боковое перемещение и повышение привилегий в сети / Хабр

habr.com/ru/companies/bastion/articles/809655

secm3n

secm3n 23 апр в 13:57

Инфраструктурный пентест по шагам: боковое перемещение и повышение привилегий в сети

11 мин

8.9K
Туториал

В предыдущих статьях мы изучили подходы к разведке и анализу целей, а также ключевые аспекты этапа сканирования. Теперь пришло время разобраться в анализе парольных политик, ACL и DNS, найти способы бокового перемещения и провести обзор основных актуальных техник повышения привилегий.

Этот этап анализа безопасности — ключевой для оценки того, насколько эффективно корпоративная сеть защищена от различных угроз. Расскажу, из каких действий он складывается и какие инструменты нужны для их реализации.

В этой статье вас ждет база — те вещи, которые должен знать каждый начинающий пентестер, занимающийся аудитами внутренней инфраструктуры.

> Статья написана по мотивам серии лекций для наших стажеров. В них мы разбирали инфраструктурный пентест от А до Я.

Инструменты разведки

В предыдущей части мы рассматривали разные подходы к аудиту внутренней инфраструктуры компаний. В частности, пытались проверить, является ли учетная запись членом группы, осуществляли разведку Active Directory без учетной записи и искали хосты. Теперь подробнее остановимся на инструментарии, который позволяет собирать информацию внутри корпоративной сети.

Инструменты	Сведения об ACL	Сведения о сети	Сведения о ADCS
Active Directory Module	Bloodhound	adidnsdump	certutil
PowerView	Adalanche	dnstool	certify
Bloodhound	ACLScanner	ADExplorer	
Adalanche			

В ситуациях, когда нужна максимальная скрытность, например, во время Red Team-проектов, лучше использовать штатный Active Directory Module, подключаемый через командлеты (обычно используется DLL-библиотека, которую скачивают с хоста). Так получают данные о парольной политике, машинах и пользователях, их привилегиях без лишнего шума. В то время как альтернативы вроде BloodHound достаточно легко попадают под прицел антивирусов, создают шум в сети (например, на контроллерах домена) и часто требуют обфускации для нормального использования.

Получение парольной политики

Во второй части краткого руководства по инфраструктурному пентесту мы уже говорили о подборе паролей и атаке Password Spraying. Тогда мы били по площадям, используя списки распространенных паролей. Получив доступ к первой

полноправной учетной записи в инфраструктуре, стоит вернуться к теме подбора паролей с новыми возможностями.

Посмотреть парольную политику можно несколькими способами.

1. Если есть возможность использовать PowerView, то с помощью PowerShell-команды Get-DomainPolicy, которая используется для получения информации о настройках групповой политики в домене:

   ```
   Get-DomainPolicy
   ```

2. При помощи протокола **SAMR** (Security Account Manager Remote), который доступен вам по умолчанию. Например, можно использовать команду **net accounts**. Если нужны настройки учетных записей домена, а не только локального компьютера, пригодится параметр **/domain**:

   ```
   net accounts /domain
   ```

3. Самый прямолинейный, но неочевидный способ — найти файл политики по пути *%SystemRoot%\SYSVOL\SYSVOL\<domain_name>\Policies* с его последующим открытием в блокноте.

Кроме того, мы часто используем команду **gpresult**, которая отвечает за отображение результатов обработки групповых политик (**GPO**) для текущего пользователя и компьютера:

```
gpresult /r
```

Так можно получить информацию о настройках политик, параметрах безопасности, скриптах входа в систему или данных для диагностики проблем с применением групповых политик.

Получение списка активных учетных записей

Чтобы получить список активных учетных записей, можно воспользоваться запросом:

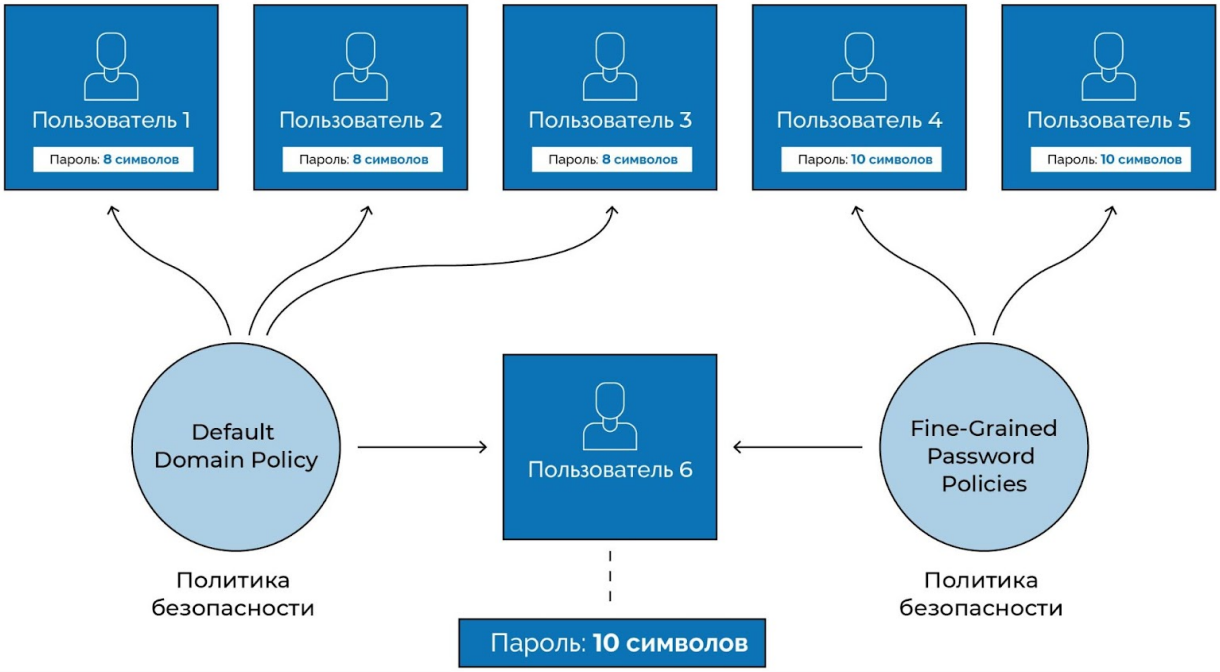
```
Get-ADUser -Server "domain.local:3268" -Filter * | Select-Object DistinguishedName
```

- **Get-ADUser** используется для получения данных о пользователях;
- **Server “domain.local:3268"** указывает сервер Active Directory и порт;
- **Filter *** применяется для выбора всех пользователей;
- **Select-Object DistinguishedName** отвечает за выдачу только уникальных имен пользователей.

Анализ альтернативных политик

Иногда сетевые администраторы используют дополнительные механизмы безопасности, такие как Fine-Grained Password Policies (**FGPP**). С их помощью устанавливают политику безопасности паролей для разных групп пользователей в пределах одного домена.

Понимание того, как работает **FGPP,** позволяет находить группы пользователей с менее строгими требованиями к паролям и ситуации, в которых настройки политик разных групп «перекрывают» друг друга.



В ситуации когда Default Domain Policy, требует пароль длиной в 8 символов, а FGPP, требует 10 символов, для пользователя будет действовать более строгая политика

Теперь можно составить уточненные словари, кастомизированные под требования конкретной парольной политики, и снова использовать атаки перебором паролей, которые я уже описывал во второй части этого цикла статей.

Анализ сведений об ACL

Парольные политики, это еще не вся информация, которая может пригодиться пентестеру. Так, в ACL содержатся списки правил, где указаны разрешения на доступ к объектам (программам, процессам или файлам), для конкретных пользователей, групп или системы в целом. Большое число уязвимостей связано именно с неправильным распределением прав доступа.

Особое внимание стоит уделить ошибкам ACL — они могут стать точкой атаки или источником утечек конфиденциальной информации.

Нам часто встречаются:

- GenericALL — ошибки в назначении прав общего доступа;

- WriteDACL **->** GenericALL — ошибки, связанные с установкой прав записи в контрольный список DACL с последующим получением прав общего доступа;
- GenericWrite **->** WriteProperty — проблемы, при которых права на общую запись приводят к получению прав записи свойств (RBCD, Shadow Credentials, Logon Script, SPN Hijacking, Targeted Kerberoasting/ Asreproasting, Add member to group
- AllExtendedRights — предоставление расширенных прав (ReadLAPS, DCSync, ForceChangePassword).

Чтобы найти потенциально уязвимые конфигурации прав доступа, можно использовать:

- **Bloodhound** — веб-приложение на базе React, Sigma.js и REST API, которое использует теорию графов для поиска некорректных настроек объектов и неочевидных связей внутри Active Directory.
- **Adalanche** — быстрый визуализатор структуры прав внутри Active Directory. Наглядно отображает, какие разрешения есть у пользователей и групп.
- **ACLScanner** — консольная утилита, написанная на PowerShell, которая генерирует отчеты о списках управления доступом (DACL) и списках управления доступом к системе (SACL) в Active Directory.

Несмотря на схожие функции, на практике эти инструменты хорошо дополняют друг друга и вместе позволяют составить более полную картину происходящего в сети. Так, например, в одном из наших проектов ACLScanner помог выявить уязвимость, которую Bloodhound не обнаружил.

Тогда пентестер получил возможность изменять один из атрибутов учетной записи, а именно — номер телефона. Он и стал ключом к домену. Процесс восстановления доступа к учетной записи администратора осуществлялся по номеру, и, подменив этот атрибут, мы смогли сбросить пароль и получить несанкционированный доступ к системе.

Анализ DNS

В процессе анализа сети также широко используется **Active Directory-Integrated DNS**. Эта подсистема позволяет серверам доменных контроллеров хранить информацию о DNS-зонах непосредственно в каталоге Active Directory. Это упрощает управление зонами DNS и обеспечивает целостность данных, поскольку информация о зонах реплицируется среди всех контроллеров домена. Пентестеры могут получить из нее информацию о структуре сети и прицельно работать по конкретным диапазонам адресов.

Рекомендуем использовать:

- **adidnsdump** — создает снимок информации о состоянии DNS Active Directory через стандартные запросы, доступные по умолчанию любому пользователю.
- **ADExplorer** — подключается к контроллеру домена и позволяет просматривать данные LDAP. Кроме того, эта утилита позволяет создавать снимки сервера, к которому вы в данный момент подключены и конвертировать их в JSON, совместимый с BloodHound.

Поиск парольной информации

Если парольная политика представляет собой набор требований, которым должен отвечать пароль, то под парольной информацией понимаются сами пароли в открытом или хешированном или шифрованном виде.

На этом этапе пентеста их можно найти в разных источниках:

- В первую очередь это хранилища паролей: файлы **/etc/passwd** и **/etc/shadow** (Linux) и SAM-файлы (для Windows);
- В 7 из 10 проектов пароли хранятся в SYSVOL. Реже, но пароли также встречаются в GPO;
- Кроме того, пароли некоторых учетных записей можно найти в поле Description;
- и просто в общедоступных сетевых папках.

И не только. Парольную информацию можно извлечь из кода некоторых программ, найти в скриптах или на хостах. Однажды мы обнаружили серверные логины и пароли, используемые для ежедневного запуска бэкапов БД на терминальном сервере 1С.

Боковое перемещение

Обычно, после получения контроля над одним из хостов, мы стремимся расширить поверхность атаки и проводим анализ структуры сети. Цель этого этапа пентеста — поиск уязвимых точек, узлов, между которыми можно перемещаться, продвигаясь по сети и отыскивая новые возможности для атак. Обычно этот этап называют боковым, или горизонтальным перемещением (Lateral Movement).

Анализ файла SAM

Начальный этап этого процесса — анализ файла **SAM (**Security Account Manager**)** и **System**, которые хранятся в C:\Windows\System32\config. Эти файлы содержат зашифрованные данные об учетных записях пользователей и дескрипторы безопасности. Их можно извлечь с помощью скрипта **secretsdump.py**в Kali Linux.

```
secretsdump.py LOCAL -sam sam -system system
```

Затем пентестер применяет атаку Hash Spraying, «распыляет» хэши на действительные учетные записи в домене, или на разные компьютеры локально. Это возможно, поскольку NT Hash не использует соль, следовательно один и тот же пароль везде имеет один и тот же хэш. Кстати, этот метод позволяет обойти блокировку учетных записей, которая активируется при частых неудачных попытках входа.

Ключевую роль в этой тактике играет **LSASS** (Local Security Authority Subsystem Service). Этот процесс взаимодействует с провайдерами поддержки безопасности **SSP** (Security Support Provider) и хранит различные данные аутентификации залогиненных пользователей (NT-хеши, билеты Kerberos, ключи от сеансов и RDP-сессий).

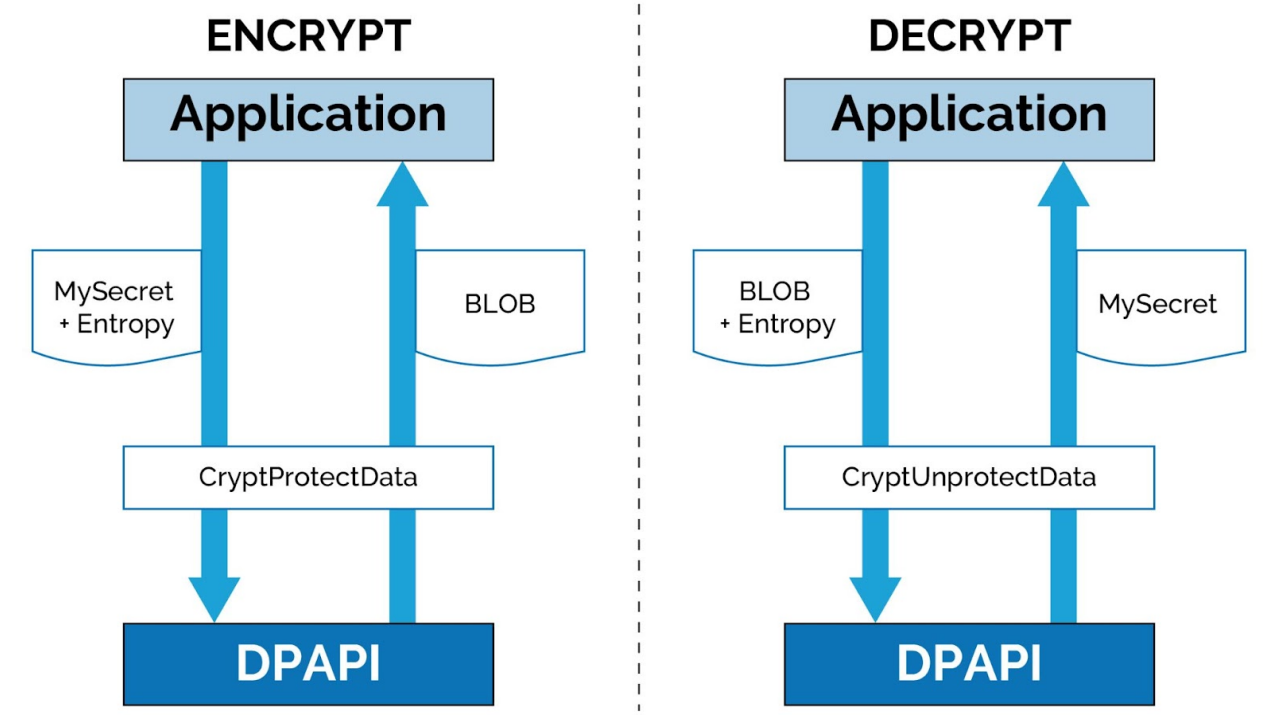
```
C:\Windows\System32\lsass.exe
```

На практике можно столкнуться с ситуацией, когда **LSASS** защищен антивирусом, но на сервере открыты сеансы **RDP.** Тогда можновыполнить дамп процессов **svchost.exe** и **mstsc.exe** и провести их анализ, например при помощиopen-source фреймворка **Volatility**.

Анализ файла SECURITY

SAM — не единственный файл, который представляет интерес для пентестера. Также мы обращаем внимание на файл **SECURITY.** Он расположен по пути C:\Windows\System32\config. Внутри хранится пароль к компьютеру в виде NTLM-хэша и креды различных сервисов, запущенных от имени конкретной учетной записи. Для его расшифровки также потребуется файл SYSTEM.

Еще один интересный для нас механизм — **DPAPI** (Windows Data Protection API). Алгоритм используется для шифрования и дешифрования учетных данных, хранящихся в системе (речь идет о закрытых ключах клиентских и системных сертификатов, wi-fi ключах, данных из браузеров и многом другом). Все, что потребуется потенциальному злоумышленнику для расшифровки этих данных — мастер-ключ, SID пользователя, хэш пароля и сами зашифрованные DPAPI-данные (пользовательские или системные).



Получение дополнительных служебных учетных записей и поиск уязвимых учетных записей по SPN

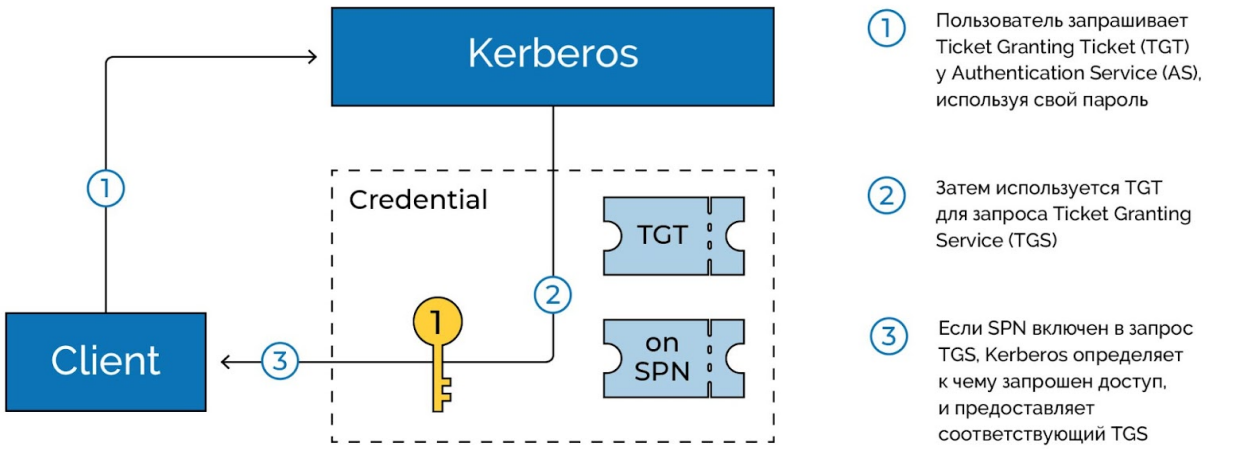
Еще один способ получить дополнительные учетные записи — отобрать при помощи BloodHound перспективные учетки с SPN и использовать против них Kerberoasting. Это достаточно известная атака, которая которая позволяет любому пользователю домена запросить TGS-билет у учетной записи с прописанным Service Principal Name.

SPN представляет собой комбинацию двух основных элементов: класса службы, имени хоста (или полного доменного имени) и иногда порта. Формат SPN выглядит следующим образом:

```
service_class/machine_name[:port][/path]
```

Существует множество классов, таких как **cifs** для файловых служб, http для веб-служб, и других.

Для обнаружения потенциально уязвимых учетных записей производится поиск всех учетных записей с не пустым атрибутом **SPN**. Затем, используя утилиту Rubeus, мы запрашиваем TGS-билеты и проводим брутфорс. Поскольку **SPN** часто указан у сервисных учетных записей, их наличие обычно связано с определенными привилегиями. Специфика **SPN** заключается в его уникальности для каждой службы.



В последнее время вместо **DES** TGS-билеты используют **AES-**шифрование. Это важный момент, поскольку брутфорс TGS-билетов с использованием AES-шифрования занимает много времени и ресурсов. Поэтому основное внимание стоит уделять поиску ошибок в разрешениях (**ACL**) с использованием инструментов типа **Bloodhound** или **ACLScanner**.

SPN есть в основном у сервисных учетных записей. Раньше среди них встречалось много привилегированных, как минимум в рамках своего сервиса (например, базы данных), однако сейчас эта атака скорее еще один способ увеличить площадь атаки. Для повышения привилегий используются другие приемы.

Повышение привилегий

Следующий шаг — получить дополнительный контроль над системой и возможность выполнить более широкий спектр вредоносных действий. Существует много подходов к повышению привилегий, которые варьируются в зависимости от конкретной конфигурации системы, используемых технологий и уровня доступа, полученного пентестером. Самые распространенные: эксплуатация уязвимостей в программном обеспечении или операционной системе, использование слабых паролей и перехват аутентификационных данных.

Анализ отдельных файлов и применение эксплоитов

Для локального повышения привилегий в системе могут пригодиться файлы:

- C:\sysprep\sysprep.inf
- C:\sysprep\sysprep.xml
- %windir%\Panther\Unattended.xml

Sysprep и Unattended присутствуют в преднастроенных образах Windows и нужны для указания параметров, которые применяются к операционной системе во время развертывания образа. В этих файлах может оказаться пароль локального

администратора. А поскольку сетевые администраторы часто берут один эталонный образ и раскатывают его на десятки хостов, этот пароль может быть чрезвычайно полезен.

Самым же простым и прямолинейным способом повышения привилегий были и остаются разнообразные эксплоиты, задействующие различные уязвимости популярных сервисов и технологий. Однако в рамках пентестов рабочей инфраструктуры их используют осторожно и по согласованию с заказчиком. Дело в том, что не все эксплоиты стабильны: многие из них с высокой вероятностью вызывают сбои в работе серверов.

Продвинутые техники атак

Имея на руках NTLM-хеш доменной административной учетной записи, можно применить технику **Pass-the-hash** или ее вариации: Over pass-the-hash и Pass-the-ticket. Они позволяют использовать хеш пароля для аутентификации в других системах без необходимости его расшифровки. Фактически, они позволяют «наращивать» свои привилегии горизонтально по сети, обходя процесс аутентификации.

Это достаточно гибкие атаки, которые можно применять разными способами. О некоторых из них я уже рассказывал в других статьях. Например, в этом случае Over-pass-the-hash позволила последовательно захватить три домена, а с ними и весь лес.

Если же с захватом LSASSвозникли проблемы, но RDP-сессия активна, можно использовать **RDP Hijacking**. Суть этой атаки в том, что, имея доступ к системе под учетной записью с привидениями SYSTEM, можно перехватить активную RDP-сессию другого пользователя, даже не зная пароль. После захвата сессии атакующий будет взаимодействовать с системой так, как если бы он сам был оригинальным пользователем RDP.

Еще один рабочий, многократно опробованный на практике вариант — **Impersonation**, техника которая позволяет украсть так называемый маркер доступа и использовать его для продвижения с привилегиями администратора и служебных учетных записей, работающих в контексте Local Service. Выполнить эту атаку можно при помощи классической утилиты **Incognito** или ее более современного и функционального аналога — **SharpImpersonation**.

Конечно, дьявол кроется в деталях. Перечисленные в статье техники и подходы, могут применяться очень по-разному в зависимости от обстоятельств, в которых оказался пентестер.

Мы продолжим рассматривать конкретные случаи в нашем блоге, но базовый, можно сказать поверхностный обзор основных этапов инфраструктурного пентеста спустя три статьи можно считать завершенным. Если после их прочтения вы хотите

с головой погрузиться в тему, **рекомендуем литературу**.

Про основы пентестов:

- Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman. В книге подробно и доступным языком описываются основные принципы и методы пентеста. Материал представляет собой прочный фундамент для тех, кто хочет продолжить свое обучение и развитие в области кибербезопасности, понять, как работают инструменты анализа трафика.

- Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation, James Forshaw. Автор подробно рассказывает о принципах работы сетевых протоколов и методах поиска и устранения уязвимостей.

Про Kali Linux:

- Kali Linux Revealed: Mastering the Penetration Testing Distribution, Raphael Hertzog, Jim O'Gorman. Издание Offensive Security подойдет в качестве руководства для подготовки к сертификации по Kali Linux Certified Professional.

- Kali Linux Wireless Penetration Testing Cookbook: Identify and assess vulnerabilities present in your wireless network, Wi-Fi, and Bluetooth enabled devices to improve your wireless security., Sean-Philip Oriyano. В книге рассматриваются методы проникновения в беспроводную сеть, включая сканирование WLAN, взлом WEP, взлом WPA/WPA2, и способы проверки полученных результатов.

Про Metasploit:

- Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni. Основатель проекта Metasploit назвал эту книгу лучшим руководством по фреймворку. Авторы рассказывают, как проводить разведку, эксплуатировать уязвимости, интегрировать Nmap, NeXpose и Nessus для автоматизации обнаружения.

- Metasploit Revealed: Secrets of the Expert Pentester: Build your defense against complex attacks, Sagar Rahalkar, Nipun Jaswal. В книге раскрываются продвинутые методики и подходы (с примерами), используемые опытными пентестерами в работе с Metasploit.

Про Active Directory

- AD Attack Vectors: Top Active Directory Vulnerabilities, Muhammad Nafees, Zahid Arafat, Nadeem Ashraf. Авторское исследование вопросов, связанных с основными уязвимостями Active Directory.

- Active Directory глазами хакера, Ralf Hacker. Сборник статей о поиске уязвимостей и разведке в атакуемой сети, повышении привилегий, боковом перемещении, поиске и сборе критически важных данных.

Журналы для пентестеров:

Nmap Guide Revisitedи Nmap Guide Free Network Scanner от Hakin9 — ежемесячные журналы, посвященные лучшим практикам взлома. Материалы включают в себя обзорные исследования по сканированию сетей, обнаружению уязвимостей, работе эксплойтов.