

НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ PXE BOOT НА БАЗЕ WINDOWS SERVER. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. Рассматривается настройка и функциональное тестирование технологии PXE boot на базе Windows Server с акцентом на безопасность сетевой загрузки. Цель исследования состоит в анализе рисков, возникающих из-за использования протоколов DHCP и TFTP, отсутствия встроенной аутентификации и передачи критических параметров загрузки по сети, а также в практической проверке меры защиты на основе сегментации. В работе систематизированы сценарии MITM-атак, Rogue DHCP, DHCP Starvation, TFTP Flood, TFTP File Injection и перезаписи DHCP-опций, приведены условия их реализации, возможные последствия и применяемые инструменты.

Экспериментальная часть выполнена на виртуальном стенде, развернутом на базе KVM в среде Proxmox VE. Сервер Windows Server 2019 выполнял роли DHCP и Windows Deployment Services, а клиентская виртуальная машина использовалась для проверки полного цикла PXE boot. Функциональное тестирование подтвердило выдачу сетевых параметров, получение загрузочного файла от WDS и запуск установки операционной системы. Дополнительно продемонстрирован сценарий Rogue DHCP, при котором клиент принимал подмененные сетевые параметры от постороннего DHCP-сервера.

Для снижения рисков PXE-инфраструктура была вынесена в отдельный VLAN с собственным DHCP-пулом и ограниченным доступом. Проверка показала, что клиент вне PXE-VLAN не получает PXE-ответов, а после назначения соответствующего VLAN успешно выполняет сетевую загрузку. Полученные результаты подтверждают практическую эффективность сетевой сегментации для ограничения доступа к широкополосному DHCP/TFTP-трафику и уменьшения поверхности атаки. В качестве дополнительных мер защиты рекомендуется применять DHCP Snooping, контроль доступа и аутентификацию, а также аудит событий инфраструктуры Windows Server.

Ключевые слова: PXE boot, DHCP, WDS, сетевая безопасность, VLAN-сегментация, TFTP.

Введение

В эпоху цифровизации и роста киберугроз технология PXE (Preboot eXecution Environment) boot в инфраструктуре Microsoft Windows Server остается ключевым инструментом для автоматизированного развертывания операционных систем в корпоративных сетях, обеспечивая сетевую загрузку устройств без локальных носителей. PXE зависит от протоколов DHCP и TFTP, которые используют UDP. Кроме того, у PXE нет встроенной системы аутентификации. Это делает ее уязвимой для различных атак, включая MITM (Man-in-the-Middle), DoS (Denial of Service) и подмену загрузочных образов.

В последнее время участились случаи компрометации инфраструктурных сетей через rogue-серверы, что делает эту проблему особенно актуальной для таких отраслей, как энергетика и IT, где устойчивость к киберугрозам критична для непрерывности бизнеса. PXE boot представляет собой стандарт для сетевой загрузки, интегрированный с DHCP-запроса клиента (DORA: Discover-Offer-Request-Acknowledge), за которым следует передача загрузочного файла (boot.wim) через TFTP порт 69. В Windows Server эта технология поддерживает опции DHCP 066 (Boot Server Host Name) и 067 (Bootfile Name), обеспечивая seamless-интеграцию с WDS для распределения образов ОС.

Модель безопасности PXE строится на принципах CIA (Confidentiality, Integrity, Availability) с особым вниманием к аутентификации. Для этого применяются DHCP Snooping на коммутаторах, авторизация через Active Directory (AD) и аудит событий в Event Viewer. Анализ уязвимостей по CVE выявляет риски, влияющие на PXE, такие как CVE-2020-1350 (ZeroLogon) для эскалации привилегий и CVE-2018-8320 (LLMNR) для spoofing, которые могут привести к подмене загрузочных процессов. В соответствии с нормативными требованиями ФСТЭК России, включая Федеральный закон № 149-ФЗ (об информации), № 152-ФЗ (о персональных данных), а также Приказы № 17 (ГИС), № 21 (ИСПДн) и № 239 (КИИ),

необходимо шифровать трафик, проводить аудит и сегментировать сеть для предотвращения несанкционированного доступа.

Технология PXE boot в Windows Server подвержена уязвимостям из-за использования UDP при атаках и отсутствия аутентификации в большинстве реализаций. Данные уязвимости можно разделить на классы: MITM-атаки, DoS-атаки и атаки на целостность данных.

Таблица 1 – Атаки на PXE boot

Тип атаки	Описание	Условия	Последствия	Инструменты
MITM через ARP-spoof (DHCP/TFTP)	Отравление ARP-кэша для перехвата PXE-трафика и подмены ответов.	Доступ к L2, отсутствие DAI.	MITM, подмена загрузочных файлов, вредоносная ОС.	Etercap 0.8.3.1- Bertillon, Scapy 2.7.0
Rogue DHCP (Options 66/67)	Навязывание ложного TFTP-сервера через поддельный DHCP.	Broadcast-доступ, нет авторизации DHCP.	On-path MITM для PXE, подмена WDS.	Dhcpig 1.6, Yersinia 0.8.2
IPv6 MITM: rogue RA/DHCPv6	Рассылка RA/DHCPv6 для навязывания параметров PXE.	Включенный IPv6, отсутствие RA Guard.	Полный MITM для сетевой загрузки в IPv6.	Mitm6 0.3.0.
DHCP Starvation	Исчерпание пула адресов поддельными запросами.	Доступ к сети, слабый мониторинг.	DoS, невозможность PXE-загрузки для новых устройств.	Yersinia 0.8.2, Gobbler 2.0.1
TFTP Flood	Флуд запросами на TFTP для перегрузки WDS.	Открытый TFTP, отсутствие rate-limiting.	DDoS, downtime развертывания ОС.	Hping3-0.0.20051105-alt8, custom scripts.
TFTP File Injection	Внедрение фальшивых файлов в PXE-процесс.	MITM-позиция, отсутствие подписи.	Подмена образов ОС, установка malware.	Scapy 2.7.0
DHCP Option Overwrite	Перезапись опций (66/67) в ответах.	Отсутствие защиты, broadcast-доступ.	Подмена boot-файлов, несанкционированное развертывание.	Scapy 2.7.0

Для иллюстрации процесса PXE boot предлагается схема на рисунке 1, построенная с использованием PlantUML.

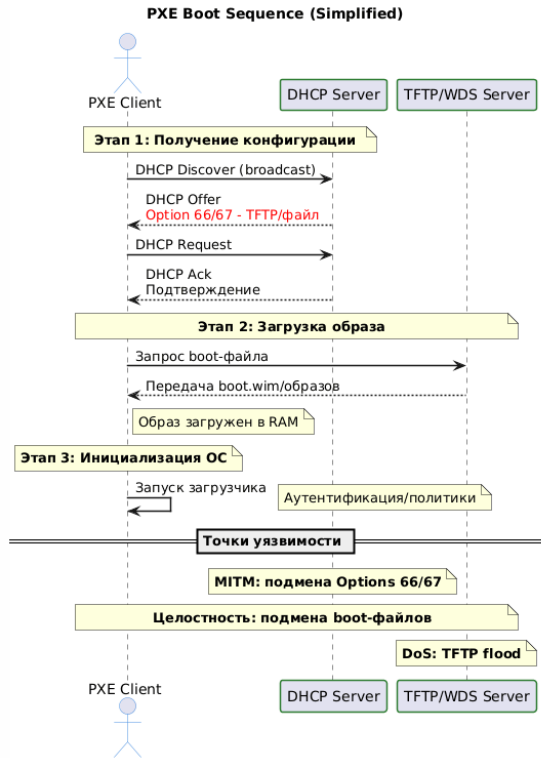


Рис. 1. Процесс PXE boot

Представленная схема последовательности визуализирует стандартизированный процесс сетевой загрузки PXE (Preboot eXecution Environment), который включает три

Рубрика 2. Методы и системы защиты информации, информационная безопасность

ключевых этапа взаимодействия между компонентами инфраструктуры. На первом этапе клиентское оборудование инициирует широковещательный DHCP Discover запрос, на который DHCP-сервер реагирует предложением сетевых параметров, включая критические опции 66 (адрес TFTP-сервера) и 67 (имя загрузочного файла). Данная фаза представляет собой наиболее уязвимую точку для атак типа «man-in-the-middle», поскольку злоумышленник может осуществить подмену параметров загрузки через rogue DHCP-сервер или посредством модификации легитимных DHCP-ответов.

Второй этап предполагает непосредственную загрузку исполняемых компонентов операционной системы через протокол TFTP, характеризующийся отсутствием механизмов аутентификации и криптографической защиты целостности передаваемых данных. Эта особенность делает возможными атаки на целостность, включая инъекцию вредоносного кода в загрузочные образы и полную подмену файлов в процессе передачи. Третий этап инициализации ОС, хотя и не детализирован в схеме в полном объеме, потенциально подвержен компрометации через уязвимости сопутствующих служб, что может привести к несанкционированному доступу или нарушению политик безопасности.

Схематически обозначенные точки уязвимости коррелируют с ранее описанными классами атак: подмена DHCP-опций соответствует MITM-атакам типа «Rogue DHCP», угроза целостности загрузочных файлов реализуется через «TFTP File Injection», а возможность перезагрузки TFTP-сервера флуд-атаками приводит к нарушению доступности службы сетевой загрузки.

Объектом исследования является инфраструктура PXE boot, реализованная в ОС Windows Server. Предметом – уязвимости, атаки и меры защиты, которые применяются в процессе настройки и тестирования рассматриваемой инфраструктуры. Целью исследования является анализ потенциальных угроз и разработка рекомендаций, направленных на обеспечение безопасности при использовании PXE boot.

Количество исследований, посвященных настройке и функциональному тестированию PXE boot на базе Windows Server с акцентом на вопросы безопасности, остается ограниченным. В основном доступна лишь официальная документация Microsoft по WDS и интеграции с DHCP [1,2]. Кроме того, есть статьи, в которых описываются общие принципы сетевой загрузки и меры защиты от атак на broadcast-протоколы в Windows-системах [3,4,5]. Но научных работ, посвященных экспериментальному анализу уязвимостей PXE в виртуальной среде и симуляцией атак с использованием инструментов, таких как Yersinia или Scapy, практически не проводилось. Это подчеркивает актуальность данной темы в условиях возрастающих киберугроз [6].

Для реализации поставленной цели был проведен детальный анализ технической документации, которая направлена на сетевую загрузку. На виртуальном стенде с Windows Server были выполнены тестовые настройки, включающие моделирование PXE boot и проверку мер безопасности. Для этого на компьютере с процессором Intel Core i7 и оперативной памятью 16 ГБ был развернут виртуальный стенд на базе гипервизора KVM, реализованного в среде Proxmox VE. Внутри нее были развернуты виртуальные машины: сервер с Windows Server 2019 и клиентская машина. Виртуальным машинам были выделены параметры: оперативная память 2048 МБ, 2 процессора, порядок загрузки с приоритетом сети, видеопамять 16 МБ, а также VDI-диск размером 60 ГБ. Эти параметры обеспечили достаточную производительность для настройки ролей, тестирования PXE и оценки уязвимостей без дополнительных сложностей.

Результаты исследования

В статье сначала исследуются риски, связанные с протоколами DHCP и TFTP, включая атаки типа MITM, DoS и подмену загрузочных образов, а также анализируются конкретные уязвимости (CVE), актуальные для Windows Server. Для проверки этих теоретических угроз и оценки эффективности мер защиты был проведен эксперимент в виртуальной среде, имитирующей корпоративную сеть. Настройка ролей DHCP и WDS на Windows Server

позволила воспроизвести реальный процесс PXE boot, включая этапы DORA и передачу загрузочных файлов через TFTP.

В рамках практической части исследования по настройке и функциональному тестированию PXE boot на базе Windows Server была использована виртуальная среда, имитирующая типичную корпоративную сеть с элементами удаленного развертывания операционных систем. Топология включает центральный сервер под управлением Windows Server, выполняющий роли DHCP-сервера и сервера Windows Deployment Services (WDS), а также клиентскую виртуальную машину, предназначенную для тестирования сетевой загрузки. Сервер и клиент соединены в изолированной виртуальной сети (например, с использованием гипервизора вроде Hyper-V или Proxmox VE), где сервер выступает в качестве источника IP-адресов и загрузочных образов, а клиент – в роли устройства, инициирующего PXE-запросы. Это обеспечивает контролируемую среду для демонстрации процесса сетевой загрузки без внешних помех, с акцентом на broadcast-трафик протоколов DHCP и TFTP.

На рисунке 2 изображена общая схема топологии сети, где сервер Windows Server (с IP-адресом из пула DHCP) подключен к виртуальному коммутатору, а клиентская виртуальная машина настроена на сетевую загрузку (PXE boot) без локального диска, что позволяет наблюдать полный цикл DORA (Discover-Offer-Request-Acknowledge) с последующей передачей загрузочного образа.

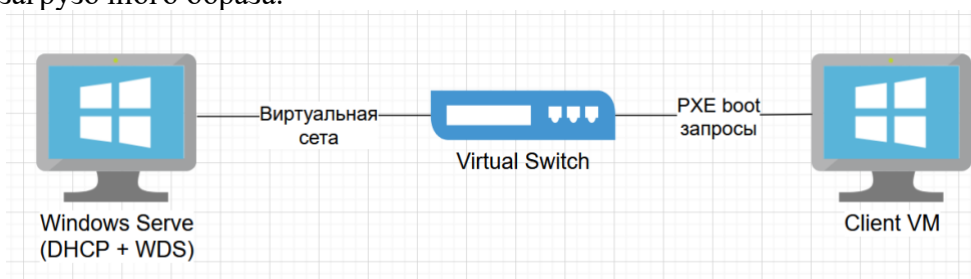


Рис. 2. Топология сети

Данная топология выбрана для минимизации внешних факторов и фокусировки на уязвимостях, связанных с отсутствием аутентификации в протоколах PXE и DHCP, что делает систему подверженной атакам типа rogue DHCP или MITM. В реальной среде такая конфигурация может быть расширена на несколько подсетей с использованием DHCP Relay Agent, но в эксперименте использована единая L2-сегментация для упрощения тестирования.

Клиентская машина, в свою очередь, инициализирует загрузку по сети, запрашивая сначала IP-адрес через DHCP, а затем – загрузочный файл через TFTP, что интегрируется с WDS для предоставления образов ОС. Это позволяет оценить функциональность и выявить потенциальные риски безопасности, такие как подмена загрузочных файлов или исчерпание пула адресов.

Суть практической части заключается в развертывании и конфигурировании инфраструктуры сетевой загрузки (PXE) на базе Windows Server. Ключевым этапом является настройка роли DHCP-сервера, которой, помимо базовой функции назначения IP-адресов, делегируется задача предоставления клиентским машинам параметров сетевой загрузки. Это включает в себя определение в DHCP-опциях (Option 66, 67) адреса TFTP-сервера и пути к загрузочному образу. В результате компьютеры, не имеющие локальной операционной системы или инициировавшие загрузку по сети, получают от сервера не только сетевой адрес, но и инструкции, позволяющие автоматически загрузить и установить ОС из централизованного образа.

Процесс ориентирован на корпоративные сценарии, где требуется автоматизированное развертывание операционных систем без физического вмешательства, но с учетом вопросов безопасности, таких как отсутствие встроенной аутентификации и зависимость от UDP-протоколов.

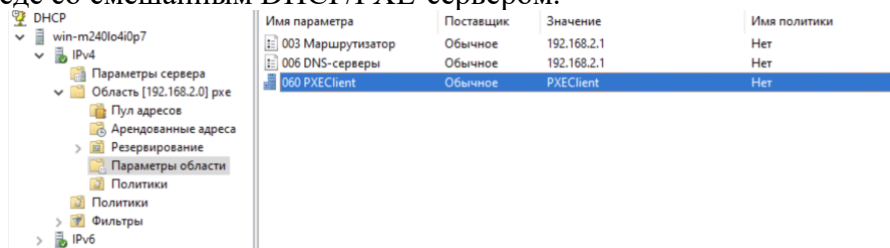
В процессе конфигурации DHCP была создана область адресов, соответствующая адресному пространству экспериментальной сети, а также заданы необходимые параметры, обеспечивающие корректную передачу PXE-клиентам сведений о загрузочном сервере и

Рубрика 2. Методы и системы защиты информации, информационная безопасность

начальном загрузочном образе. Дополнительно были настроены опции DHCP, используемые в сценариях сетевой загрузки, что позволило обеспечить корректное взаимодействие между PXE-клиентами и сервером.

В службе WDS был добавлен загрузочный образ операционной системы, используемый для тестирования процесса сетевой загрузки. Указанные действия являются стандартными для развертывания PXE-инфраструктуры и не представляют самостоятельного исследовательского интереса, в связи с чем далее основное внимание уделяется вопросам сегментации сети и механизмам защиты от сетевых атак.

На рисунке 3 показана конфигурация параметров области DHCP. Помимо стандартных опций (003 – шлюз, 006 – DNS-сервер), задан критически важный параметр 060 (PXEClient) со значением «PXEClient». Это указывает DHCP-серверу на необходимость идентифицировать себя для PXE-клиентов, что является обязательным условием для корректной работы сетевой загрузки в среде со смешанным DHCP/PXE-сервером.



Имя параметра	Поставщик	Значение	Имя политики
003 Маршрутизатор	Обычное	192.168.2.1	Нет
006 DNS-серверы	Обычное	192.168.2.1	Нет
060 PXEClient	Обычное	PXEClient	Нет

Рис. 3. Детальные настройки области DHCP-сервера

Для проведения тестирования создается виртуальная машина без предустановленной операционной системы, настроенная на PXE boot в BIOS/UEFI. Благодаря этому можно наблюдать в реальном времени процесс загрузки. Функциональное тестирование подтверждает корректность настройки: виртуальная машина получает IP-адрес от DHCP, загружает boot-файл от WDS и инициирует установку операционной системы. Таким образом, демонстрируется работоспособность PXE в контролируемых условиях, но также выявляет уязвимости, такие как риск подмены сервера без аутентификации. На рисунке 4 представлен успешный результат загрузки, с отображением меню WDS.

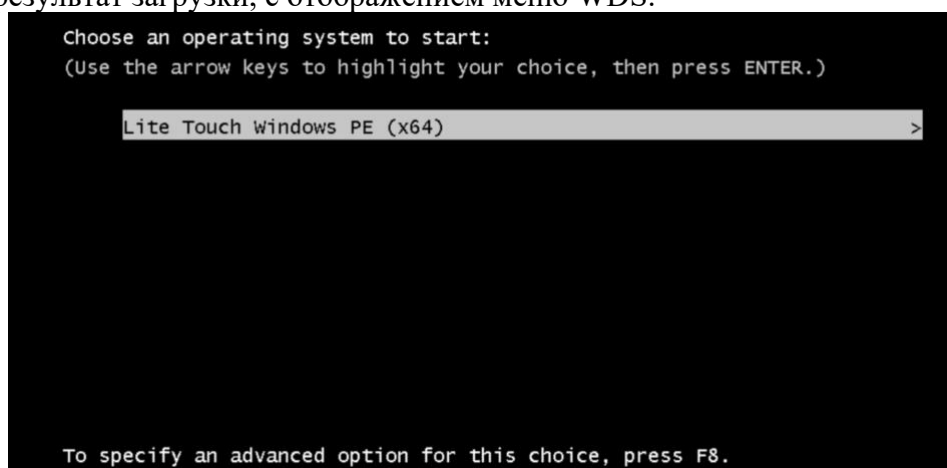


Рис. 4. Создание виртуальной машины

В рамках практической части исследования была продемонстрирована уязвимость PXE boot к атакам типа rogue DHCP и MITM, как описано в таблице 1. Проведем эксперимент, фокусирующийся на внедрении меры защиты через сетевую сегментацию. Этот подход позволяет не только подтвердить риски, но и продемонстрировать практическое решение, повышающее безопасность инфраструктуры в целом.

Для анализа подмены DHCP был поднят левый DHCP-сервер в изолированной сети, и в выводе видно, что клиент действительно ловит ответы на DHCP REQUEST/ACK, что дает возможность подменить параметры (например, серверы или загрузочные файлы). Это демонстрирует потенциальные уязвимости, если сеть не разделена должным образом. Если бы

сеть не была сегментирована, злоумышленник мог бы использовать такую уязвимость для подмены DHCP и дальше манипулировать процессом PXE boot.

```
[*] Please set a network interface for sniffing ARP and DHCP requests ...
[*] Your interface list:
+-----+
| Index | Interface name |
+-----+
| 1     | eth0           |
| 2     | eth1           |
+-----+
[*] Set network interface from range (1-2): 2
[*] Network interface: eth1
[*] Your IP address: 192.168.2.2
[*] Your MAC address: 08:00:27:00:00:00
[*] First offer IP: 192.168.2.2
[*] Last offer IP: 192.168.2.253
[*] DHCP server mac address: 08:00:27:00:00:00
[*] DHCP server ip address: 192.168.2.2
[*] Router IP address: 192.168.2.2
[*] DNS server IP address: 192.168.2.2
[*] TFTP server IP address: 192.168.2.2
[*] Create list with free IP addresses in your network ...
[*] ARP scan on interface: eth1 is running ...
[*] Interface: eth1 ARP scan percentage: 100%
[*] Waiting for a ARP or DHCP request ...
[*] DHCP REQUEST from 08:00:27:00:00:00 requested ip: 192.168.2.3
[*] DHCP ACK to: 08:00:27:00:00:00 192.3
```

Рис. 5. DHCP REQUEST/ACK и возможность подмены параметров в процессе PXE

Эксперимент заключался в создании изолированного VLAN (Virtual Local Area Network) специально для PXE-инфраструктуры. В этой конфигурации все клиентские машины, требующие сетевой загрузки, первоначально подключаются к отдельному VLAN, где работает PXE boot. После успешной загрузки операционной системы MAC-адрес машины добавляется в whitelist (белый список), и устройство автоматически переносится в основной офисный VLAN. Эта настройка обеспечивает, что PXE-процесс происходит в контролируемой, изолированной среде, минимизируя взаимодействие с основной сетью.

Процесс настройки включал следующие действия. Сначала активируется опция VLAN-aware на сетевом оборудовании, что позволяет коммутатору распознать и обрабатывать VLAN-теги для сегментации трафика. Это обеспечивает изоляцию без необходимости в физическом разделении сетей. На рисунке 6 показан процесс активации данной опции в настройках виртуального коммутатора.

Рис. 6. Активация опции VLAN-aware

Далее назначается отдельный VLAN для PXE-сервера (Windows Server с ролями DHCP и WDS). Это включает конфигурацию VLAN ID (например, VLAN 20) для порта сервера, чтобы весь PXE-трафик был ограничен этой виртуальной сетью. На рисунке 7 иллюстрируется назначение VLAN для сервера в интерфейсе виртуализации.

Рис. 7. Назначение VLAN для сервера

Затем создается новая область (scope) в DHCP для изолированного VLAN, с соответствующим пулом IP-адресов (например, 192.168.10.0/24), отличающимся от основной офисной сети. Одновременно изменяется IP-адрес самого сервера на адрес из новой подсети, чтобы он функционировал исключительно в рамках VLAN. Это предотвращает утечку

Рубрика 2. Методы и системы защиты информации, информационная безопасность

broadcast-трафика в другие сегменты. На рисунке 8 представлено создание отдельной области DHCP.

Рис. 8. Создание отдельной области DHCP

На рисунке 9 показан процесс изменения IP-адреса сервера, подтверждающий его интеграцию в изолированный VLAN.

Рис. 9. Изменение IP-адреса сервера

Для проверки работы на клиентской машине изначально проводится тест в основном VLAN: клиент не получает PXE-ответов, и процесс загрузки не запускается, что подтверждает эффективность изоляции. Это демонстрирует, что без доступа к PXE-VLAN атаки, такие как rogue DHCP или MITM, становятся невозможными. На рисунке 10 изображен результат проверки на клиенте без тегирования – отсутствие активности.

```
SeaBIOS (version rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org)
Machine UUID aa6f48cf-8432-42d7-956d-157815548fc3
Booting from Hard Disk...
Boot failed: not a bootable disk

Booting from DVD/CD...
Boot failed: Could not read from CDROM (code 0003)
Booting from ROM...
IPXE (PCI 00:12.0) starting execution...ok
IPXE initialising devices...ok

IPXE 1.20.1+ (q4bd0) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP ISCSI TFTP AoE ELF MBOOT PXE bzImage Menu PXEXT

net0: bc:24:11:72:7f:3c using 82540em on 0000:00:12.0 (open)
(Link up, TX:0 TXE:0 RX:0 RXE:0)
Configuring (net0 bc:24:11:72:7f:3c)..... ok
net0: 192.168.2.13/255.255.255.0 gw 192.168.2.1
Nothing to boot: No such file or directory (http://ipxe.org/2d03e13b)
No more network devices

Press Ctrl-B for the iPXE command line..._
```

Рис. 10. Проверка работы на клиенте без тегирования

Наконец, тегруется порт клиента для доступа к PXE-VLAN (присваивается соответствующий VLAN ID), и проводится повторная проверка. Клиент успешно получает IP

от DHCP в изолированной сети, загружает boot-файл от WDS и инициирует установку ОС. После завершения MAC-адрес добавляется в whitelist (например, через скрипт или AD-политику), и машина переносится в офисный VLAN. На рисунке 11 показана настройка тегирования клиента.

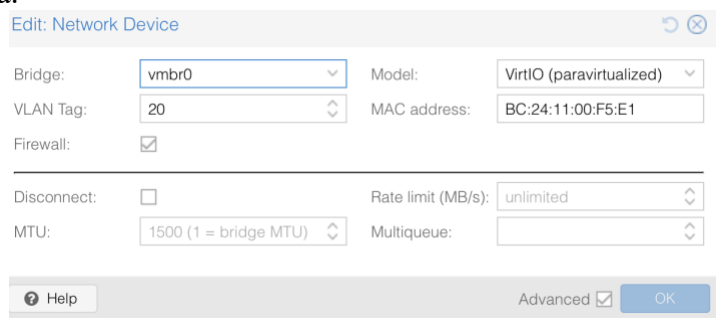


Рис. 11. Тегирование клиента

На рисунке 12 иллюстрируется успешная проверка после тегирования, с отображением процесса PXE boot в изолированной среде.

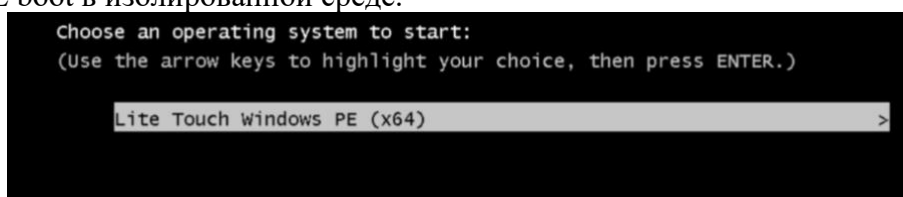


Рис. 12. Проверка работы после тегирования

Для анализа подмены DHCP был поднят левый DHCP-сервер в сегменте VLAN 10 (192.168.2.0/24). Этот сервер начал отвечать клиентам и раздавать им параметры сети (шлюз, DNS, TFTP), так что все указывало на атакующего. В выводе видно DHCP REQUEST/ACK – это означает, что клиент принял неправомерные данные и получил адрес.

На рисунке 13 показан результат такой атаки, где видно, что DHCP клиент действительно получает IP-адрес, назначенный атакующим сервером. Если сеть не нарезана и все в одном L2, то любой злоумышленник может подключить свой DHCP-сервер, начать раздавать параметры и манипулировать PXE-загрузкой, что приводит к потенциальным угрозам безопасности.

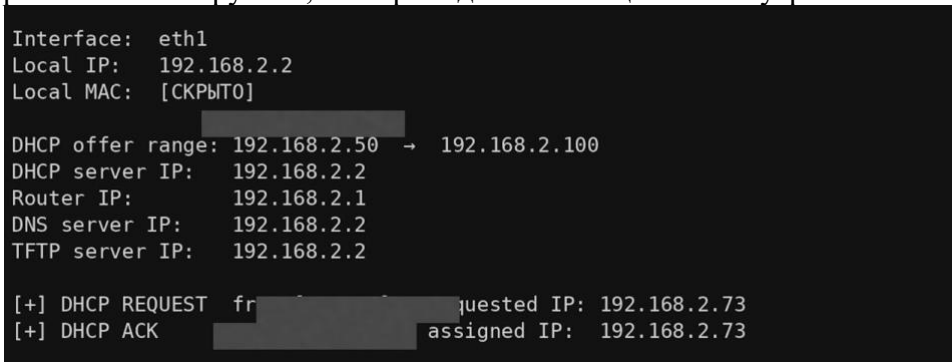


Рис. 13. Пример подмены DHCP с использованием Rogue DHCP сервера в VLAN

Заключение

Проведенная настройка и тестирование PXE boot на базе Windows Server выявили эффективность интеграции DHCP и WDS для автоматизированного развертывания, но также подчеркнули риски безопасности, связанные с UDP-broadcast и отсутствием шифрования. Рекомендуется внедрение мер, таких как DHCP Snooping и аутентификация, для минимизации угроз в производственных сетях.

В ходе эксперимента была продемонстрирована атака с использованием Rogue DHCP, где злоумышленник, поднявший левый DHCP-сервер, мог подменить параметры для PXE-загрузки. Это наглядно продемонстрировало уязвимость в отсутствии сегментации сети. На рисунке 5 показано, как клиент получил подмененные параметры и IP-адрес от атакующего сервера. Эксперимент подтвердил, что такие атаки возможны в незащищенной сети.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Вторая часть эксперимента демонстрирует эффективность сетевой сегментации как комплексной меры защиты, которая предотвращает все типы атак, перечисленных в таблице 1. Изоляция PXE в отдельном VLAN создает «воздушный зазор» на уровне L2/L3, где злоумышленник не может получить доступ к broadcast-трафику DHCP/TFTP без физического или конфигурационного подключения к этому VLAN. Это показывает, что простая сегментация сети может радикально снизить поверхность атаки, делая PXE-инфраструктуру недоступной для внешних угроз.

Как показали результаты эксперимента, после применения изоляции с VLAN атаки типа Rogue DHCP (где злоумышленник подменяет параметры загрузки) и MITM (где атакующий может манипулировать процессом загрузки) были полностью исключены. Все эти атаки были продемонстрированы до применения VLAN-сегментации, и защита, основанная на изоляции сети, эффективно решает данные угрозы.

1. Защита от MITM через ARP-spoof (DHCP/TFTP): атака требует доступа к L2-сегменту для определения ARP-кэша. В изолированном VLAN злоумышленник не может перехватывать трафик, если не подключен напрямую.
2. Защита от Rogue DHCP (Options 66/67): поддельный сервер не сможет навязывать параметры, поскольку broadcast-запросы ограничены VLAN, и клиент в основном сегменте не видит PXE-трафик.
3. Защита от IPv6 MITM (rogue RA/DHCPv6): аналогично, IPv6-атаки требуют сетевой доступ, сегментация предотвращает рассылку RA в основной сети.
4. Защита от DHCP Starvation: исчерпание пула адресов возможно только внутри изолированного VLAN, не затрагивая офисную сеть.
5. Защита от TFTP Flood: флуд-атаки на TFTP ограничены VLAN, минимизируя DoS-эффект на всю инфраструктуру.
6. Защита от TFTP File Injection: внедрение фальшивых файлов требует MITM-позиции, которая невозможна без доступа к VLAN.
7. Защита от DHCP Option Overwrite: перезапись опций в broadcast-доступе блокируется сегментацией.

Эксперимент подтверждает, что такая изоляция предотвращает атаки, основанные на использовании поддельных DHCP/PXE-серверов, обеспечивая безопасный переход загруженной машины в офисный VLAN.

Библиографический список

1. Microsoft Docs. Windows Deployment Services Overview. URL: <https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-services-overview> (дата обращения: 11.12.2025).
2. Microsoft Docs. DHCP Server Role in Windows Server. URL: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-server-role> (дата обращения: 11.12.2025).
3. Иванов А.В. Настройка PXE-сервера для автоматизированного развертывания ОС в корпоративной сети // Информационные технологии и вычислительные системы. 2020. № 2. С. 45-52.
4. Петрова Е.С. Уязвимости протоколов DHCP и TFTP в системах сетевой загрузки // Безопасность информационных технологий. 2021. № 3. С. 67-75.
5. Смирнов К.А. Защита от атак на PXE boot в инфраструктуре Windows Server // Журнал сетевых решений/LAN. 2019. № 4. С. 34-41.
6. Уймин А.Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1: учебно-методическое пособие. – Саратов, Москва: Лань, 2021. - 480 с.
7. Федоров И.П. Актуальные угрозы кибербезопасности в сетевых протоколах: обзор // Вестник РГУ нефти и газа. 2022. № 1. С. 112-120.
8. Уймин А. Г. Разработка методики тегирования системы безопасности автоматизированных систем управления процессами на основе корпоративного

стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65. – EDN VSLWIA.

References

1. Microsoft Docs. Windows Deployment Services Overview. URL: <https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-services-overview> (accessed: 11.12.2025).
2. Microsoft Docs. DHCP Server Role in Windows Server. URL: <https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-server-role> (accessed: 11.12.2025).
3. Ivanov, A.V. *PXE Server Setup for Automated OS Deployment in Corporate Networks* // Information Technologies and Computing Systems. 2020. No. 2. P. 45-52.
4. Petrova, E.S. *Vulnerabilities of DHCP and TFTP Protocols in Network Boot Systems* // Information Security Technologies. 2021. No. 3. P. 67-75.
5. Smirnov, K.A. *Protection Against Attacks on PXE Boot in Windows Server Infrastructure* // Network Solutions Journal/LAN. 2019. No. 4. P. 34-41.
6. Uymin, A.G. *Network and System Administration*. Demonstration Exam CODE 1.1: Educational and Methodical Guide. – Saratov, Moscow: Lan, 2021. - 480 p.
7. Fedorov, I.P. *Current Cybersecurity Threats in Network Protocols: An Overview* // Bulletin of Gubkin Russian State University of Oil and Gas. 2022. No. 1. P. 112-120
8. Uymin, A.G. *Development of a Security Tagging Methodology for Automated Process Control Systems Based on Corporate Standard* / A.G. Uymin // Automation and Informatization of the Fuel and Energy Complex. – 2024. – No. 5(610). – P. 59-65. – EDN VSLWIA.

Информация об авторе

Долгова Любовь Владимировна – студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: dolgovaLyubov2000@icloud.com

CONFIGURATION AND FUNCTIONAL TESTING OF PXE BOOT BASED ON WINDOWS SERVER. SECURITY ISSUES

Dolgova L. V.¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article examines the configuration and functional testing of PXE boot technology based on Windows Server, with particular attention to the security of network boot infrastructure. The purpose of the study is to analyze risks caused by the use of DHCP and TFTP, the absence of built-in authentication, and the transmission of critical boot parameters over the network, and to verify a protection measure based on network segmentation. The paper systematizes MITM, Rogue DHCP, DHCP Starvation, TFTP Flood, TFTP File Injection, and DHCP option overwrite scenarios, describing the conditions required for their implementation, possible consequences, and tools. The experimental part was carried out on a virtual test bed based on KVM in Proxmox VE. A Windows Server 2019 host provided DHCP and Windows Deployment Services, while a client virtual machine was used to test the complete PXE boot cycle. Functional testing confirmed address assignment, retrieval of the boot file from WDS, and initiation of operating system installation. A Rogue DHCP scenario was also demonstrated, in which the client accepted substituted network parameters from an unauthorized DHCP server. To reduce these risks, the PXE infrastructure was moved to a dedicated VLAN with its own DHCP scope and restricted access. Tests showed that a client outside the PXE VLAN received no PXE responses, whereas assigning the required VLAN enabled successful network boot. The results support network segmentation as a practical method for limiting access to broadcast DHCP/TFTP traffic and reducing the attack surface.

Keywords: PXE boot, DHCP, WDS, network security, VLAN segmentation, TFTP.

Information about the author

Dolgova Lyubov Vladimirovna – 3rd year student, Faculty of Integrated Safety of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: dolgovaLyubov2000@icloud.com