Teach Me Skills

PENTEST

Практика

Teach
Me
Skills

Собираемся и отмечаемся

Teach
Me
Skills

Вопросы по предыдущим темам или ДЗ

Teach Me Skills

Mini-quize по прошлым темам:

1. **Из каких основных этапов состоит пентестинг?**
2. **Какие типы уязвимостей могут быть выявлены в результате пентеста?**
3. **Зачем при пентесте составлять ТЗ?**
4. **Что позволит оценить пентест/редтиминг?**
5. **Какие негативные последствия могут быть для белого хакера?**
6. **Что, по вашему мнению, важно указать в отчете?**
7. **В чем особенность тестирования «черного ящика»?**

Teach Me Skills

Mini-quize по новой теме:

1. **Какие вы знаете сервисы которые использую порт на хосте, какие порты вы знаете?**
2. **Каким методами можно проводить брутфорс паролей?**
3. **Какое средство поможет нам проверить web ресурс на уязвимости?**
4. **Можно ли брутить zip архивы?**

Teach
Me
Skills

План занятия

1. Рассмотрим варианты получения доступа
2. Попробуем получить флаги доступа
3. Рассмотрим алгоритмы проведения пентеста

Активная разведка: сканирование сетевой инфраструктуры

Teach Me Skills

Одна из первых задач хакера/пентестера - провести сканирование сети на наличие работающих **хостов** (host discovery).

Инструменты, которые вы можете использовать на этом этапе:

- Nmap
- Masscan
- Netdiscover
- ARPScan

Как делать:

`$ netdiscover <IP range>` - обнаружить узлы с помощью ARP-запросов **в локальной сети**

`nmap -sn <IP range>` (No port scan) - aka Ping Sweep or Ping Scan. (В старых версиях Nmap `-sP`)

Эта опция указывает Nmap **не проводить сканирование портов** после обнаружения хоста, fa только вывести хосты, которые ответили на запросы.

```
$ nmap -F <IP range>
```

```
$ masscan <IP range>
```

Активная разведка: сканирование сетевой инфраструктуры

Teach Me Skills

Одна из первых задач хакера/пентестера - провести сканирование сети на наличие работающих **хостов** (host discovery).

Инструменты, которые вы можете использовать на этом этапе:

- Nmap

списки для копирования в nmap:

1. `21,22,25,53,80,143,443,8080,8000,8443,3389`
2. `21,22,445,623,4848,1433,5432,5555,8080,1521,3050,8081,8400,8888,8180,8443,4786,1099,27017,6379`
3. `21,22,23,25,80,111,135,139,161,179,389,443,445,623,1099,1433,1521,1540,1541,2049,2375,3306,3389,4786,5432,5555,5601,5900,6379,7001,8000,8008,8080,8443,9000,9200,10250,27017`

Сканирование портов

Опции nmap:

`-sS` - TCP SYN (выполняется по дефолту с sudo)

`-sT` - TCP CONNECT (выполняется по дефолту без sudo)

`-sU` - UDP

`-o` - определение ОС

вместо `-sT -sU -sV` можно писать `-sTUV`

`-p<порты>` - можно через запятую, можно диапазоном, можно диапазонами через запятую

`-p-` - все порты, заменяет `-p0-65535`

`-iL-` - загрузить список узлов из файла

`-Pn-` - отключает “пинги”

Активная разведка: сканирование сетевой инфраструктуры

Teach Me Skills

Для ускорения сканирования можно использовать списки наиболее интересных портов:

Порт	Сервис
21	ftp
22	ssh
2222	ansible
23	telnet
80, 8000, 8001, 8002, 8004, 8006, 8007, 8008, 8080, 8888	http
88	kerberos
139	netbios
389	ldap
443,8443,9443	https
445	smb
623, 49152	ipmi
636	ldaps
873	rsync
1099	websphere
1433, 1434	mssql
2181	zookeeper
2375,2376	docker

Активная разведка: сканирование сетевой инфраструктуры

Teach Me Skills

Примеры использования скриптов nmap

Поиск MySQL серверов, позволяющий вход root без пароля или анонимный вход

Поиск уязвимостей.
Скрипт mysql-empty-password:

```
nmap --script-help mysql-empty-password
```

OSINT, поиск виртуальных хостов на одном IP адресе.
Таких скриптов три:

- hostmap-bfk,
- hostmap-ip2hosts,
- hostmap-robtex.

```
nmap -sn --script="hostmap-ip2hosts"
example.com
```

Брутфорс директорий и файлов на веб-сервере (веб-сайте)

```
nmap --script="http-enum"
example.com
```

SecLists

SecLists - это коллекция из нескольких типов списков, используемых при оценке безопасности, собранных в одном месте.
Типы списков включают имена пользователей, пароли, URL-адреса, шаблоны чувствительных данных, полезные нагрузки для фаззинга, веб-оболочки и многое другое.

git clone https://github.com/danielmiessler/SecLists.git

YAWR

git clone https://github.com/empty-jack/YAWR.git

git clone https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

Другие словари

http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt

https://github.com/wallarm/jwt-secrets

Атаки на пароли

Teach Me Skills

Первый шаг - извлечение хэшей. При тестировании на проникновение мы обнаружим хэши в различных местах. Например, если мы получим доступ к системе баз данных, то сможем сделать дамп таблицы базы данных, содержащей хэшированные пароли пользователей.

Какие хеши встречаются в пентесте:

- NTLM
- Net-NTLMv2
- sha256/512
- Domain Cached Credentials 2 (DCC2), MS Cache 2
- хеши CMS (Joomla, etc)
- KeePass

JohnTheRipper умеет определять тип хеша автоматически.

В хешкете последних версий также реализовано автоматическое определение типа хеша.

Таблица поддерживаемых hashcat хешей с примерами:

https://hashcat.net/wiki/doku.php?id=example_hashes

Онлайн определение типа хеша:

https://hashes.com/ru/tools/hash_identifier

Атаки на пароли

Teach Me Skills

Запуск:

```
hashcat [опции]... хеш|файл_хеша|файл_hccapx [словарь|маска|директория]...
```

`-m` - тип хеша (если не указать - попробует определить автоматически)

`-a` - режим атаки,
по словарю `-a 0`
полный брутфорс по маске `-a 3`
(также можно не указывать - определиться автоматом в зависимости от того, словарь вы указали или маску)

Атака по маске - гибкий тип атаки, который позволяет как реализовать полный перебор, так и перебор по тонко настроенным критериям.

Пример (пароль имеет длину от шести до десяти символов):

```
hashcat64.exe -m 0 -a 3 -i --increment-min=6 --increment-max=10 <хеш> ?l?l?l?ll?l?l?l?l?l?
```

Hashcat: практические примеры

https://miloserdov.org/?p=5426#14

https://hackware.ru/?p=14217

Атаки на пароли

Teach Me Skills

Онлайн брутфорс

Hydra

https://github.com/vanhauser-thc/thc-hydra

SMTP:

```
hydra -L /home/mironich/login.txt -P /home/mironich/pass.txt
smtp.yandex.ru smtp-auth
```

RDP:

```
hydra -L /usr/share/wordlists/dirb/others/names.txt -p
"SuperS3cure1337#" rdp://192.168.50.202
```

```
hydra -l nadine -P rockyou.txt rdp://192.168.219.227
```

Опции Hydra :
-R восстановить предыдущую прерванную/оборванную сессию
-S выполнить SSL соединение
-s ПОРТ если служба не на порту по умолчанию, то можно задать порт здесь
-l ЛОГИН или -L ФАЙЛ с ЛОГИНАМИ (именами), или загрузить несколько логинов из ФАЙЛА
-p ПАРОЛЬ или -P ФАЙЛ с паролями для перебора, или загрузить несколько паролей из ФАЙЛА
-x МИНИМУМ:МАКСИМУМ:НАБОР_СИМВОЛОВ генерация паролей для брутфорса, наберите “-x -h” для помощи
-e nsr “n” — пробовать с пустым паролем, “s” — логин в качестве пароля и/или “r” — реверс учётных данных
-C ФАЙЛ формат где “логин:пароль” разделены двоеточиями, вместо опции -L/-P
-M ФАЙЛ список серверов для атак, одна запись на строку, после двоеточия ‘:’ можно задать порт
-o ФАЙЛ записывать найденные пары логин/пароль в ФАЙЛ вместо стандартного вывода
-f / -F выйти, когда пара логин/пароль подобрана (-M: -f для хоста, -F глобально)
-t ЗАДАЧИ количество запущенных параллельно ЗАДАЧ (на хост, по умолчанию: 16)
-w / -W ВРЕМЯ время ожидания ответов (32 секунды) / между соединениями на поток
--q не печатать сообщения об ошибках соединения

Teach Me Skills

Meduza

https://github.com/jmk-foofus/medusa

Medusa и Hydra во многом похожи они модульные и «многопоточные», с хорошо настраиваемыми возможностями. Основное различие в том, как распараллеливается процесс перебора: у Medusa – потоками, у Hydra – процессами.

Опции Medusa :

-h [TARGET] : указываем имя узла или IP адрес для брута
-H [FILE] : файл с именами или IP дресами для брута
-u [TARGET] : имя пользователя
-U [FILE] : файл с именами пользователя
-p [TARGET] : пароль
-P [FILE] : файл с паролями для перебора
-C [FILE] : файл с сотавными записями для перебора формат записи host:user:password … либо же можно указать PwDump файл (userlm:ntlm:::)
-O [FILE] : лог файл для записи информации об успешности/неуспешности попыки
-e [n/s/ns] : дополнительные опции при подборе, -n подставлят качестве пароля пустой пароль, -s имя пользователя
-M [TEXT] : выбор модуля(протокола) для пербора
-m [TEXT] : параметры для передачи в модуль
-d : вывести список модулей
-n [NUM] : определяет нестандартный TCP порт
-s : использовать SSL

Teach Me Skills

Patator

https://github.com/lanjelot/patator

Patator – это многоцелевой брут-форсер, с модульным дизайном и гибким использованием.

Например, если SMTP-серверу нужно представиться командой helo\ehlo, в модуле присутствует такая возможность. Команда будет выглядеть например так:

```
patator smtp_login host=192.168.17.129 helo='ehlo 192.168.17.128'
user=FILE1 password=FILE0 0=/usr/share/john/password.lst
1=/usr/share/john/usernames.lst
```

Модули:

- ftp_login : Brute-force FTP
- ssh_login : Brute-force SSH
- telnet_login : Brute-force Telnet
- smtp_login : Brute-force SMTP
- smtp_vrfy : Enumerate valid users using SMTP VRFY
- smtp_rcpt : Enumerate valid users using SMTP RCPT TO
- finger_lookup : Enumerate valid users using Finger
- http_fuzz : Brute-force HTTP
- ajp_fuzz : Brute-force AJP
- pop_login : Brute-force POP3
- pop_passd : Brute-force poppassd
- imap_login : Brute-force IMAP4
- ldap_login : Brute-force LDAP
- и т.д.

Patator

FTP:

```
patator ftp_login host=example.com user=hackeru password=FILE0
0=/home/kali/YAWR/passwords/realyBest.txt -x ignore:mesg='Login
incorrect.'
```

SSH:

```
patator ssh_login host=192.168.195.201 port=2222 user=george
password=FILE0 0=rockyou.txt -x ignore:mesg='Authentication failed.'
```

HTTP Basic Auth:

```
patator http_fuzz url=http://192.168.195.201/ method=GET
header='Authorization: Basic _@_admin:FILE0_@_' -e _@_:b64
0=rockyou.txt follow=1 accept_cookie=1 -x
ignore:fgrep='Unauthorized'
```

ZIP : взломать защищенный паролем ZIP-файл (старое шифрование pkzip не поддерживается в JtR).

```
patator unzip_pass zipfile=challenge1.zip password=FILE0 0=rockyou.dic -x
ignore:code!=0
```

Модули:

- ftp_login : Brute-force FTP
- ssh_login : Brute-force SSH
- telnet_login : Brute-force Telnet
- smtp_login : Brute-force SMTP
- smtp_vrfy : Enumerate valid users using SMTP VRFY
- smtp_rcpt : Enumerate valid users using SMTP RCPT TO
- finger_lookup : Enumerate valid users using Finger
- http_fuzz : Brute-force HTTP
- ajp_fuzz : Brute-force AJP
- pop_login : Brute-force POP3
- pop_passd : Brute-force poppassd
- imap_login : Brute-force IMAP4
- ldap_login : Brute-force LDAP
- и т.д.

Поиск уязвимости

Teach Me Skills

Exploit-DB - Exploit DB
https://www.exploit-db.com
Проект компании Offensive Security, одна из самых популярных бесплатных баз данных эксплойтов, большая пополняемая база.

searchsploit

Это автономная (оффлайн) CLI-версия exploit-db
Инструкция здесь:
https://www.exploit-db.com/searchsploit

Rapid7

https://www.rapid7.com/db/
Rapid7 предлагает быстрый и удобный способ поиска уязвимостей и эксплойтов (модулей), позволяя вам изучить результаты для любого заданного запроса

CXSecurity

Эта база данных предлагает прямой доступ к последним эксплойтам через веб-интерфейс, где вы сможете отфильтровать и найти эксплойты для локальных или удаленных уязвимостей, узнать уровень риска и другие подробности, такие как автор и дата публикации.
https://cxsecurity.com/exploit/

Vulnerability Lab

Vulnerability Lab предлагает большую базу данных уязвимостей с эксплойтами и PoC для исследовательских целей.

https://www.vulnerability-lab.com

Применение эксплойтов

Teach Me Skills

За последние несколько лет было разработано несколько фреймворков для эксплуатации и пост-эксплуатации, включая

- Metasploit
- Covenant
- Cobalt Strike
- PowerShell Empire

Metasploit Framework - это среда тестирования на проникновение от Rapid7, которая помогает находить и использовать уязвимости.

```
msfconsole
```

Вы увидите, что приглашение терминала изменилось на

```
msf >
```

Показать все эксплойты:

```
show exploits
```

`search <keyword>` - контекстный поиск по модулям, возвращает список найденных модулей с номерами в таблице

`use <путь к файлу модуля>` или `use <номер из выдачи search>`- перейти к использованию определенного модуля

`show options` или `options` - показывает настройки модуля. Каждый эксплойт или полезная нагрузка имеют свои опции в коде модуля:

Добавление нового модуля

1. Найдите нужный эксплойт на сайте https://exploit-db.com или где-то еще.
   Например, для Joomla, популярной CMS с открытым исходным кодом.
2. Вставка нового эксплойта
   Пользовательские папки MSF находятся в скрытой директории `.msf4` в домашней папке пользователя

Сделайте копию эксплойта (скопируйте код в буфер обмена и вставьте его в текстовый файл, как пример).
Чтобы загрузить новый модуль, необходимо создать новый каталог в формате, который Metasploit сможет понять и прочитать.

Используйте команду `mkdir` с опцией `-p` для создания директории/поддиректорий.

```
mkdir -p ~/.msf4/modules/exploits/unix/joomla
cd ~/.msf4/modules/exploits/unix/joomla
```

Переместите эксплойт в созданную директорию

```
mv ~/Desktop/joomla_kickstart.rb ~/.msf4/modules/exploits/unix/joomla
```

3) Перезагрузите модули и настройки MSF
в msfconsole:

```
reload_all
```

Сканирование

Teach Me Skills

OWASP ZAP (Zed Attack Proxy) - инструмент для тестирования безопасности веб-приложений. Open-source проект - разрабатывается сообществом Open Web Application Security Project (**OWASP**).

1.Прокси-сервер и Перехват трафика: ZAP может выступать как прокси-сервер, позволяя анализировать и модифицировать HTTP- и HTTPS-трафик между клиентом и сервером. Применяется при инъекциях, кросс-сайтовом скриптинге (XSS) и других атаках.
2.Автоматизированный сканер уязвимостей: ZAP предоставляет автоматизированный сканер, который может обнаруживать широкий спектр уязвимостей, включая SQL-инъекции, межсайтовый скриптинг (XSS), небезопасные конфигурации и т.д.
3.Crawling: ZAP может автоматически обходить веб-приложение для поиска всех доступных страниц и ресурсов.
4.Генерация отчетов: После завершения сканирования, ZAP позволяет генерировать детальные отчеты об обнаруженных уязвимостях. Эти отчеты часто включают рекомендации по устранению найденных проблем.
5.Поддержка взаимодействия с другими инструментами: ZAP можно интегрировать с другими инструментами и средствами автоматизации тестирования.
6.Расширяемость через плагины: ZAP поддерживает использование плагинов, что позволяет расширять его функциональность в соответствии с требованиями проекта.

BadUSB

Teach Me Skills

BadUSB – вектор атаки, связанный с злонамеренным использованием USB-устройств с целью атаки на компьютерные системы.
Идея же BadUSB заключается в том, что USB-устройства, такие как флеш-накопители или клавиатуры, могут быть программированы, чтобы они выполняли вредоносные действия.

Разнообразие атак: BadUSB может принимать различные формы атак, включая эмуляцию клавиатуры для ввода команд, изменение сетевых настроек, внедрение вредоносного программного обеспечения и другие манипуляции.
Невидимость для пользователя: Пользователь, подключающий USB-устройство, может не заметить изменений, поскольку BadUSB не требует физических изменений внешнего вида устройства.
Обнаружение и предотвращение: Обнаружение BadUSB может быть сложной задачей, поскольку атаки происходят на уровне прошивки устройства.

Защита от атак: Для защиты от потенциальных атак BadUSB, производители усиливают меры безопасности прошивок, реализовывают механизмы проверки целостности и используют аппаратные средства для предотвращения изменений в прошивке.

Принцип действия: BadUSB-атака может быть реализована путем изменения прошивки USB-устройства.

Атаки на дефолтные пароли и мисконфиги роутеров

https://kali.tools/?p=501

https://hackware.ru/?p=1880

Атаки на уязвимости специфических сервисов и функции роутеров

Что атакуем:

1. Уязвимые девайсы/прошивки, операционки роутеров
2. Уязвимые второстепенные службы

Роутеры, кроме своих обычных функций, могут быть файловыми серверами, веб-серверами, торрент-клиентами и т. д.

routersploit

https://github.com/threat9/routersploit

Teach
Me
Skills

Спасибо за внимание!