

CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 10: Host Attack Vectors
and Cloud Technologies Attacks

Module Objectives (1 of 3)

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

1. Describe nonoperating specific host attacks such as taking advantage of permission configuration errors, accessing stored credentials, exploiting defaults, and brute-forcing credentials
2. Describe various remote access attack methods such as hiding attacks using SSH, NETCAT/Ncat, Metasploit framework remote access, and proxies
3. Describe Linux/Unix host attacks such as SUID/GUID SUDO, shell upgrade, and kernel exploits, credential harvesting, and password cracking

Module Objectives (2 of 3)

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

4. Describe Windows host attacks such as credential hash, LSA secrets, SAM database, and kernel exploits, credential harvesting, and password cracking
5. Describe attacks against virtualization such as virtual machine (VM), hypervisor, and VM repository exploits, VM escaping, and container exploits

Module Objectives (3 of 3)

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

6. Describe attacks against cloud-based targets such as account, misconfiguration, and data storage exploits, malware injection, denial-of-service and resource exhaustion attacks, and direct-to-origin exploits
7. Describe cloud attack tools and their usage
8. Describe attacks against cloud-based data storage

Attacking Hosts (1 of 31)

Non-operating System-Specific Exploits

- Some exploits are useful and independent of platform or operating system
- Examples include exploiting configuration mistakes or other administration errors

File System Permission Configuration Errors

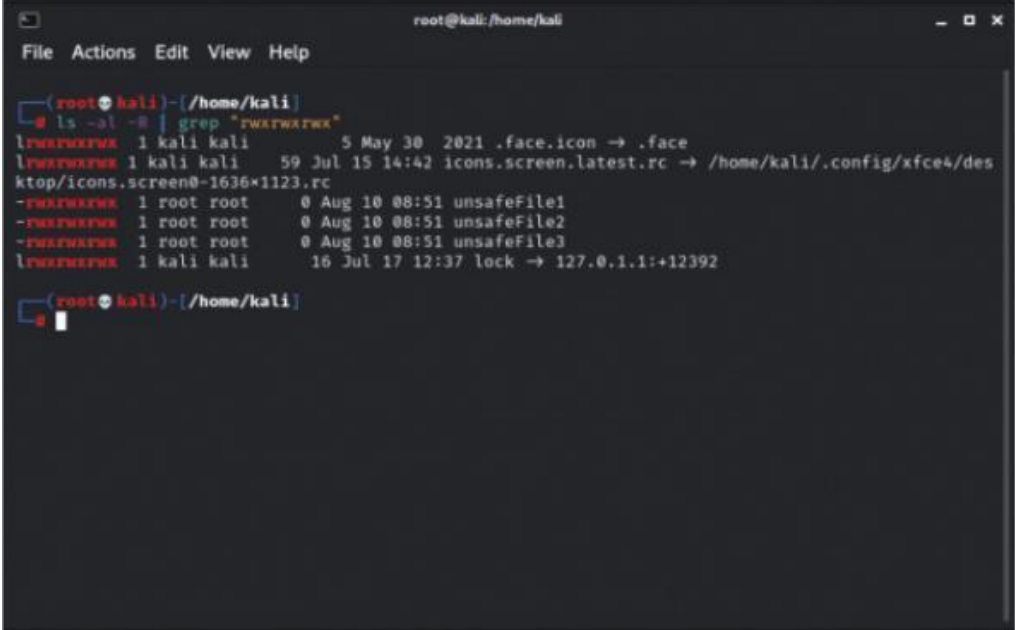
- A host computer's file system is protected by elaborate set of permissions to provide access to authorized users and deny others

Attacking Hosts (2 of 31)

Non-operating System-Specific Exploits

File System Permission Configuration Errors

- Permission assignment errors can deny legitimate users the access they are entitled to and can open doors to threat actors and snoops
- Linux hosts can use the `ls` and `grep` tools to scan entire file systems for permission errors



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~[/home/kali]
# ls -al -R | grep "rwxrwxrwx"
lrwxrwxrwx 1 kali kali      5 May 30  2021 .face.icon -> .face
lrwxrwxrwx 1 kali kali    59 Jul 15 14:42 icons.screen.latest.rc -> /home/kali/.config/xfce4/desktop/icons.screen@-1636x1123.rc
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile1
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile2
-rwxrwxrwx 1 root root      0 Aug 10 08:51 unsafeFile3
lrwxrwxrwx 1 kali kali    16 Jul 17 12:37 lock -> 127.0.1.1:+12392

(root@kali)~[/home/kali]
#
```

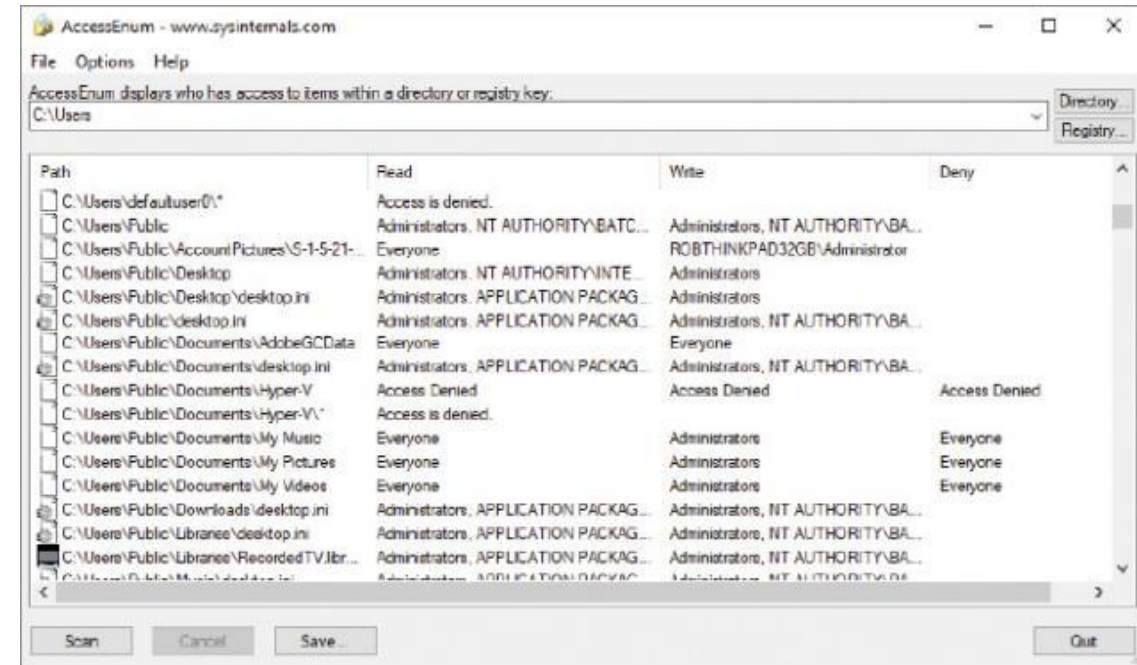
`ls` and `grep` used to find insecure files

Attacking Hosts (3 of 31)

Non-operating System-Specific Exploits

File System Permission Configuration Errors

- Windows tools from Sysinternals like AccessEnum and Accesschk can discover file system permission errors
- Windows PowerShell also has powerful commands to perform these tasks



Sysinternals AccessEnum tool

Attacking Hosts (4 of 31)

Non-operating System-Specific Exploits

Stored Credentials

- Applications and operating systems may store credentials for users
 - Often done for convenience in web browsers and other apps
- These credentials may be stored in the Windows registry
- Registry is a collection of databases of Windows configuration settings
- Gaining access to a computer may provide access to user password manager tools or other credential storage locations

Attacking Hosts (5 of 31)

Non-operating System-Specific Exploits

Defaults

- Unchanged default settings are a security vulnerability
- Best practices dictate changing many default settings, especially credentials
- Default credentials for systems and applications may provide access
- Configuration settings may also be left at higher-than-recommended access levels by default

Attacking Hosts (6 of 31)

Non-operating System-Specific Exploits

Credential Brute Forcing

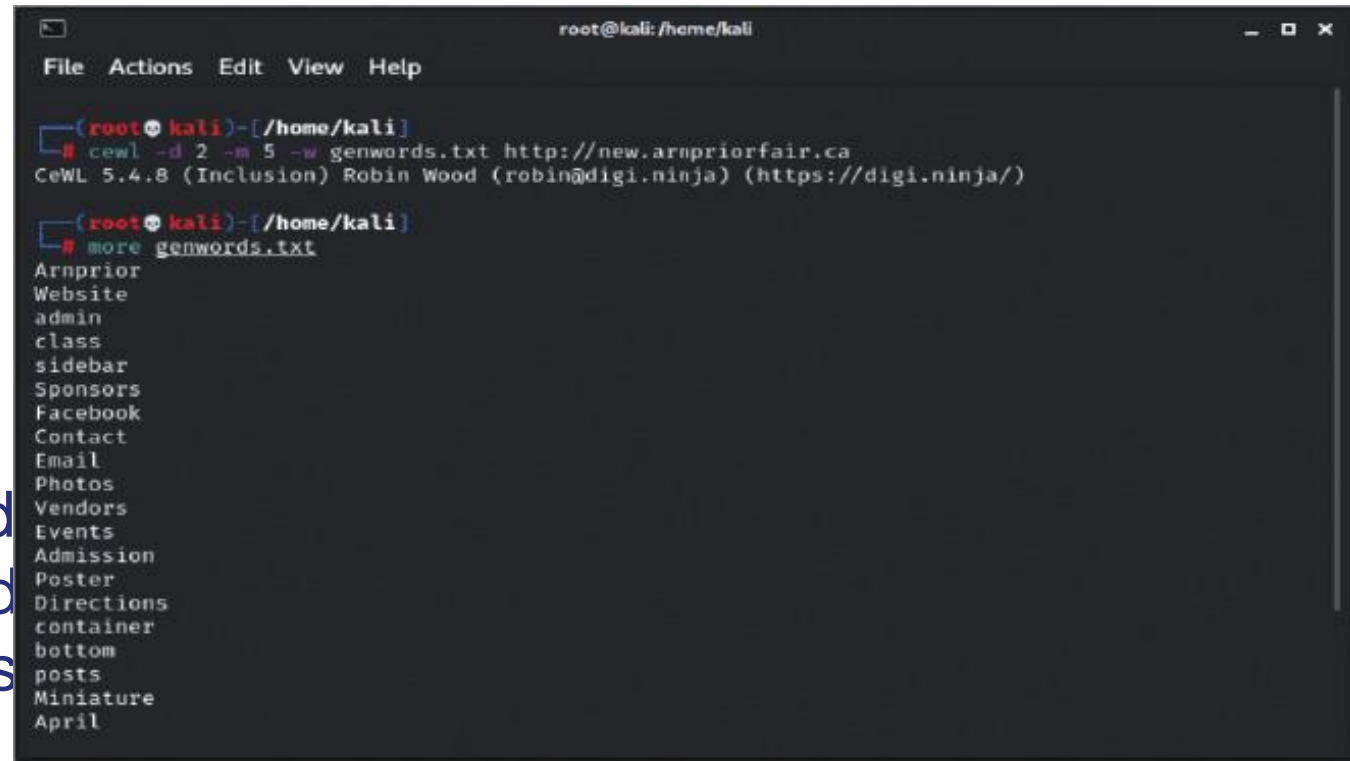
- Various tools exist to perform brute force attacks
 - THC-Hydra, Medusa, and Patator support wide variety of methods
- Attacks can be directed at operating systems or applications
- Commonly attacked entities include OS logins, web apps, databases
- Protocols often targeted for brute force are SSH, SMB, SMB, but many can be attacked this way

Attacking Hosts (7 of 31)

Non-operating System-Specific Exploits

Credential Brute Forcing

- Lists generated from account breaches can be used in credential attacks
- Tools like Custom Word List Generator (CeWL) can scrape and analyze a website and create word list and create lists by other means



```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)~/home/kali
$ cewl -d 2 -m 5 -w genwords.txt http://new.arnpriorfair.ca
CeWL 5.4.8 (Inclusion) Robin Wood (robin@diginiinja) (https://diginiinja/)

(root@kali)~/home/kali
$ more genwords.txt
Arnprior
Website
admin
class
sidebar
Sponsors
Facebook
Contact
Email
Photos
Vendors
Events
Admission
Poster
Directions
container
bottom
posts
Miniature
April
```

CeWL generating a wordlist by scanning a website

Attacking Hosts (8 of 31)

Non-operating System-Specific Exploits

Secure Shell (SSH)

- SSH – common remote access method for regular users, pen testers, system administrators, and threat actors
- SSH's encryption capabilities allow threat actors to hide actions; can also be used to tunnel other protocols and traffic
- SSH port forwarding can stealthily relay traffic between systems
- User file system directories can contain SSH keys
- SSH often runs by default on Linux hosts

Attacking Hosts (9 of 31)

Non-operating System-Specific Exploits

NETCAT and Ncat

- Netcat and successor Ncat are compact network tools used to create remote sessions and many other useful applications for pen testers
- Command line `nc` tool can set up a reverse shell from a host
- `nc` commands for Linux and Windows are similar
- Ncat may be used as a remote listener or backdoor
- Some antimalware tools detect `nc` as potentially unwanted application

Attacking Hosts (10 of 31)

Non-operating System-Specific Exploits

Metasploit Framework Remote Access Exploits

- Metasploit and its well-known payload Meterpreter support many reverse and bind shells on targets
- Reverse shell initiates from compromised host to attacker's system

Proxies

- Proxy server acts as an intermediary between users and other servers
- Communicating through multiple proxies is known as proxy chaining and is another method for hiding traffic

Attacking Hosts (11 of 31)

Linux/Unix Hosts

- Linux and Unix come in many different releases or distributions (distros)
- Each has similar underlying OS or kernel, but various applications, interfaces, configurations, and purposes
 - Red Hat is an enterprise-level distribution
 - Ubuntu is focused on home users but has evolved its offerings
 - Many commercial and free Unix variations also exist
- Linux's flexibility and open licensing makes it common on embedded systems, networking devices, IoT, and other systems

Attacking Hosts (12 of 31)

Linux/Unix Hosts

Exploiting SUID/GUID

- Set user ID (SUID or SETUID) and set group ID (GUID) are permission bits set to either 1 or 0 to indicate executable file run privilege
- If root user creates executable and sets SUID bit to on or 1, it will always execute with root level privilege even if the program is run by standard user
- GUID permission bit can be set to run with permissions of group owner

Attacking Hosts (13 of 31)

Linux/Unix Hosts

Exploiting SUID/GUID

- Command Linux commands such as `cp` and `find` will be set to allow these commands to perform actions that would normally be beyond executing user's privileges
- Determining SUID and GUID on executables may help further pen-test activities on Linux target

```
(root@kali)~# find / -perm -u+s -type f 2>/dev/null
/usr/sbin/mount.nfs
/usr/sbin/mount.cifs
/usr/sbin/pppd
/usr/sbin/exim4
/usr/bin/newgrp
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/su
/usr/bin/kismet_cap_ti_cc_2540
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/ntfs-3g
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/kismet_cap_nrf_52840
/usr/bin/kismet_cap_linux_wifi
/usr/bin/pkexec
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/kismet_cap_nrf_51822
/usr/bin/mount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/mysql/plugin/auth_pam_tool_dir/auth_pam_tool
/usr/lib/xorg/Xorg.wrap
/usr/lib/virtualbox/VBoxSDL
/usr/lib/virtualbox/VBoxNetNAT
/usr/lib/virtualbox/VBoxNetAdpCtl
/usr/lib/virtualbox/VirtualBoxVM
/usr/lib/virtualbox/VBoxNetDHCP
/usr/lib/virtualbox/VBoxHeadless
/usr/libexec/polkit-agent-helper-1
/usr/libexec/spice-client-glib-usb-acl-helper
(root@kali)~#
```

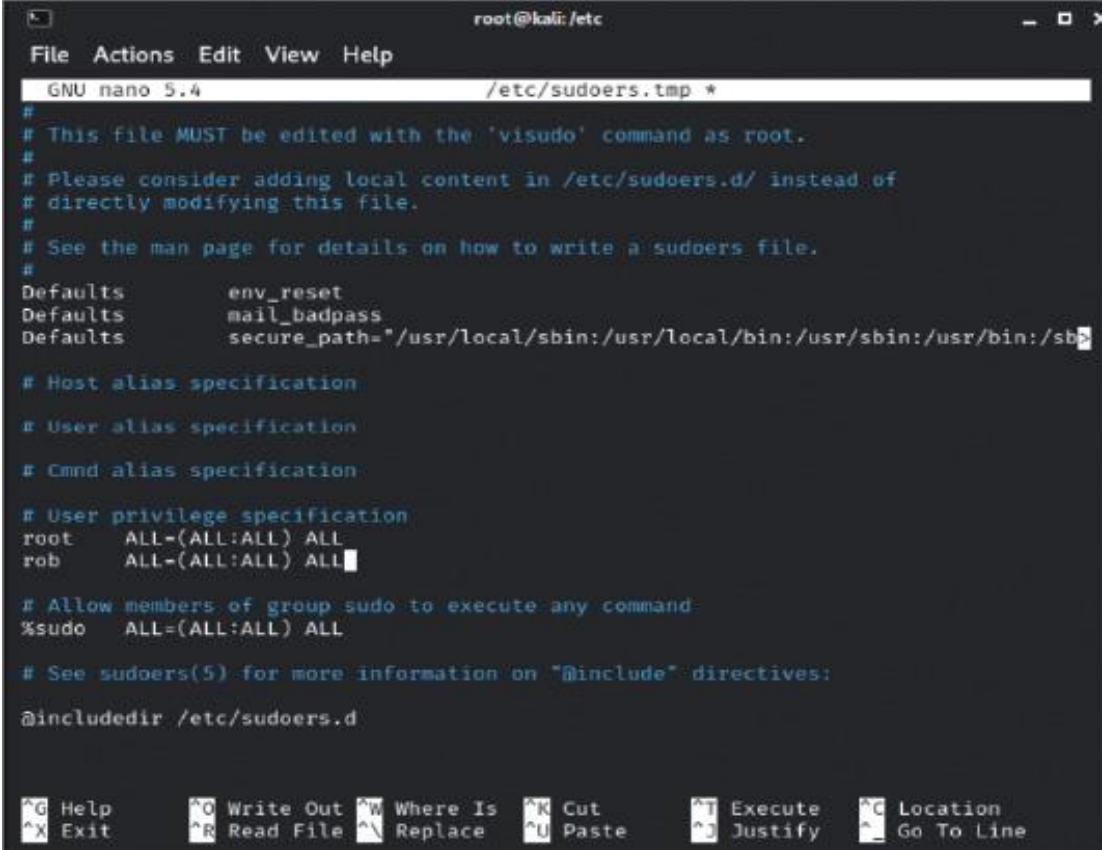
Finding files with SUID set

Attacking Hosts (14 of 31)

Linux/Unix Hosts

Exploiting SUDO

- Super User Do (SUDO) allows user to elevate privilege to that of Super User or root to execute a specific command
- The Linux file /etc/sudoers lists which users are allowed to use `sudo`
 - Threat actor could modify this file
- Sudoers file can specify which commands a user can run as root or allow all



```
root@kali: /etc
File Actions Edit View Help
GNU nano 5.4 /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
rob     ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "@include" directives:
@include /etc/sudoers.d

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

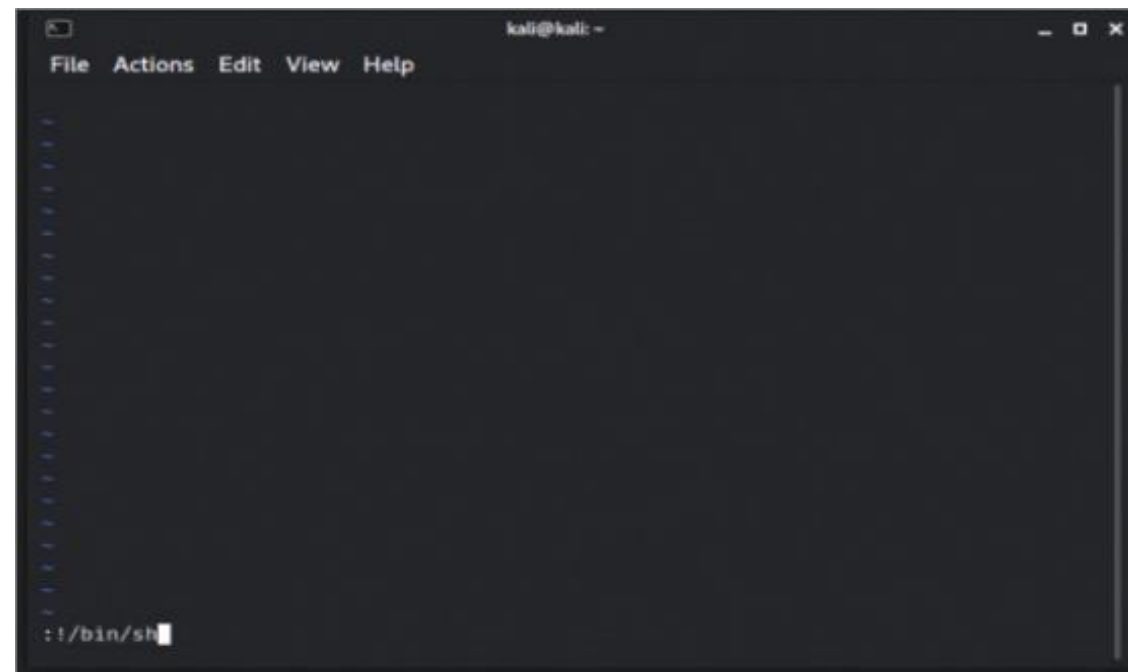
The Linux sudoers file

Attacking Hosts (15 of 31)

Linux/Unix Hosts

Shell Upgrade Exploits

- Shell upgrade exploit involves finding way to escape shell restrictions
- Shell restrictions on users restrict ability to perform elevated tasks
- The vi editor and other tools may allow users to execute commands within
 - Can exploit to upgrade to root shell by launching in vi editor which runs with SUID for root



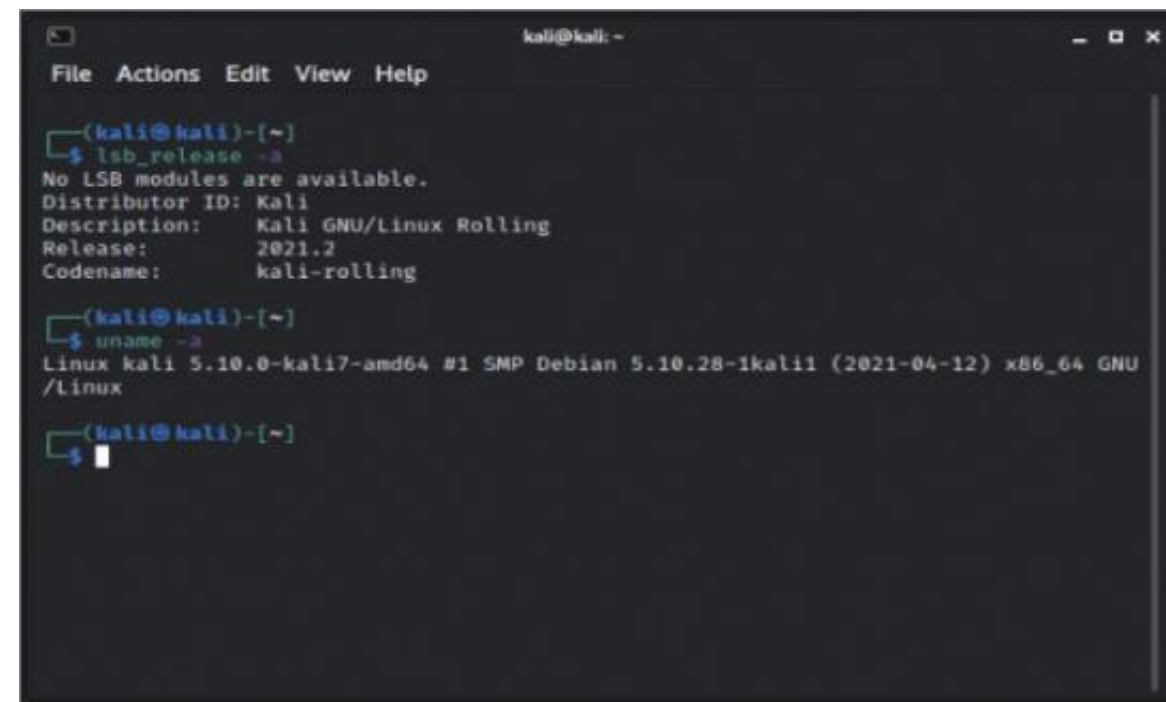
Using the vi editor to attempt to start a terminal shell

Attacking Hosts (16 of 31)

Linux/Unix Hosts

Kernel Exploits

- Kernel is core of an OS handling I/O, CPU access, and memory management
- Many Linux kernel versions exist, some with very serious vulnerabilities
- Determining the specific kernel of a target Linux system can identify potential vulnerabilities
- Exploits for kernel vulnerabilities are very powerful but challenging to use



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ lsb_release -a  
No LSB modules are available.  
Distributor ID: Kali  
Description:   Kali GNU/Linux Rolling  
Release:      2021.2  
Codename:     kali-rolling  
  
(kali@kali)-[~]  
$ uname -a  
Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux  
  
(kali@kali)-[~]  
$
```

Using lsb_release and uname to determine the distribution and version of a Linux operating system

Attacking Hosts (17 of 31)

Linux/Unix Hosts

Credential Harvesting

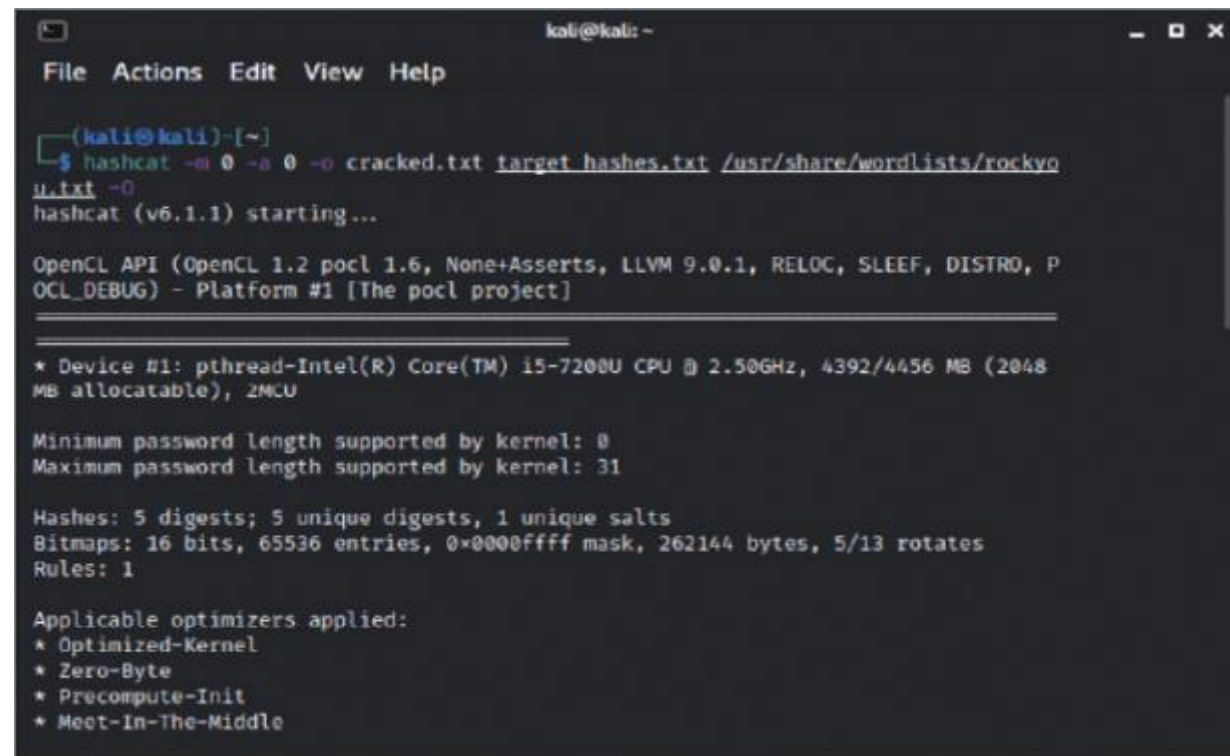
- Once a system has been compromised, acquiring local credential stores for system usernames and passwords is a common attacker tactic
- Linux systems store credentials in two locations:
 - /etc/passwd – contains cleartext user accounts, often readable by all
 - /etc/shadow – location of hashed passwords of Linux users
 - Hashed password stolen after system compromised
 - Password cracking – next procedure typically performed

Attacking Hosts (18 of 31)

Linux/Unix Hosts

Password Cracking

- Password hashes stored in cryptographically irreversible form
- Several tools exist to attack these hashes, uncover passwords
- Difficulty level depends on type of hash and hashing procedure



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ hashcat -m 0 -a 0 -o cracked.txt target_hashes.txt /usr/share/wordlists/rockyou  
u.txt -o  
hashcat (v6.1.1) starting...  
  
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, P  
OCL_DEBUG) - Platform #1 [The pocl project]  
  
-----  
* Device #1: pthread-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 4392/4456 MB (2048  
MB allocatable), 2MCU  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 31  
  
Hashes: 5 digests; 5 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1  
  
Applicable optimizers applied:  
* Optimized-Kernel  
* Zero-Byte  
* Precompute-Init  
* Meet-In-The-Middle
```

Using Hashcat to crack password hashes

Discussion Activity 10-1

In this module, security of Windows and Linux host operating systems is presented. Some attacks are common to both OSs. Both Windows and Linux also have attacks and vulnerabilities that are specific to each.

Discuss various OS attacks that are unique to one operating system or the other. Does the open source licensing model under which most versions of Linux are released promote or inhibit security for the OS? Why or why not?

Attacking Hosts (19 of 31)

Windows Hosts

- Microsoft Windows has 75% market share of laptops and desktops*
- Windows Server OS makes up 73% of server system deployments*

Exploiting Credential Hashes

- NT LAN Manager (NTLM) – Windows authentication mechanism that uses password hashes
- NTLM was default authentication tool for legacy Windows systems from Windows 2000 and earlier
- May still be in use for backwards compatibility

*As of time of course book writing

Attacking Hosts (20 of 31)

Windows Hosts

Exploiting Credential Hashes

- NTLM hash dumping can be achieved using Mimikatz and other tools
- NTLM hashes are unsalted and weak; trivial to crack
 - Salted hash adds a value to password before hashing
 - Salted password hashes are more difficult to crack
- Some password hashes replay captured hashes to circumvent authentication mechanisms

Attacking Hosts (21 of 31)

Windows Hosts

Exploiting LSA Secrets

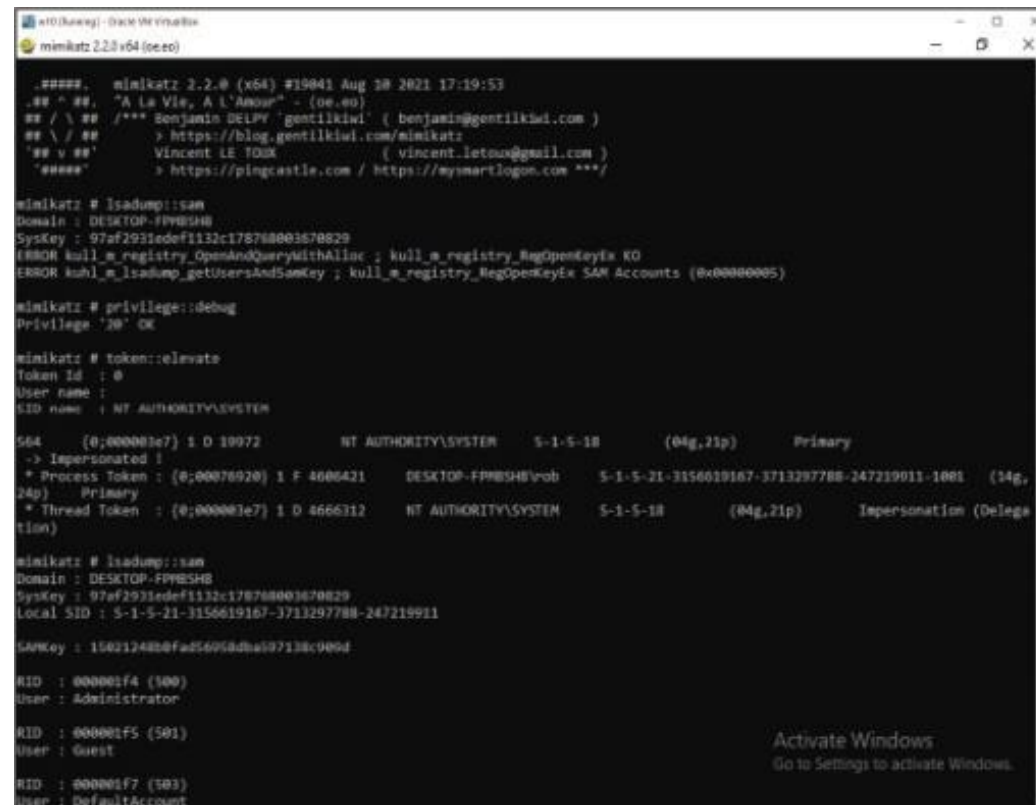
- LSA secrets – Windows registry location storing currently logged-in user password in encrypted form
- Administrative access to Windows host can allow for obtaining these password hashes and associated keys
- Decrypting current user password may then be possible

Attacking Hosts (22 of 31)

Windows Hosts

SAM Database Exploits

- Security Accounts Manager (SAM) database contains password hashes
- Often first item targeted by pen testers and threat actors
- Dumping SAM database requires elevated system credentials



```
mimikatz 2.2.0 (x64) #19041 Aug 20 2021 17:19:53
.####. m[mimikatz 2.2.0 (x64) #19041 Aug 20 2021 17:19:53
..#.#.#. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'#####' Vincent LE TOUX ( vincent.letoux@gmail.com )
> https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::sam
Domain : DESKTOP-FPWB5H8
SysKey : 97af2931def1132c178788001670829
[ERROR] kuhl_m_registry_OpenAndQueryWithAlias : kuhl_m_registry_RegOpenKeyEx KO
[ERROR] kuhl_m_lsadump_getUsersAndSamKey : kuhl_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

564 (0;000001e7) 1 D 10072 NT AUTHORITY\SYSTEM 5-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : (0;00070920) 1 F 4606421 DESKTOP-FPWB5H8\rob 5-1-5-21-3156019167-3713297788-247219011-1001 (14g,
24p) Primary
* Thread Token : (0;000001e7) 1 D 4666312 NT AUTHORITY\SYSTEM 5-1-5-18 (04g,21p) Impersonation (Delega
tion)

mimikatz # lsadump::sam
Domain : DESKTOP-FPWB5H8
SysKey : 97af2931def1132c178788001670829
Local SID : 5-1-5-21-3156019167-3713297788-247219911
SAMKey : 150212480fad5695adba97138c900d

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

Activate Windows
Go to Settings to activate Windows.
```

Using Mimikatz to dump the SAM database

Attacking Hosts (23 of 31)

Windows Hosts

Kernel Exploits

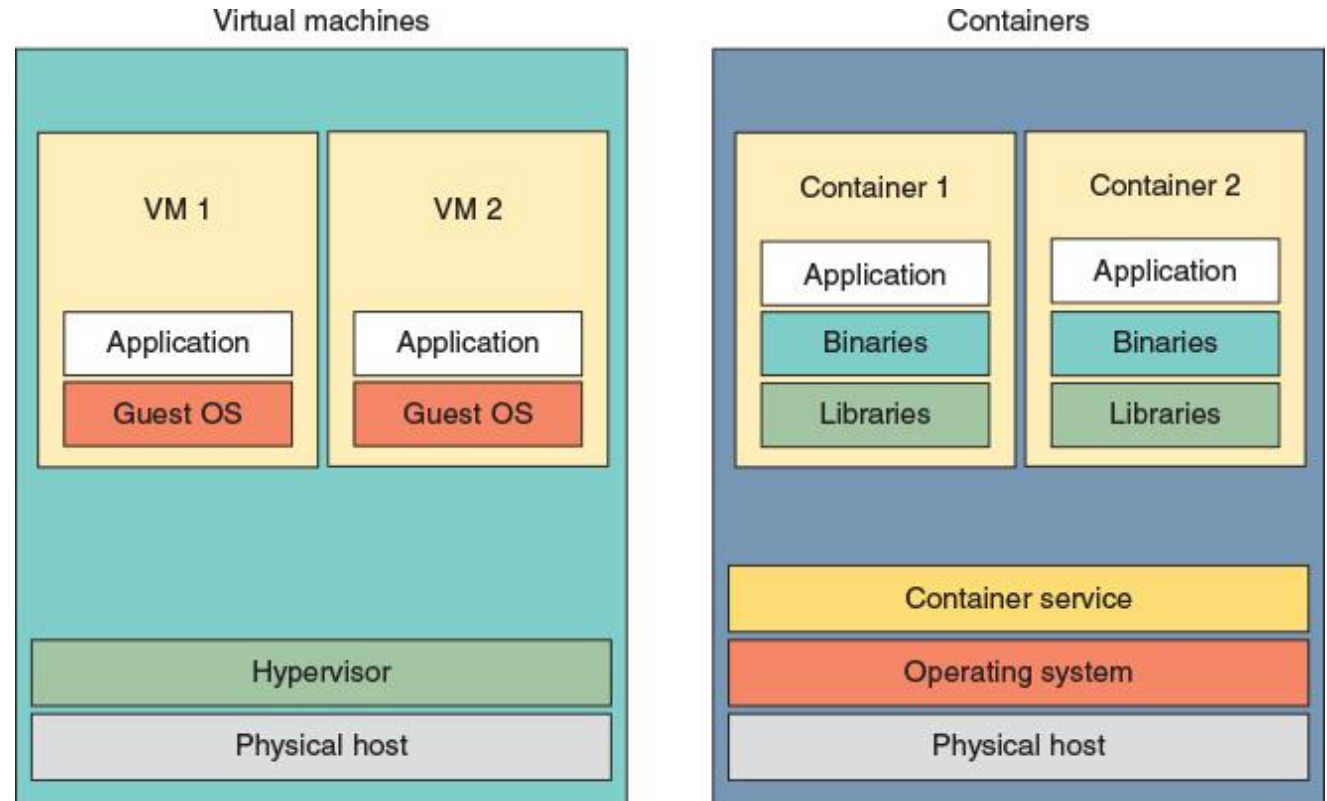
- Windows kernel exploits require local access; most successful after access to target already achieved
- Microsoft patches kernel vulnerabilities as soon as possible
- Missing patches for kernel vulnerabilities is a critical administration task

Attacking Virtualization (1 of 2)

- Virtualization has changed the computing paradigm
- Applications and operating systems can easily move from one computing platform to another
- Hypervisor virtualization uses concept of virtual machines (VM) with fully contained operating systems and applications
- Hypervisor acts as layer between VM and host operating system
 - Coordinates access to host physical hardware via emulated virtualized hardware
- Container virtualization runs applications directly on host operating system but isolated and within virtualized container

Attacking Virtualization (2 of 2)

- Multiple platforms exist for virtualization
- Each has differences in approach to virtualization and capabilities
 - Oracle VirtualBox
 - Microsoft Hyper-V
 - VMware



Virtual machine and container virtualization

Attacking Hosts (24 of 31)

Virtual Machine Exploits

- VMs behave like physical computers; may not be obvious if a target is a physical machine or a virtualized host
- Attack methods for VMs same as physical hosts
- Compromise of VM might be only way of telling target is virtualized
- Searching for virtualized hardware on target can indicate it is a VM
- Other methods identifying whether a target is virtualized exist and vary by guest operating system and hypervisor or host OS in use

Attacking Hosts (25 of 31)

Virtual Machine Exploits

- Examining the disk hardware details can determine if host is a VM

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command '\$ ls -l /dev/disk/by-id' is entered. The output shows five entries for VM disks, each with a long ID and a symlink to a device path. The IDs are 'ata-VBOX_CD-ROM_VB2-01700376', 'ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a', 'ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part1', 'ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part2', and 'ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part5'. The symlinks are 'sr0', 'sda', 'sda1', 'sda2', and 'sda5' respectively. The prompt is '(kali@kali)-[~]' and the cursor is on a new line.

```
(kali@kali)-[~]
$ ls -l /dev/disk/by-id
total 0
lrwxrwxrwx 1 root root 9 Aug 8 10:10 ata-VBOX_CD-ROM_VB2-01700376 -> ../sr0
lrwxrwxrwx 1 root root 9 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a -> ../sda
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part1 -> ../sda1
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part2 -> ../sda2
lrwxrwxrwx 1 root root 10 Aug 8 10:10 ata-VBOX_HARDDISK_VB0e7a7962-9e459a1a-part5 -> ../sda5

(kali@kali)-[~]
$
```

Using disk IDs to determine if a Linux target is a VM

Attacking Hosts (26 of 31)

Virtual Machine Exploits

Hypervisor and VM Repository Exploits

- Virtualization platforms and hypervisors are complex and subject to software flaws and vulnerabilities and other problems
- VM cloud host platforms such as Amazon Web services and Microsoft Azure provide preconfigured VMs for customers to easily use their deployments
- If one of these VMs was compromised or contained a backdoor, all systems built from that template could be exploited
- Cloud VM hosting platforms have their own pen-testing rules

Attacking Hosts (27 of 31)

Virtual Machine Exploits

Escaping a VM

- Attacking a host computer from within a VM is “escaping” the VM
- VM escape vulnerabilities patched very quickly, narrowing exploit window

Attacking Hosts (28 of 31)

Virtual Machine Exploits

Escaping a VM

- Attacking a host computer from within a VM is “escaping” the VM
- VM escape vulnerabilities patched very quickly, narrowing exploit window

Container Exploits

- Container exploits start by targeting the application running inside the container and might use standard exploits for that application
- Compromising the container may lead to exploitation of the host on which the containerization platform runs

Attacking Hosts (29 of 31)

Virtual Machine Exploits

Container Exploits

- Docker and Kubernetes are popular containerization platforms
- Docker is suite of development tools for creating, sharing, and deploying containers
- Kubernetes is a system used to deploy and operate containers across cluster of host computers

Attacking Hosts (30 of 31)

Virtual Machine Exploits

Container Exploits

- Docker and Kubernetes are commonly deployed as cloud services
- Amazon Elastic Container Service (ECS) is a cloud container host service
- Attacking cloud-based containers requires knowledge of cloud services and underlying infrastructure
- Container workload attacks exploit vulnerable container applications
- Container misconfiguration attacks include vulnerabilities of varying types, including permissions errors and insecure exposed APIs

Attacking Cloud-Based Targets (1 of 7)

Account Exploits

- Cloud host platforms like AWS, Google Cloud Platform (GCP), and Microsoft Azure are widely popular for many compelling reasons
- Organizations have shifted from deploying hardware in their server rooms to deploying VMs on the services
- Cloud services environments include accounts and credentials
- The varying types of cloud accounts with differing permission levels and access to service management tools can be intimidating
- Cloud platforms are accessible via internet by their nature, making them potentially easier to attack than local or on-premise target systems

Attacking Cloud-Based Targets (2 of 7)

Account Exploits

- Cloud credentials can be acquired through same means as traditional
 - Brute force, directory scanning, and online breach dumps are sources
- Multifactor authentication (MFA) is widely implemented
 - MFA misconfigurations can occur
 - MFA attacks likely send notices to targeted account's owner
- Compromised account takeover can allow for metadata service attacks
 - Targets cloud server temporary credentials for cloud resource needs
 - Considerable actionable intelligence potentially accessible

Attacking Hosts (31 of 31)

Windows Hosts

Credential Harvesting

- After compromising target Windows system credential harvesting using previous methods or one of several other tools to do so
- Mimikatz – frequent choice and used post-exploitation, after compromise

Password Cracking

- Hashed or encrypted Windows passwords must be cracked or reversed
- Commonly used tools include Hashcat, John the Ripper, and RainbowCrack

Attacking Cloud-Based Targets (3 of 7)

Misconfiguration Exploits

- Identity and Access Management (IAM) refers to processes, procedures, and methods to make authentication and authorizations more secure
- IAM can be misconfigured or left with weak default settings
- Best practices for IAM configurations can be ignored or neglected
- Data storage locations, such as an Amazon S3 bucket are cloud targets
 - Storage may be publicly accessible; inadvertently open to file actions
- Federation misconfiguration involve flaws in trust relationships like those between traditional Active Directory and Azure AD

Attacking Cloud-Based Targets (4 of 7)

Malware Injections

- Cloud malware injection attacks are MITM attack redirecting victims to threat actor's cloud VMs and services
 - Cross-site scripting can be used to do this

Denial of Service and Resource Exhaustion

- Cloud service pricing model can vary widely
 - Paying for amount of resources used is common model
 - Overloading cloud service to point of resource exhaustion causes DoS scenario
 - This type of DoS attack can be costly to target

Attacking Cloud-Based Targets (5 of 7)

Side-Channel Exploits

- Multiple VMs run side-by-side on a virtualization host
 - Side-channel-attack seeks to use one VM to access another VM or gain actionable intelligence

Direct-to-Origin Exploits (D2O)

- D2O is DDoS targeting infrastructure of content delivery networks (CDN)
- By obtaining the true IP address of a target host, cloud security bypassed
 - Bypasses load balancers, DoS mitigation services, and proxies

Attacking Cloud-Based Targets (6 of 7)

Cloud Attack Tools

Several tools for different cloud attack tools are available:

- Cloud Custodian – Generates reports on cloud environment weaknesses
- CloudBrute – enumerates application and storage resources
- Pacu – AWS exploitation framework with many exploits
- ScoutSuite – open source audit tool for multiple cloud providers
- Software development kits (SDKs) – provided by cloud providers to assist software developers to build cloud features into their apps
 - Used for resource enumeration, creating testing scripts, and more

Attacking Cloud-Based Targets (7 of 7)

Data Storage Exploits

- Data storage exploits target cloud storage objects
- Enumeration of cloud storage can be used for further exploits
- Default credentials and weak permissions also possible

Discussion Activity 10-2

Cloud technologies and virtualization have revolutionized the modern computing landscape. What challenges might exist when pen testing a cloud environment? Are there attacks or methods for cloud pen testing that might be easier than a traditional computing environment?

Summary (1 of 3)

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

1. Describe nonoperating specific host attacks such as taking advantage of permission configuration errors, accessing stored credentials, exploiting defaults, and brute-forcing credentials
2. Describe various remote access attack methods such as hiding attacks using SSH, NETCAT/Ncat, Metasploit framework remote access, and proxies
3. Describe Linux/Unix host attacks such as SUID/GUID SUDO, shell upgrade, and kernel exploits, credential harvesting, and password cracking

Summary (2 of 3)

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

4. Describe Windows host attacks such as credential hash, LSA secrets, SAM database, and kernel exploits, credential harvesting, and password cracking
5. Describe attacks against virtualization such as virtual machine (VM), hypervisor, and VM repository exploits, VM escaping, and container exploits

Summary (3 of 3)

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

6. Describe attacks against cloud-based targets such as account, misconfiguration, and data storage exploits, malware injection, denial-of-service and resource exhaustion attacks, and direct-to-origin exploits
7. Describe cloud attack tools and their usage
8. Describe attacks against cloud-based data storage