инструменты, методологии и разведка / Хабр

habr.com/ru/companies/bastion/articles/767704

secm3n November 21, 2023

Простой

9 мин

55K
Туториал

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

Начнем с теории — того, по каким схемам действуют хакеры и как знание этих шаблонов помогает в работе пентестера. Затем перейдем к выбору операционных систем и полезным фреймворкам. Рассмотрим гаджеты, которые чаще всего применяются на практике во время атак на организации. Закончим разбором и анализом UDP и TCP-портов, через которые можно захватить первую учетную запись в чужой инфраструктуре.

> Недавно закончилась наша программа стажировки для начинающих безопасников. Эта статья написана по мотивам лекций, в которых мы разбирали инфраструктурный пентест от А до Я.

Этапы и методологии инфраструктурных пентестов

Все разнообразие атак на сетевую инфраструктуру можно свести к некому алгоритму, одной из нескольких абстрактных логических схем, методологий.

Наиболее известны:

- ISSAF — Information systems security assessment framework;
- PTES — Penetration Testing Execution Standard;
- OSSTMM — The Open Source Security Testing Methodology Manual.

По своей сути и основным этапам все они похожи. Выделяют шесть этапов пентеста:

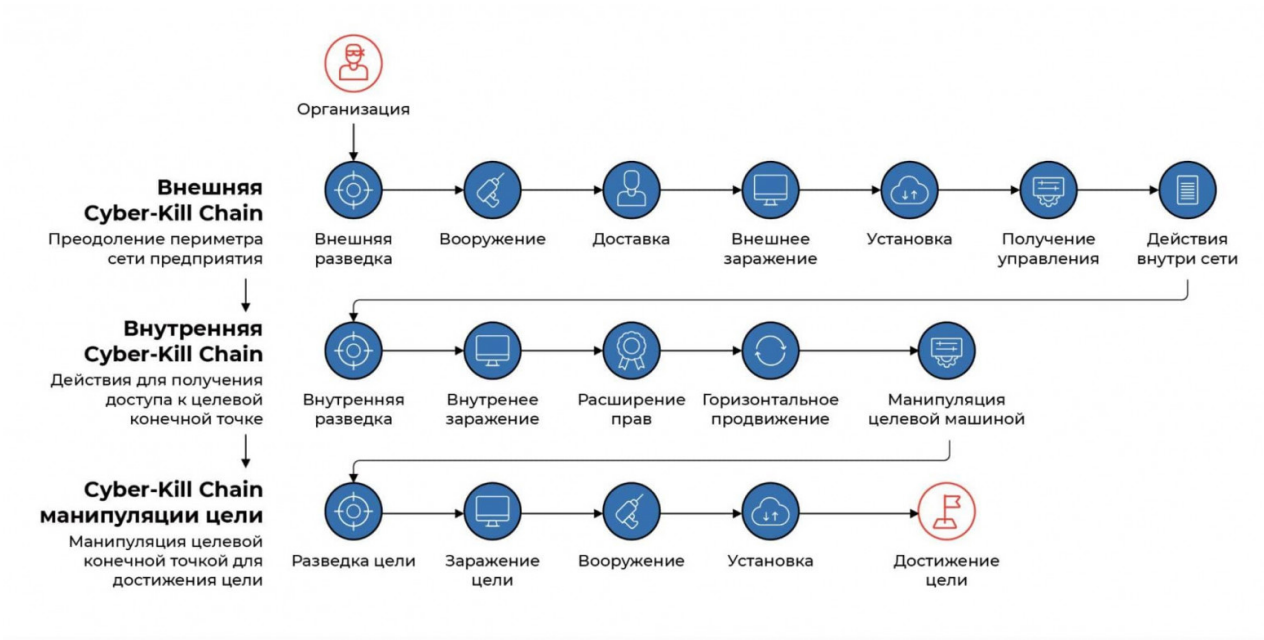
1. Разведка.
2. Сканирование.
3. Получение доступа.
4. Закрепление в системе.
5. Удаление следов.
6. Подготовка отчета.

Разведка и идущее за ней сканирование — не одно и то же. Перечисленные фреймворки, методологии и стандарты описывают комплексный пентест, который затрагивает и внешние сервисы компании. Поэтому под разведкой здесь понимается OSINT — поиск IP-адресов, имен учетных записей, доменных имен и так далее по открытым источникам. Сканирование, соответственно, подразумевает исследование уже найденных IP-адресов.

Фреймворк ISSAF примечателен тем, что по сути является 1000-страничной инструкцией. Каждый этап атаки в этой методологии сопровождается конкретными командами. Следуя по этой методологии шаг за шагом, в принципе, можно провести полноценный пентест. Впрочем, даже последняя редакция ISSAF стремительно устаревает.

PTES не такой емкий. В нем преобладает теория, но приводятся ссылки на инструменты, которые можно использовать в работе. В то же время он несколько шире и рассматривает, в том числе и тему Wi-Fi.

В своей работе мы, как правило, используем OSSTMM, разработанный Институтом безопасности и открытых методологий (ISECOM). Этот фреймворк представляется наиболее актуальным на сегодняшний день. Впрочем, помимо методологий PTES, ISSAF и OSSTMM существует еще пара известных подходов: MITRE ATT&CK и Kill Chain от специалистов Lockheed Martin.



Они описывают те же процессы, но ориентированы на Blue Team. То есть сделаны с оглядкой на потребности тех, кто предотвращает и расследует инциденты. Эти методологии поэтапно разбирают то, как атакующие продвигаются внутри сети. Пентестерам также стоит их знать. На Red Team-проектах необходимо тесно взаимодействовать с Синей Командой. Мы синхронизируем свои действия на каждом из этапов по времени, и нам надо хорошо понимать друг друга.

MITRE делит свою методологию на тактики, техники и процедуры.

- **Тактика** — это тактическая цель злоумышленника, причина совершения действия. Например, атакующему может быть необходимо просканировать инфраструктуру, повысить привилегии или закрепиться в системе. Всего в MITRE существует 14 тактик. Каждая из них отвечает на вопрос «почему?» — почему выполняется техника или подтехника.

- **Техника** отвечает на вопрос «как?» — как злоумышленник достигает тактической цели, выполняя определенное действие. Например, атакующий может создать или модифицировать системный процесс, чтобы закрепиться в системе.
- **Процедура** — конкретная реализация техники. Например, атакующий модифицирует системный сервис через реестр Windows посредством утилиты Reg.exe, изменяя значение ключа ImagePath на путь к вредоносному исполняемому файлу. Процедуры классифицируются в ATT&CK как варианты реализации техник, выявленные в реальных компьютерных атаках. Они перечислены на страницах с описанием техник в секции «Procedure Examples».

Инструменты пентестера

От теории перейдем к практике и сначала поговорим об инструментах, которые позволяют реализовать все эти методологии в деле.

Операционные системы

Мы испытывали различные специализированные дистрибутивы операционных систем и даже написали про них отдельную обзорную статью с парой десятков наименований. Однако не все они хорошо подходят для инфраструктурных пентестов. Выделим шесть сборок:

- **Commando VM 2.0** (база Windows 10);
- **BackBox**, база Ubuntu, 300+ утилит;
- **Parrot Security OS**, база Debian, 600+ утилит;
- **BlackArch**, база Arch Linux, 2300 утилит;
- **Black Spider** (база Windows 10);
- **Kali Linux**, база Debian, 600+ утилит.

В итоге наш отдел остановился на последних Kali Linux и банальной Windows. Дело в том, что практически все работы с доменом связаны с аутентификацией Kerberos, а работать с Kerberos удобней всего именно из под Windows. Кроме того, все наши основные инструменты, Rubeus, Mimikatz, Certify, Coercer написаны на дотнет.

Из преимуществ Linux стоит отметить то, что на нем проще выполнять атаки, связанные с сетью, например NTLM Relay. Для такого перехвата на Windows нужна дополнительная настройка, которая требует перезагрузки хоста и не всегда уместна в рамках проектов.

Впрочем, если вы пока не собрали собственный инструментарий, вам вполне могут подойти готовые сборки на Windows — Black Spider, Commando VM. А из академического интереса стоит изучить все перечисленные проекты.

Фреймворки и учебные пособия

Фреймворки типа Cobalt Strike и Covenant мы используем редко. Исключение составляет Metasploit, так как он снабжен достаточно широким набором сканеров и инструментов для брутфорса имен и паролей от учетных записей.

Кроме того, с Metasploit удобно работать из-за особенностей его базы данных. Мы сохраняем все сканы в XML, который без проблем импортируется в БД Metasploit. А оттуда можно буквально парой команд вызвать сервисы, которые нужно побрутить. Указав номер порта, можно вытащить из базы данных все хосты или открыть 445-й порт и, например, применить к нему модуль по проверке на MS17-010. Поэтому Metasploit стоит освоить хотя бы из-за встроенной базы данных. Тут можно рекомендовать Metasploit: The Penetration Tester's Guide, Mastering Metasploit и Metasploit Revealeds.

Также стоит уделить время освоению Nmap. Например, в книге Nmap Guide представлено достаточно много примеров по организации работы с Nmap и с точки зрения скорости работы сканера, и с точки зрения скрытности.

В Red Team-проектах необходимо уметь атаковать Wi-Fi. Соответствующий инструментарий лучше осваивать по Kali Linux Wireless Penetration Testing Cookbook и Offensive Security Wireless Attacks Course.

Девайсы для получения начального доступа

В большинстве внутренних пентестов мы имеем дело с доменными инфраструктурами и, как правило, для проведения работы нам предоставляют низкопривелегированную доменную учетную запись. Однако есть заказчики, для

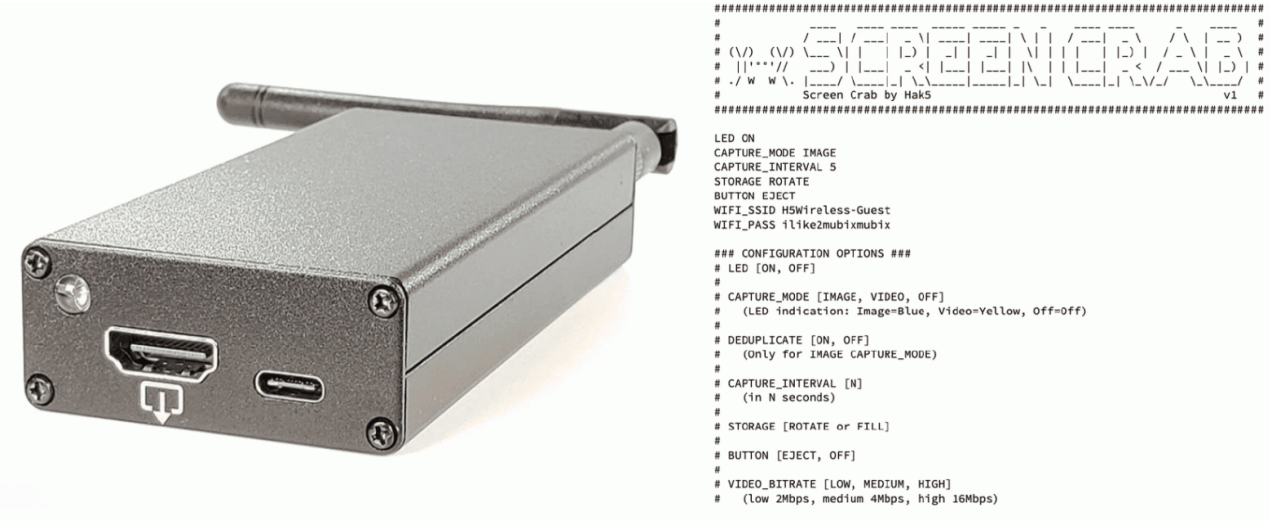
которых актуальны более сложные тесты. Бывает так, что нам нужно самостоятельно обнаружить точку входа. Существует много мелких гаджетов, которые могут пригодиться на этом этапе пентеста. Расскажу про наиболее практичные.

Shark Jack подключается к сетевой розетке и за 15 минут работы от аккумулятора сканирует сеть. Затем его можно забрать и спокойно изучить результаты аудита, сохраненные во внутренней памяти.

LAN Turtle представляет собой USB-Ethernet-адаптер — имплант в LAN сеть, который подключается в разрыв между сетевым кабелем и компьютером. Так он обеспечивает скрытый удаленный доступ, сбор сетевых данных и выполнение атак типа man-in-the-middle. Питается от USB, имеет слот для SIM-карты и может оставаться незамеченным достаточно долго.

LAN Turtle

Screen Crab тоже устанавливается в разрыв, на этот раз между компьютером и монитором. Он перехватывает и ретранслирует по Wi-Fi сигнал, идущий по HDMI-кабелю. Может делать скриншоты по таймеру или стримить картинку в режиме реального времени.



```
################################################################################
#                                                                              #
#  ____   ____ ____  _____ _____ _   _    ____ ____      _    ____           #
# / ___| / ___|  _ \| ____| ____| \ | |  / ___|  _ \    / \  | __ )          #
# \___ \| |   | |_) |  _| |  _| |  \| | | |   | |_) |  / _ \ |  _ \          #
#  ___) | |___|  _ <| |___| |___| |\  | | |___|  _ <  / ___ \| |_) |         #
# |____/ \____|_| \_\_____|_____|_| \_|  \____|_| \_\/_/   \_\____/          #
#            Screen Crab by Hak5                                    v1       #
################################################################################

LED ON
CAPTURE_MODE IMAGE
CAPTURE_INTERVAL 5
STORAGE ROTATE
BUTTON EJECT
WIFI_SSID H5Wireless-Guest
WIFI_PASS ilike2mubixmubix

### CONFIGURATION OPTIONS ###
# LED [ON, OFF]
#
# CAPTURE_MODE [IMAGE, VIDEO, OFF]
#   (LED indication: Image=Blue, Video=Yellow, Off=Off)
#
# DEDUPLICATE [ON, OFF]
#   (Only for IMAGE CAPTURE_MODE)
#
# CAPTURE_INTERVAL [N]
#   (in N seconds)
#
# STORAGE [ROTATE or FILL]
#
# BUTTON [EJECT, OFF]
#
# VIDEO_BITRATE [LOW, MEDIUM, HIGH]
#   (low 2Mbps, medium 4Mbps, high 16Mbps)
```

Screen Crab

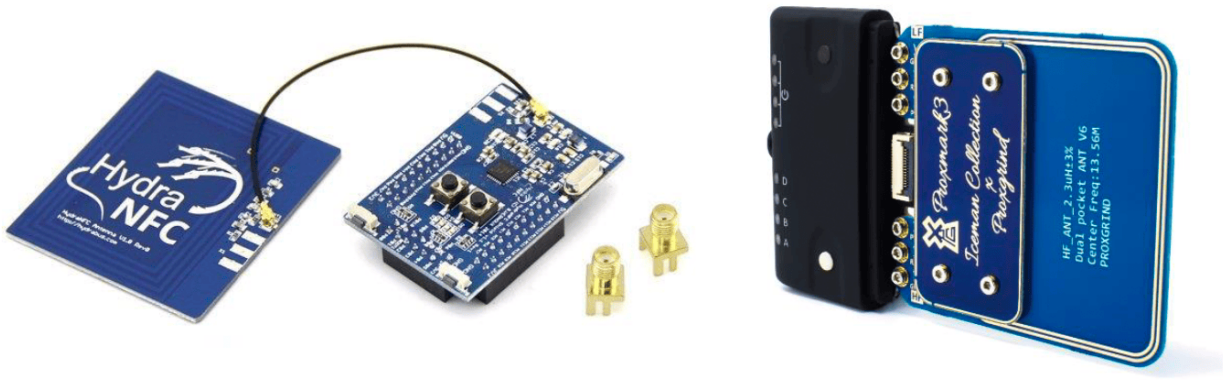
Rubber Ducky и **Bash Bunny** актуальны в проектах, связанных с социальной инженерией. Обычно пентестеры оставляют оставляют неприметные вредоносные флешки в туалетных комнатах и переговорках, а брендированные девайсы скорее предназначены для быстрых атак на незапароленные компьютеры. При подключении они автоматически выполняют ту или иную полезную нагрузку. **Bash Bunny** отличается от Rubber Ducky тем, что позволяет выбирать между несколькими пейлоудами.

Bash Bunny u Rubber Ducky

Wi-Fi Pineapple — знаменитый в узких кругах комбайн для перехвата и атак на Wi-Fi. Обеспечивает визуализацию Wi-Fi-ландшафта, мониторит и собирает данные о сети и устройствах в ней, поддерживает атаки на WPA и атаки типа man-in-the-middle. Имеет собственный веб-интерфейс и экосистему дополнительных загружаемых приложений.

Wi-Fi Pineapple

Hydra NFC и Proxmark3 RDV4 — популярные устройства для клонирования всевозможных NFC-брелков, карт доступа и ключей, работающих на базе RFID-меток с частотами 13.56 МГц и 125 кГц. Удобны тем, что позволяют вносить изменения в созданные дампы. В некоторых случаях, изменив пару бит в коде, можно значительно расширить доступ. Отчасти теряют актуальность с появлением Flipper Zero.



Hydra NFC и Proxmark3 RDV4

Разведка

Когда нам не выдают заранее подготовленные доступы, приходится сканировать инфраструктуру компании в поисках способа получить первоначальную учетную запись. Рассмотрим, скажем так, топ UDP и TCP-портов, которые стоит просканировать в такой ситуации, и обсудим наиболее интересные из них.

TCP-порты

```
nmap -Pn -n -sV --min-rate=200 --min-parallelism=400 -
p21,22,111,2049,445,623,1433,1521,5432,5555,6379,8080,8081,8180,8443,4786,3306,338
9,1099,27017 --open -oAresult -v
```

Среди TCP-портов в основном представлены базы данных. Мы охотимся на них, потому что до недавнего времени в Redis были опасные уязвимости, позволяющие пробиться в шелл операционной системы, а на PostgreSQL, Oracle и, например, MSSQL было достаточно много CVE. Нам все еще попадаются непропатченные машины, которые служат удобной точкой входа. К тому же, на базах данных банально может быть не настроена аутентификация.

UDP-порты

```
UDP-ports:
161, 162 -- SNMP
500 - IKE (VPN)
69 -- DHCP

TCP-ports:
111 -- RPC
623 -- IMPI
1433 -- MSSQL
2049 -- NFS
1521 -- Oracle
3306 -- MySQL
5432 -- Postgresql
5555 -- HP Data Protector (возможно RCE, есть модуль MSF:
exploit/windows/misc/hp_dataprotector_cmd_exec)
4786 -- Cisco Smart Install (RCE)
6379 -- RedisDB
1099 -- Java RMI
27017 -- MongoDB (no-auth)
```

161, 162–SNMP отвечают за Simple Network Management Protocol, который используется разным сетевым оборудованием. Существует три версии SNMP. Две из них требуют аутентификации, третья — нет.

Если мы имеем дело с первыми двумя версиями, то можем попробовать подключиться по этому протоколу к оборудованию и получить полезную информацию. В Kali Linux есть специальный инструмент, который позволяет выяснить, какие сетевые диапазоны и маски существуют. Зачастую так можно узнать имя учетной записи администратора или дескрипшены, которые подскажут назначение сети.

500–IKE (VPN) — этот порт использует протокол туннелирования IKEv2 на основе IPSec и предназначен для равноправной связи между VPN-устройствами. IKE-протокол может работать в двух режимах — это MainMode и AggressiveMode. В MainMode для установления соединения используется шестиэтапное рукопожатие, в AggressiveMode для ускорения соединения применено трехэтапное.

Если сервер работает в агрессивном режиме, то, зная ID-группы для подключения к VPN-серверу, можно попробовать получить хэш той или иной учетной записи, например, при помощи утилиты IKEscan. Если его удастся сбрутить, то получится подключиться к VPN.

Порт 69-DHCP — порт, через который работает Dynamic Host Configuration Protocol. Изредка он может пригодиться для атаки на так называемые сервера WDS (Windows Deployment Services), на которых хранятся эталонные образы Windows.

Когда загружается новый компьютер, он обращается к DHCP, который сообщает адрес WDS — оттуда можно забрать и затем развернуть образы. Существует атака, во время которой хакер выдает себя за WDS-сервер. К нему приходит компьютер, чтобы запросить образ, и пытается авторизоваться. Зачастую он делает это под учетной записью администратора, и в этот момент ее можно захватить. Такой вот спуфинг.

2049 — по NFS-портам можно найти незапароленные файловые шары с интересным содержимым — например бэкапами ОС, из которых можно извлечь учетные данные.

```
nmap-p 111 --script nfs* 10.10.10.8 showmount-e 10.10.10.8 mount -t nfs
10.10.10.8:/var/backups /mnt/backups
```

SMB — то же самое касается SMB, но кроме того, этот порт интересен с точки зрения старых уязвимостей, например, EternalBlue.

```
smbmap-H 10.10.10.8 nmap--script smb-vuln* -p139,445 -T4 -Pn 10.10.10.8
```

623 IPMI (Intelligent Platform Management Interface) — по сути это мини-операционная система на материнской плате компьютера-сервера, которая позволяет подключиться к нему в обход основной ОС. И там тоже есть свои учетные записи.

Часто к IPMI можно подключиться, зная логин и пароль по умолчанию. Кроме того, существует модуль Metasploit, который позволяет провести энумерацию учетных записей, понять, какие записи существуют, а какие нет. Задаем словарь и прогоняем скрипт по наиболее популярным.

Если вы знаете имя учетной записи IPMI и столкнулись с IPMI версии 2.0, то можно извлечь дамп с хэш-паролем для этой учетной записи. Для этого существует готовое решение. Забираем хэш и нет нет, он может и сбрутиться. Затем при помощи IPMI tools можно подключиться к IPMI, получить доступ к жесткому диску и забрать с него что-нибудь полезное.

4786 — Cisco Smart Install аналог виндового WDS, куда залиты эталонные образы для сетевого оборудования. На сегодняшний день о нем можно говорить, как об истории, и мы проверяем этот сервис скорее по старой памяти. Несколько лет назад для Smart Install существовала опасная RCE, которая позволяла, не зная пароля, получить доступ к оборудованию, сбросить пароль администратора, включить режим EXEC, либо прочитать через консоль конфигурацию и даже сдампить ее.

Со всеми этими сервисами можно что-то сделать, не имея никаких привилегий, однако это только начало инфраструктурного пентеста. Получив базовую учетную запись, мы начинаем работу с доменом. Об этом, об Active Directory и аутентификации Kerberos я расскажу в следующей статье.

В завершении хочется подчеркнуть, что тщательно проведенная разведка закладывает фундамент для исследования корпоративной сети, экономит массу времени на более поздних этапах проекта и во многом определяет успешность всех действий пентестера.

Продолжение следует.