Брандмауэра Windows

35. Введите «Port 21 Blocked» в поле имени и нажмите кнопку «Finish».

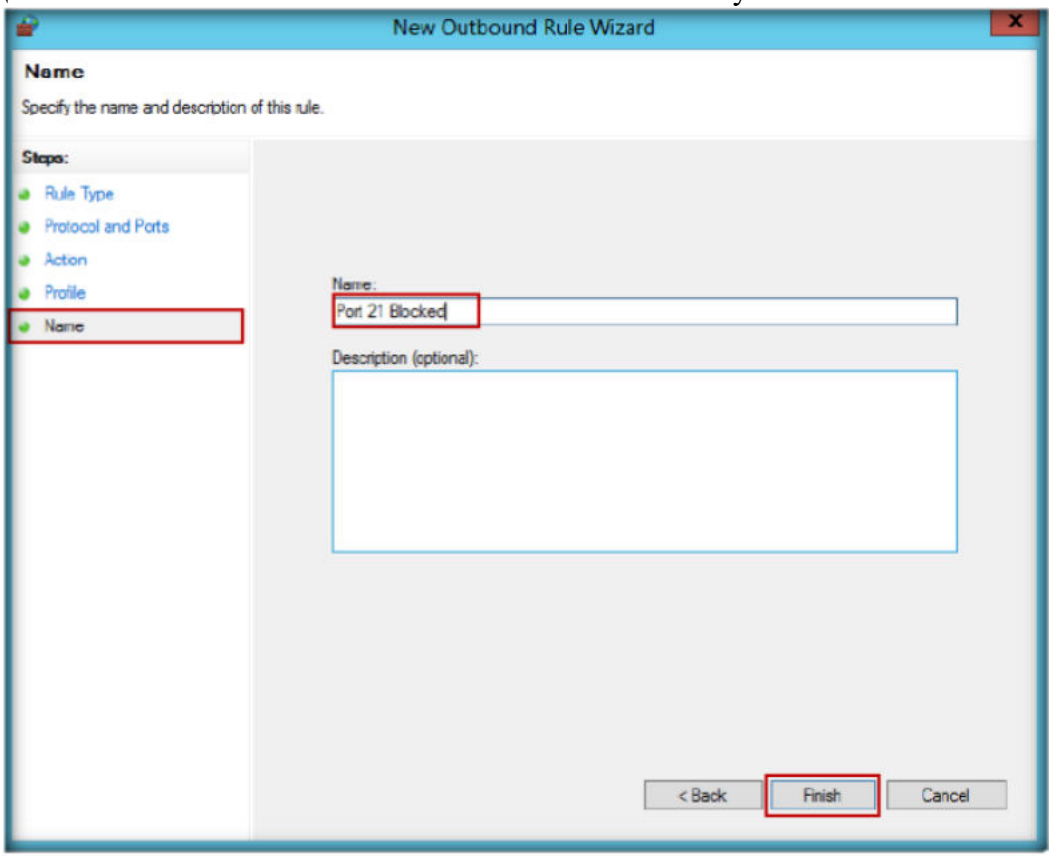


РИСУНОК 14.18: Брандмауэр Windows присваивает имя порту

36. Новое правило «Port 21 Blocked» создается как показано в следующем снимке экрана.

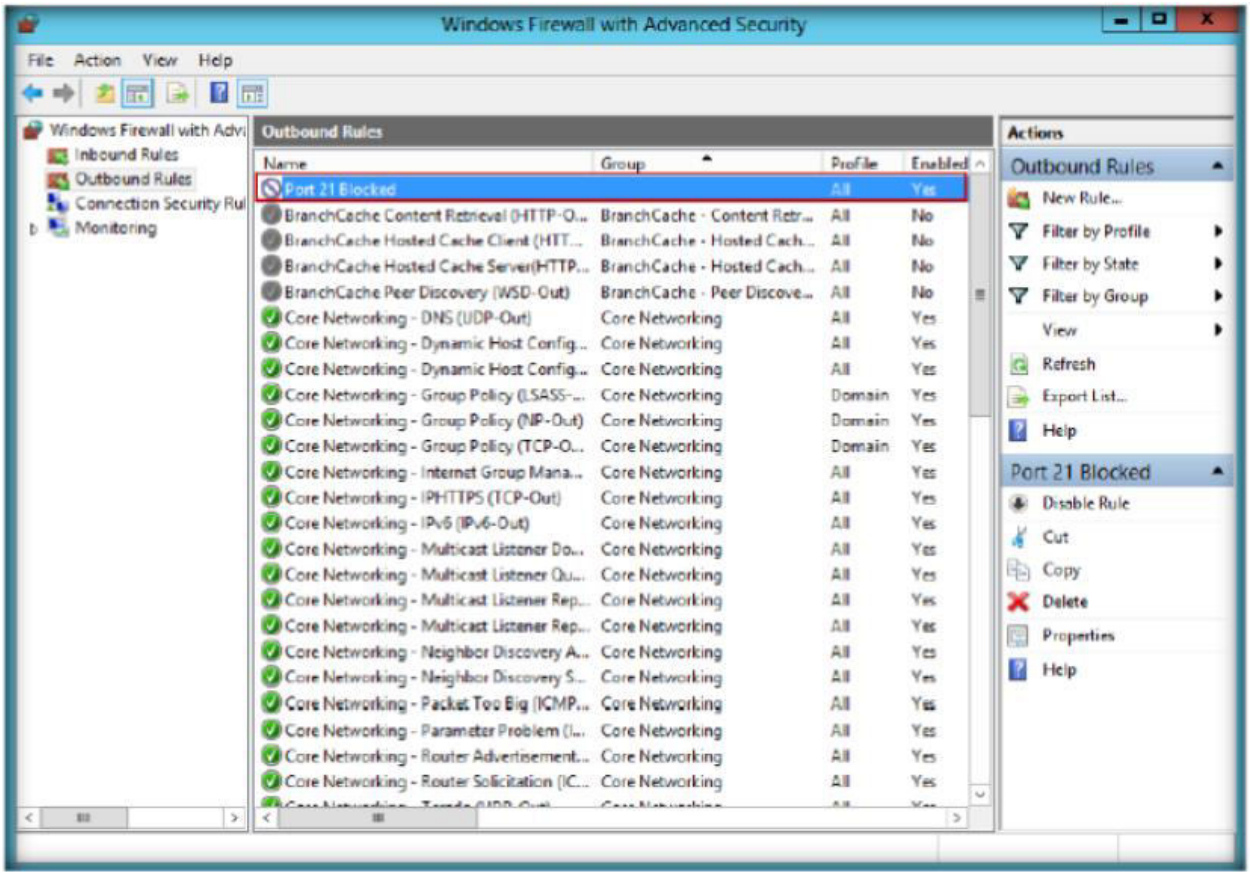


РИСУНОК 14.19: Новое правило брандмауэра Windows

37. Щелкните правой кнопкой по недавно созданному правилу и выберите «Properties».

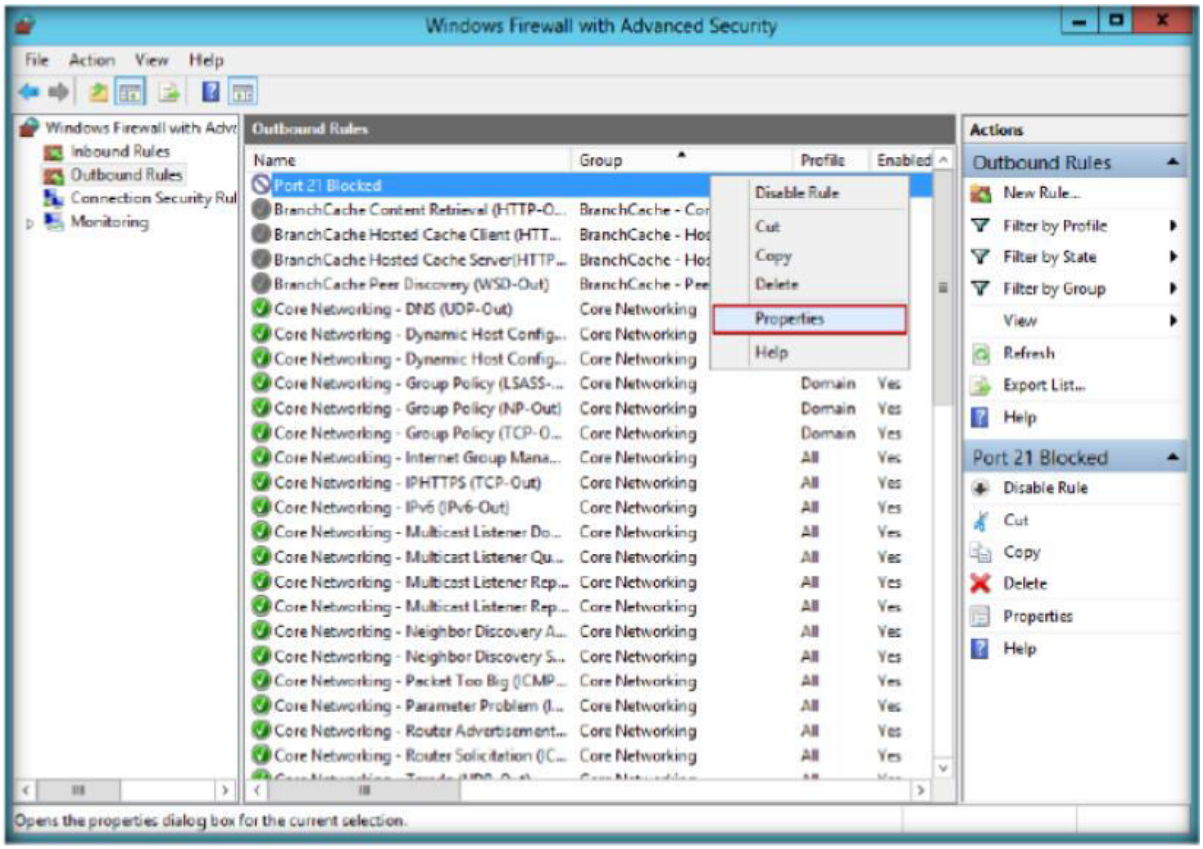


РИСУНОК 14.20: Новые свойства правила врандмауэра Windows

38. Выберите вкладку «Protocols and Ports». Измените опцию «Remote Por»t на «Specific Ports» (определенные порты) и введите в «Port number» 21.
39. Оставьте другие параметры настройки по умолчанию и нажмите «Apply», когда нажмете "OK".

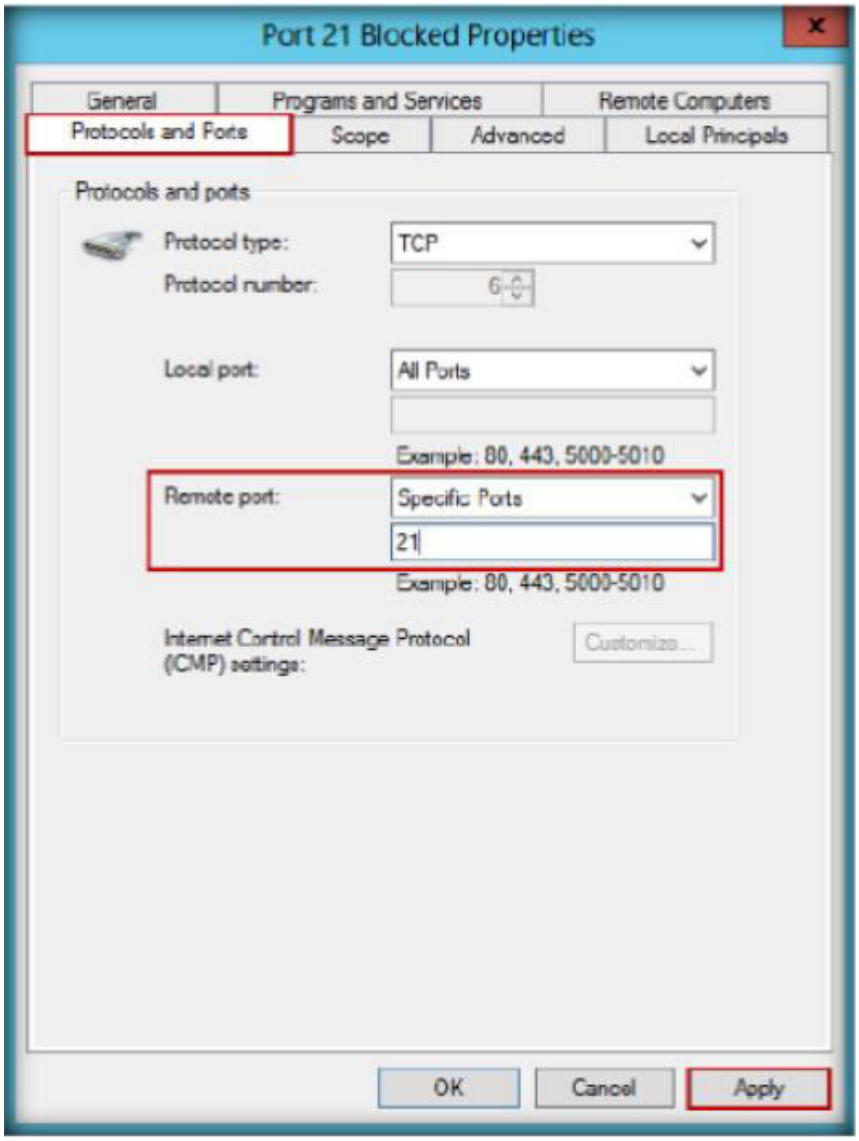


РИСУНОК 14.21: Свойство блокирования порта брандмауэра 21

40. Введите ftp ftp.certifiedhacker.com в командной строке и нажмите Enter. В Windows Server 2008 брандмауэром соединение блокировано.

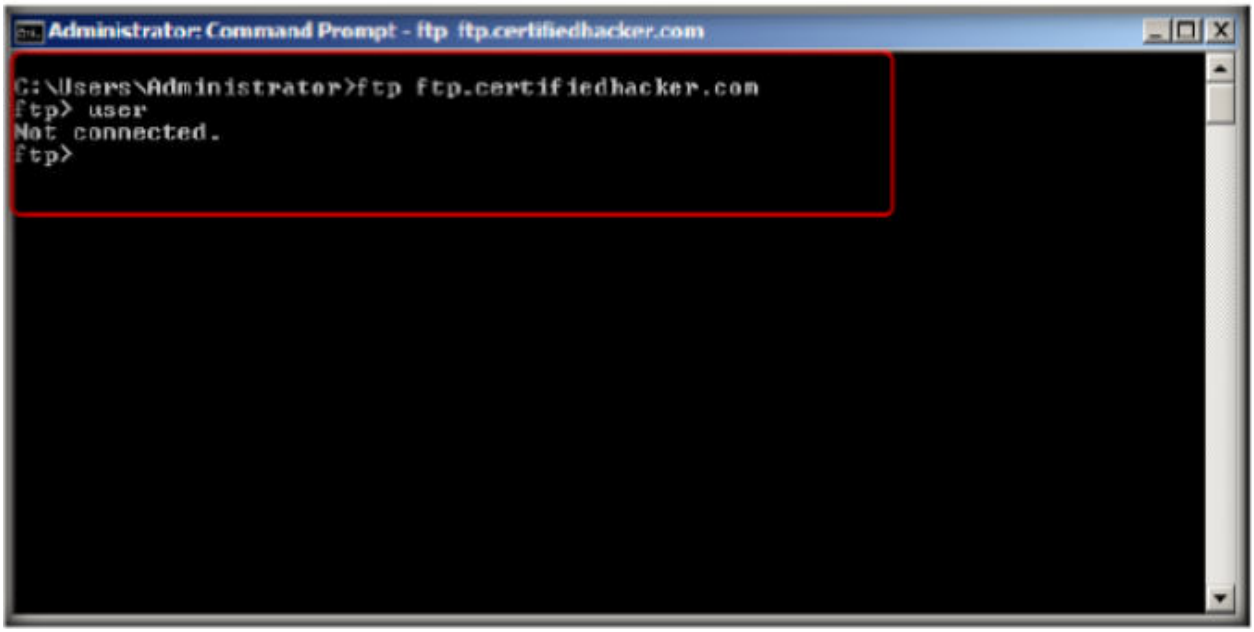


РИСУНОК 14.22: соединение блокировано ftp

41. Теперь откройте командную строку на хост-машине Windows Server 2012 и введите ftp 127.0.0.1 и нажмите Enter.

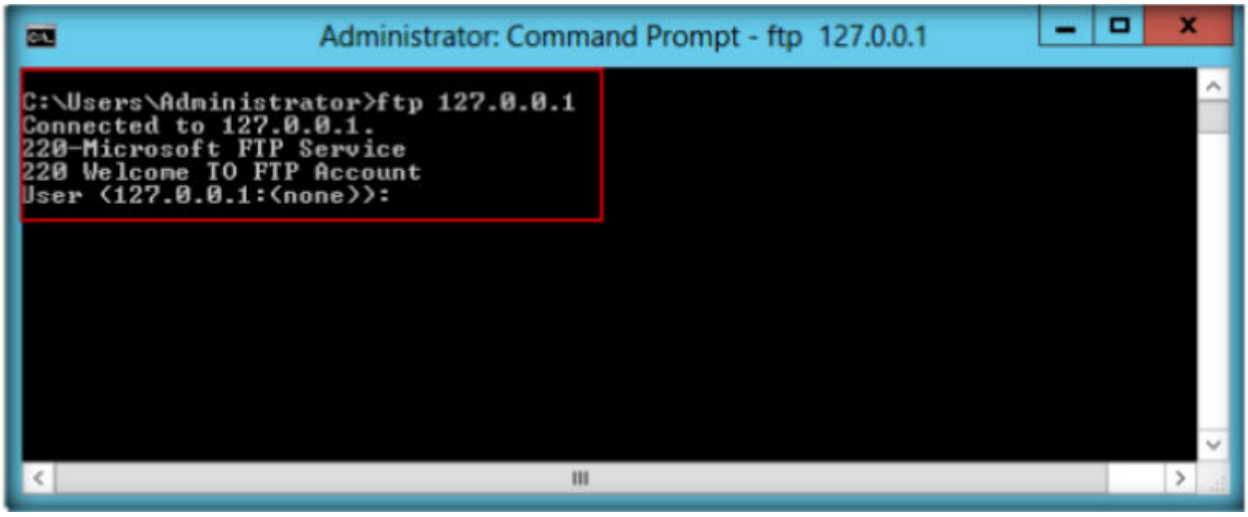


РИСУНОК 14.23: Выполнение команды ftp

Анализ практической работы

Запишите все IP-адреса, откройте порты и приложения запуска и протоколы, которые Вы обнаружили во время выполнения практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
HTTPort	**Используемый прокси-сервер:** 10.0.0.4
	Порт отсканирования: 80
	Результат: ftp 127.0.0.1 соединялся с 127.0.0.1

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы

1. Как Вы устанавливаете HTTPort, чтобы использовать почтовый клиент (Outlook, Messenger, и т.д.)?
2. Когда программное обеспечение не позволяет редактировать адрес, чтобы установить соединение? Исследуйте.

Практическое занятие №15. Основной поиск и устранение неисправностей сети с помощью MegaPing

Цели работы

Эта Практическое занятие дает понимание проверки с помощью ping-назначения списка адресов. Она учит:

- Проверке с помощью ping-запросов списка адресов назначения
- Пользованию Traceroute
- Как выполнить сканирование NetBIOS

Средства лабораторной работы

Чтобы выполнить лабораторную работу, Вам нужно:

- MegaPing расположен в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing
- Вы можете также загрузить последнюю версию Мегаping по ссылке http://www.magnetosoft.com/
- Если Вы решаете загрузить последнюю версию, то снимки экрана, показанные в лабораторной работе могут отличаться от тех, что получите Вы.
- Административные привилегии для пользования инструментами
- Правильно сконфигурированные параметры настройки TCP/IP и доступный сервер DNS
- Эта Практическое занятие будет выполняться в среде лаборатории CEH, на Windows Server 2012, Windows 2008 и Windows 7

Краткие теоретические сведения Обзор Ping

Команда ping отправляет пакеты эхо-запроса Internet Control Message Protocol (Протокола межсетевых управляющих сообщений) (ICMP) в целевой узел и ожидает ответа ICMP. Во время этого процесса запрос-ответ, ping измеряет время от передачи до приема, известного как круговая задержка, и записывает любые потери пакетов.

Постановка задачи

1. Запустите Меню "Пуск".

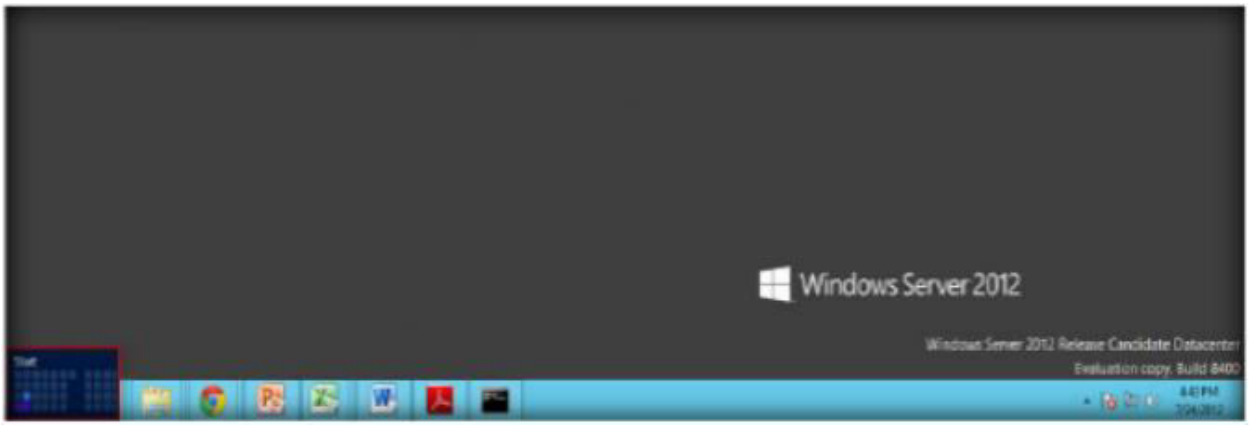


РИСУНОК 15.1: Windows Server 2012 – Рабочий стол

2. Щелкните по приложению MegaPing, чтобы открыть окно MegaPing.

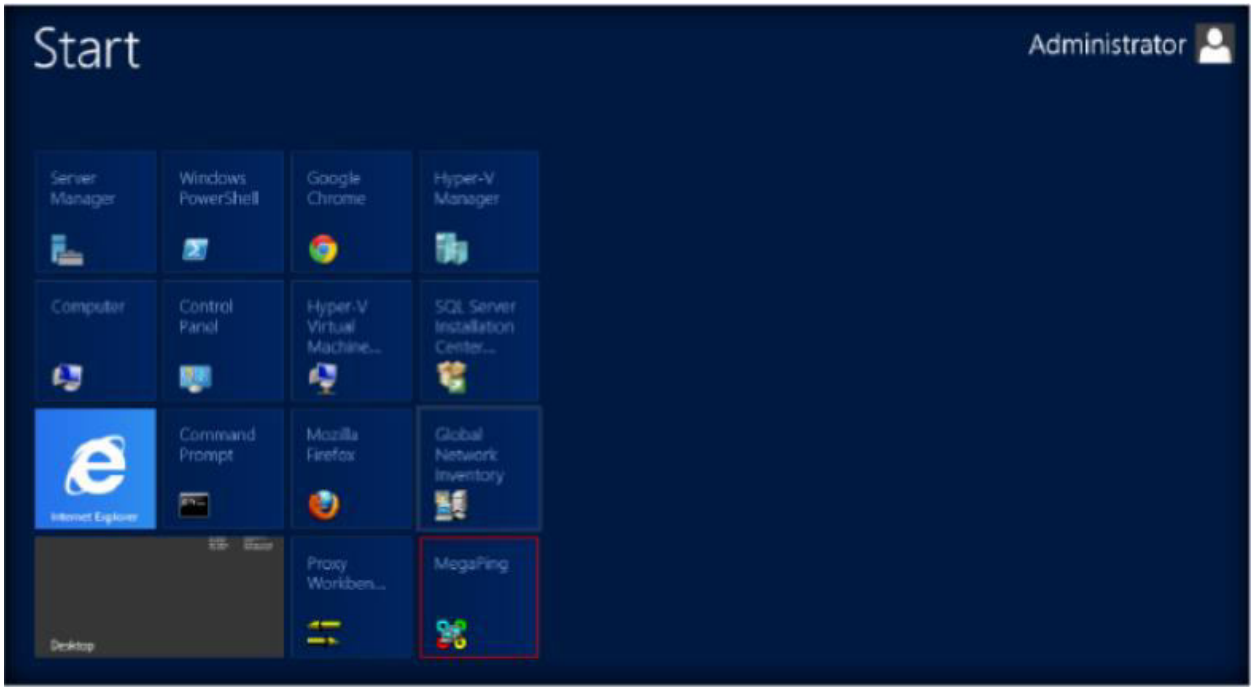


РИСУНОК 15.2: Windows Server 2012 - приложения

3.Откроется главное окно MegaPing.

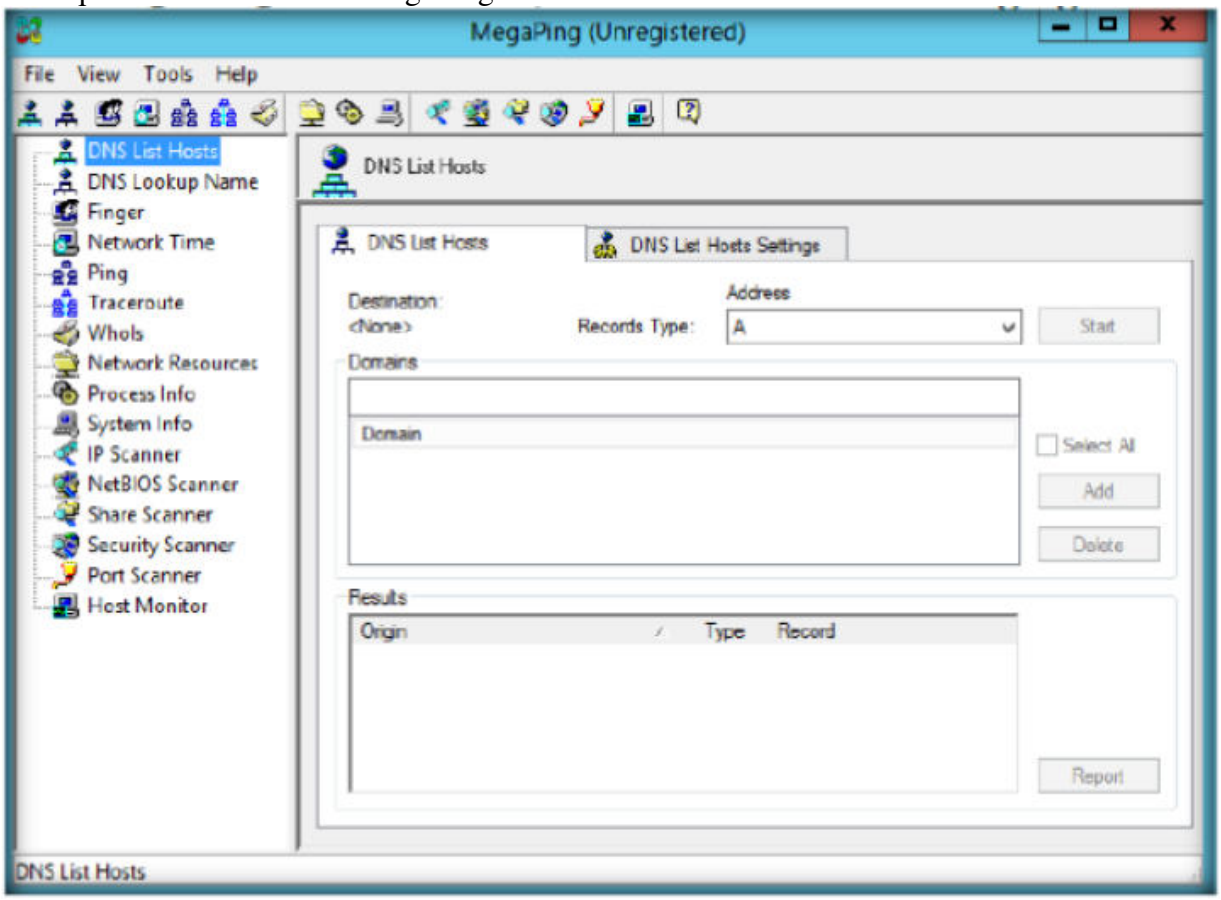


Figure15.3: Главное окно MegaPing

4. Выберите любую из опций она левой панели окна.
5. Выберите «IP scanner» (сканнер IP) и введите в «IP range» в поле «From» и «To»

диапазон IP от 10.0.0.1 до 10.0.0.254. Нажмите " Start ".
6. Вы можете выбрать диапазон IP в зависимости от своей сети.

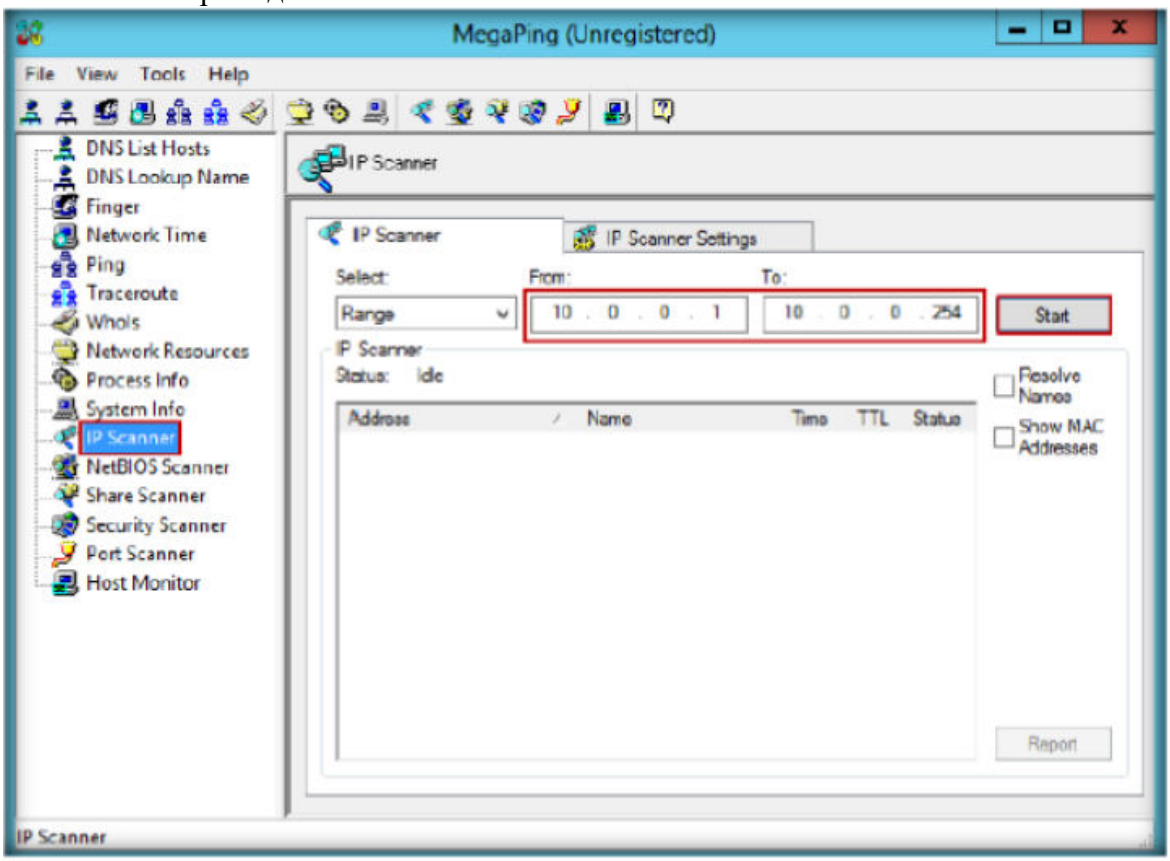


РИСУНОК 15.4: MegaPing

7. Вы получите перечисление всех IP-адресов под выбранным диапазоном с их TTL (Time to Live - Время жизни), Status - состоянием (неактивный или активный), и статистика неактивных и активных узлов.

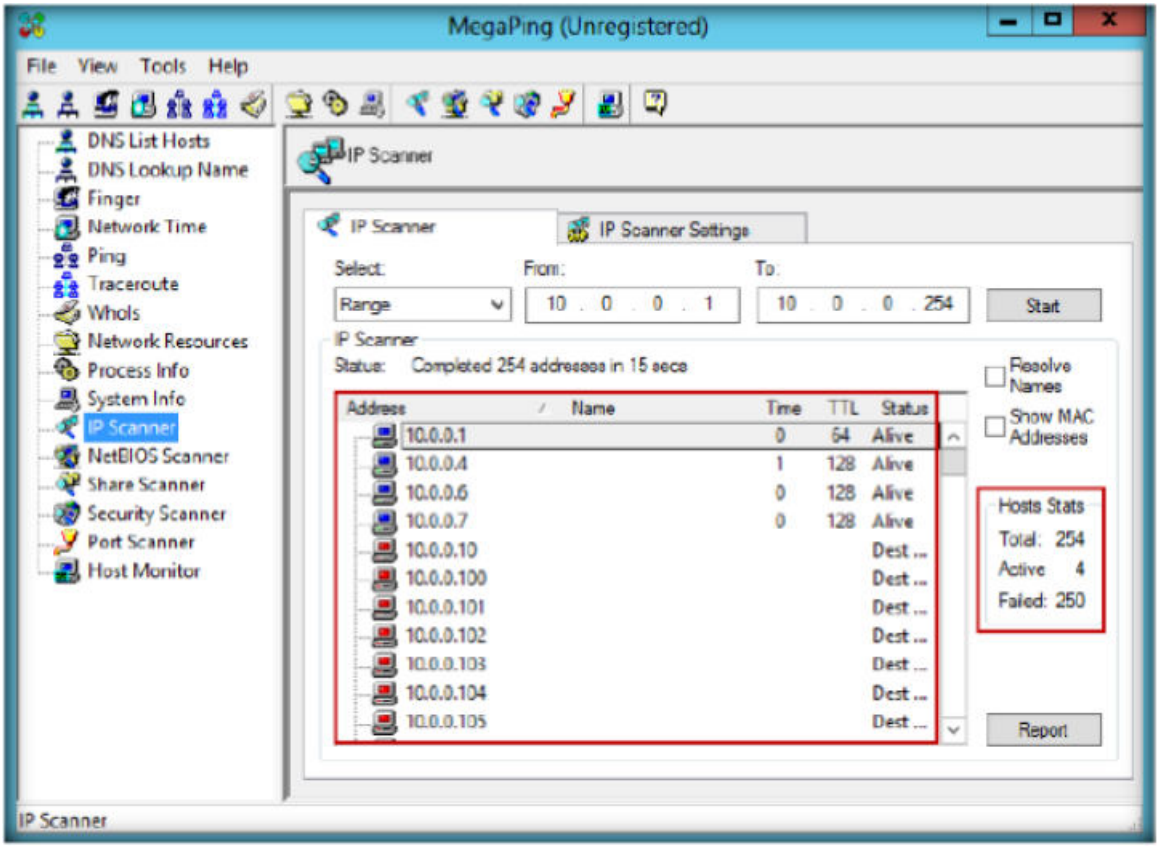


РИСУНОК 15.5: Отчет сканирования IP

8. Выберите «NetBIOS Scanner» на левой панели и диапазон IP в полях «From» и «To». В этой лабораторной работе диапазон IP от 10.0.0.1 до 10.0.0.254, Нажмите «Star»t.

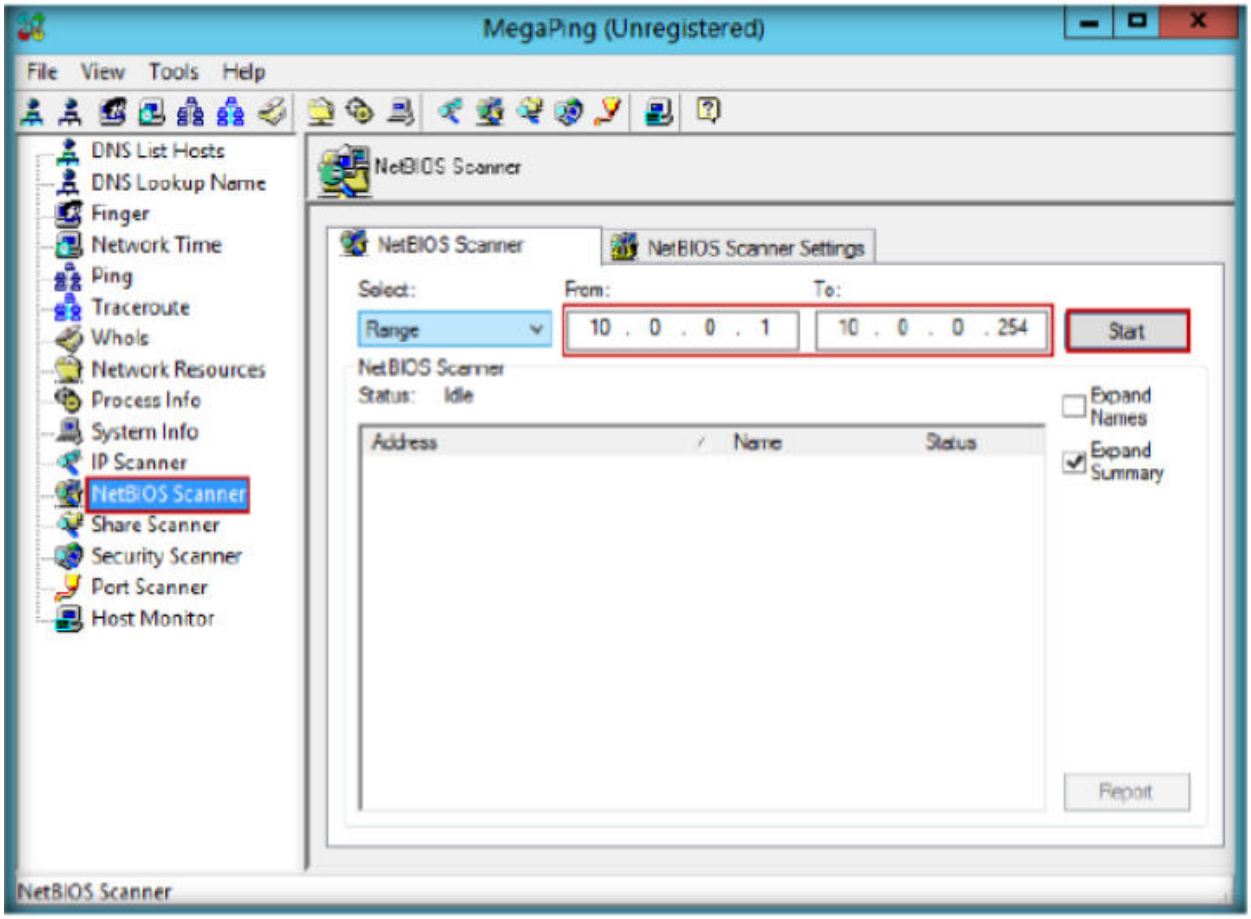


РИСУНОК 15.6: Сканирование NetBIOS

9. Сканирование NetBIOS перечислит все узлы с их именами NetBIOS и адресами адаптера.

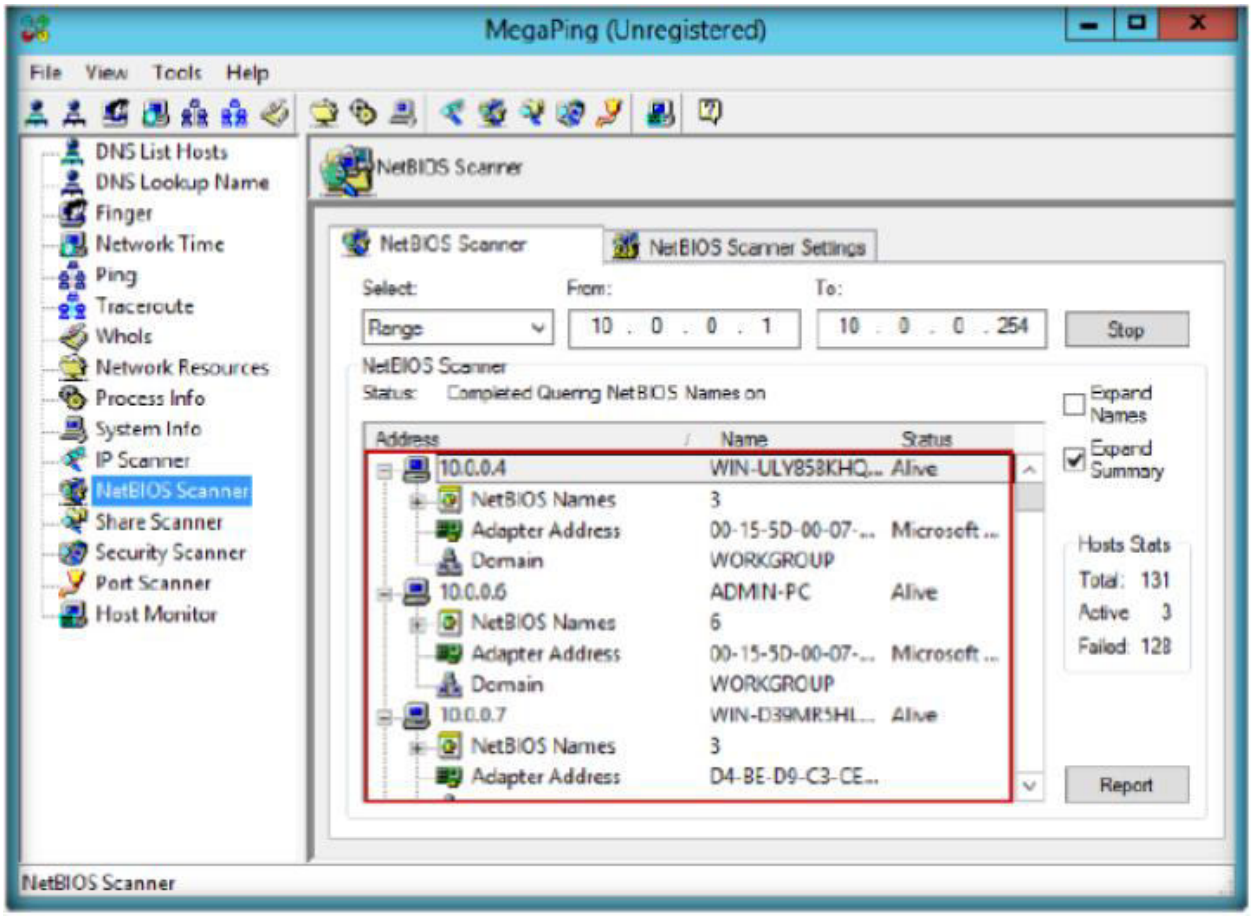


РИСУНОК 15.7: Отчет сканирования NetBIOS

10. Щелкните правой кнопкой по IP-адресу. В этой лабораторной работе выбранный IP 10.0.0.4. Это будет отличаться в Вашей сети.
11. Затем щелкните правой кнопкой и выберите опцию «Traceroute».

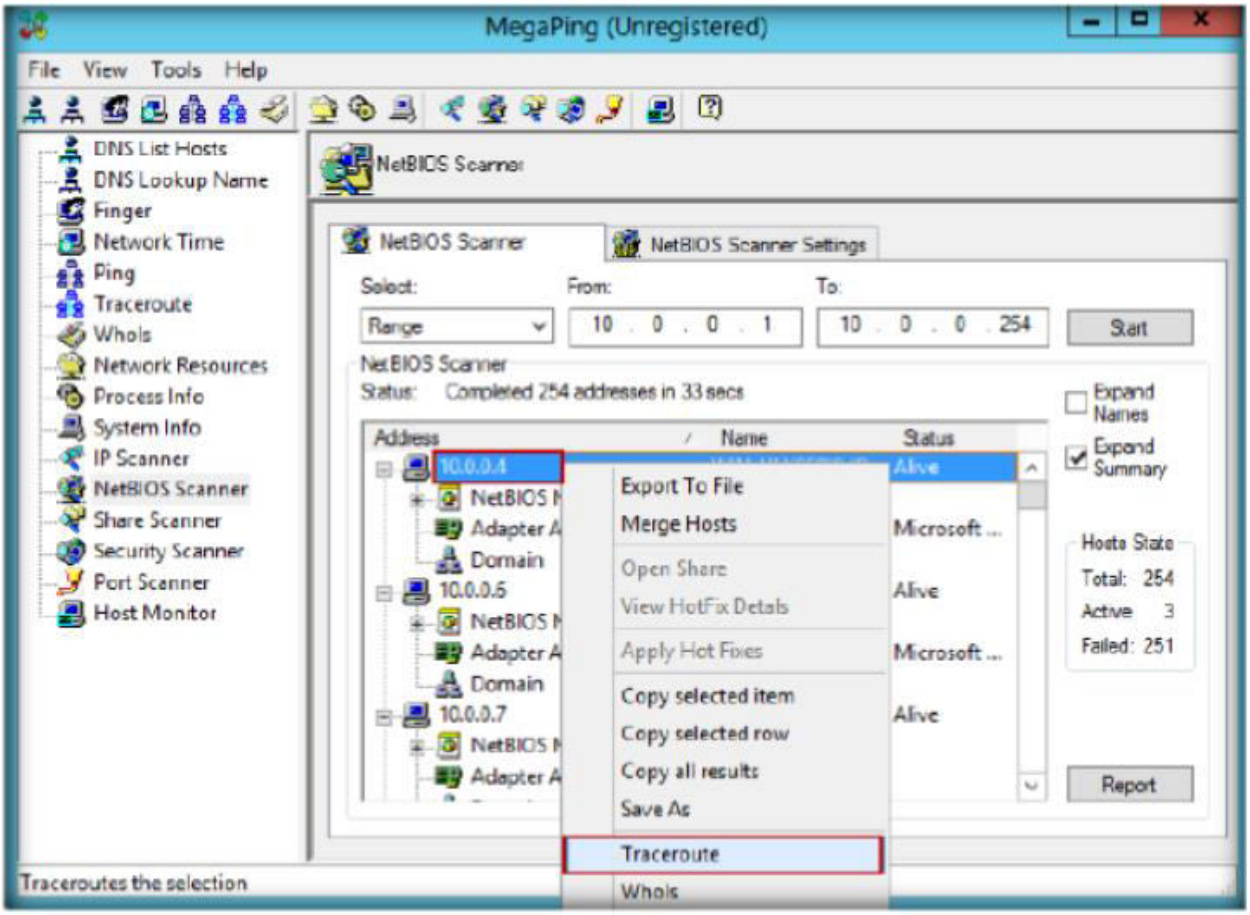


РИСУНОК 15.8: Traceroute

12. Это откроет окно «Traceroute» и проследит выбранный IP-адрес.

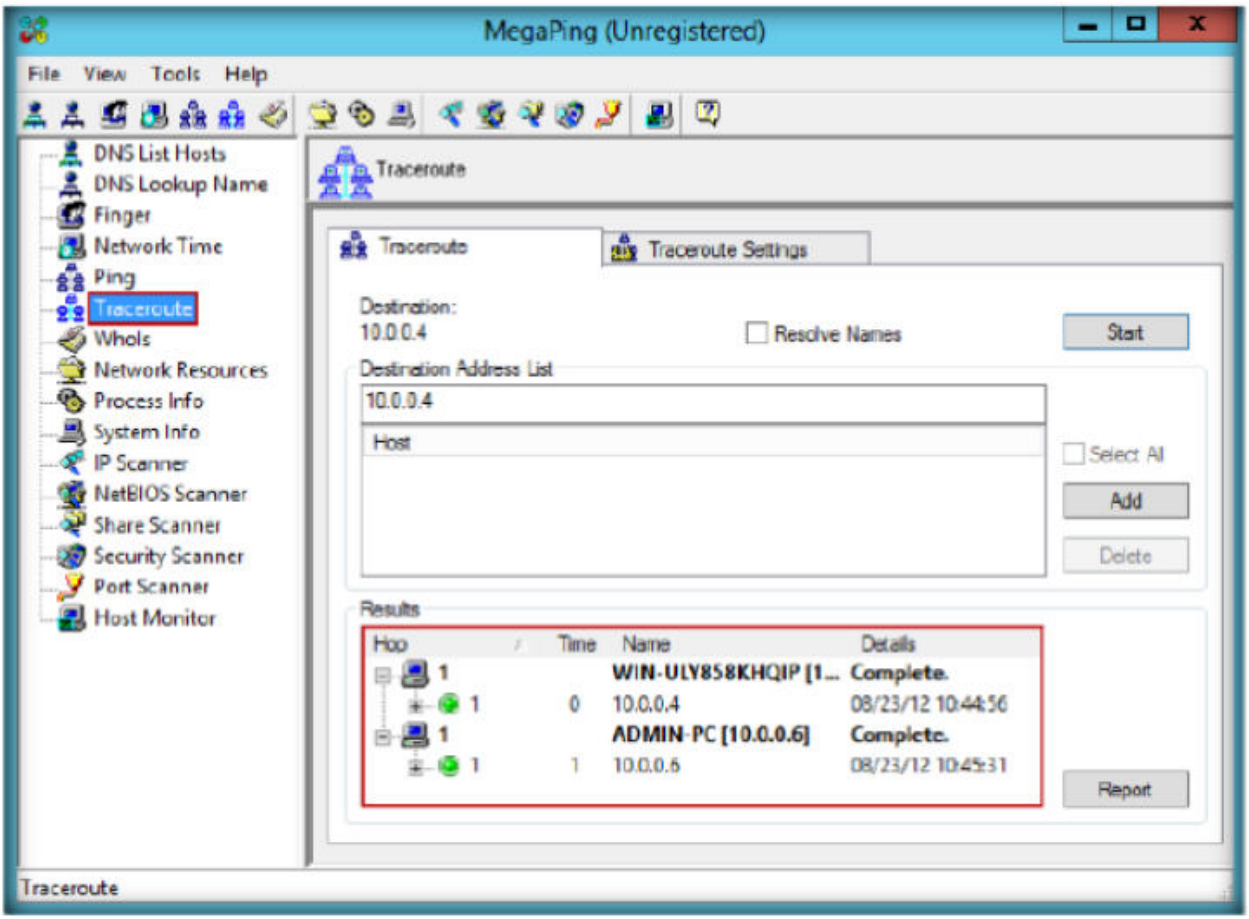


РИСУНОК 15.9: Отчет Traceroute

13. Выберите «Port Scanner» на левой панели и добавьте www.certifiedhacker.com в «Destination Address List» (Списке Адреса назначения) и затем нажмите кнопку «Start».
14. После нажатия кнопки «Start» это переключится, чтобы остановиться
15. Будут перечисляться порты, связанные с www.certifiedhacker.com с ключевым словом, риском и номером порта.

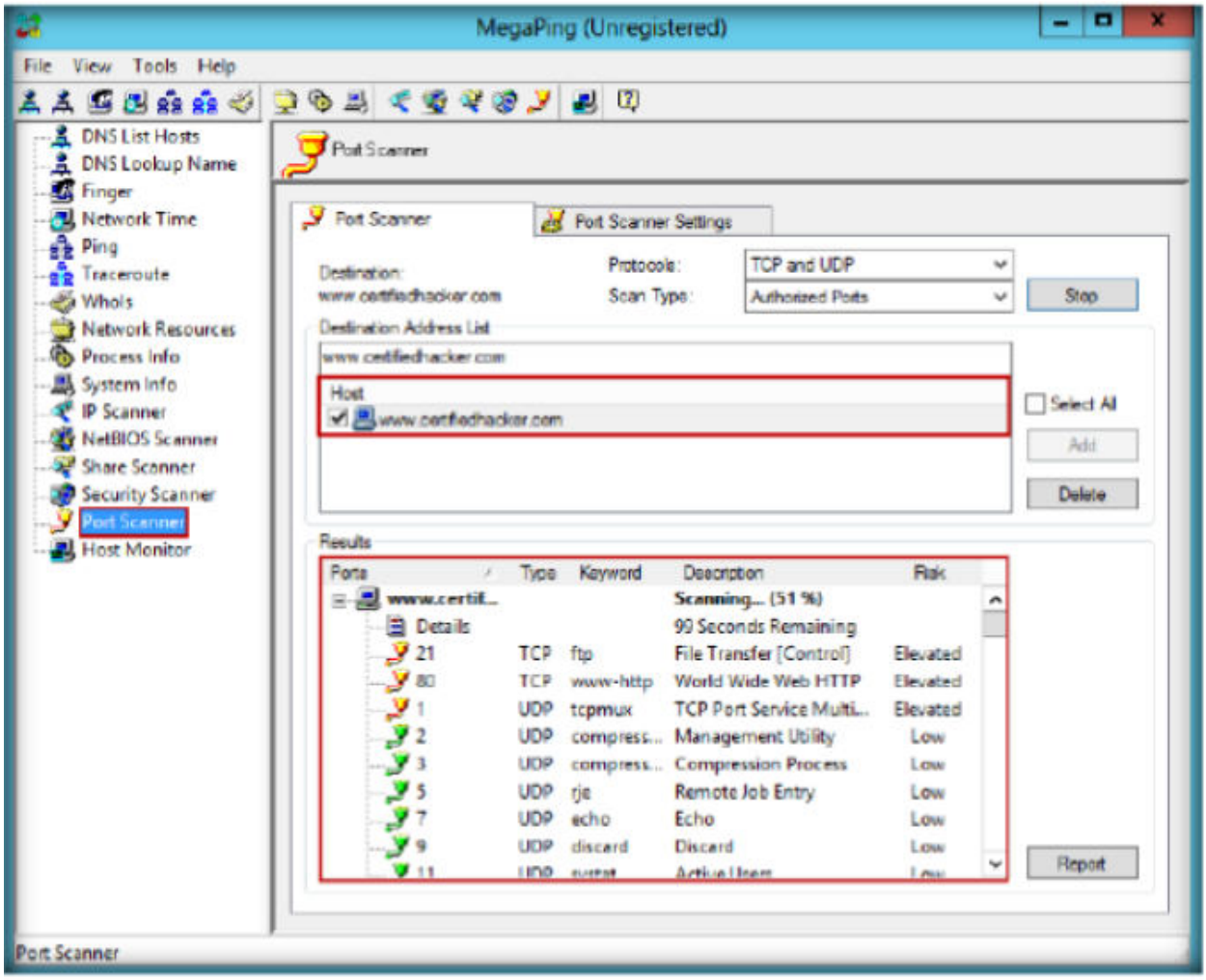


РИСУНОК 15.10: отчет сканирования портов MegaPing

Анализ практической работы

Запишите все IP-адреса, откройте порты и приложения запуска и протоколы, которые Вы обнаружили во время практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
MegaPing	**Диапазон сканирования IP:** 10.0.0.1 — 10.0.0.254
	Выполненные действия: • Сканирование IP • Сканирование NetBIOS • Traceroute • Сканирование портов
	Результат: • Список активного узла • Имя NetBios • Имя адаптера

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы

1. Как MegaPing обнаруживает уязвимости системы обеспечения безопасности в сети?
2. Исследуйте генерацию отчета MegaPing.

Практическое занятие №16. Обнаружение, удаление и блокирование cookie Google с помощью GZapper

Цели работы

Эта Практическое занятие объясняет, как G-Zapper автоматически обнаруживает и чистит cookie Google каждый раз, когда Вы используете свой веб-браузер.

Средства практической работы

Чтобы выполнить лабораторную работу, Вам нужно:

- G-Zapper расположен в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Anonymizers\G-Zapper
- Вы можете также загрузить последнюю версию G-Zapper по ссылке http://www.dunmiysoftware.com/
- Если Вы решаете загрузить последнюю версию, то снимки экрана, показанные в практическому занятию могут отличаться от тех, что получите
- Установите G-Zapper в Windows Server 2012 с помощью мастера установки.
- Административные привилегии для пользования инструментами
- Компьютер с Windows Server 2012

Краткие теоретические сведения

Обзор G-Zapper

G-Zapper помогает защищать Ваши идентификационные данные и поисковую историю. G-Zapper находит cookie Google, установленные на Вашем PC, выведет на экран дату, когда они были установлены, определит сколько времени Ваши поиски были прослежены и выведет на экран Ваши поиски Google. G-Zapper позволяет Вам автоматически удалять или полностью блокировать cookie поиска Google от будущей установки.

Постановка задачи

1. Запустите Меню "Пуск".

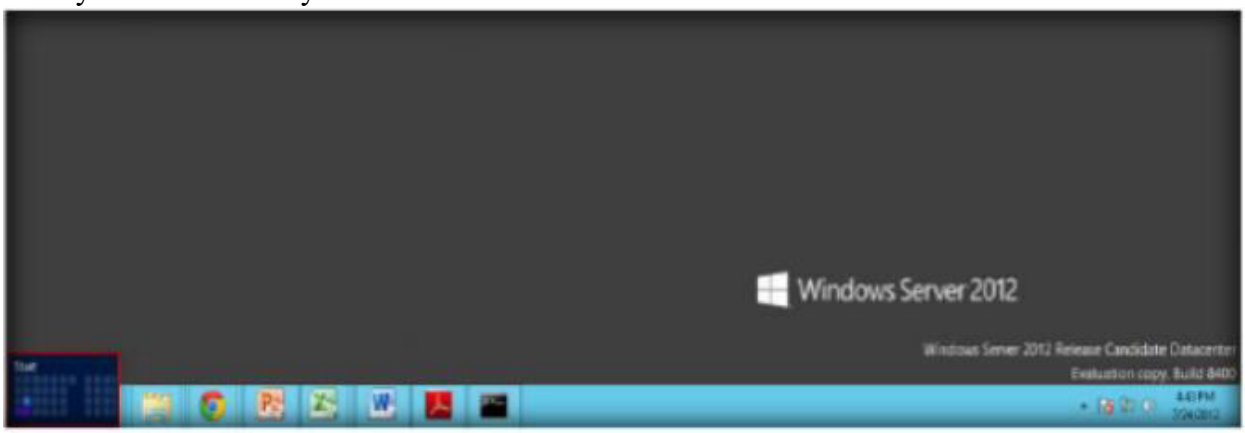


РИСУНОК 16.1: Windows Server 2012 – Рабочий стол

2. Щелкните по приложению G-Zapper, чтобы открыть окно G-Zapper.

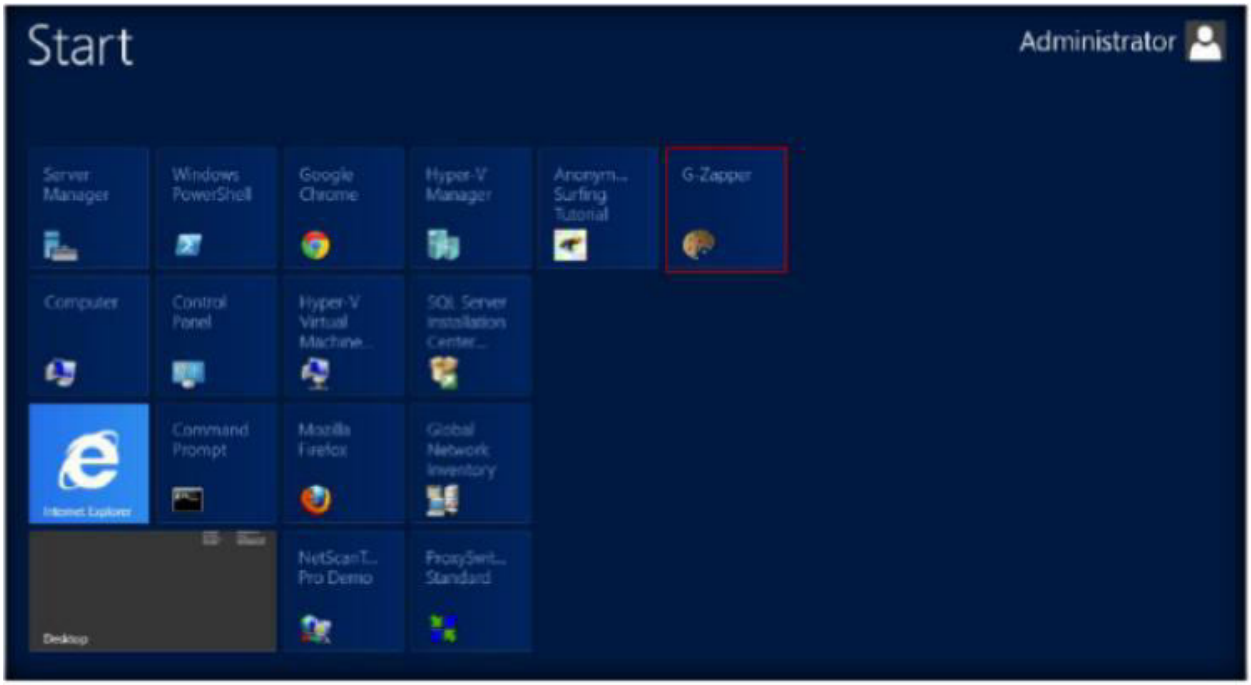


РИСУНОК 16.2: Windows Server 2012 - приложения

3. Появится главное окно G-Zapper.

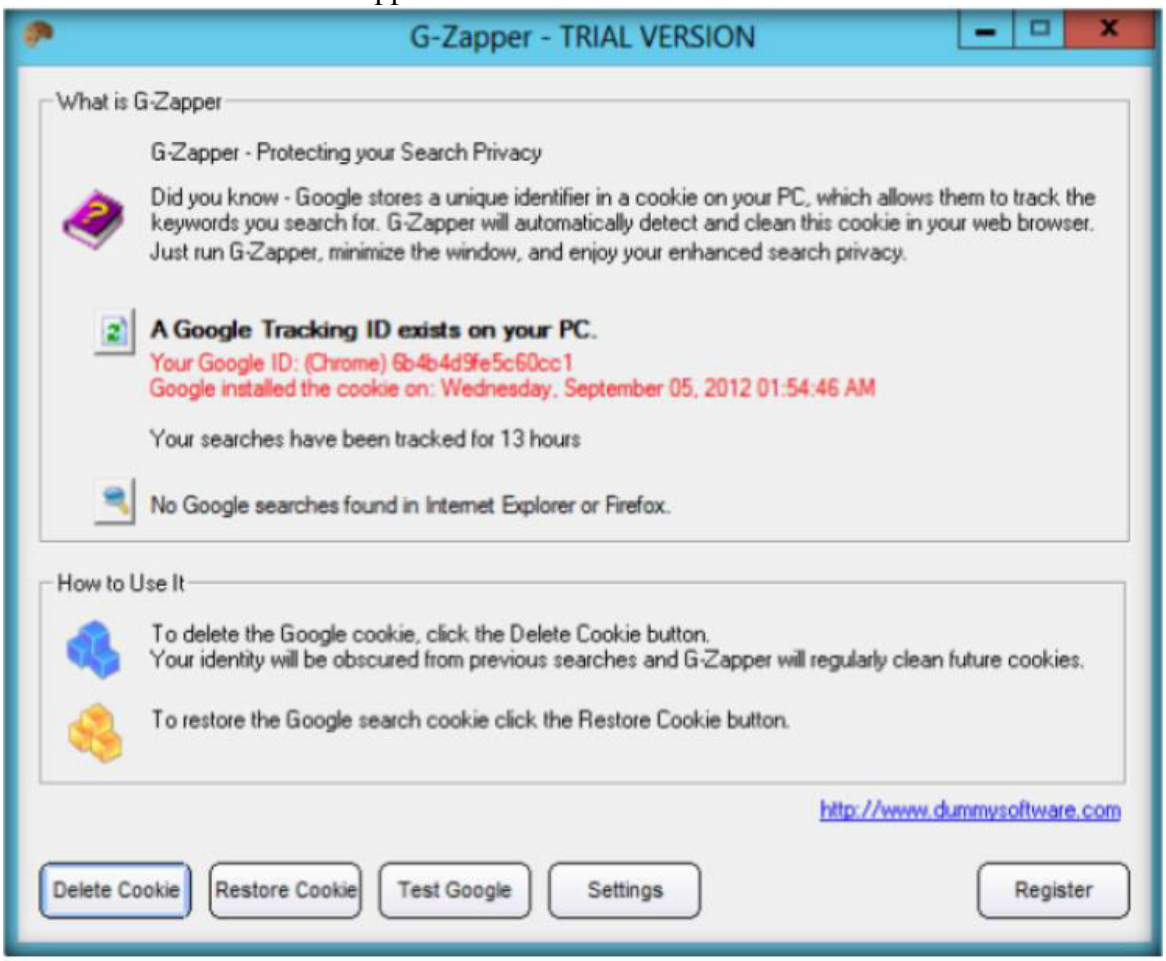


РИСУНОК 16.3: Главные окно G-Zapper

4. Чтобы удалить cookie поиска Google, нажмите кнопку «Delete Cookie». Появится окно, которое даст информацию об удаленном расположении cookie. Нажмите "OK".

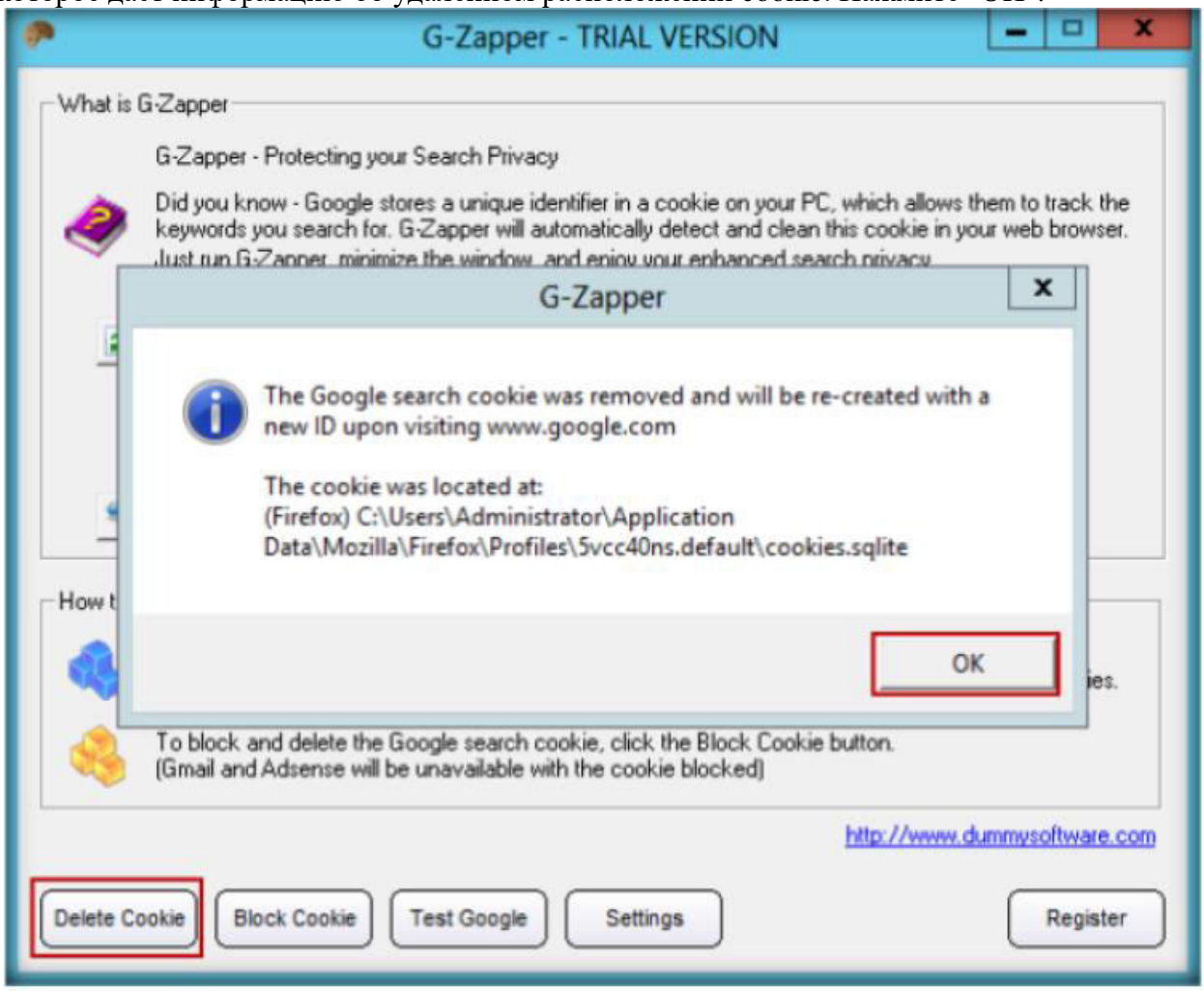


РИСУНОК 16.4: Удаление поисковых cookie

5. Чтобы заблокировать cookie поиска Google, нажмите «Block cookie». Если Вы захотите вручную заблокировать cookie Google нажмите кнопку «Yes».

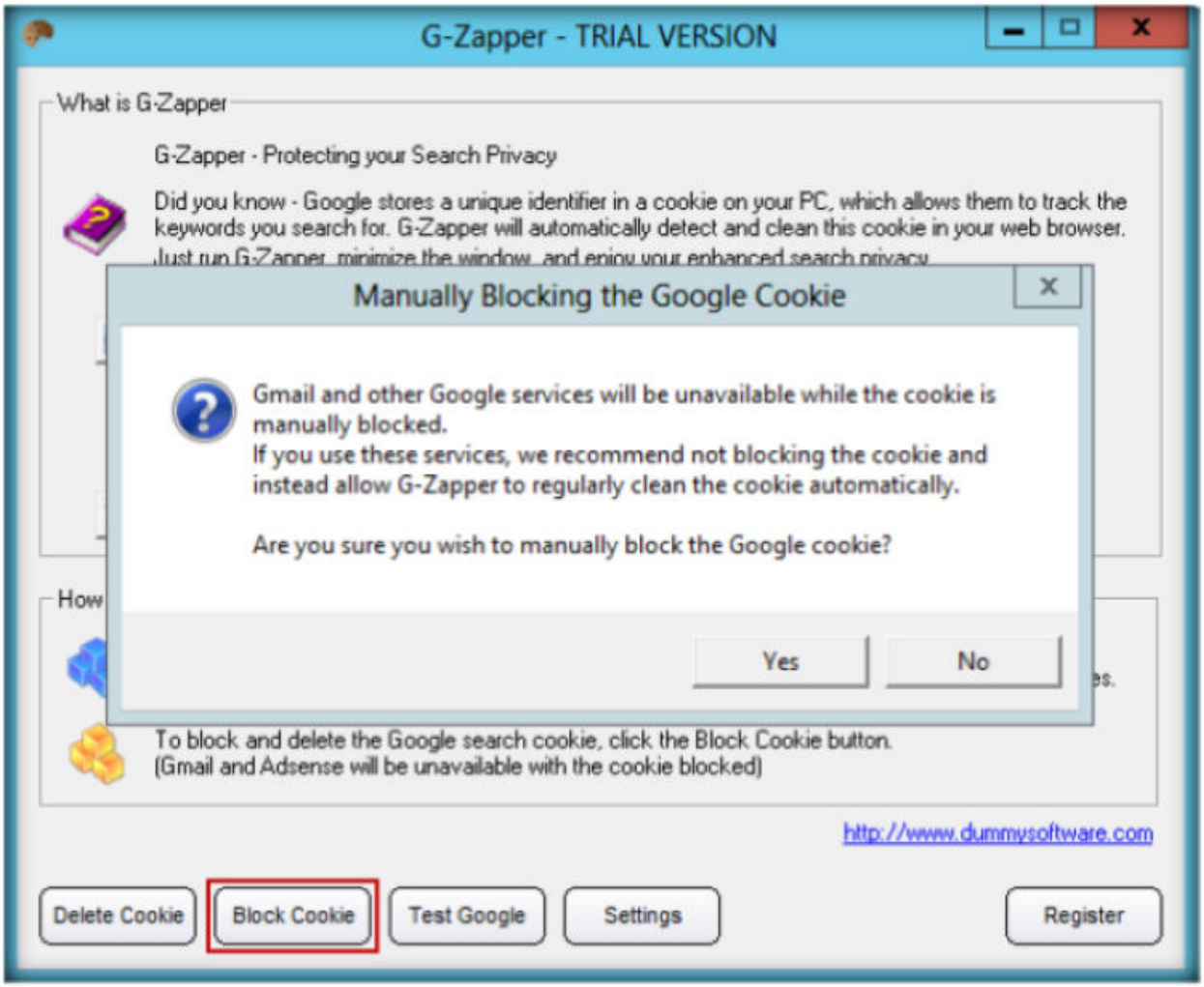


РИСУНОК 16.5: Блокирование cookie Google

6. Выйдет сообщение, что cookie Google были заблокированы. Чтобы проверить нажмите "OK".

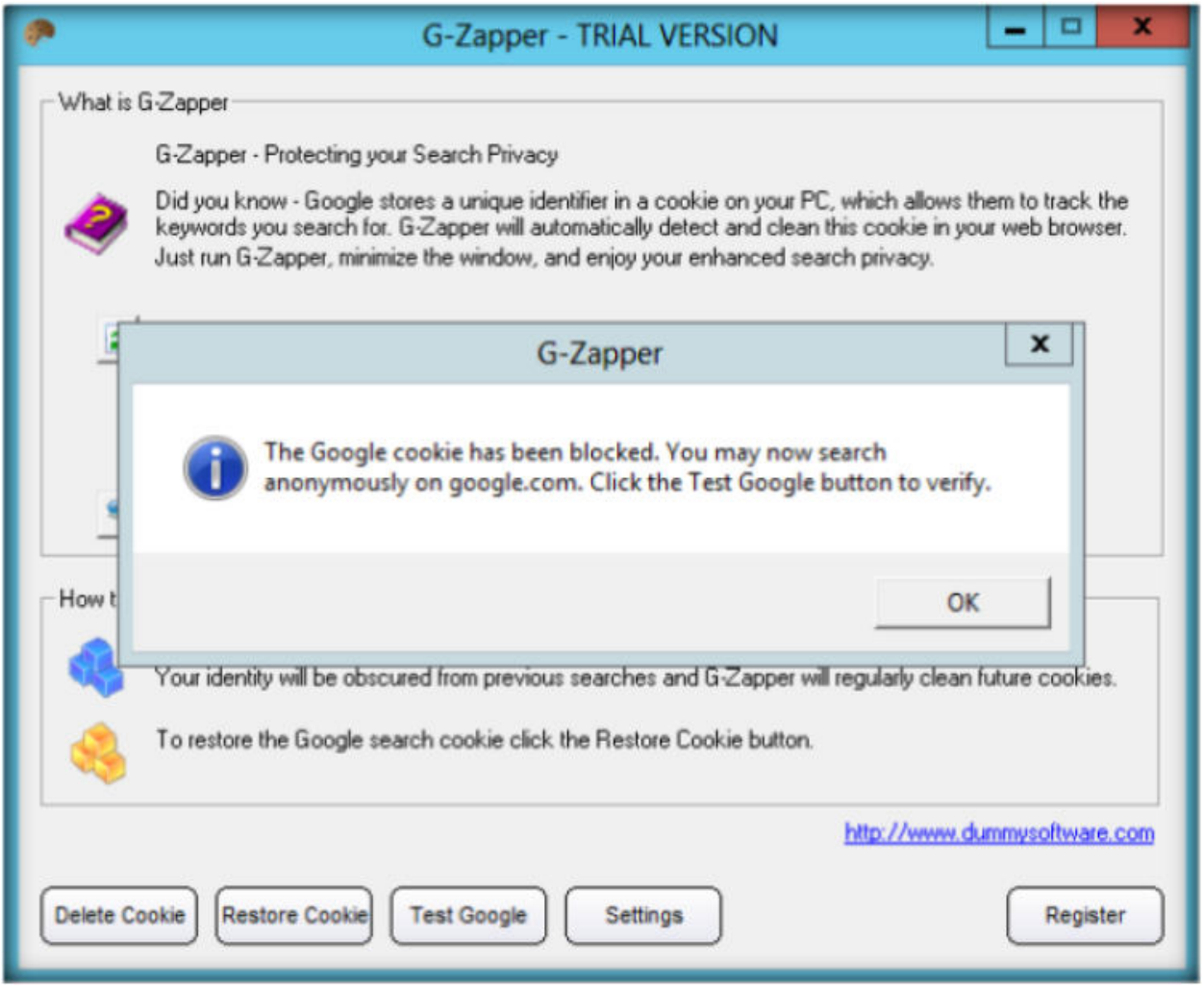


РИСУНОК 16.6: Блокирование cookie Google (2)

7. Чтобы протестировать cookie Google, который был заблокирован, нажмите кнопку «Test Google».
8. Ваш веб-браузер по умолчанию теперь откроет страницу Preferences Google. Нажмите "OK".

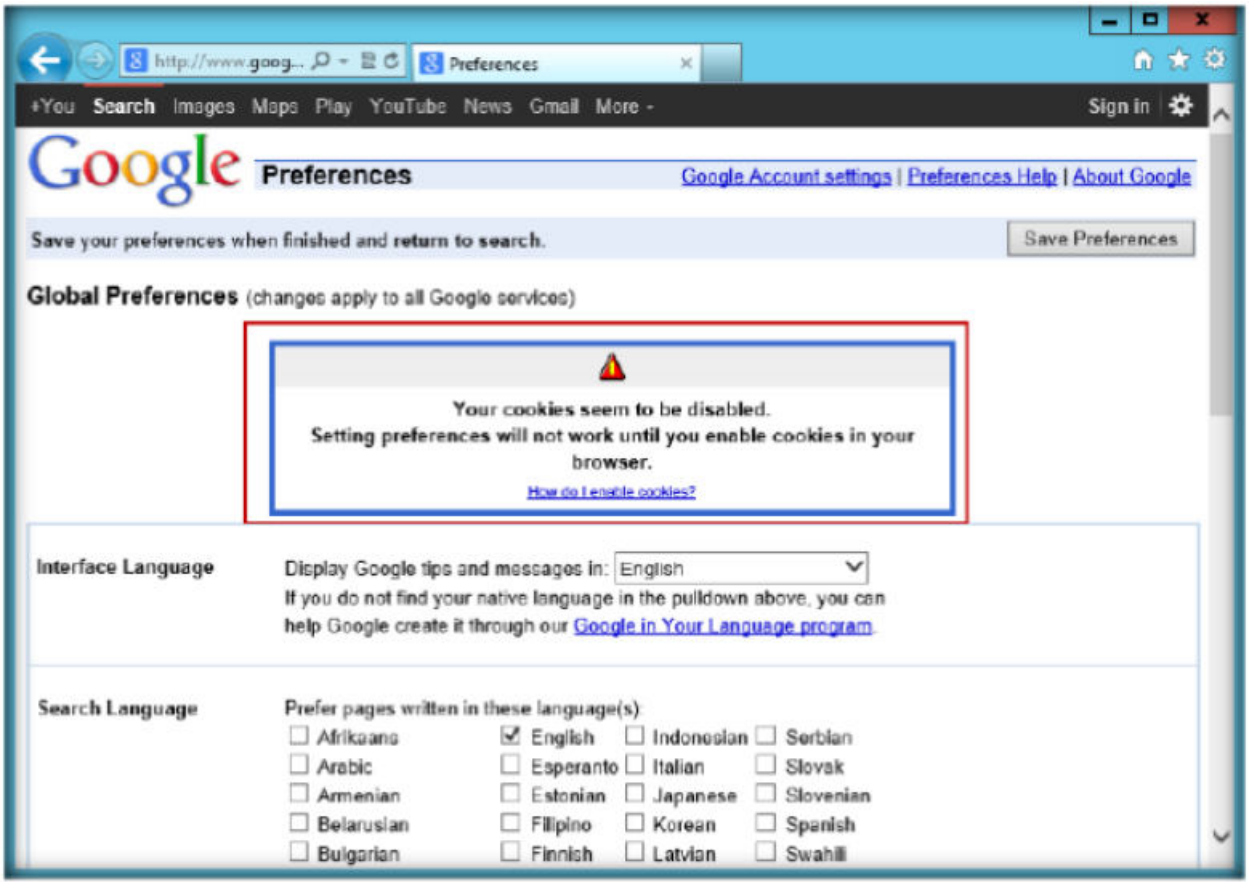


РИСУНОК 16.7: Отключение сообщения Cookie

9. Чтобы просмотреть удаленную информацию о cookie, нажмите кнопку «Setting» и «View Log» в «cleaned cookies log».

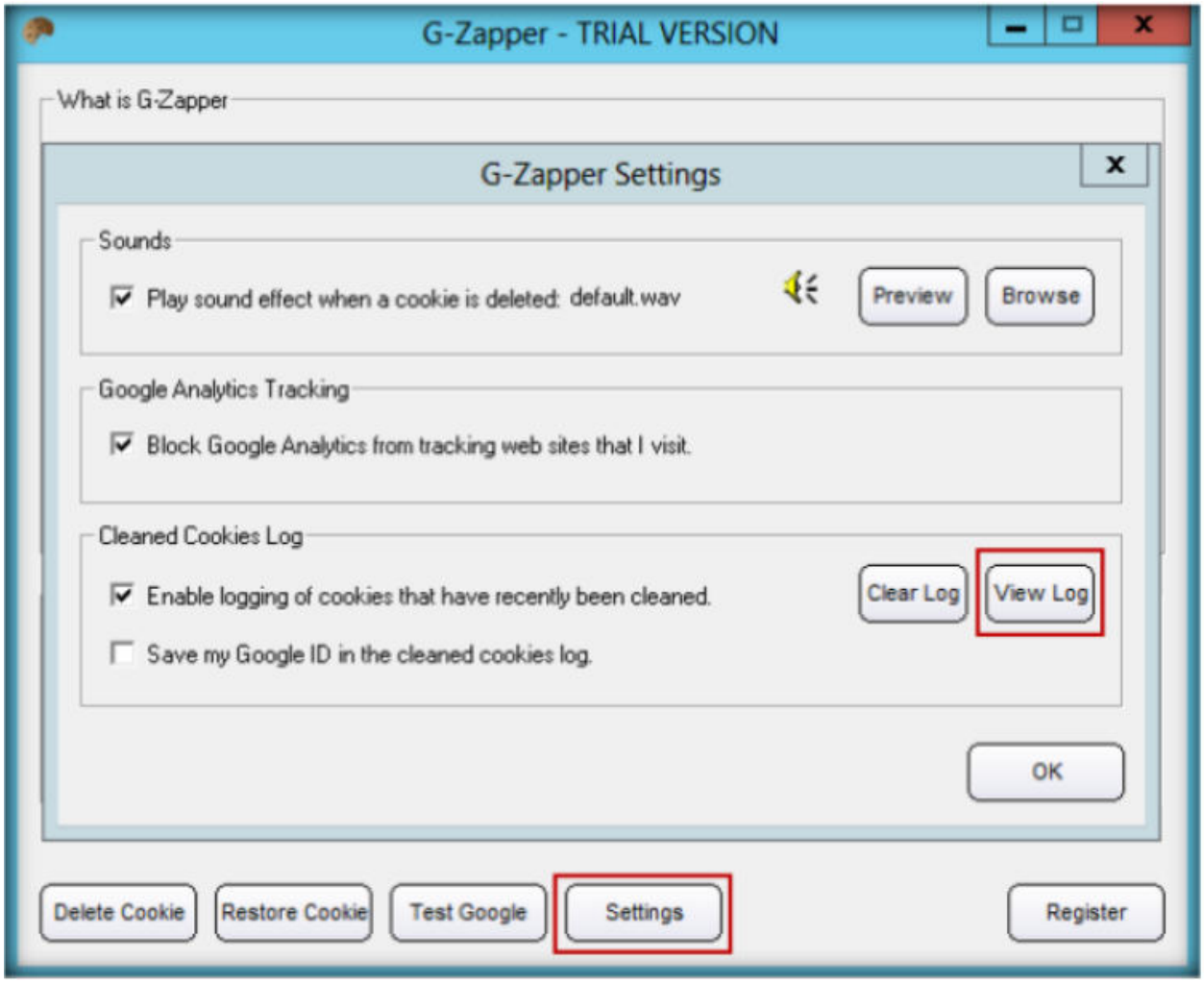


РИСУНОК 16.8: Просмотр удаленных регистраций

10. Удаленная информация о cookie открывается в Блокноте.

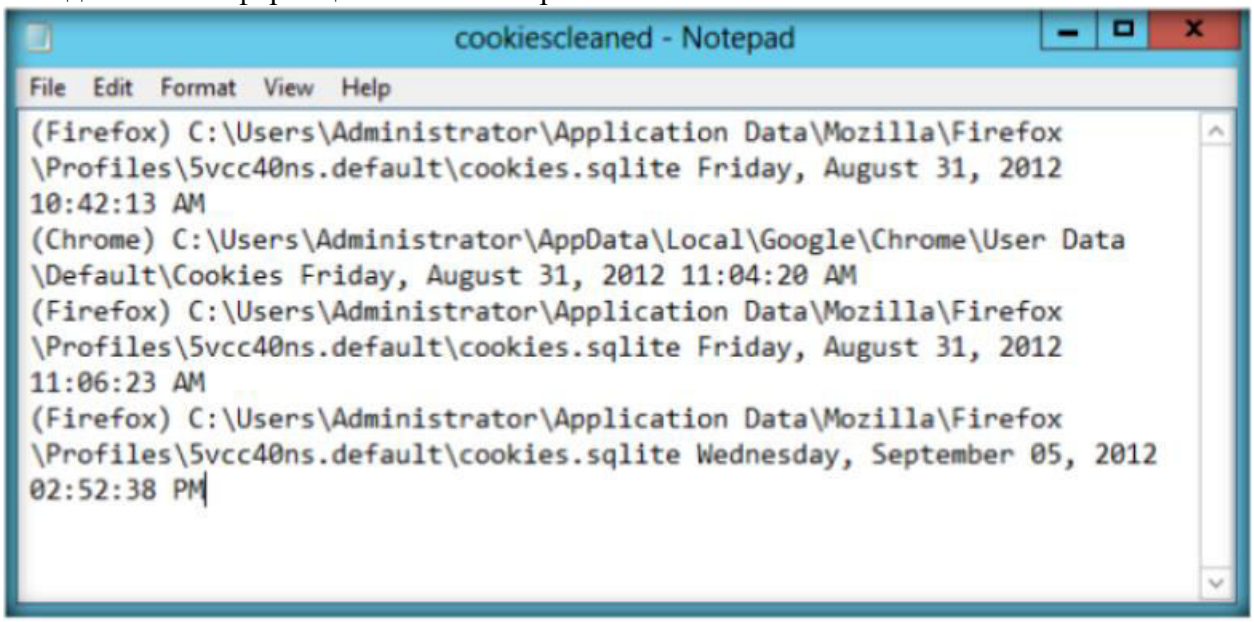


РИСУНОК 16.9: Удаленный Отчет регистрации

Анализ практической работы

Запишите все IP-адреса, откройте порты и приложения запуска и протоколы, которые Вы обнаружили во время практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
G-Zapper	**Выполненное действие:** • Обнаружьте cookie • Удалите cookie • Блокируйте cookie
	Результат: Удаленные cookie сохранены в C:\Users\Administrator\Application Data

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

Вопросы

1. Исследуйте, как G-Zapper автоматически чистит cookie Google.
2. Проверьте блокирует ли G-zapper cookie на сайтах кроме Google.

Практическое занятие №17. Сканирование сети с помощью Colasoft Packet Builder

Цели работы

Цель этой практической работы состоит в том, чтобы укрепить понятие политики сетевой безопасности, стратегического осуществления и стратегических аудитов.

Средства пракической работы

Для выполнения этой практической работы Вам нужно:

- Colasoft Packet Builder располагался в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Custom Packet Creator\Colasoft Packet Builder
- Компьютер с Windows Server 2012 как хост-машина
- Window 8 работающее на виртуальной машине как целевая машина
- Вы можете также загрузить последнюю версию Colasoft Packet Builder по ссылке http://www.colasoft.com/download/products/download_packet_builder. php
- Если Вы решите загрузить последнюю версию, то снимки экрана, показанные в практическому занятию могут отличаться от того, что получите
- Веб-браузер с Интернет-соединением, работающим в хост-машине

Краткие теоретические сведения

Обзор Colasoft Packet Builder

Colasoft Packet Builder создает и включает пользовательские сетевые пакеты. Этот инструмент может использоваться, чтобы проверить сетевую защиту от атак и злоумышленников. Функции редактора декодирования Colasoft Packet Builder разрешают пользователям отредактировать значения полей протокола.

Пользователи также в состоянии отредактировать информацию о декодировании в двух редакторах: Decode Editor и HEX-редактор. Пользователи могут выбрать любой из обеспеченных шаблонов: Пакет Ethernet, Пакет IP, Пакет ARP или Пакет TCP.

Постановка задачи

1. Установите и запустите Colasoft Packet Builder**.**

2. Запустите Меню "Пуск".

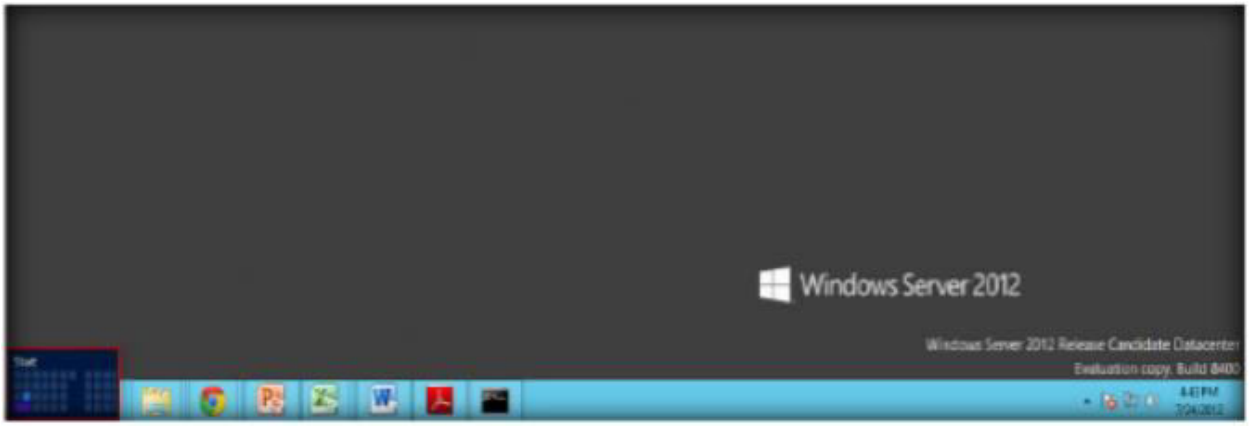


РИСУНОК 17.1: Windows Server 2012 – Рабочий стол

3. Нажмите на приложение Colasoft Packet Builder 1.0, чтобы открыть его.

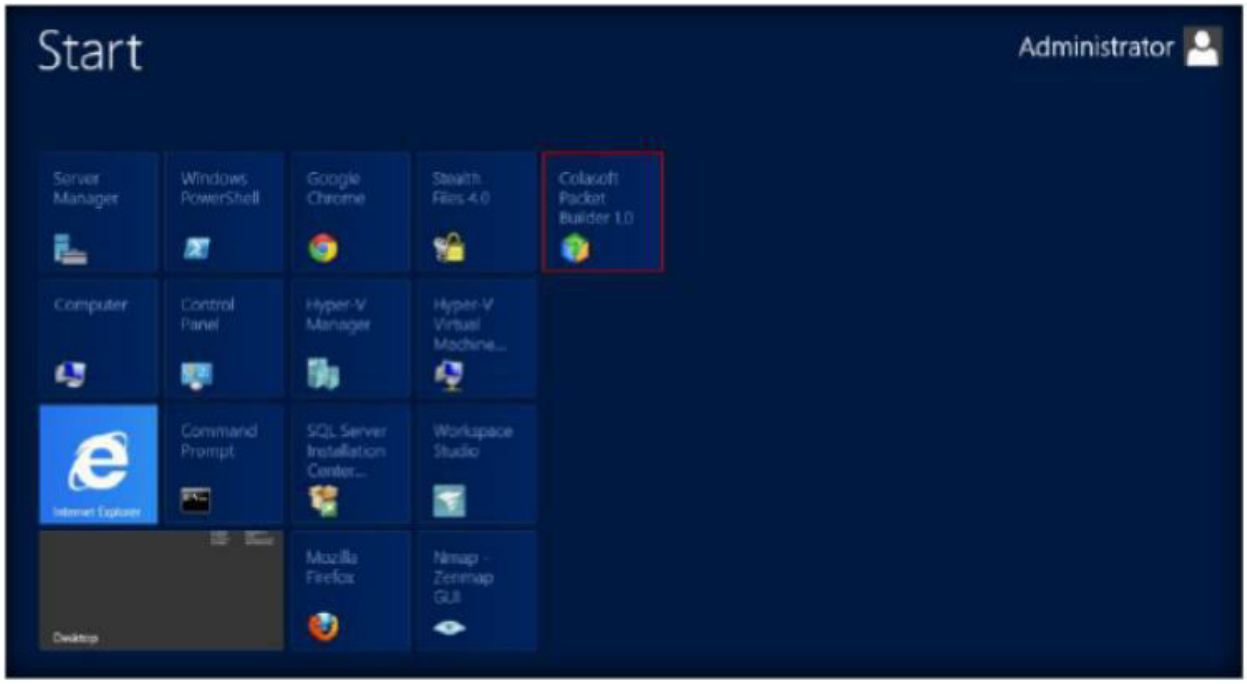


РИСУНОК 17.2: Windows Server 2012 - приложения

4. Появится главное окно Colasoft Packet Builder.

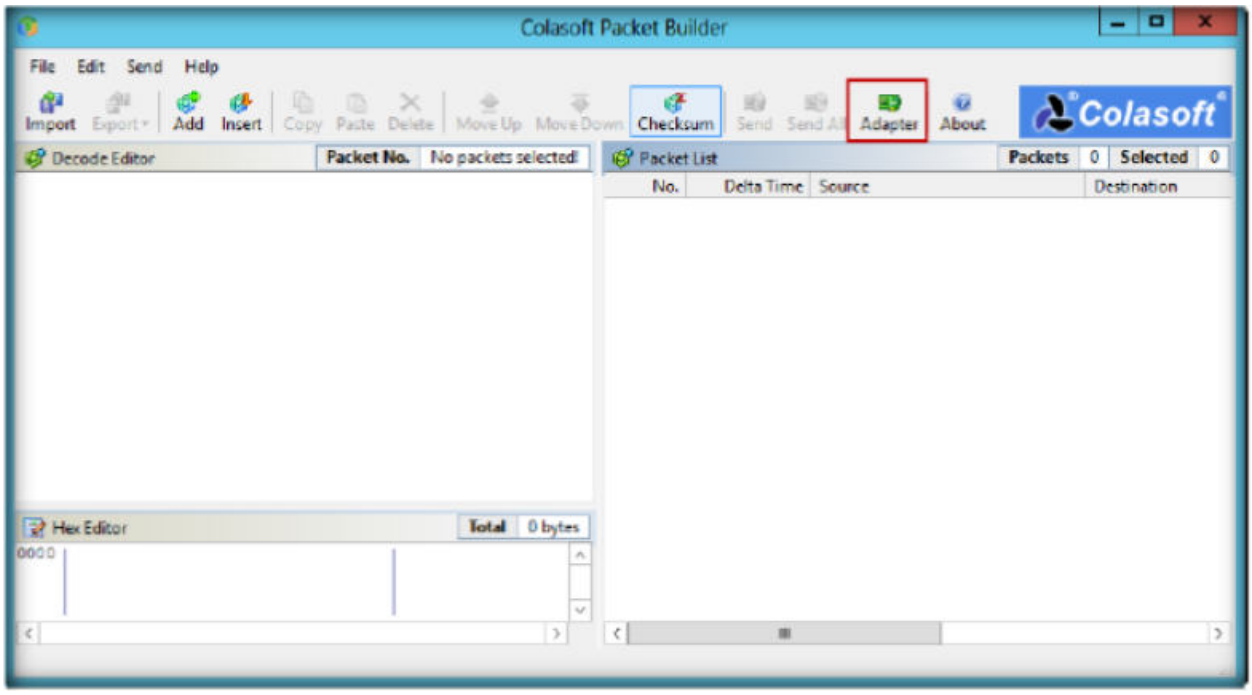


РИСУНОК 17.3: Основная страница Colasoft Packet Builder

5. Проверьте, что параметры настройки Адаптера собираются принять значение по умолчанию и затем нажмите "OK".

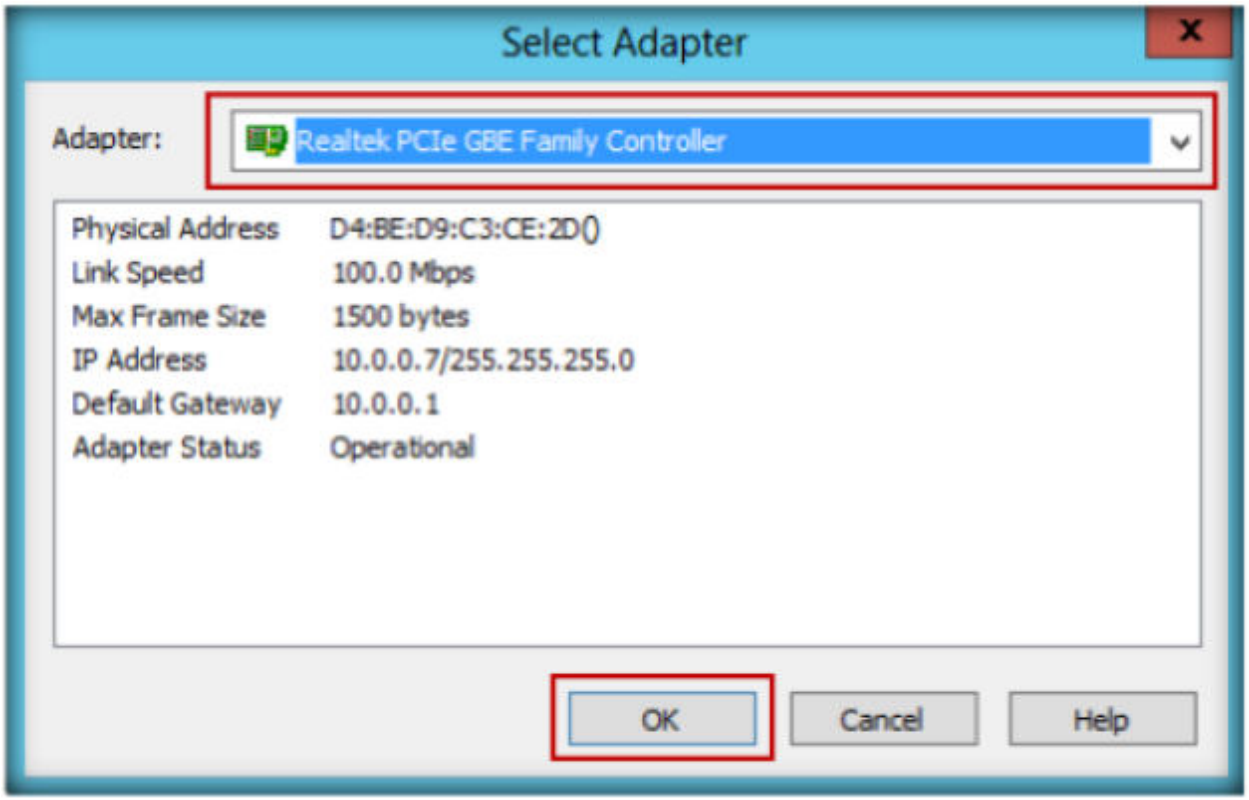


РИСУНОК 17.4: параметры настройки Colasoft Packet Builder Adapter

6. Чтобы добавить или создать пакет, нажмите «Add» в разделе меню.

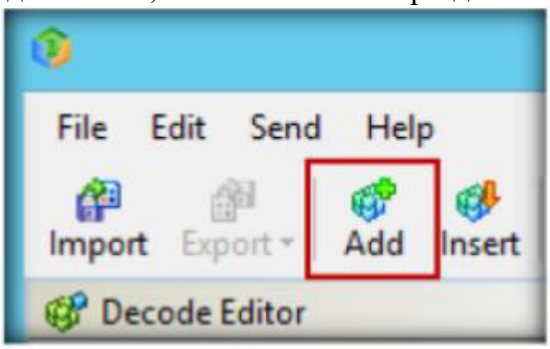


РИСУНОК 17.5: Создание пакета в Colasoft Packet Builder

7. Когда раскроется окно Add Packet, Вы должны выбрать шаблон и нажать "OK".

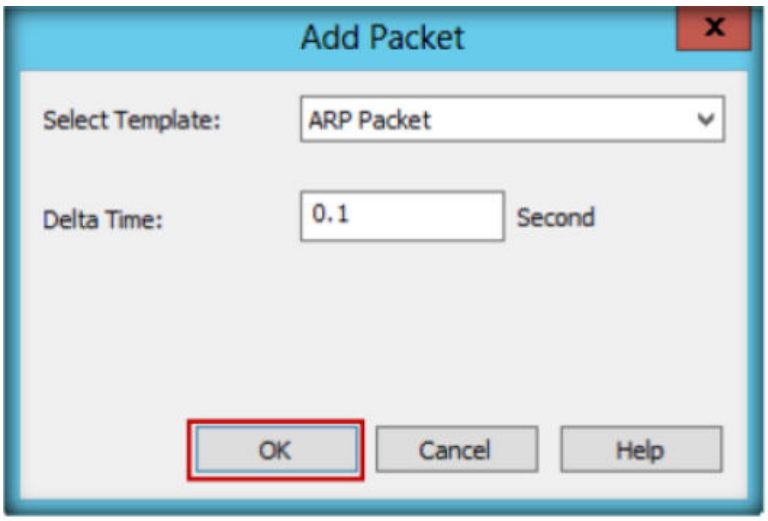


РИСУНОК 17.6: Окно Add Packet

8. Вы можете просмотреть добавленный пакетный список на правой стороне Вашего окна.

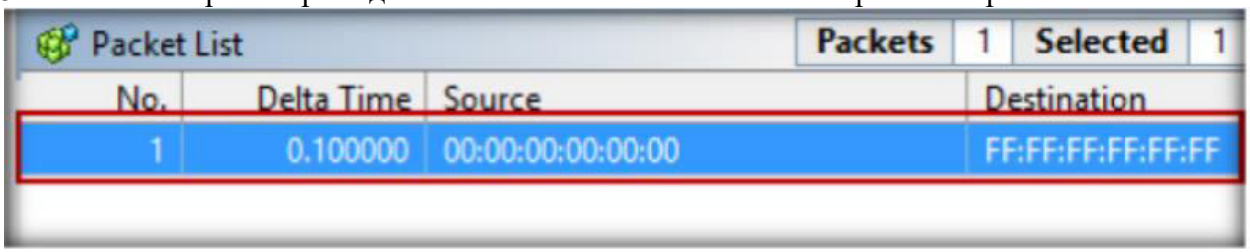


РИСУНОК 17.7: Пакетный список

9. Colasoft Packet Builder позволит Вам редактировать информацию о декодировании в этих двух редакторах: Decode Editor и Hex Editor.

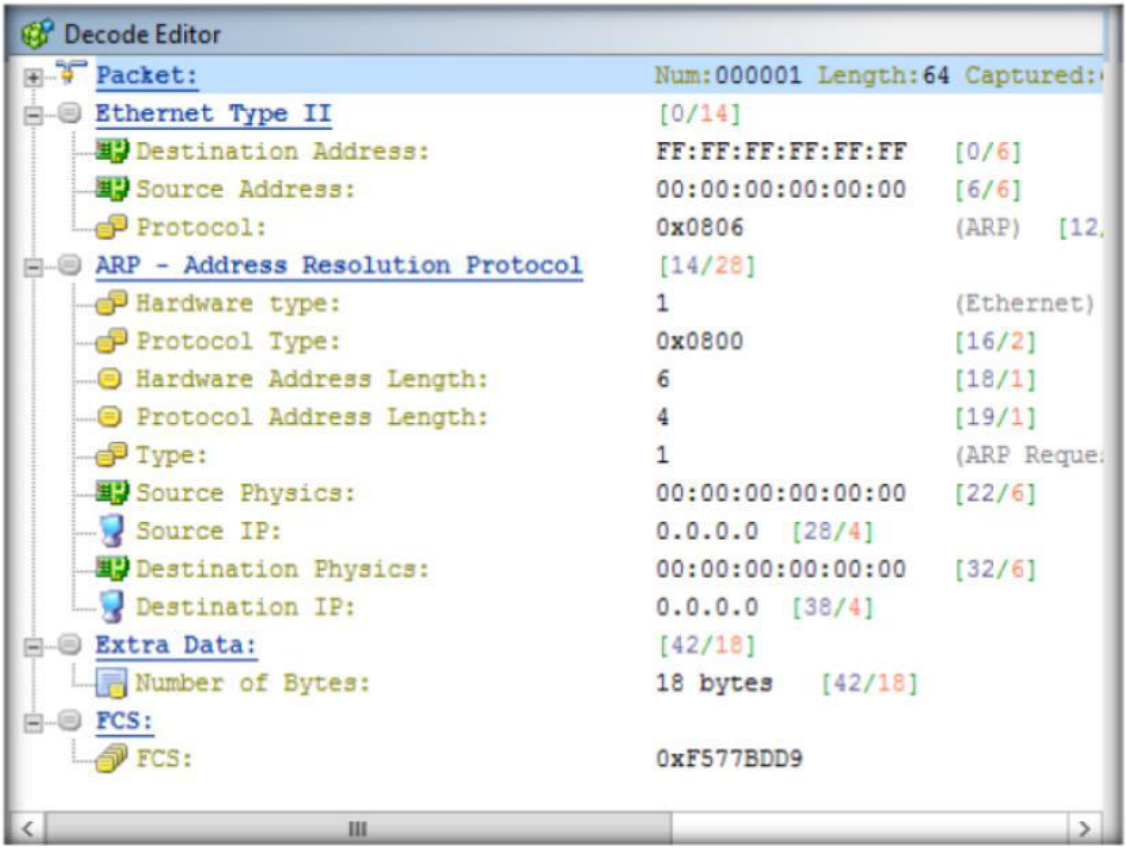


РИСУНОК 17.8: Decode Editor

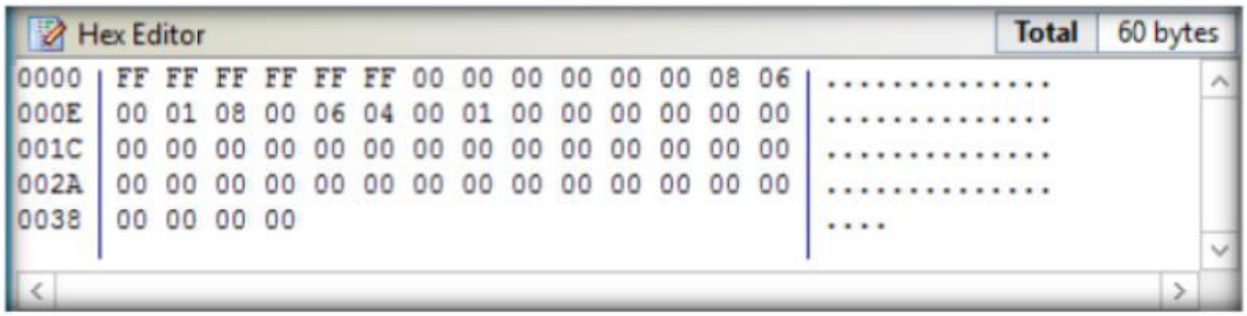


РИСУНОК 17.9: Hex Editor

10. Чтобы отправить все пакеты в определенное время, нажмите «Send All» от строки в меню.
11. Проверьте опцию «Burst Mode» в диалоговом окне «Send All Packets», и затем нажмите «Start».

РИСУНОК 17.10: Кнопка Send All

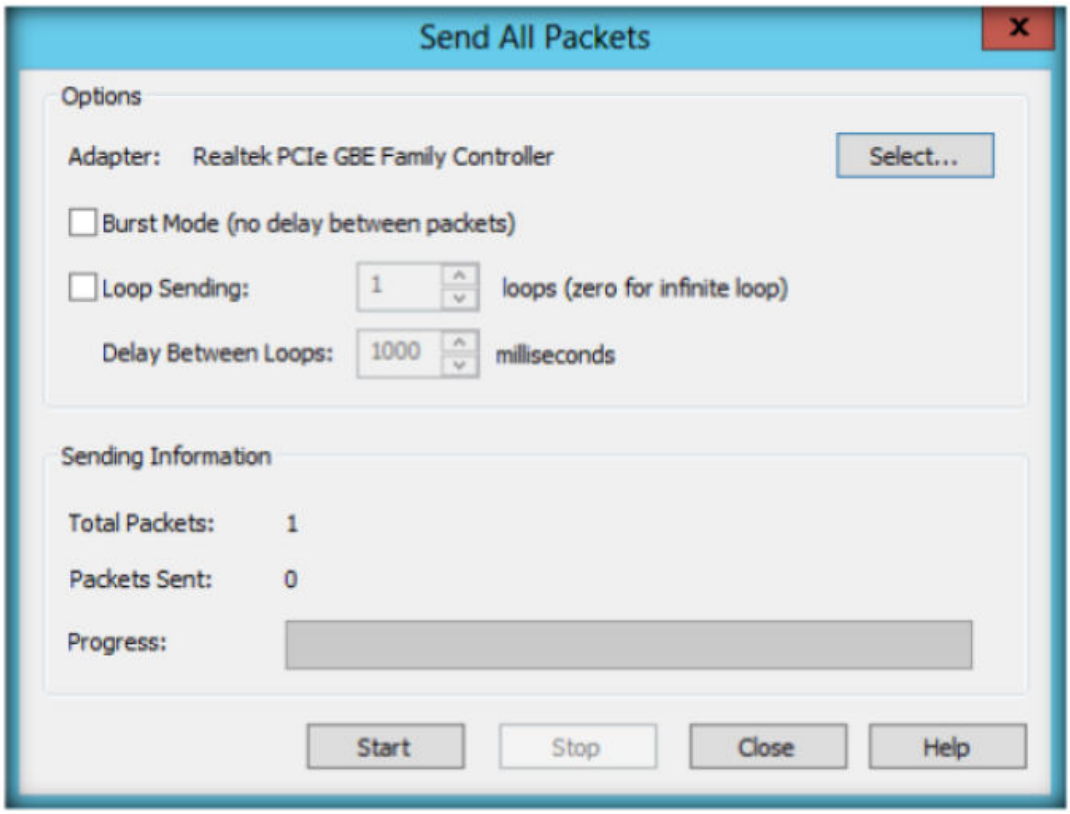


РИСУНОК 17.11: Colasoft Packet Builder отправляет все пакеты

12. Нажмите "Пуск"

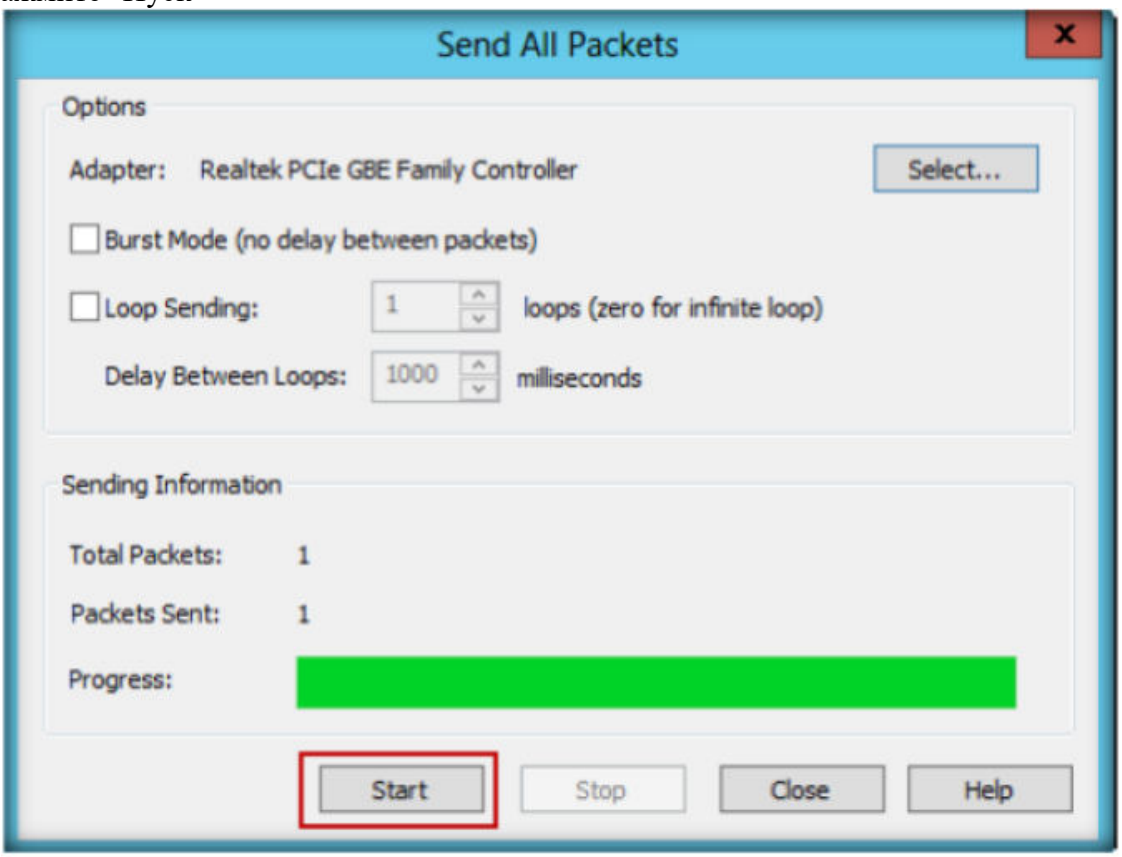


РИСУНОК 17.12 Colasoft Packet Builder отправляет все пакеты

13. Чтобы экспортировать все пакеты выберите в меню File → Export → All Packets.

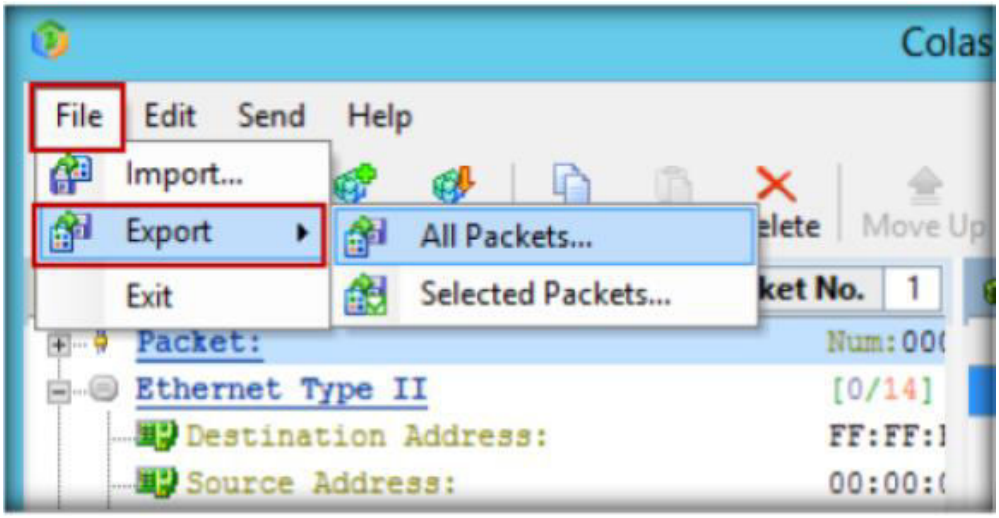


РИСУНОК 17.13: Экспортирование всех пакетов

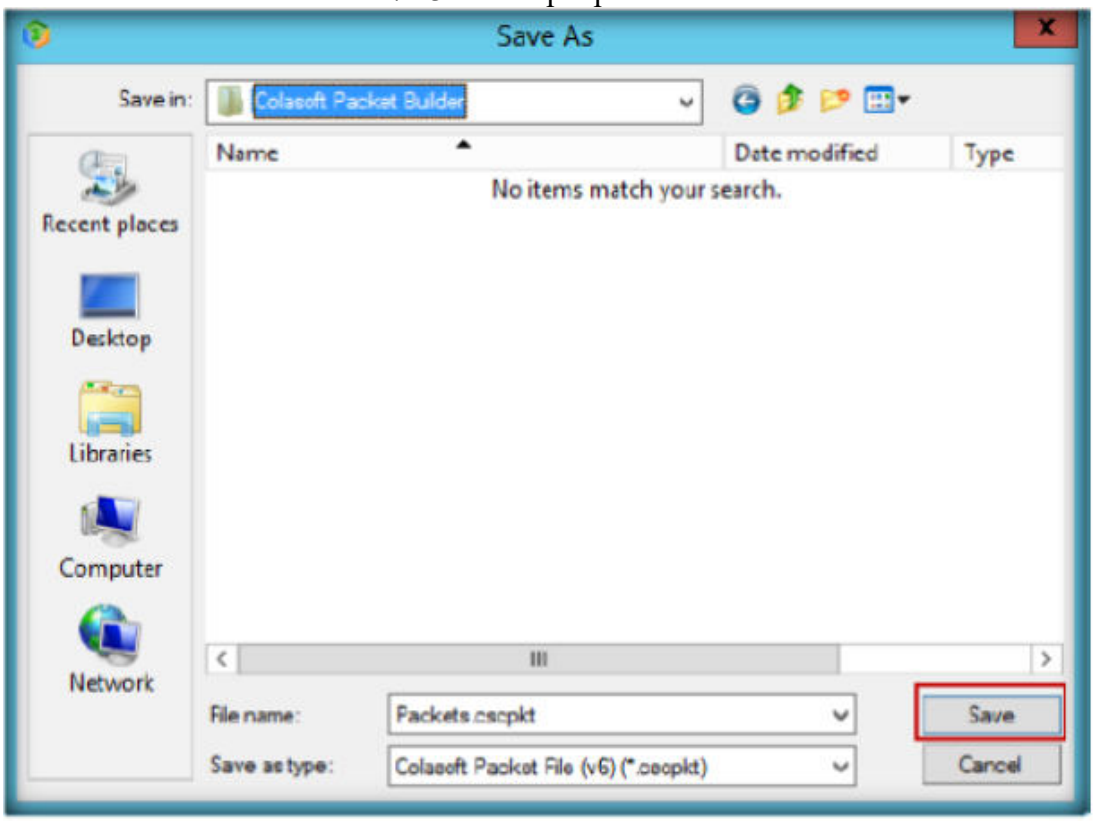


РИСУНОК 17.14: Выберите расположение, чтобы сохранить экспортируемый файл

РИСУНОК 17.15: Экспортированный пакет Colasoft Packet Builder

Анализ практической работы

Проанализируйте и запишите результаты, связанные с осуществлением практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
Colasoft Packet Builder	**Используемый адаптер:** Realtek PCIe Family Controller
	Выбранное пакетное имя: ARP Packets
	Результат: Полученные пакеты сохранены в packets.cscpkt

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОЙ РАБОТЕ.

Вопросы

1. Проанализируйте, как Colasoft Packet Builder влияет на Ваш сетевой трафик при анализе сети.
2. Оцените, какие типы мгновенных сообщений контролирует Capsa.
3. Определите, буферизуется ли пакет производительности влияния. Если да, то, какие шаги Вы делаете, чтобы избежать или уменьшить его эффект на программное обеспечение?

Практическое занятие №18. Сканирование устройства в сети с помощью Dude

Цели работы

Цель этой практической работы состоит в том, чтобы продемонстрировать, как отсканировать все устройства в указанных подсетях, расположить на карте Вашу сеть и службы монитора.

Средства практической работы

Чтобы выполнить лабораторию, Вам нужно:

- Dude расположен в D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\The Dude
- Вы можете также загрузить последнюю версию Dude по ссылке http://www.mikrotik.com/thedude.php
- Если Вы решаете загрузить последнюю версию, то снимки экрана, показанные в практическому занятию от тех, что получите
- Компьютер с Windows Server 2012
- Дважды щелкните по Dude и выполните шаги мастера установки, чтобы установить Dude.
- Административные привилегии для пользования инструментами

Краткие теоретические сведения

Обзор чувака

Монитор сети Dude - новое приложение, которое может существенно улучшить способ, которым Вы управляете своей сетевой средой. Оно автоматически отсканирует все устройства в указанных подсетях, установит карту Ваших сетей, службы монитора Ваших устройств, и предупредит Вас в случае, если у некоторой службы есть проблемы.

Постановка задачи

1. Запустите Меню "Пуск".

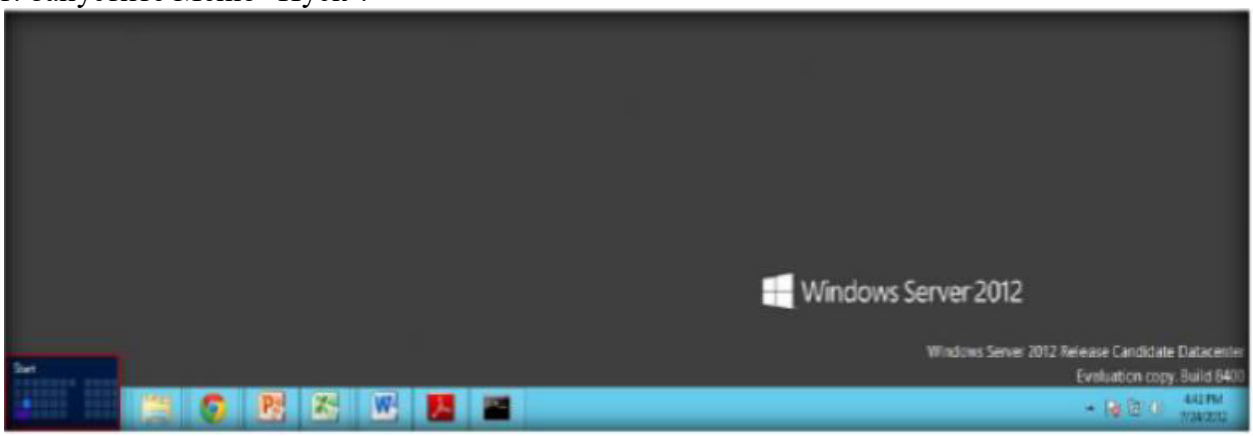


РИСУНОК 18.1: Windows Server 2012 – Рабочий стол

2. В Меню "Пуск" щелкают по значку Dude.

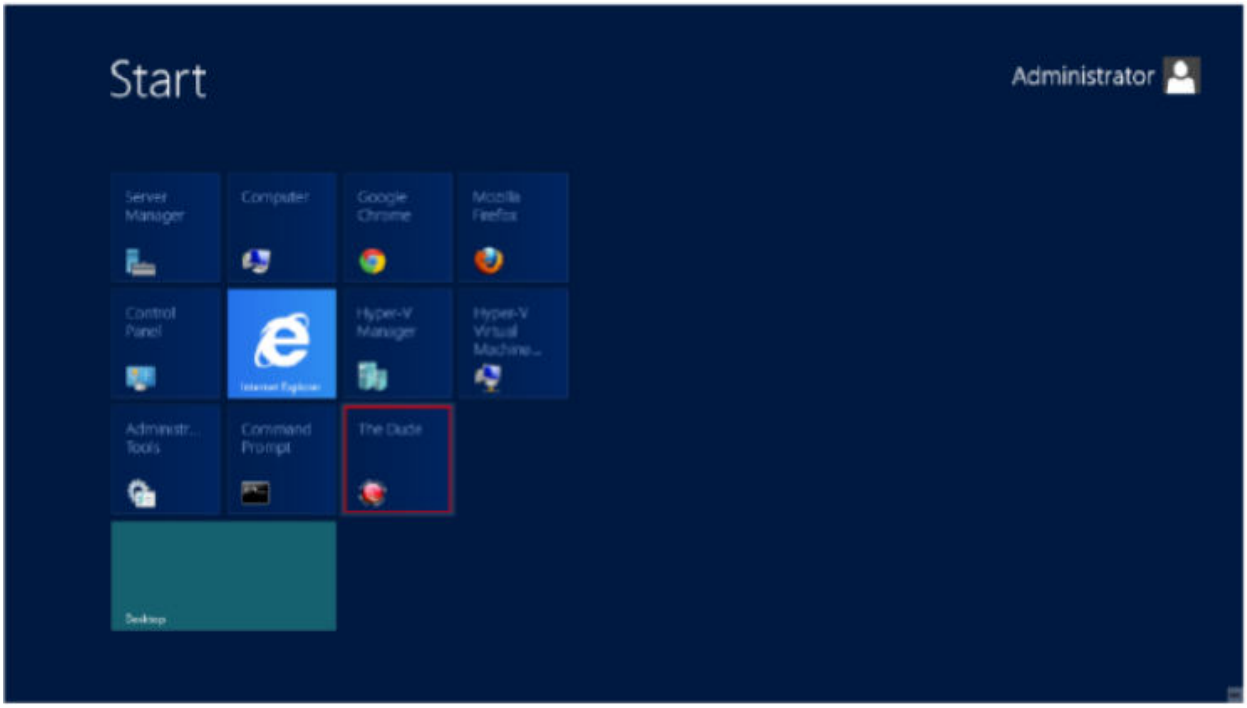


РИСУНОК 18.2Windows Server 2012 - Меню "Пуск"

3. Появится главное окно Dude.

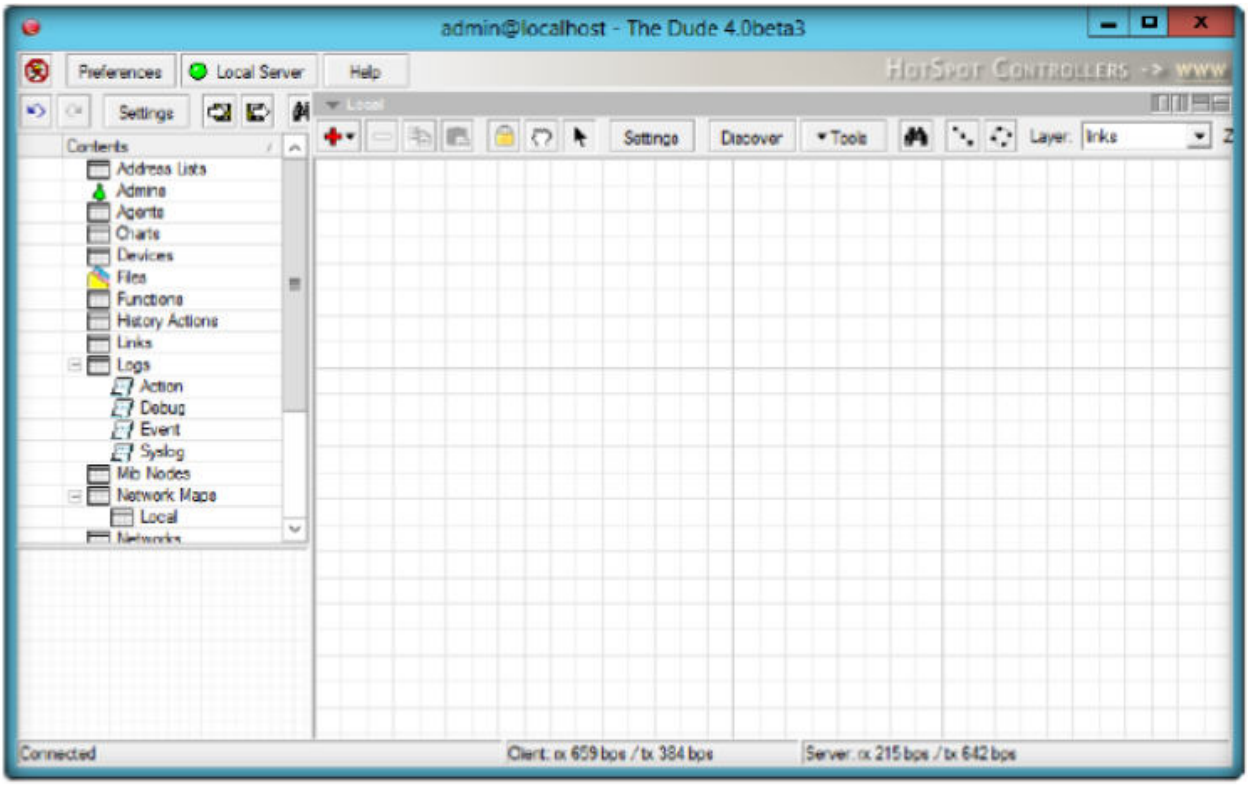


РИСУНОК 18.3: Главное окно Dude

4. Нажмите кнопку «Discover» на панели инструментов главного окна.

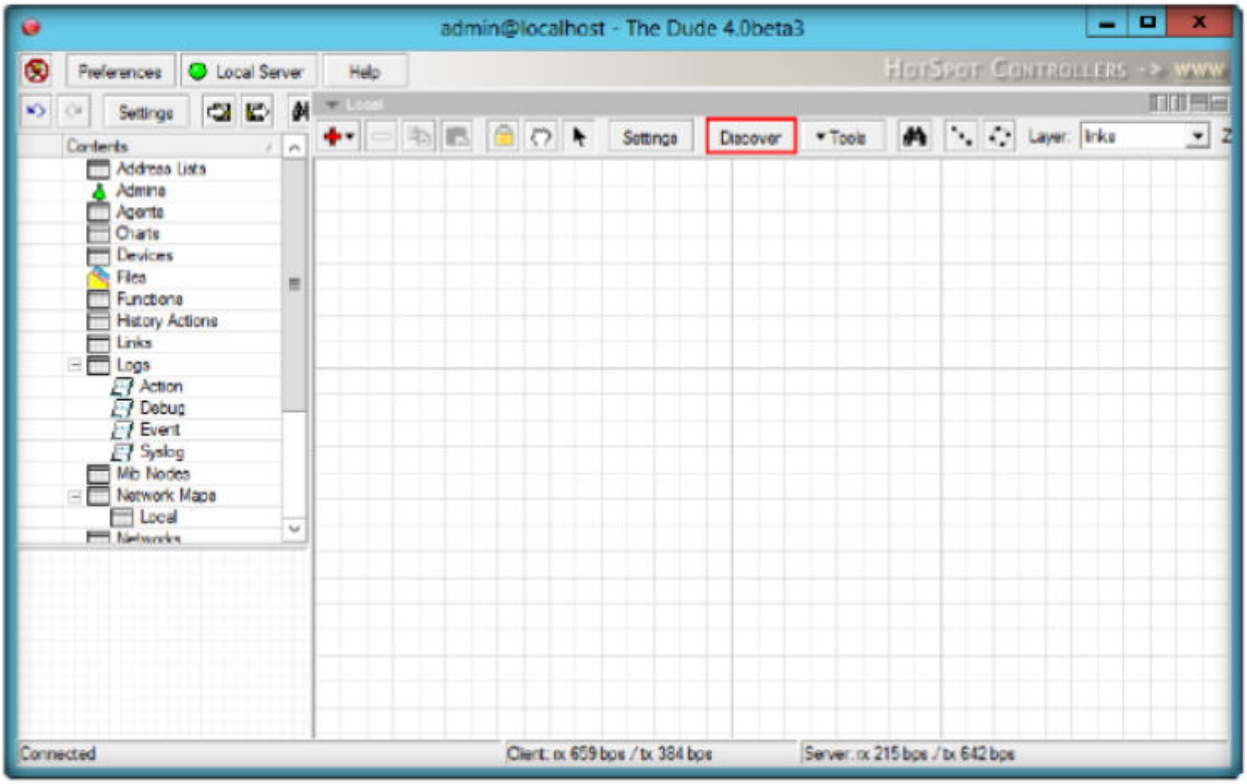


РИСУНОК 18.4: Кнопка «Discover»

5. Появится окно Device Discovery.

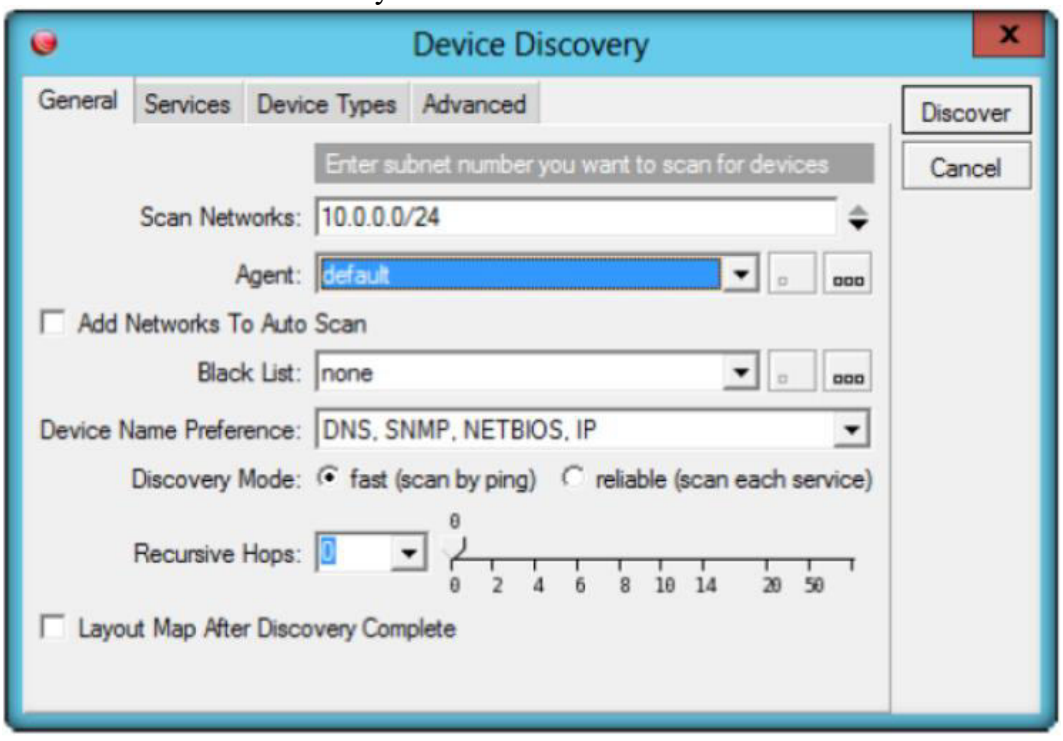


РИСУНОК 18.6: Окно Device Discovery

6. В окне Device Discovery определите диапазон Сетей Сканирования, выберите значение по умолчанию из выпадающего списка «Agent», выберите DNS, SNMP, NETBIOS и IP из выпадающего списка «Device Name Preference», и нажмите «Discover».

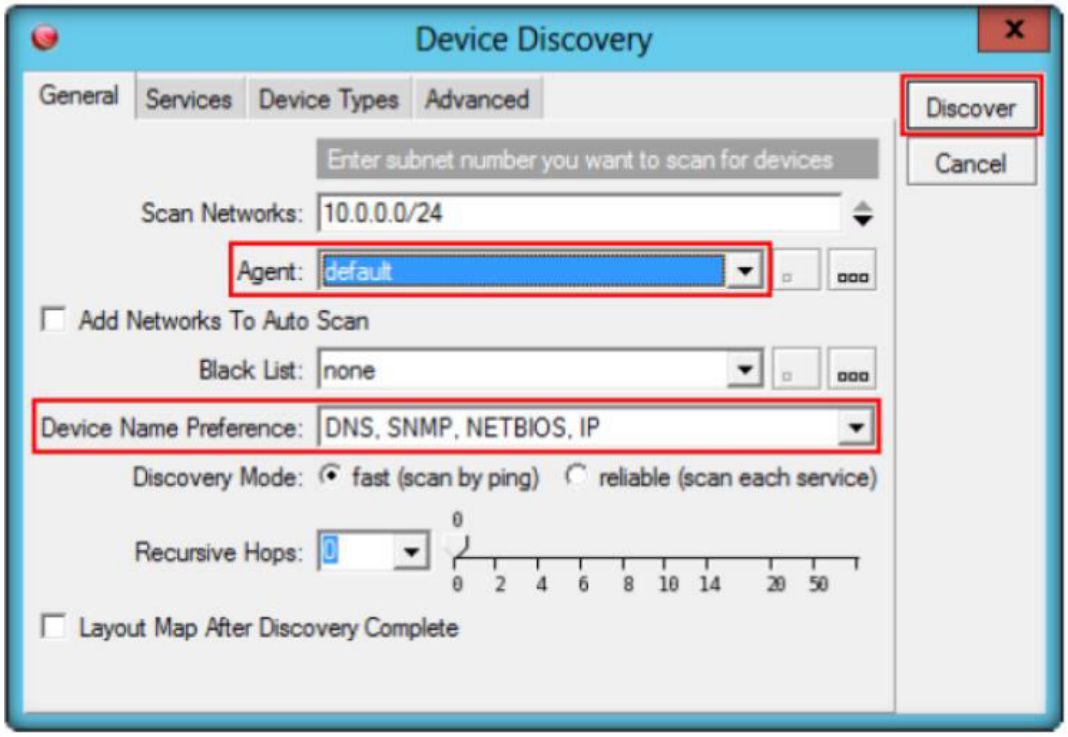


РИСУНОК 18.7: Выбор имени устройства

7. Как только сканирование завершится, все устройства, соединенные с определенной сетью, будут выведены на экран.

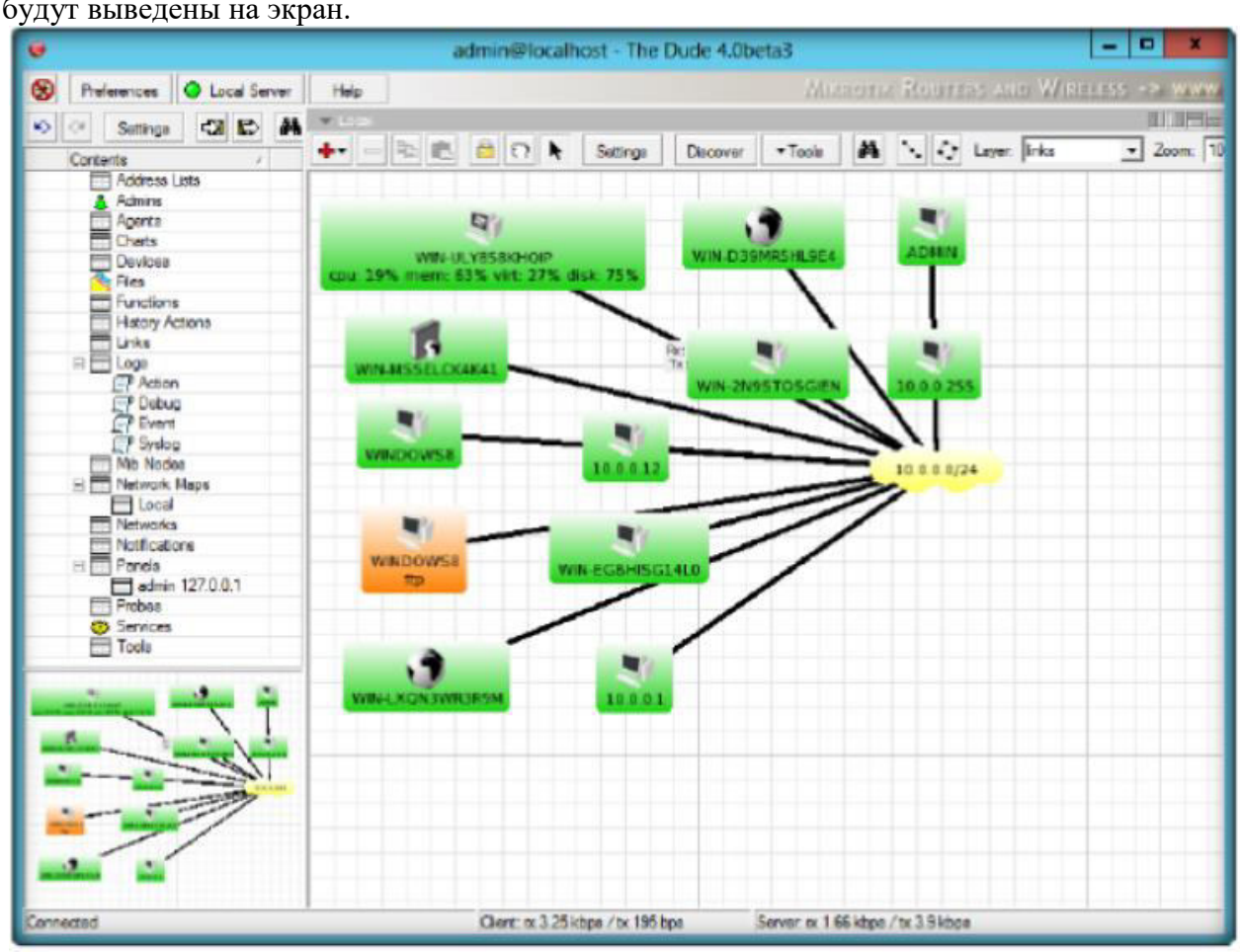


РИСУНОК 18.8: Обзор сетевого соединения

8. Выберите устройство и установите курсор мыши на него, чтобы вывести на экран подробную информацию об устройстве.

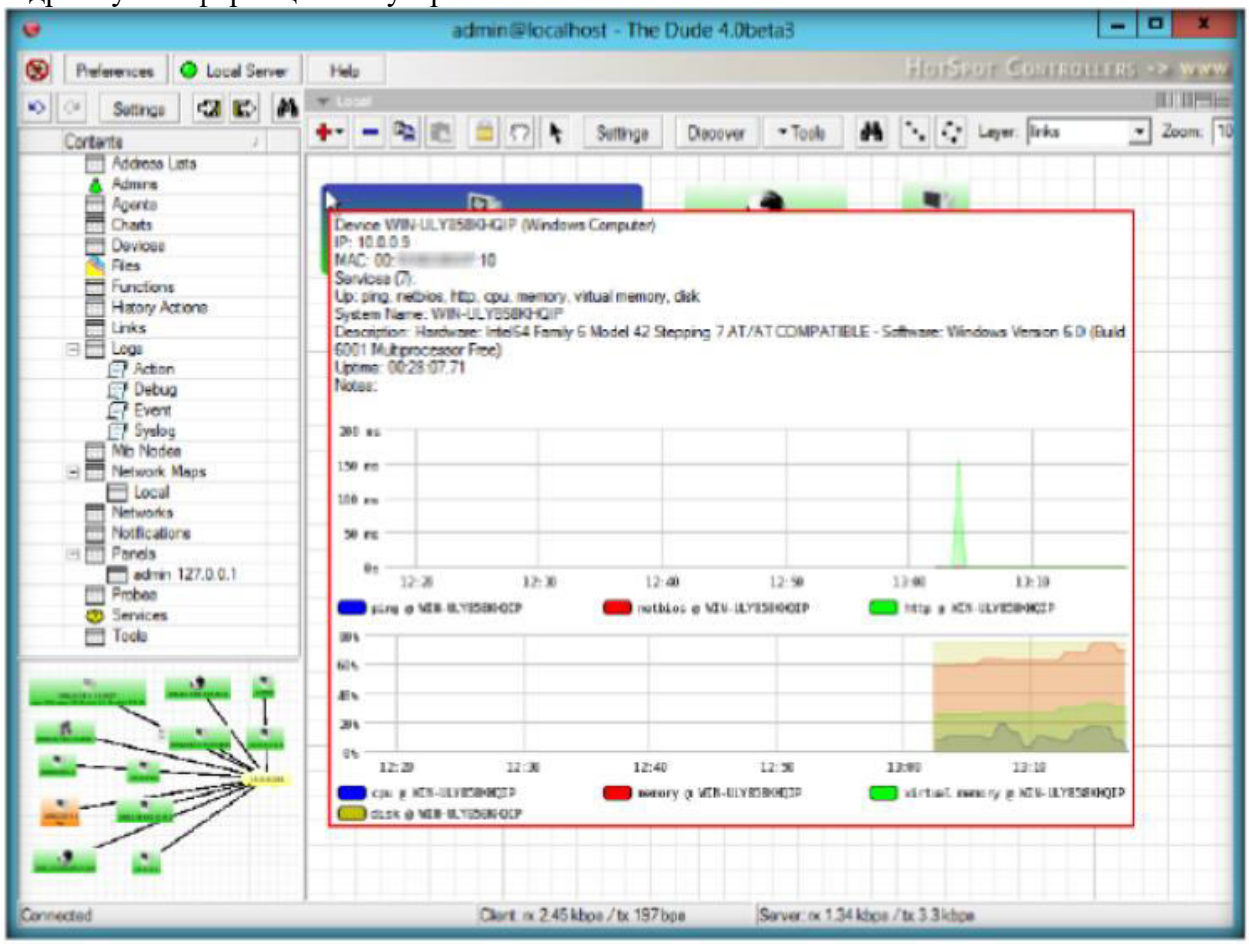


РИСУНОК 18.9: Подробная информация устройства

9. Теперь, щелкните по стрелке вниз. Из локального выпадающего списка можно увидеть информацию о «History Actions» (действиях истории), «Tools» (Инструментах), «Files» (Файлах), «Logs» (Регистрациях) и т.д.

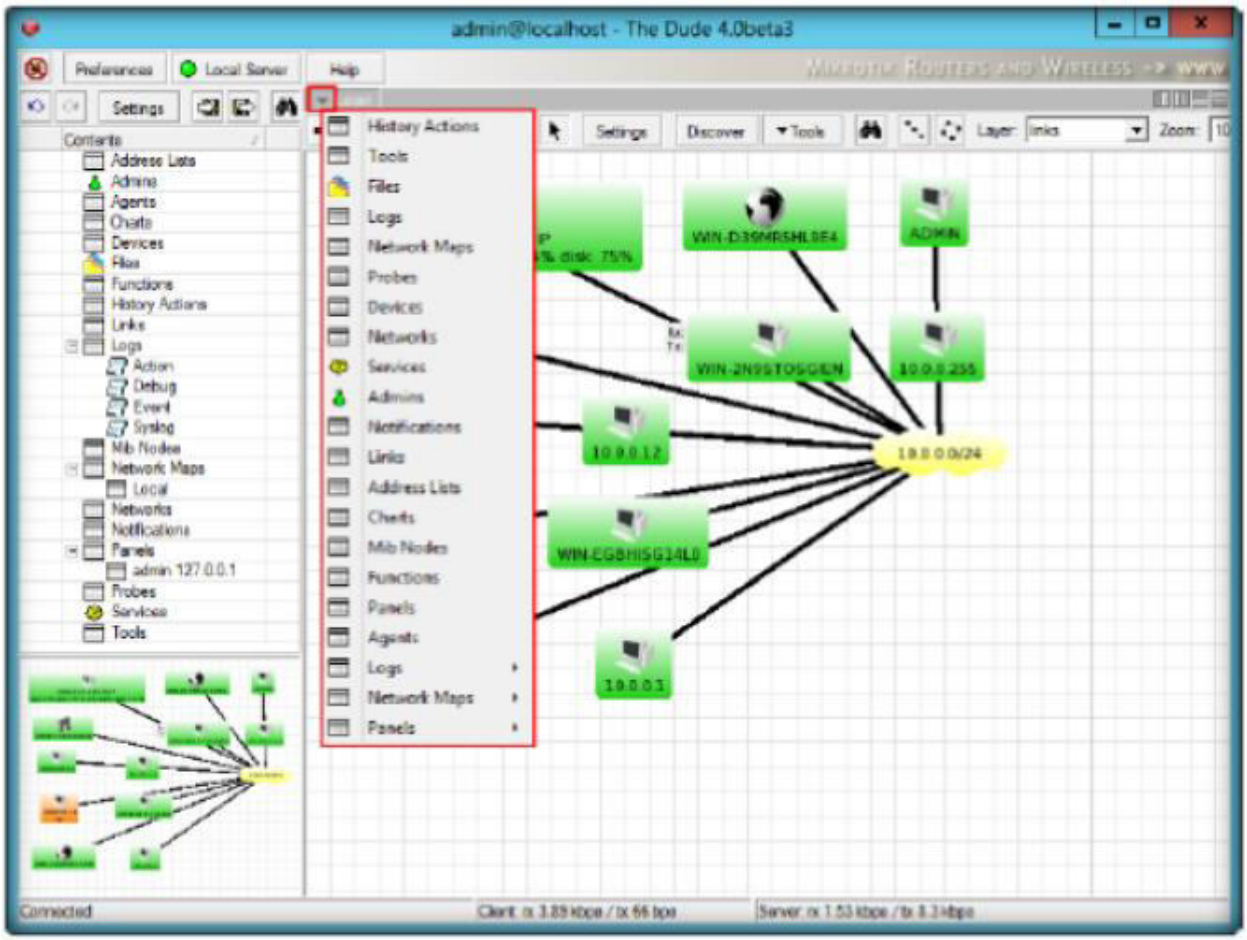


РИСУНОК 18.10: Выбор локальной информации

10. Выберите опции из выпадающего списка, чтобы просмотреть полную информацию.

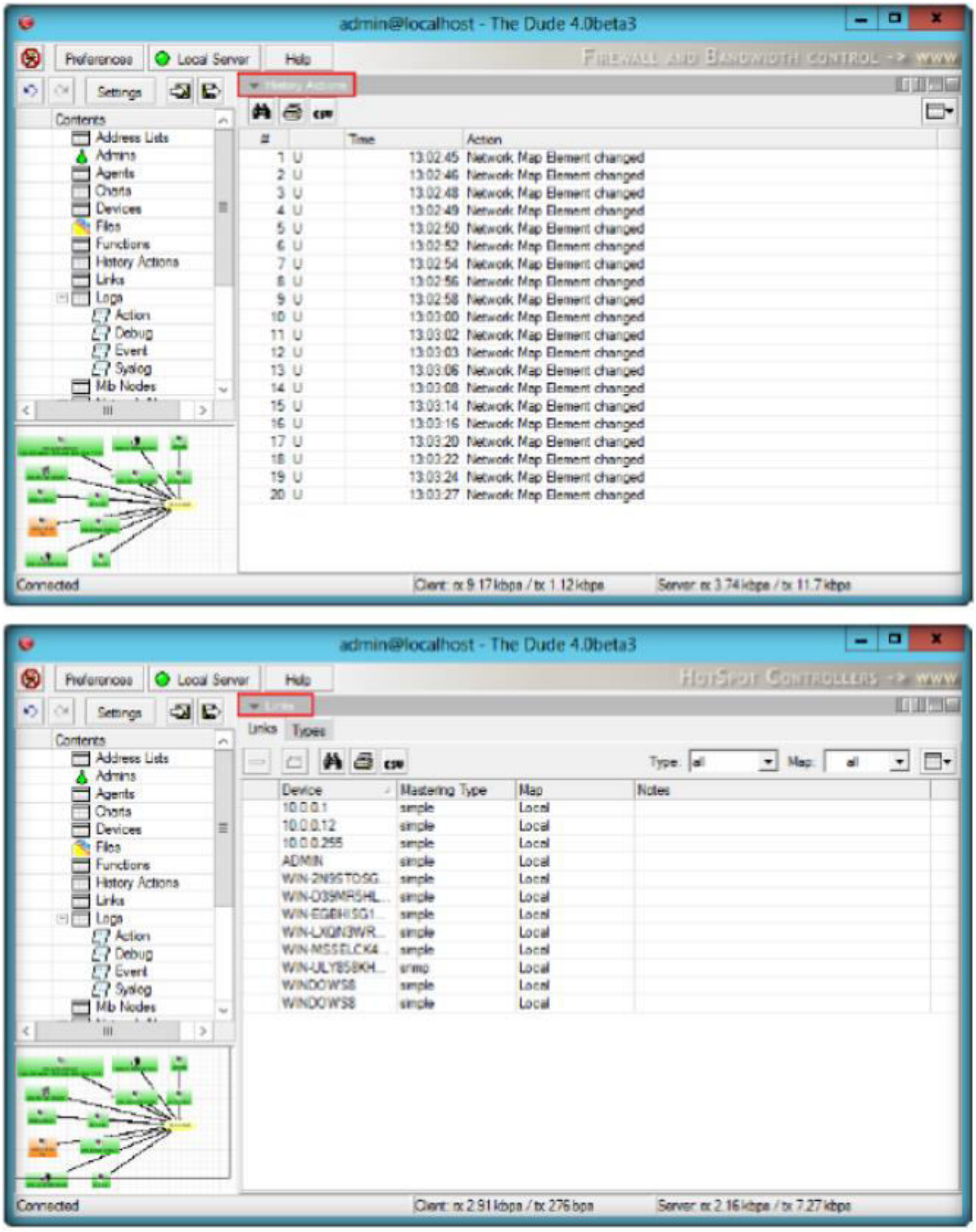


РИСУНОК 18.11: Полная отсканированная сетевая информация

11. Как описано ранее, Вы можете выбрать все другие опции из выпадающего списка, чтобы просмотреть соответствующую информацию.

12. Как только сканирование завершится, щелкните по кнопке  , чтобы разъединиться.

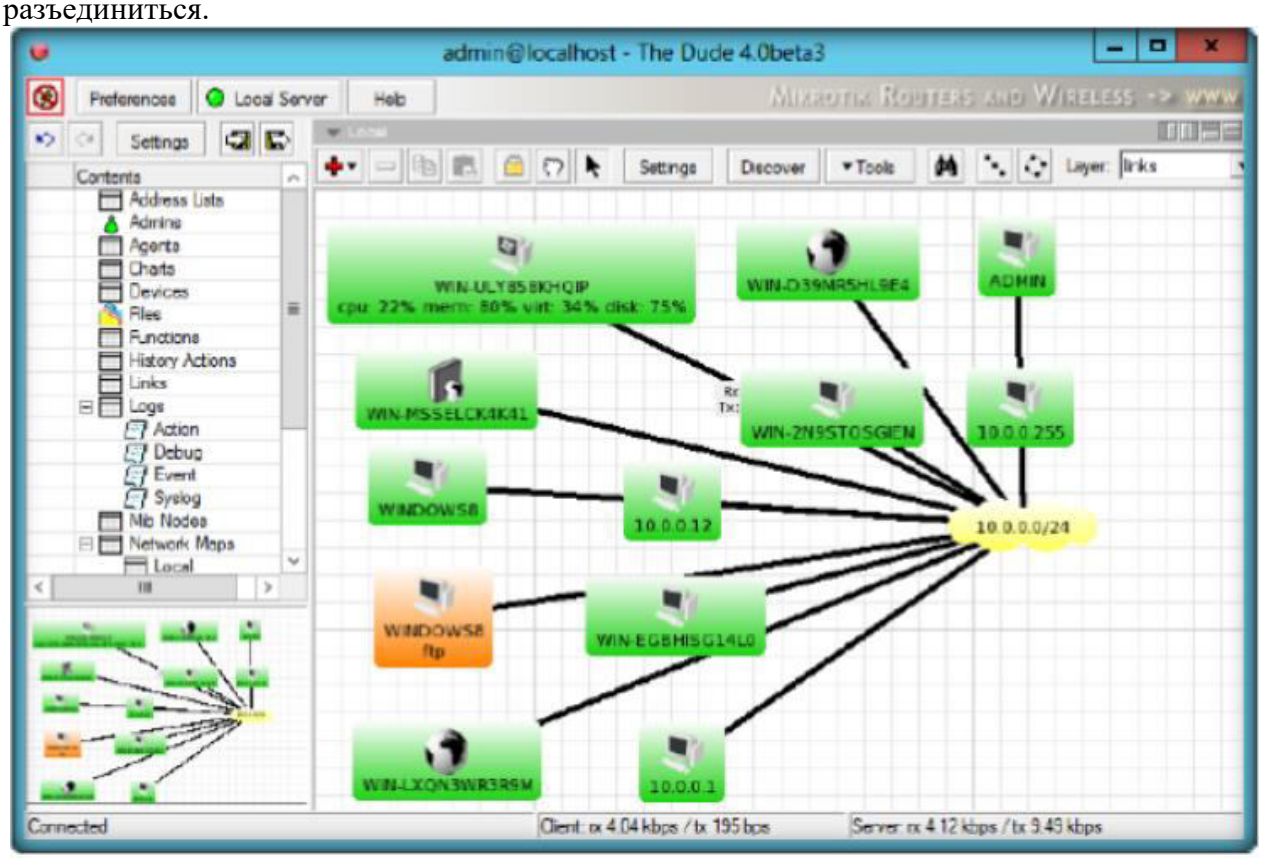


РИСУНОК 18.12 Соединение систем в сети

Анализ практической работы

Проанализируйте и запишите результаты, связанные с осуществлением практической работы.

Инструмент/Утилита	Собранная информация / Достигнутые цели
Dude	**Диапазон IP-адреса:** 10.0.0.0 - 10.0.0.24
	Предпочтительные имена устройств: DNS, SNMP, NetBIOS, IP
	Вывод: Список связанной системы, устройств в сети

ПОГОВОРИТЕ СО СВОИМ ПРЕПОДАВАТЕЛЕМ, ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО ДАННОЙ ПРАКТИЧЕСКОМУ

ИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы по дисциплине
«Анализ уязвимостей программного обеспечения»
для студентов направления подготовки 10.04.01 «Информационная безопасность»
(направленность (профиль) “Математическое и программное обеспечение защиты информации”)

Ставрополь2025 г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации

по организации самостоятельной работы обучающихся
по дисциплине «АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ»
для студентов направления подготовки /специальности
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

СОДЕРЖАНИЕ

Введение

Целью изучения дисциплины «Анализ уязвимостей программного обеспечения» является получение теоретических знаний о принципах построения и архитектуре современных операционных систем, обеспечивающих организацию вычислительных процессов в корпоративных информационных системах экономического, управленческого, производственного, научного и другого назначения, а также практических навыков по созданию (настройке) вычислительной среды в корпоративных сетях (интрасетях) предприятий.

Задачи курса:

– формирование фундаментальных знаний обеспечивающих разработку и эксплуатацию программного обеспечения компьютерных сетей, автоматизированных систем, вычислительных комплексов;

– формирование практических навыков разработки и эксплуатации программного обеспечения компьютерных сетей.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Структура и компонентный состав компетенций.

Перечень компонентов	Технологии формирования компетенции	Средства и технологи и оценки
Знать: классификацию уязвимостей программного обеспечения. Уязвимости системного и прикладного ПО	Лекции, практические занятия. Самостоятельная работа	Собеседование, решение типовых задач, тестирование
Уметь: обнаруживать уязвимости ПО, проводить анализ уязвимостей в исходных кодах ПО.	Практические занятия Самостоятельная работа	Собеседование, тестирование, решение типовых задач,
Владеть: методами поиска уязвимостей в ПО, методами и средствами автоматизированного тестирования ПО.	Практические занятия Самостоятельная работа	Собеседование, тестирование, решение типовых задач,

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области теории сложности комбинаторных алгоритмов. На лабораторных работах и практических занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные

пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям и тестовые задания, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

– самостоятельное изучение учебного материала по заданным темам;

– подготовка к практическим занятиям, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображение структуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы;

– тестирование в программе компьютерного тестирования «Iren»;

3) для формирования умений:

– подготовка к лабораторным занятиям;

– решение задач и практических заданий;

– подготовка отчетов по лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы студента

№	Вид деятельности	Итоговый	Средства и	Обьем

	студентов	продукт самостоятельной работы	технологии оценки	часов
7 семестр				
1	Изучение литературы по темам лекций № 1-18	Конспект	Собеседование, тестирование	20
2	Подготовка к практическим занятиям	Отчеты по самостоятельному решению задач индивидуального задания	Самостоятельное решение задач по вариантам инд.задания	20
3	Подготовка к практическим занятиям	Отчеты по самостоятельному решению задач индивидуального задания	Собеседование, тестирование	10
Итого за 2 семестр				54

3. Самостоятельное изучение тем лекций

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополни-тельная	Методи-ческая	Интернет-ресурсы
1	Тема: Методы поиска уязвимостей в программном обеспечении.	1-4	1-3	1	
2	Тема: Средства статического и динамического анализа.	1-4	1-3	1	
3	Тема: Статические и динамические методы анализа уязвимостей в исходных кодах ПО.	1-4	1-4	1	

4. Паспорт фонда оценочных средств для проверки самостоятельной работы

□ □/□	№ темы	Тип контроля	Вид контроля	Количество элементов, шт.	
				Базовый	Повышенный
1	1-3	текущий	Вопросы для собеседования по самостоятельному изучению тем дисциплины	6	6
2	2-5	текущий	Вопросы для собеседования по самостоятельному изучению	5	2

			тем дисциплины		

5. Вопросы для собеседования по самостоятельному изучению темдисциплины

Базовый уровень

1.Каково назначение команд и директив языка ассемблера?

2.Перечислите арифметические команды с целочисленнымиоперандами и дайте их назначение.

3.Куда помещается результат при умножении двухбайтовыхоперандов? Какой операнд берется по умолчанию при умножении однобайтовых операндов? двухбайтовых? четырехбайтовых?

4.Где находится делимое при целочисленном делении операндов?Куда помещаются неполное частное и остаток при делении целочисленных операндов?

Повышенный уровень

1.Каким образом осуществляется создание проекта в редакторе Quick Editor ассемблера MASM32?

2.Какие директивы описывают начало сегментов кода и данных в программе на языке ассемблера MASM32?

3.Что называется точкой входа в программу? Каким образом в программах на языке ассемблера определяется точка входа?

4.С помощью каких команд осуществляется вызов процедуры и возврат из процедуры в программах на языке ассемблера?

5.Какие суффиксы употребляются для данных, представленных в различных системах счисления?

6.Каково назначение макросов `sstr$`, `ustr$` и `uhex$`?

7. Чем отличаются выполняемые функции директив `include` и `includelib`?

Базовый уровень

1. В чем отличие между дизассемблером и отладчиком?

2. Каковы основные и дополнительные возможности интерактивного дизассемблера IDA Pro?

3. Каким образом выполняется дизассемблирование исполняемых модулей формата PE в IDA Pro?

Повышенный уровень

1. Для чего используется граф вызова процедур и как он может быть построен в IDA Pro?
2. Как найти точку входа программы в IDA Pro?
3. Как осуществляется отладка программы в IDA Pro?

Критерии оценки для проверки уровня обученности:

Оценка «отлично» выставляется студенту, если студент показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок.

Оценка «хорошо» выставляется студенту, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка.

Оценка «удовлетворительно» выставляется студенту, если студент

показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме; были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует ответ на вопрос, либо студент отказался его сдавать.

6. Список рекомендуемой литературы

Основная литература:

Проскурин В.Г. Защита программ и данных.-М.: Академия, 2012

Дополнительная литература:

ГОСТ 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.- М. Стандартинформ,2015

Методическая литература:

1. Методические пособия по дисциплине

Интернет-ресурсы:

1. http://www.anti-virus.by/
2. http://www.linuxrsp.ru/
3. http://www.interface.ru/
4. http://www.computerinform.ru/
5. http://www.windows.ru/

Программное обеспечение:

1. Операционные системы UNIX, Windows, LINUX, IBM

Материально-техническое обеспечение дисциплины

1. Мультимедийная лекционная аудитория № 431.

2. Аудитории, оснащённые компьютерами с установленным требуемым программным обеспечением, для проведения лабораторных работ .