

CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 6: Exploitation Methods and Tools

Module Objectives (1 of 2)

By the end of this module, you should be able to:

1. Describe methods and tools used in the exploitation and post-exploitation process
2. Explain how to select targets for exploitation
3. Describe different exploitation frameworks and their capabilities
4. Describe common exploits executed against a target

Module Objectives (2 of 2)

By the end of this module, you should be able to:

5. Identify post-exploitation methods and tools
6. Describe persistence and how to maintain persistence
7. Describe pivoting, evading detection, and clean-up methods and requirements

Selecting Targets to Exploit (1 of 16)

Key Terms

Pen testers perform exploitation to prove that discovered vulnerability is a legitimate threat, not to cause damage

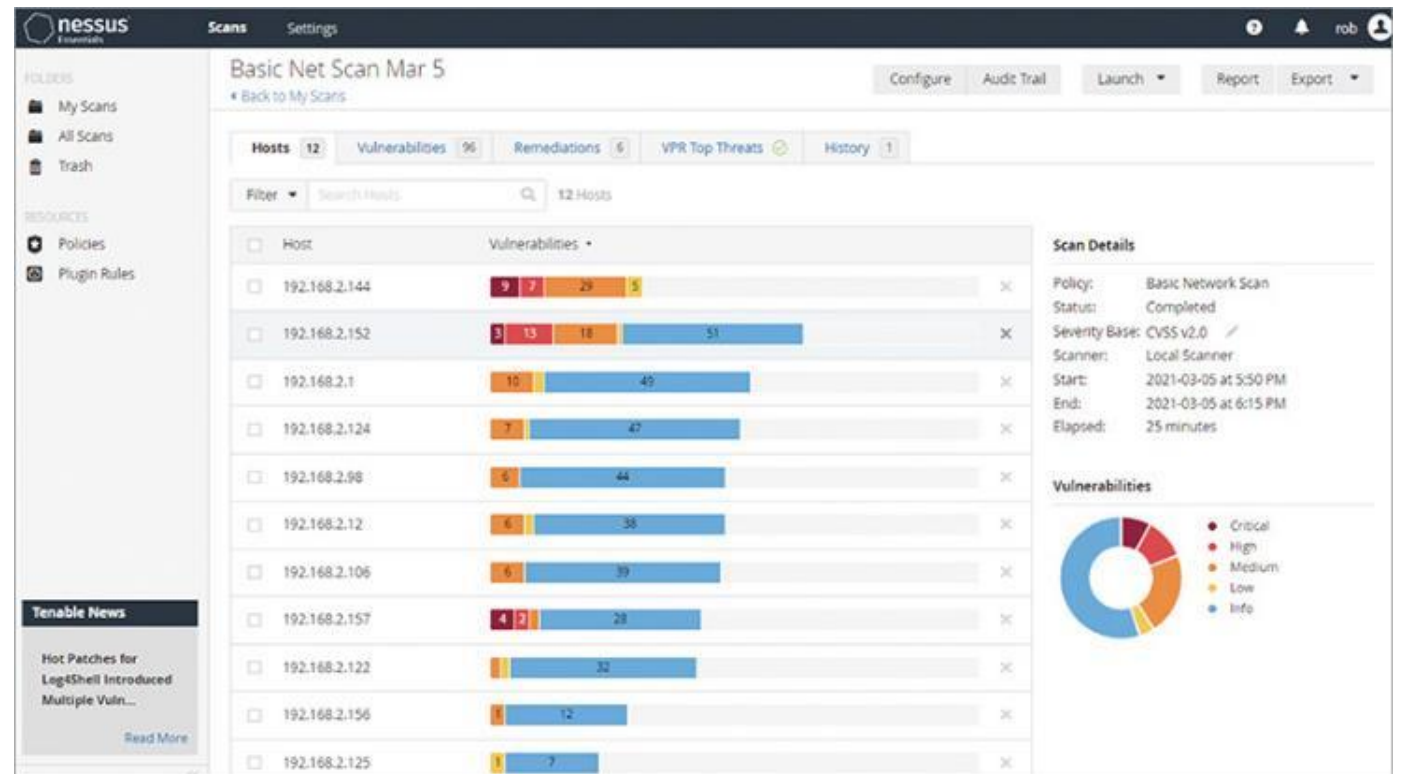
Exploitation – act of using vulnerabilities to compromise a system and gain access to it

Exploit framework – set of tools and code used to automate exploitation

Selecting Targets to Exploit (2 of 16)

Vulnerability Scanning Information

- Vulnerability scanning tools may reveal targets for potential exploitation
- Systems with most critical vulnerabilities are often targeted for exploitation

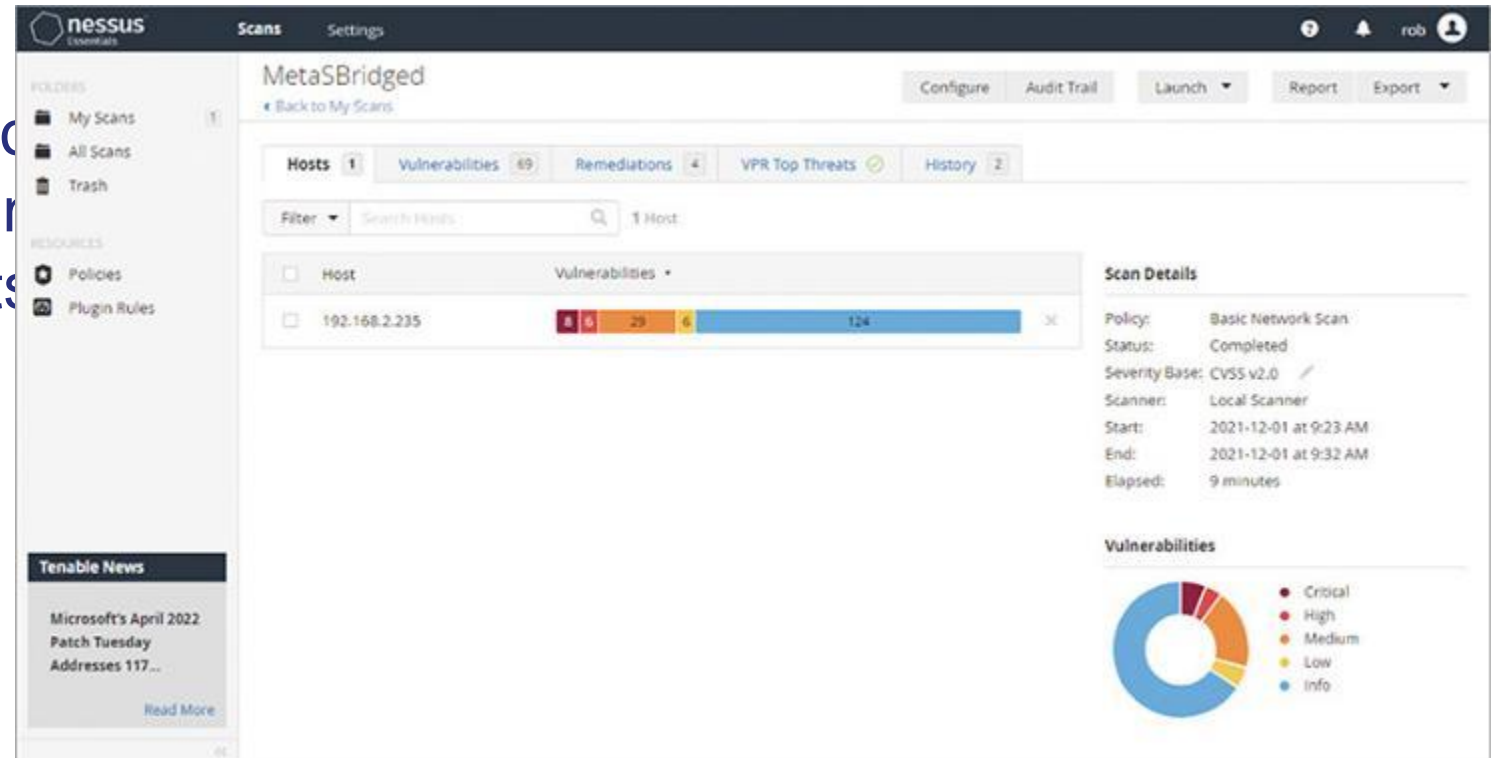


Nessus scan results

Selecting Targets to Exploit (3 of 16)

Vulnerability Scanning Information

- Severity rankings of vulnerabilities is important to take into consideration when selecting exploitation targets



Vulnerability results for one target

Selecting Targets to Exploit (4 of 16)

Using Enumeration Information

- Enumeration is part of info-gathering phase; involves collecting detailed information from target systems
 - User accounts
 - Installed applications
 - Sensitive data
 - Group/domain info
 - Operating systems
 - Unencrypted files
- Enumeration details direct focus on exploits applying to target system

Selecting Targets to Exploit (5 of 16)

Using Enumeration Information – User Accounts

- Valid user accounts help with authentication and credential-based exploits
- Valid list of user accounts can be built in many ways:
 - Guessing usernames and passwords manually
 - Brute-force tools to automate guessing thousand of credentials combos
 - Using OSINT to gather email addresses
 - Harvesting info from Active Directory on Windows systems
 - Extracting Linux system usernames from /etc/passwd file

Selecting Targets to Exploit (6 of 16)

Using Enumeration Information – Groups

- Security groups contain accounts as members to enable permissions to be assigned more efficiently
- Enumerating groups may help select groups to add members to
- Admin-level groups helps identify admin accounts
- Group information can be enumerated in multiple ways
 - Linux system group info stored in /etc/group
 - Windows domain group info located in Active Directory or locally
 - PowerShell commands can query for group info

Selecting Targets to Exploit (7 of 16)

Using Enumeration Information – Forests

- Windows targets joined to a domain are governed by Active Directory
- Forests are collections of related domains
 - Allow domains to interact by still are administratively independent
- Forests may have trust relationships with other forests
 - Exploiting target in one domain or forest may allow access to others
- Active Directory systems contain NTD.S.DIT file, which is a database of user accounts, groups, security systems, computer names and more
 - Very useful if this file can be obtained

Selecting Targets to Exploit (8 of 16)

Using Enumeration Information – Sensitive Data

- Only should be accessible by authorized individuals or accounts
- May include security info, intellectual property, personally identifiable info
- Enumerating sensitive data by pen tester is indicative of security flaw
- Sensitive data should be encrypted, requiring decryption tools to access
- PCI DSS and other regulations require data to be protected properly

Selecting Targets to Exploit (9 of 16)

Using Enumeration Information – Unencrypted Files

- Easy to read and may reveal useful exploit info
- Configuration files may be unencrypted and be useful to pen tester
 - Example: Apache web server config located in /etc/apache2 folder
- Command line tools or text editor can help determine if files are encrypted

Selecting Targets to Exploit (10 of 16)

Using Enumeration Information – Installed Applications and Operating Systems

- Target's operating system gives details to uncover vulnerabilities
- Exploits are typically specific to target OS
- Applications running on target are also keys to selecting exploits to try

Selecting Targets to Exploit (11 of 16)

Choosing Exploits

Low or Medium CVSS Vector AC Complexity

- Medium or Low Attack Complexity (AC) require quicker and may provide better results for tester

Vulnerabilities That Can Lead to Terminal or Shell Access

- An exploit that enables access to command line of target is valuable
- Much post-exploitation work can be achieved with CLI or shell access

Selecting Targets to Exploit (12 of 16)

Choosing Exploits

Several vulnerabilities may be found on targets; choosing which exploits is important and should consider:

Critical and High Vulnerabilities

- More severe flaws may leave target very vulnerable to exploit

Vulnerabilities with Known Exploit Code

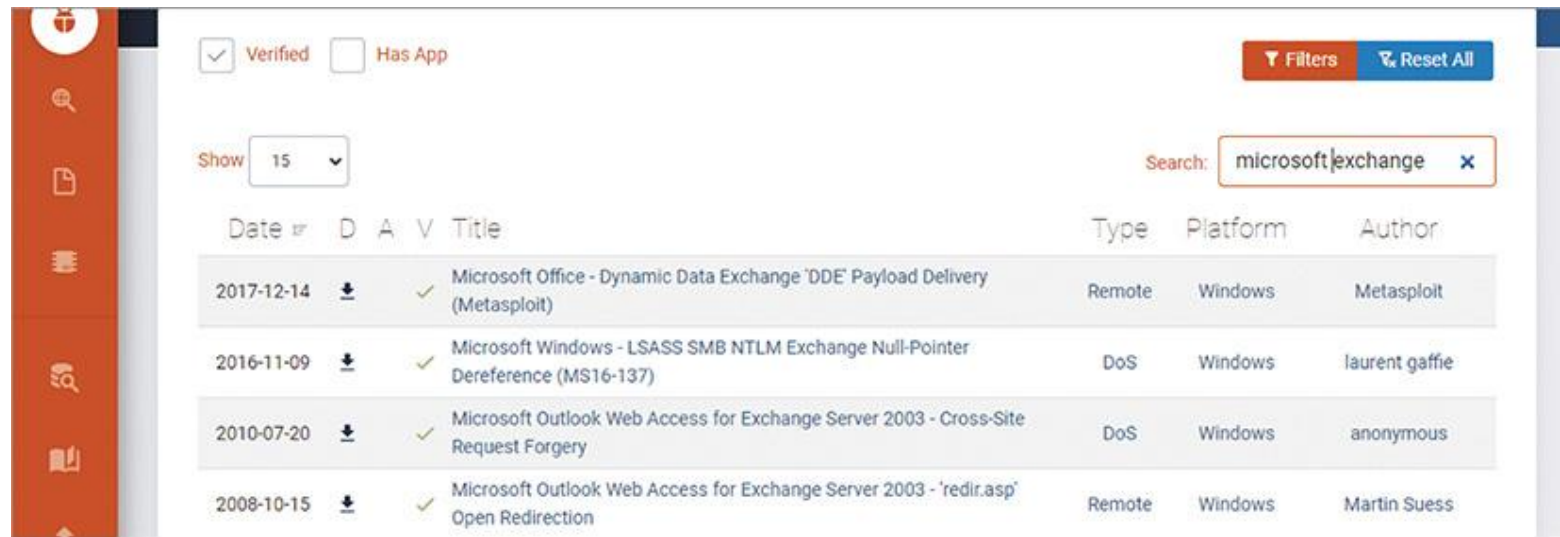
- Existing and readily available exploit code may save effort for the pen testers

Selecting Targets to Exploit (13 of 16)

Exploit Information Databases

Exploit Database –<https://exploit-db.com>

- Website with many resources
 - Exploits
 - GHDB
 - Advanced search
 - Papers written on exploit topics



The screenshot shows the Exploit Database search results for the query 'microsoft|exchange'. The interface includes a sidebar with navigation icons, a top filter bar with 'Verified' and 'Has App' checkboxes, a 'Show 15' dropdown, and a search bar with the query 'microsoft|exchange'. The results are displayed in a table with columns for Date, D (download), A (author), V (verified), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2017-12-14	↓		✓	Microsoft Office - Dynamic Data Exchange 'DDE' Payload Delivery (Metasploit)	Remote	Windows	Metasploit
2016-11-09	↓		✓	Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)	DoS	Windows	laurent gaffie
2010-07-20	↓		✓	Microsoft Outlook Web Access for Exchange Server 2003 - Cross-Site Request Forgery	DoS	Windows	anonymous
2008-10-15	↓		✓	Microsoft Outlook Web Access for Exchange Server 2003 - 'redir.asp' Open Redirection	Remote	Windows	Martin Suess

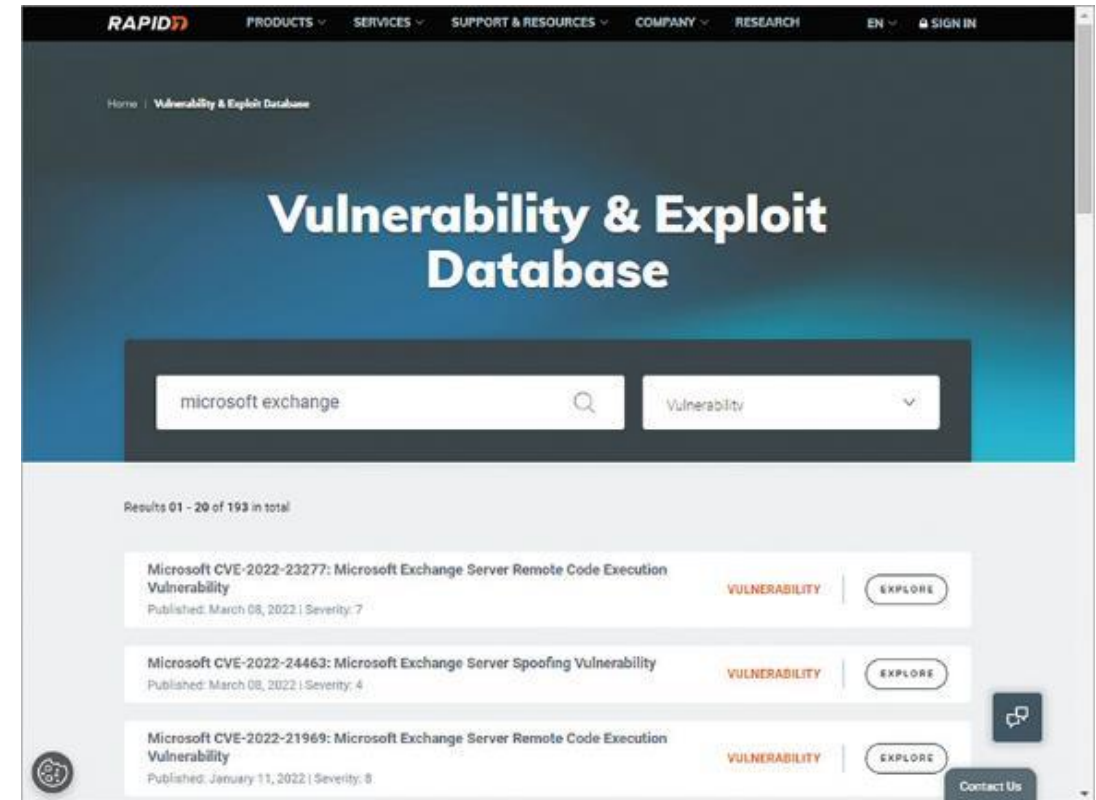
Exploit database Microsoft Exchange search results

Selecting Targets to Exploit (14 of 16)

Exploit Information Databases

Rapid7 vulnerability and exploit database <https://www.rapid7.com/db>

- Makers of Metasploit family of security and exploit software
- Integrated with Metasploit Framework
- Invaluable if using Rapid7's exploit tools like Metasploit Framework



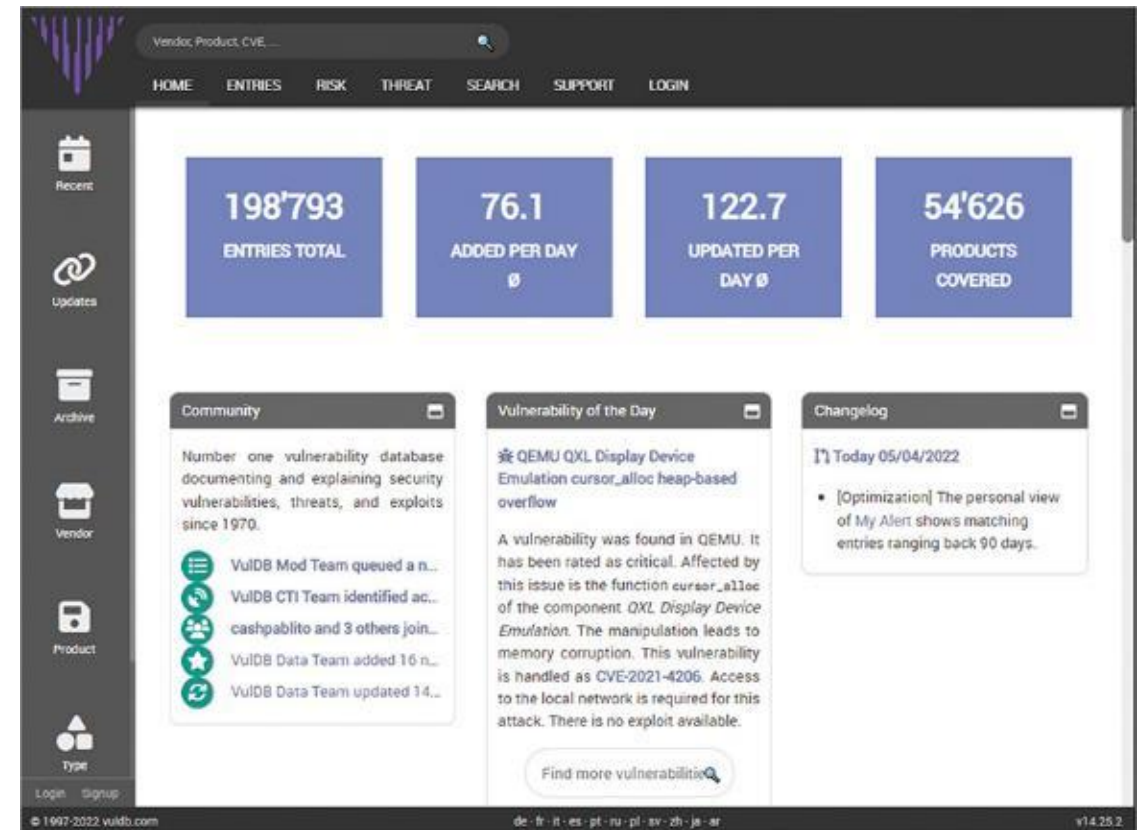
Rapid7 Vulnerability & Exploit Database

Selecting Targets to Exploit (15 of 16)

Exploit Information Databases

VulDB is a crowdsourced vulnerability database

- Contains exploit price estimates
 - How much is a particular exploit worth?



VulDB vulnerability database

Selecting Targets to Exploit (16 of 16)

Exploit Information Databases

NIST's National Vulnerability Database

- <https://nvd.nist.gov>



NIST NVD

Discussion Activity 6-1

A pen tester has numerous potential sources to gain target information or even just general information about the target's environment. These sources can then help plan an attack for exploitation.

In small groups, discuss the myriad of sources and resources that assist a pen tester in selecting targets to exploit. Create a list of the top 5 sources for targets based on how likely they may result in selecting exploit targets that can be easily compromised. Be prepared to provide justification for items on the list.

Exploit Frameworks (1 of 10)

Steps to Exploit a Vulnerability (1 of 2)

1. Attempt to connect to the target using a discovered vulnerability
2. Provide expected input and responses to the target so that the connection is accepted
3. Provide or circumvent login or credential requirements
4. Once connected, upload a small program or task so that if session is eventually rejected, connection can be more easily re-established

Exploit Frameworks (2 of 10)

Steps to Exploit a Vulnerability (2 of 2)

5. Perform reconnaissance
6. Gather data
7. Provide or circumvent login or credential requirements
8. Take steps to hide presence on the target
9. Clean up when are finished

Exploit Frameworks (3 of 10)

Steps to Exploit a Vulnerability

- Process is predictable and repeated for each exploit attempt
- Automation through programming speeds process; makes more reliable
- Exploit framework contains software tools, scripts, payloads and user interface for pen testers to perform these steps

Exploit Frameworks (4 of 10)

Metasploit

- Exploit framework created by Rapid7, a cybersecurity company offering:
 - Pen testing
 - Cloud security
 - Vulnerability management
 - Threat intelligence
- Metasploitable2 is a vulnerable target machine used in pen-test lab
- Metasploit is a free-to-use version included in Kali
- Metasploit Pro is the commercial version with enhanced features

Exploit Frameworks (5 of 10)

Metasploit

Provides function to execute the exploit steps 1 to 5

1. Start the console
2. Choose an exploit to use
3. Configure parameters needed by the exploit
4. Choose a payload if needed
5. Run the exploit

```
[+] Creating initial database schema

.:ok000kdc'          'cdk000ko:
.x00000000000000c   c0000000000000x.
:000000000000000k,  ,k00000000000000:
'000000000kkkk00000: :0000000000000000'
o0000000.   .o0000o000l.   ,0000000o
d0000000.   .c00000c.   ,00000000x
l0000000.   ;d;   ,0000000l
.0000000.   .;   ,0000000.
c000000.   .00c.   'o00.   ,0000000c
o00000.   .0000.   :0000.   ,000000o
l00000.   .0000.   :0000.   ,00000l
;0000'   .0000.   :0000.   ;0000;
.d00o   .0000o0000000.   x00d.
,k0l   .0000000000000.   .d0k,
:kk;.000000000000.c0k:
;k00000000000000k:
,x000000000000x,
.l0000000l.
.d0d,
-

=[ metasploit v6.0.45-dev ]
+ -- --[ 2134 exploits - 1139 auxiliary - 364 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 8 evasion ]

Metasploit tip: View missing module options with show
missing

msf6 > |
```

Metasploit Framework command-line console

Exploit Frameworks (6 of 10)

Metasploit – Choosing an Exploit

- Metasploit has many built-in vulnerabilities to select and with which to easily attempt exploit
- Show exploits command lists all available exploits
- “Rank” indicates likelihood of exploit to work

```
msf6 > show exploits
```

Exploits					
#	Name	Disclosure Date	Rank	Check	Description
-	-	-	-	-	-
0	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes	ibstat \$PATH Privilege Esc
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes	Xorg X11 Server Local Priv
2	exploit/aix/rpc_cmds_opcode21	2009-10-07	great	No	AIX Calendar Manager Servi
low					
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No	ToolTalk rpc.ttdbserverd _
4	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server R
5	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	No	Samsung Galaxy KNOX Androi
6	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx
7	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebVie
8	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader for Android a
9	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-F
10	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex
11	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signatur
12	exploit/android/local/put_user_vroot	2013-09-06	excellent	No	Android get_user/put_user
13	exploit/android/local/su_exec	2017-08-31	manual	No	Android 'su' Privilege Esc
14	exploit/apple_ios/browser/safari_jit	2016-08-25	good	No	Safari Webkit JIT Exploit
15	exploit/apple_ios/browser/safari_libtiff	2006-08-01	good	No	Apple iOS MobileSafari Lib
16	exploit/apple_ios/browser/webkit_createthis	2018-03-15	manual	No	Safari Webkit Proxy Object
17	exploit/apple_ios/browser/webkit_trident	2016-08-25	manual	No	WebKit not_number definePr
18	exploit/apple_ios/email/mobilemail_libtiff	2006-08-01	good	No	Apple iOS MobileMail LibTI

Metasploit Framework Exploits list

Exploit Frameworks (7 of 10)

Metasploit

- Metasploit Framework is very powerful and flexible
- More info contained in course text and countless online resources
- Contains many “payloads”, or code that successful exploits execute
 - Payloads are what an exploit makes happen on target
 - Opening network back door
 - Installing malicious software
 - Executing remote commands

Exploit Frameworks (8 of 10)

Metasploit

PowerSploit

- Windows PowerShell scripts
 - Bypass antivirus
 - Execute code
 - Exfiltrate data
 - Perform recon
 - Maintain persistence
 - Extract Credentials

```
> Executing "powersploit"  
> powersploit ~ PowerShell Post-Exploitation Framework  
/usr/share/windows-resources/powersploit  
├─AntivirusBypass  
├─CodeExecution  
├─Exfiltration  
├─Mayhem  
├─Persistence  
├─PowerSploit.psdl  
├─PowerSploit.psm1  
├─Privesc  
├─README.md  
├─Recon  
├─ScriptModification  
├─Tests  
└─  
(kali㉿kali)-[/usr/share/windows-resources/powersploit]  
$
```

PowerSploit in Kali Linux shell

Exploit Frameworks (9 of 10)

Metasploit

Empire

- Windows PowerShell and Python-based libraries
- Perform post-exploit actions
- Hides communication by using encryption
- CLI similar to Metasploit

```
=====
[Empire] Post-Exploitation Framework
=====
[Version] 3.2.1 BC-Security Fork | [Web] https://github.com/BC-SECURITY/Empire
=====
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
=====

  EMPiRE

  299 modules currently loaded
  0 listeners currently active
  0 agents currently active

(Empire) > |
```

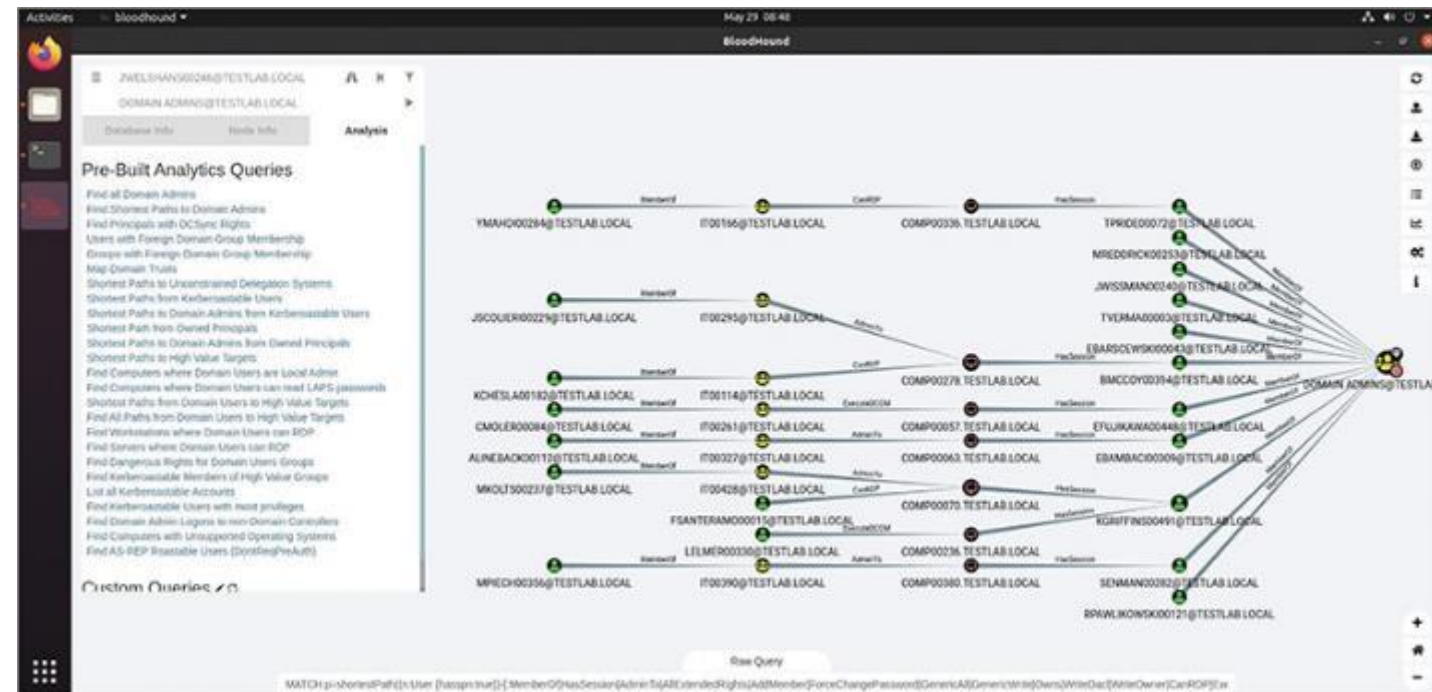
Empire command-line interface

Exploit Frameworks (10 of 10)

Metasploit

BloodHound

- Visualizes Active Directory
- AD info must be acquired first
- Graphically displays relationships between AD groups, accounts, and security settings



BloodHound graphical user interface

Discussion Activity 6-2

The Metasploit Framework is by far the most common and comprehensive exploit framework available to pen testers and security students alike.

Spend some time researching the advanced and additional features not discussed in this course. Discuss how they work in the context of a penetration test. What are the most useful features?

What are some of the features and tools that are available in the commercial versions of Metasploit Pro? How might they be useful in a pen test?

Common Exploits (1 of 9)

Remote Procedure Call/Distributed Component Object Model

- RPC/DCOM is Windows client-to-server communication model
- Allows clients to send and execute requests to servers
- Successful exploit allows remote code execution on target

PsExec

- Windows Sysinternals tool allows execution of programs on targets
- Primarily uses TCP port 445 and Server Message Block (SMB) protocol
- Modified version included as Metasploit payload

Common Exploits (2 of 9)

PSRemoting and WinRM

- WinRM in Windows 7 and later allows remote PowerShell execution
- Disabled by default; can be enabled by admin command on target

Windows Management Instrumentation

- WMI supports management operation and query on remote hosts
- Network management and inventory tools commonly employ WMI
- Can remotely execute commands and transfer files to a target
- PowerShell exploit tools can utilize WMI for remote actions

Common Exploits (3 of 9)

Fileless Malware

- Malware stored on target's disk can be detected by antivirus
- Malware loaded directly into memory; bypasses disk access

Living off the Land

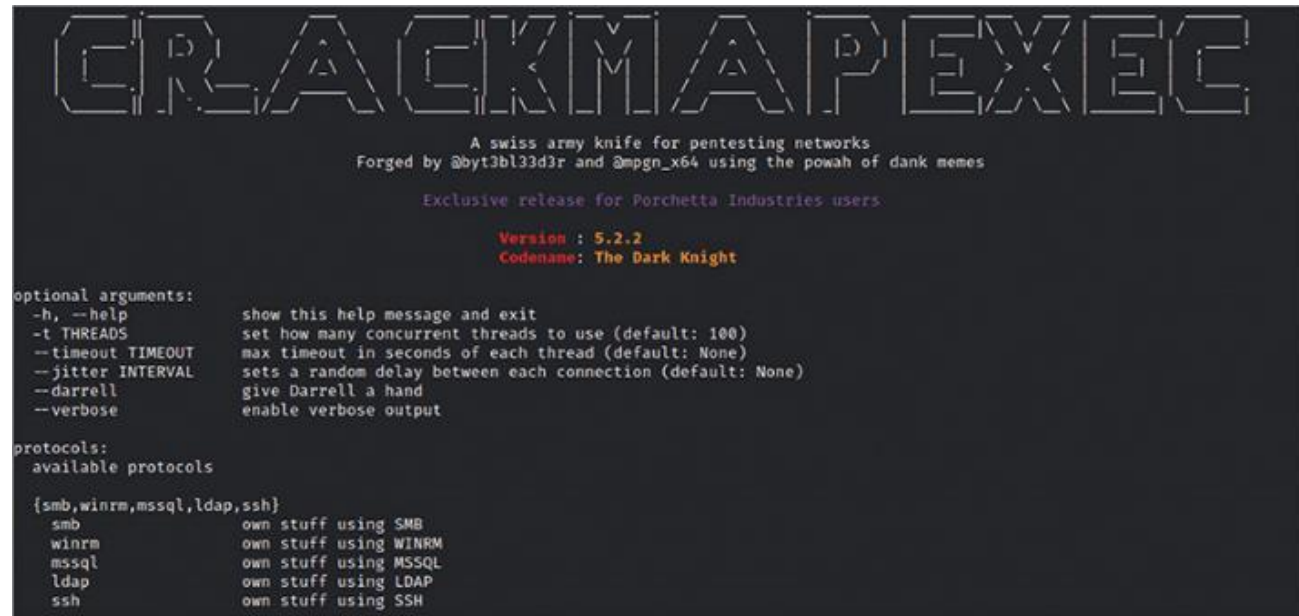
- Term describes use of native OS tools for remote pen-test actions
- PowerShell commands, file and process tools, and similar software
- Active Directory tools useful for network recon and actions

Common Exploits (4 of 9)

Living off the Land

CrackMapExec

- Exploit software uses native AD tools
- Performs multiple attacks
 - Null sessions
 - Pass-the-hash
 - Brute force &
 - Password spraying
 - Data gathering

The image shows the starting screen of CrackMapExec. At the top, the title 'CRACKMAPEXEC' is displayed in a large, stylized, outlined font. Below it, a subtitle reads 'A swiss army knife for pentesting networks', followed by 'Forged by @byt3bl33d3r and @mpgn_x64 using the powah of dank memes'. A line of text states 'Exclusive release for Porchetta Industries users'. The version 'Version : 5.2.2' and codename 'Codename: The Dark Knight' are shown in red. The screen then lists 'optional arguments' with their descriptions: '-h, --help' (show this help message and exit), '-t THREADS' (set how many concurrent threads to use), '--timeout TIMEOUT' (max timeout in seconds), '--jitter INTERVAL' (sets a random delay), '--darrell' (give Darrell a hand), and '--verbose' (enable verbose output). Below this, it lists 'protocols: available protocols' and shows a list of protocols: smb, winrm, mssql, ldap, and ssh, each with a description of what it does (e.g., 'own stuff using SMB').

```
CRACKMAPEXEC

A swiss army knife for pentesting networks
Forged by @byt3bl33d3r and @mpgn_x64 using the powah of dank memes

Exclusive release for Porchetta Industries users

Version : 5.2.2
Codename: The Dark Knight

optional arguments:
-h, --help            show this help message and exit
-t THREADS            set how many concurrent threads to use (default: 100)
--timeout TIMEOUT    max timeout in seconds of each thread (default: None)
--jitter INTERVAL    sets a random delay between each connection (default: None)
--darrell            give Darrell a hand
--verbose            enable verbose output

protocols:
available protocols

{smb,winrm,mssql,ldap,ssh}
smb                own stuff using SMB
winrm              own stuff using WINRM
mssql              own stuff using MSSQL
ldap               own stuff using LDAP
ssh                own stuff using SSH
```

CrackMapExec starting screen

Common Exploits (5 of 9)

Scheduled Tasks

- Utilizing OS native scheduling tools can be useful to retain access
- Scheduled Task system in Windows and Cron jobs in Linux
- Tasks can be timed to reload payload regularly in case of discovery and termination by target

Leaked Keys

- Targets may use key-based authentication instead of usernames and passwords to automate logins for efficiency and security
- Discovered or leaked keys can provide pen testers access to targets
- Keys may be unintentionally stored in public resources like GitHub

Common Exploits (6 of 9)

Server Message Block (SMB)

- Powerful platform independent protocol for multiple purposes
 - File sharing
 - Authentication
 - Authorization
 - Printer sharing
 - Name resolution
- Multiple versions still in use: SMB, SMB2, and SMB3 versions
- Security has improved greatly over protocol's evolution
 - Open shares with no authentication requirement still in use
- Impacket is Python-based toolset and libraries for SMB attacks
 - SMB hash playback
 - WMI persistence
 - MS-SQL authentication
 - Replicating PSEXEC
 - Remote data dumps

Common Exploits (7 of 9)

Domain Name System (DNS)

- DNS is a network service providing IP info and name resolution to hosts
- Systems first check local “hosts” file for manually set IP resolution
- DNS is common target of exploits
 - Modify hosts file with malicious IP to direct target to specific host
 - Take over DNS server to provide targets with bogus IP resolution
 - Intercept DNS or DHCP requests and redirect to malicious server
 - Perform DoS attacks against DNS servers, preventing resolution

Common Exploits (8 of 9)

Remote Desktop Protocols (RDP)

- Windows RDP allows access to remote system via GUI console tools
- Supports remote control of systems as if sitting at console directly
- Uses TCP/UDP port 3389
- Intercepting RDP traffic may allow access to login credentials or hashes
- Wide variety of vulnerabilities and exploits exist in RDP

Virtual Network Computing (VNC)

- Platform-independent tool providing similar access to target as RDP
- Metasploit payload remotely executes VNC and provides access to target

Common Exploits (9 of 9)

Secure Shell (SSH)

- Protocol and tool for remote access to a computer system
- Command line access rather than remote GUI; powerful admin tool
- Various SSH server and protocol vulnerabilities and exploits are available

Network Segments and Virtual Local Area Networks (VLANs)

- Networks commonly divided into segments for multiple reasons
- VLANs separate layer 2 segments; layer 3 devices must connect VLANs
- Packet sniffing can provide VLAN information about target networks
- “VLAN hopping” and “double tagging” are VLAN attack method

Knowledge Check Activity 6-1

Exploiting which of the following network protocols (and the associated servers that run it as a service) may interfere with the hosts on a network from accessing the internet resources due to incorrect address information?

- a. RPC
- b. SSH
- c. SMB
- d. DNS

Knowledge Check Activity 6-1: Answer

Exploiting which of the following network protocols (and associated servers running it as a service) may interfere with a host or multiple hosts on a network from accessing the internet resources due to incorrect address information?

Answer: DNS

The Domain Name System or DNS protocols and servers are responsible for providing IP address responses to queries from clients seeking name resolution of a hostname such as www.mitre.org. Several techniques exist to perform attacks to disrupt or manipulate proper DNS operation.

Post Exploitation (1 of 6)

Post exploitation – actions threat actor takes after gaining access

Password Attacks

- Attempt to circumvent or provide credentials to a target
- Aim to harvest credentials from compromised system
- Social engineering and internet password dumps can be source of data
- Brute forcing – attempting countless credential combos; very detectable
- Wordlists available online as resource for password attacks like spraying
- Many tools and methods are available for password attacks

Post Exploitation (2 of 6)

Password Attacks

- John The Ripper is a well-known password and hash- cracking tool
- Can decode password hashes and revert to the original using multiple techniques

```
(kali㉿kali)-[~]
$ john --help
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

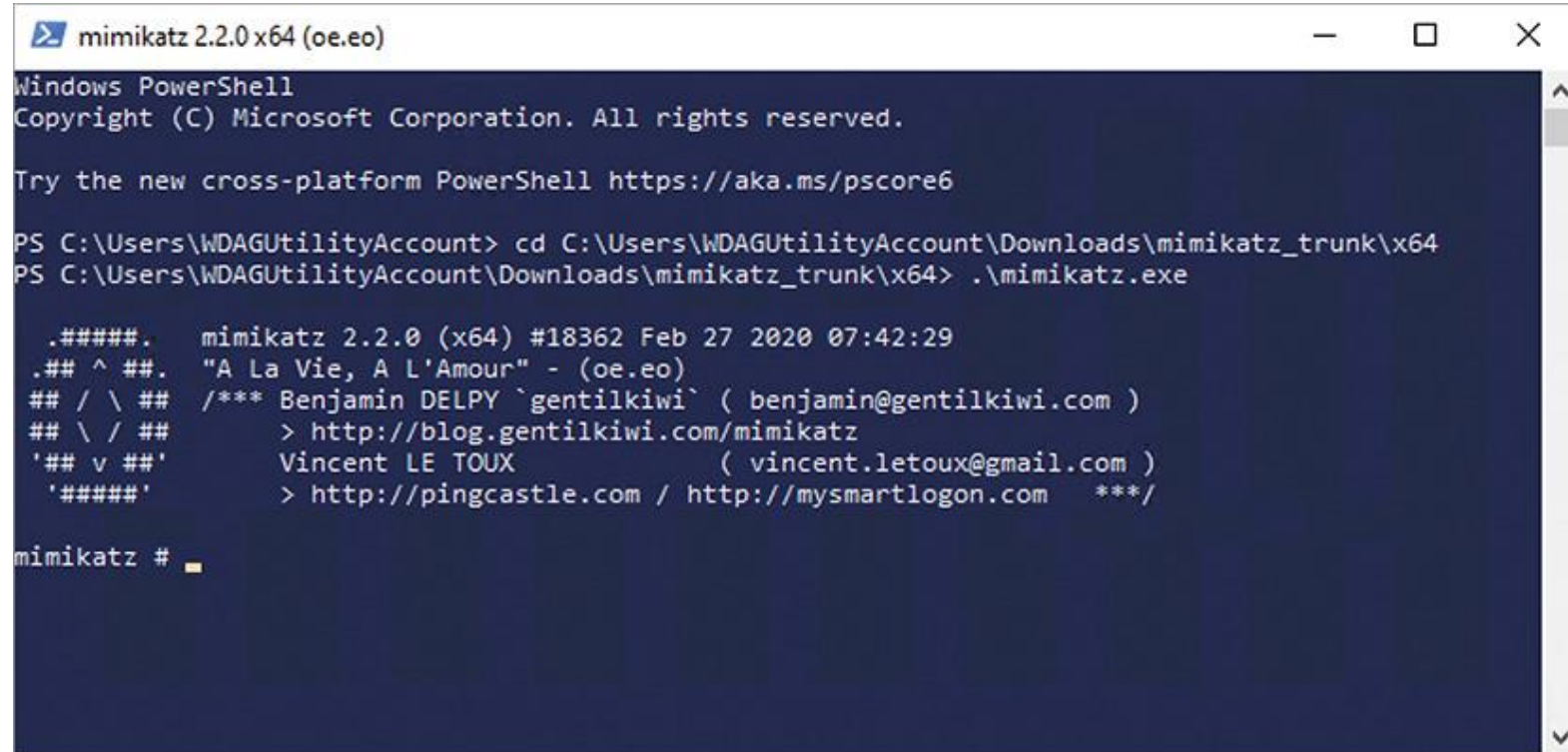
Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[, ..]]  "single crack" mode, using default or named rules
--single=:rule[, ..]      same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                        --pipe  like --stdin, but bulk reads, and allows rules
--loopback[=FILE]         like --wordlist, but extract words from a .pot file
--dupe-suppression        suppress all dupes in wordlist (and force preload)
--prince[=FILE]           PRINCE mode, read words from FILE
--encoding=NAME           input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[, ..]]  enable word mangling rules (for wordlist or PRINCE
                        modes), using default or named rules
--rules=:rule[, ..]      same, using "immediate" rule(s)
--rules-stack=SECTION[, ..] stacked rules, applied after regular rules or to
                        modes that otherwise don't support rules
--rules-stack=:rule[, ..] same, using "immediate" rule(s)
--incremental[=MODE]      "incremental" mode [using section MODE]
--mask[=MASK]             mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]        "Markov" mode (see doc/MARKOV)
--external=MODE           external mode or word filter
--subsets[=CHARSET]       "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
```

John the Ripper help information

Post Exploitation (3 of 6)

Mimikatz Tool

- Popular and feature-rich post-exploitation tool
- Dumps Windows passwords from:
 - Memory
 - Hashes
 - Kerberos tickets



```
mimikatz 2.2.0 x64 (oe.eo)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\WDAGUtilityAccount> cd C:\Users\WDAGUtilityAccount\Downloads\mimikatz_trunk\x64
PS C:\Users\WDAGUtilityAccount\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #18362 Feb 27 2020 07:42:29
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***

mimikatz #
```

Mimikatz executed in PowerShell

Discussion Activity 6-3

The topic of password attacks is complex and ranges widely. Attacks can range from the simple guessing of passwords to an account of someone an attacker knows to the brute forcing of stolen hashes employing cloud computing resources to perform the processing at a large scale.

Dig deeper into the topic of password attacks and choose two attack types and the associated tools that perform them. Discuss the information found, and consider whether it would be a useful tactic for a pen-test engagement.

Post Exploitation (4 of 6)

Privilege Escalation

- After system compromise, pen-tester permissions are of standard user
- Privilege escalation raises permissions and access level
 - Vertical escalation – raise in privilege; admin level is ultimate goal
 - Horizontal escalation – gain access to accounts with same level
- Poor security design and configuration can make easier
- Privilege escalation can occur on many target types and objects
 - OS or kernel
 - Databases
 - Applications and services

Post Exploitation (5 of 6)

Data Exfiltration

- Process of accessing and removing info from compromised hosts
- Can use standard sharing protocols and apps like FTP, SSH, or SMB
- May use subtle, concealed, and encrypted methods to avoid detection
- Steganography – technique to embed data in image, audio, or other files

Cross Compiling

- Takes source code for software on specific platform and rebuilds for another
- Example: to execute a Windows exploit on Android target

Post Exploitation (6 of 6)

Shell Escape and Upgrade

- Command line access gained by pen tester on target may be limited
- Linux hosts challenge-privileged command execution with root password
- Shell vulnerabilities can be exploited to “escape” a limited shell
- Shell “upgrade” is when limited shell is “escaped” to privileged shell

Social Engineering

- Attackers can use social engineering exploits by manipulating people and leveraging human weaknesses
- Info gained by traditional exploits may inspire social engineering attempts

Persistence (1 of 3)

Persistence involves using tools and methods to maintain access to compromised target hosts

Scheduled Jobs and Tasks

- Scheduling tasks and Cron jobs can be easy persistence tool
- Use to reload backdoor or exploit tool after reboot or periodically

Inetd Modules

- Linux's Inted service starts up services to provide network functionality
- Malicious service can be added to Inetd's config file to load backdoor

Persistence (2 of 3)

Daemons and Services

- Daemon – hidden program; runs in background; common Linux term
- Services are similar but may specifically provide features or data access
- Either could be corrupted to execute malware or maintain access\

Backdoors

- Metasploit's Meterpreter payload can create backdoor shell from compromised to target to pen tester's system running Metasploit
- Traditional services may be replaced by attacker with versions that have known vulnerabilities to exploit for persistent access

Persistence (3 of 3)

Creating Accounts

- Compromised hosts may allow for creating new accounts by attacker
- New accounts less likely to be detected than compromised accounts
- Adhering to naming scheme of target organization helps avoid discovery
- Command line tools can create accounts and easily grant access

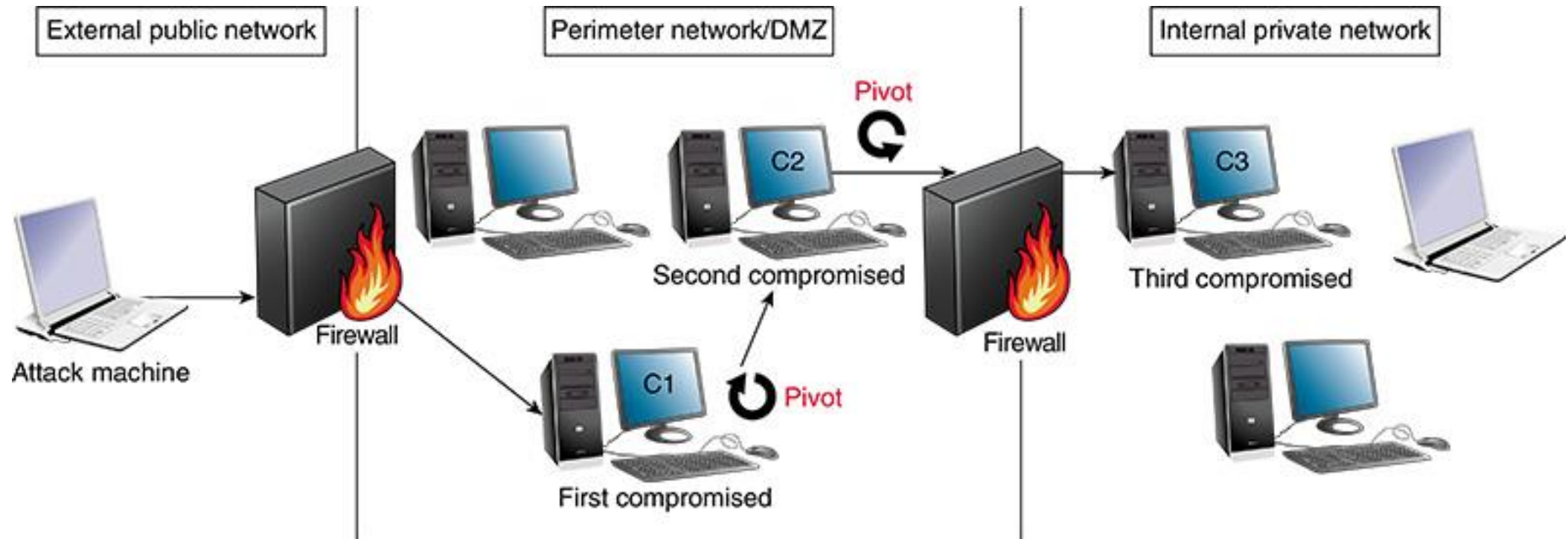
Pivoting, Evading, and Cleaning Up (1 of 3)

Pivoting

- Once a system is compromised, it can be used to launch further attacks
- Pivoting – using compromised targets to explore and attack other targets
- Pivoting can also occur within a single target
 - Using compromised web app to explore and exploit SQL server
- A well-placed compromised host sits on internal network, allowing access to segments that may have been unavailable to pen tester

Pivoting, Evading, and Cleaning Up (2 of 3)

Pivoting



Pivoting through the DMZ to an internal private network

Pivoting, Evading, and Cleaning Up (3 of 3)

Evading and Cleaning Up

- In pen testing, cleanup includes removal of tools from compromised systems and traces of activities performed
 - Tools or files uploaded
 - Deleting logs or editing log entries
 - Removing temporary files
- Threat actor may leave no traces or Indicators of Compromise (IOC)
- Obvious IOCs like ransomware screens and locked files may remain
- Encryption and obfuscation tools can also help with evading detection

Summary (1 of 2)

By the end of this module, you should be able to:

1. Describe methods and tools used in the exploitation and post-exploitation process
2. Explain how to select targets for exploitation
3. Describe different exploitation frameworks and their capabilities
4. Describe common exploits executed against a target

Summary (2 of 2)

By the end of this module, you should be able to:

5. Identify post-exploitation methods and tools
6. Describe persistence and how to maintain persistence
7. Describe pivoting, evading detection, and clean-up methods and requirements