Exploiting Host-Based Vulnerabilities

- Exploit Windows-Based Vulnerabilities
- Exploit *nix-Based Vulnerabilities

Commonalities Among Windows-Based Vulnerabilities (Slide 1 of 2)

- OSs and most applications based on C, which has no default bounds-checking.
  - Susceptible to buffer overflows, arbitrary code execution, and privilege escalation.
- Developers need to use security best practices and unit testing.
- Proprietary product, so source code is not publicly available.
  - Fewer reviews open the door for undiscovered weaknesses.
- Complexity enables vulnerabilities to remain undetected after release.
- Microsoft doesn't patch all vulnerabilities—they release new versions.
  - This leaves the vulnerability unaddressed in older installations.

Commonalities Among Windows-Based Vulnerabilities (Slide 2 of 2)

- Servers: Network-based vulnerabilities; workstations: Application-based vulnerabilities.
- Uses standard protocols and technologies.
  - Susceptible to cross-platform exploits.
- Physical access puts hosts at greater risk.
  - Connecting cables to administrative console ports.
  - Booting to a different OS.
  - Using removable media.
  - Stealing and damaging hardware.
- Social engineering is required to expose certain vulnerabilities.

Windows Operating System Vulnerabilities

Category	Description
Remote code execution	Any condition that allows attackers to execute arbitrary code.
Buffer or heap overflow	A programming error that allows attackers to overwrite allocated memory addresses with malicious code.
Denial of service	Any condition that allows attackers to use resources so that legitimate requests can't be served.
Memory corruption	A programming error that allows attackers to access a program's memory space and hijack the normal execution flow.
Privilege escalation	Any condition that allows attackers to gain elevated access to a compromised system.
Information disclosure	Any condition that allows attackers to gain access to protected information.
Security feature bypass	A software weakness that allows attackers to circumvent policies, filters, input validation, or other security safeguards.
XSS	A vulnerability that allows attackers to inject malicious scripts into a trusted website so that they can be downloaded and executed by other users' browsers.
Directory traversal	Any condition that allows attackers to access restricted areas of a file system.
XSRF	A vulnerability that allows unauthorized commands to be sent from a user to a web app.

Frequently Exploited Windows Features (Slide 1 of 3)

Feature	Description	Exploits
Null sessions	• Allowed anonymous connections to the IPC$ share. • Enabled attackers to elicit system details. • CVE 1999-0519.	Enum4Linux, WinScanX, smb-enum-users.nse, smb-enum-shares.nse, getacct.exe, winfingerprint-x
LM password hash	• A weak hashing algorithm used in early versions of Windows. • Still available in Windows Server 2016 and Windows 10. • Converts passwords to uppercase, and divides the hash into two 7-byte parts. • Cracking LM hashes is simple and in some cases trivial.	Cain & Abel, Hydra, John the Ripper, Medusa, Ophcrack, L0phtCrack, Hashcat, NetBIOS Auditing Tool (NAT)
IIS 5.0 Unicode	• Some Unicode characters cause IIS 5.0 to behave unexpectedly, allowing for directory traversal, information disclosure, and remote code execution from a browser URL. • This was a major vector in the spread of the nimda worm.	Internet Explorer 5 or other browsers from that time period, HTML-based email messages

Frequently Exploited Windows Features (Slide 2 of 3)

Feature	Description	Exploits
IIS 5.0 WebDAV	• Buffer overflow against the ntdll.dll SEARCH WebDAV method. • Gave the attacker SYSTEM level remote code execution capabilities. • CVE-2003-0109. • Worked on Windows 2000, any service pack.	Metasploit module exploit/windows/iis/ms03_007_ntdll_webdav https://www.exploit-db.com/exploits/16470/
RPC DCOM	• RPCSS controls DCOM messaging between software components on networked computers. • The original exploit worked on Windows Server 2000, 2003, and XP. • A buffer overflow that provides remote code execution at the SYSTEM level. • CVE-2003-0352. • A new variant works on Windows 8.1. (CVE-2015-2370).	Metasploit module: exploit/windows/dcerpc/ms03_026_dcom, https://downloads.securityfocus.com/vulnerabilities/exploits/dcom.c Windows 8.1: https://www.exploit-db.com/exploits/37768/

Frequently Exploited Windows Features (Slide 3 of 3)

Feature	Description	Exploits
SMB NetAPI	• Microsoft Server service relative path stack corruption. • A weakness in NetAPI32.dll path parsing code permits a buffer overflow that grants remote code execution in SYSTEM privilege. • Works on Windows 2000–XP, and 2003 targets. • CVE-2008-4250.	Metasploit module exploit/windows/smb/ms08_067_netapi https://www.exploit-db.com/exploits/40279/

Password Cracking in Windows

The act of trying to guess or decode encrypted passwords.

- Windows passwords authenticate users, services, and computers.
- Other apps can require passwords.
- Stored in cleartext or as hashed values.
- Other authentication methods can be targeted.
  - Private keys, certificates, Kerberos tickets, and LSA secrets.
- SAM stores local user names and passwords.
  - LM or NT hash.
- SYSKEY utility encrypted various passwords, but could be circumvented.

Password Cracking Options (Slide 1 of 2)

- Brute forcing across the network.
- Dumping credentials from memory.
  - LSA secrets, hashes, tokens, copies of old passwords.
- Offline cracking.
- Extracting the SYSKEY boot key.
- Dumping locally cached domain login information.
- Stealing GPP files to extract stored passwords.
- Dumping the administrator password from an unattended installation answer file.

Password Cracking Options (Slide 2 of 2)

- Alternatives to cracking:
  - Use privileges from buffer overflow, etc., to create a new account.
  - Use a dumped hash to create a new account or Kerberos ticket.
  - Keylogging.
  - Social engineering.
  - Boot into another OS and overwrite existing password storage.

Password Cracking Tools (Slide 1 of 6)

Technique	Tools
Network brute forcing	• Hydra • Medusa • Ncrack • AET2 Brutus • L0phtCrack • Metasploit auxiliary/scanner modules
Dumping LSA secrets	• Cain & Abel • Mimikatz • Metasploit module post/windows/gather/lsa_secrets • LSAdump • Procdump • PWDumpX • secretsdump.py • Creddump • CacheDump • QuarksDump • Gsecdump • hobocopy

Password Cracking Tools (Slide 2 of 6)

Technique	Tools

Online SAM cracking	• Meterpreter hashdump
	• Metasploit modules:
	  • post/windows/gather/hashdump
	  • post/windows/gather/credentials/credential_collector
	• Cachedump
	• Samdump2
	• fgdump.exe
	• pwdump7.exe
	• Gsecdump
	• PWDumpX
	• hobocopy

Impersonating user tokens	• Meterpreter `steal_token` command (formerly Incognito)
Dumping Windows Vault passwords	• Built-in Windows Credential Manager (for the user to manage their own credentials).\ • NirSoft VaultPasswordView

Password Cracking Tools (Slide 3 of 6)

Technique	Tools
Kerberoasting	• Mimikatz • PowerSploit • John the Ripper • Hashcat • Kerberoasting tool kit https://github.com/nidem/kerberoast • Empire • Impacket • Metasploit module auxiliary/gather/get_user_spns
Recovering the SYSKEY bootkey	• bkhive • bkreg (pre-Service Pack 4 machines)
Dumping cached domain logon information	• Cain & Abel • Creddump • Passcape's Windows Password Recovery • Cachedump • Fgdump • PWDumpX

Password Cracking Tools (Slide 4 of 6)

Technique	Tools
Offline SAM cracking	• Cain & Abel • John the Ripper • Hashcat • L0phtCrack • Ophcrack • Vssown.vbs

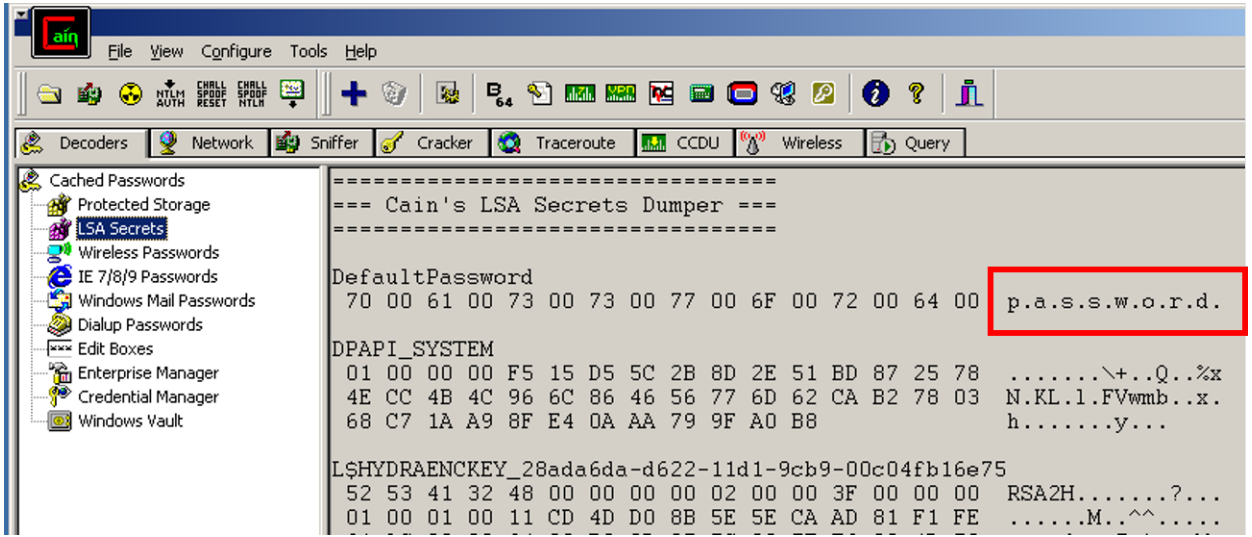
Offline Active Directory cracking	• ntdsutil.exe
	• VSSAdmin
	• PowerSploit NinjaCopy
	• DSInternals PowerShell module
	• ntds_dump_hash.zip
	• Metasploit modules:
	  • post/windows/gather/ntds_location
	  • post/windows/gather/ntds_grabber

Dumping GPP file cPasswords	• Metasploit module post/windows/gather/credentials/gpp • PowerSploit Get-GPPPassword.ps1 • gpprefdecrypt.py

Password Cracking Tools (Slide 5 of 6)

Technique	Tools
Keylogging	• Meterpreter `keyscan_start` and `keyscan_dump` commands • USB keyloggers
Social engineering	• Kali Social Engineering Toolkit (SET) • WiFi-Pumpkin
Dumping unattended installation file passwords	• Text editor • Knowledge of and access to answer file location
Hard drive overwriting	• Ultimate Boot CD for Windows • Offline NT Password & Registry Editor • http://pogostick.net/~pnh/ntpasswd/

Password Cracking Tools (Slide 6 of 6)



Windows Service and Protocol Configurations (Slide 1 of 3)

- All network-based services listen on at least one open port.
  - This makes them a target for remote attacks.
- Protocols used by all Windows versions are likely to have version-specific exploits.
  - For example, there are SMB exploits for every version of Windows since NT 4.0.
- Do not overlook ports that are unfamiliar to you.
  - They may have known exploits.
- IPv6 can carry exploits to the same TCP and UDP ports as well as IPv4.

Windows Service and Protocol Configurations (Slide 2 of 3)

- Some services open secondary ports.
  - Even if current exploits do not target the secondary port by default, the process could still have vulnerabilities.
- Banner grabbing and `nmap -sV` interrogation can identify many services.
  - Even if the port is non-standard.
- Many services can be downgraded to a less secure protocol or configuration. Services tend to be the least secure out of the box.
  - The administrator must apply patches, change defaults, and set firewall rules.
  - Many administrators are not trained sufficiently or are not diligent enough to do this properly.

Windows Service and Protocol Configurations (Slide 3 of 3)

- Many administrators reuse the same user account or password for different services across the domain.
- Many services use accounts with higher privilege levels than necessary.
  - Especially on older platforms.
- Many administrators configure services too loosely.
  - Unfamiliarity with the actual security level a service needs.
  - Unfamiliarity with security best practices.
- Most exploits allow you to change the target port.
  - Adjusting your attack to account for security by obscurity.
  - Experimenting to see if secondary ports react the same way as primary ports.
- Services with a lower privilege level can be used as a stepping stone to escalate privilege.

Windows File Systems (Slide 1 of 2)

- Permissions
  - Biggest security issue due to default read permissions.
- ADS
  - Enables hidden files.
- Unquoted service paths
  - Enables executables named after partial paths to be run.
  - DLL hijacking.

Windows File Systems (Slide 2 of 2)

- Weak or nonexistent encryption
  - NTFS encryption
  - SYSKEY to encrypt the SAM
  - EFS
  - BitLocker
- Code vulnerabilities
  - NTFS 3.1 Master File Table DoS Exploit
  - Windows 10 NTFS Owner/Mandatory Label Privilege Bypass Escalation of Privilege Exploit
  - Windows NTFS DoS Exploit

Windows Kernel Vulnerabilities (Slide 1 of 3)

Windows kernel: The core part of the Windows operating system that manages memory, schedules processing threads, and manages device I/O.

- Runs at Ring 0 and has priority over all other processes.
- Exploits that attack the kernel escalate privileges and destabilize the entire system.

Vulnerability	Description
EternalBlue	• CVE-2017-0143, MS17-010 - EternalBlue SMB Remote Windows Kernel Pool Corruption buffer overflow. • SMB 1.0 improper handling of certain requests. • Affects Windows Server 2016, 2008 R2, and Windows 7 (x64 all service packs).
Kernel mode drivers	• CVE-2016-7255, MS16-135 - Windows kernel mode drivers incorrectly handle objects in memory. • Local privilege elevation. • Affects Windows Server 2016, Windows 8.1, 8, and 7.

Windows Kernel Vulnerabilities (Slide 2 of 3)

Vulnerability	Description
Secondary Logon Service	• CVE-2016-0099, MS16-032 - Secondary Logon Handle Local privilege elevation. • Exploits lack of sanitization of standard handles in Windows Secondary Logon Service. • Affects Windows Vista through Server 2016, all platforms and service pack levels.
Kernel mode drivers	• CVE-2015-1701, MS15-051 - Windows kernel mode drivers allow local privilege elevation and arbitrary code. • Affects Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, and Windows Server 2012.
Null pointer dereference	• CVE-2014-4113, MS14-058 - WindowsTrackPopupMenu Win32k NULL Pointer Dereference. • Exploits vulnerabilities in how Windows kernel-mode drivers handle objects in memory. • Affects Windows Server 2003, Windows Server 2008, Windows Server 2012, 7, and 8.

Windows Kernel Vulnerabilities (Slide 3 of 3)

Vulnerability	Description
Kernel vulnerability	• CVE-2013-5065, MS14-002 - Windows Kernel Vulnerability. • Affects Windows XP, Windows Server 2003.
Kernel mode drivers	• CVE-2013-008, MS13-005 - Kernel Mode Driver. • Allows a lower-level process to broadcast to a higher-level process, thus effecting a privilege escalation. • Affects Windows Server 2003, Windows Server 2008, 7, 8, and Windows Server 2012.
Kernel vulnerability	• CVE-2010-0232, MS10-015 - Kernel vulnerabilities create a new session with SYSTEM privilege. • Exploit relies on kitrap0d.x68.dll and does not run on x64 editions. • Affects Windows Server 2003, Windows Server 2008, 7, XP.

Privilege Escalation in Windows (Slide 1 of 3)

- Often the primary objective.
- Can take several attempts to gain the level you need.
- Exploits against the kernel, services, drivers, and applications in privileged mode.

Vulnerability/ Technique	Description
SAM file	• Dump the contents of the SAM file to get cleartext or hashed passwords. • Copy the SAM file using Volume Shadow Service or by booting into another OS to crack passwords offline.
User application compromise	• Compromise applications such as Internet Explorer, Adobe Reader, or VNC to gain access to a workstation. • Then use UAC bypass techniques to escalate privilege. • Attacks typically require a victim to open a file or web page through social engineering.

Privilege Escalation in Windows (Slide 2 of 3)

Vulnerability/ Technique	Description
Local UAC bypass	• Bypass local Windows UAC. • Example: Use process injection to leverage a trusted publisher certificate.
Weak process permissions	Find processes with weak controls and see if you can inject malicious code into those processes.
Shared folders	Search for sensitive information in shared folders (it is common for them to have few or no access restrictions).
DLL hijacking	• Elevate privileges by exploiting weak folder permissions, unquoted service paths, or applications that run from network shares. • Replace legitimate DLLs with malicious ones.
Writable services	• Edit the startup parameters of a service, including its executable path and account. • Use unquoted service paths to inject a malicious app that the service will run as it starts up.
WebDAV	• Microsoft WebDAV clients could elevate privilege with specially crafted requests. • Affects Windows Server 2008, Vista, 7. • CVE-2016-0051, MS16-016.

Privilege Escalation in Windows (Slide 3 of 3)

Vulnerability/ Technique	Description
Ancillary Function Driver	• Ancillary Function Driver (AFD) does not properly validate input before passing it from user mode to the kernel. • This could grant a local attacker elevation of privilege. • Affects Windows Server 2003, Windows Server 2008, 7, 8, Windows Server 2012. • CVE-2014-1767, MS14-040.
Task Scheduler 2.0	• Task Scheduler 2.0 does not properly determine the security context of its scheduled tasks, allowing an attacker to escalate privilege. • Affects Windows Vista SP1/SP2, Windows Server 2008 Gold, SP2/R2, Windows 7. • CVE-2010-3338, MS10-092.
Missing patches and misconfigurations	Search for missing patches or common misconfigurations that can lead to privilege escalation.

Memory Vulnerabilities

- Program flaws that result in improper access or handling of objects stored in memory.
- Memory corruption can lead to arbitrary code execution or DoS.
- Often not logged by the OS.
- Results in system destabilization.
- Common Windows memory exploits:
  - Use-After-Free
  - Buffer overflow
  - Heap overflow
  - Integer overflow
  - Memory leak DoS

Default Accounts in Windows (Slide 1 of 2)

Account	Description	Exploit
Guest	• No password required • Limited user-level access • Disabled by default • RID 501	• Add to any user group, including administrators • Use it to run privilege escalation exploits: https://github.com/WindowsExploits/Exploits/tree/master/CVE-2017-0213
Administrator	• Performs any action on a system • Cannot be locked out • RID 500	Use Meterpreter `getsystem` command to elevate to SYSTEM privilege
krbtgt	• Encrypts and digitally signs all Kerberos tickets • RID 502	• Dump the account password hash, and use it to create an unauthorized Golden ticket for access to Active Directory • post/windows/escalate/golden_ticket golden_ticket_create kerberost_ticket_use

Default Accounts in Windows (Slide 2 of 2)

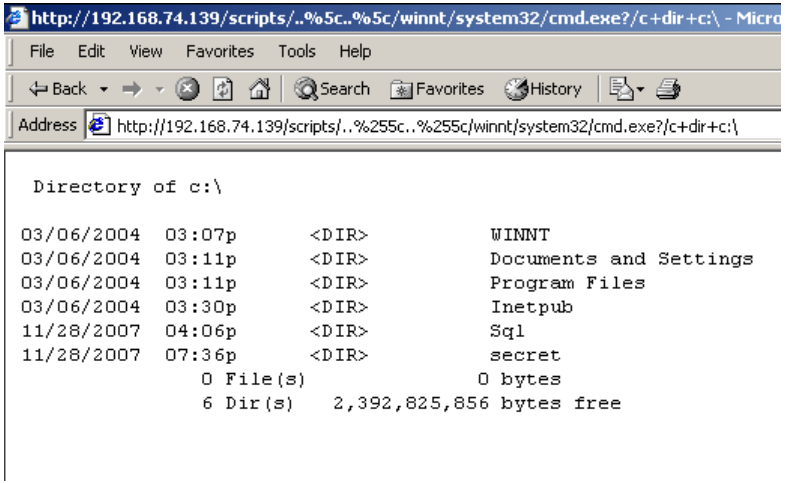
Account	Description	Exploit
DefaultAccount	• Added in Windows 10 and Windows Server 2016 • Managed by SYSTEM • RID 503	• Can be added to any user group, including administrators • Can have its password changed
WDAGUtilityAccount	• Used by Windows Defender Application Guard • RID 504	• Can be added to any user group, including administrators • Can have its password changed
defaultuser0	• Created during Windows 10 installation before any user accounts are created • RID 100x (depending on install)	• Can be added to any user group, including administrators • Can have its password changed

Windows Account Manipulation

To Do This:	Run This Command:
List all users	`net user`
See information about guest	`net user guest`
Search the status of guest to determine if it's active (enabled) or not	`net user guest | findstr /C:"active"`
Activate (enable) guest	`net user guest /active:yes`
Set/change the guest password to Pa22w0rd	`net user guest Pa22w0rd`
Add guest to the local administrators group	`net localgroup administrators /add guest`
View the SID of each account	`wmic useraccount get name,sidnet user`

Default Configurations in Windows

- Default configurations are predictable—easy to study for vulnerabilities.
- Early Windows versions shipped with easily exploited default configurations.
  - Simple passwords that never expired.
  - Unnecessary services installed by default.
- Today's Windows versions are more restrictive, but still need patching and security policies applied.
- Common vulnerable defaults:
  - Unnecessary services
  - Support for SMB 1.0
  - Domain account password caching
  - Default accounts
  - Default security logging



Sandbox Escapes (Slide 1 of 2)

Sandbox: An environment used to isolate a computer process away from other processes, as well as the host.

Sandbox Escape: An exploit in which the guest breaks free of the sandbox

Types of sandboxes:

- VMs
- Docker containers
- Web browsers
- Web browser plug-in content
- Web pages
- Mobile apps
- PDFs and documents
- Unknown file temporary quarantine/ scanning
- Antivirus quarantine
- Attachment sandboxing

Vulnerability	Description
CVE-2017-4901 - VMware Escape Exploit before VMware WorkStation 12.5.5	• Drag and drop functionality in VMWare Workstation 12.x (pre-12.5.5) has an out-of-bounds memory access vulnerability. • A guest may be able to execute code on the host OS.

Sandbox Escapes (Slide 2 of 2)

Sandbox evasion techniques:

- Extended sleep
- Polymorphic malware
- Rootkits and bootkits
- Sandbox detection
- Encrypted archives
- Botnet command and control
- Logic bombs
- Binary packers
- Network fast flux

Vulnerability	Description
CVE-2016-3321 - Internet Explorer Iframe Sandbox File Name Disclosure	• When used with HTML5 sandbox iframes, IE can disclose the existence of a local file on the host. • Works against IE 10 & 11.
CVE-2015-0016, MS15-004 - Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape	• Targets the MS RemoteApp and Desktop connections runtime proxy TSWbPrxy.exe. • Allows the attacker to escape Protected Mode and execute code.

Guidelines for Exploiting Windows-Based Vulnerabilities (Slide 1 of 3)

- Use port scans, vulnerability scans, and OS fingerprinting to identify likely vulnerability starting points.
- When cracking passwords:
  - Try to dump hashes or steal a copy of the SAM or ntds.dit, then crack offline to avoid detection and account lockouts.
  - Use large dictionary files or large rainbow tables.
- When confronted with passwords that are difficult to crack, consider passing the hash or stealing a token to impersonate a user instead.
- As you review port scan output, do not overlook unusual ports—they may be used by a vulnerable service.

Guidelines for Exploiting Windows-Based Vulnerabilities (Slide 2 of 3)

- Many services can be downgraded to a less secure protocol version.
- When targeting the file system, consider exploiting weak permissions, unquoted service paths, or vulnerable file system driver code.
- Remember that kernel exploits can evade detection and give you system privilege, but they can also destabilize the target.
- Try to escalate to SYSTEM level privilege for maximum exploit effectiveness.
- Keep in mind that buffer overflows, while considered to be the "gold standard" of exploits, will by their very nature destabilize the target service.
  - Create your backdoor and get out.

Guidelines for Exploiting Windows-Based Vulnerabilities (Slide 3 of 3)

- Take advantage of default accounts and SIDs that cannot be changed.
- Target the user account krbtgt to create a Golden ticket for access to the domain.
- Remember that Windows still ships with vulnerable defaults.
  - Most of these are code weaknesses that are allowed for backward compatibility.
- As more servers and applications are moved into a virtual environment, stay informed on upcoming sandbox escapes that you can use.

Commonalities Among *nix-Based Vulnerabilities

- General risks:
  - Physical, administrative, coding, and social engineering.
- All *nix kernels written in a variant of C.
  - Same issues with input validation and bounds-checking.
- Multiple developers cause inconsistency in implementing secure coding practices.
  - Apple iOS: Very strict approval and installation process.
  - Linux and Android: Allow side-loading apps.
- Uses standard protocols and technologies.
  - Susceptible to cross-platform exploits.

Linux Operating System Vulnerabilities

Linux distribution: A version of the open source Linux operating system kernel that is packaged with other components such as installation programs, management tools, and other software.

- Similar categories of vulnerabilities as in Windows:
  - DoS
  - Information disclosure
  - Buffer or heap overflow
  - Privilege escalation
  - Remote code execution
  - Memory corruption
  - Security feature bypass
  - Directory traversal

Frequently Exploited Linux Features (Slide 1 of 3)

Feature	Description	Exploits
ret2libc	• Existing function in the C library. • Eliminates the need for the attacker to inject their own shell code to take control of a target. • This result allows arbitrary code execution and escalation of privilege.	https://www.exploit-db.com/docs/english/28553-linux-classic-return-to-libc-&-return-to-libc-chaining-tutorial.pdf
Insecure sudo	Under certain conditions, this vulnerability allows attackers to circumvent protections and execute commands that would normally require a password, resulting in privilege escalation.	Exploit-db.com lists 24 sudo-related exploits.
Sticky bits	• Permission bits set on (mostly) directories. • Only the owner can delete or rename files in that directory. • Especially useful in the shared directories /var/tmp and /tmp. • Sticky bit exploits can be disruptive and cause DoS.	• https://www.exploit-db.com/exploits/16216/ • https://www.thegeekdiary.com/what-is-suid-sgid-and-sticky-bit/ • https://gist.github.com/anonymous/10165224

Frequently Exploited Linux Features (Slide 2 of 3)

Feature	Description	Exploits
SUID executables	• SUID allows a user to run a command as another user. • Often used by administrators to change a user's password. • When an application needs to run as the owner, an SUID permissions bit is set to allow this. • Many executables use SUID, but are poorly coded and can allow an attacker to escalate privilege.	https://www.pentestpartners.com/security-blog/exploiting-suid-executables/
Dirty COW Bug	• A race condition in mm/gup.c leverages incorrect handling of copy-on-write (COW) feature by kernel memory subsystem /proc/self/mem. • Allows writing to private, read-only memory mappings. • Affects Linux kernel 2.6.22 < 3.9 (x86/x64). • CVE-2016-5195.	• https://www.exploit-db.com/exploits/40839/ • https://www.exploit-db.com/exploits/40616/

Frequently Exploited Linux Features (Slide 3 of 3)

Feature	Description	Exploits
Five Year Bug	• A race condition created by raw mode PTY local echo permits privilege escalation. • Affects Linux kernel 3.14-rc1 < 3.15-rc4 (x64). • CVE-2014-0196.	https://www.exploit-db.com/exploits/33516/
Remote Root Flaw	• Unsafe second checksum in udp.c can give a remote attacker complete control of a system via UDP traffic. • Affects pre-4.5 Linux kernel. • CVE-2016-10229.	https://www.rapid7.com/db/vulnerabilities/panos-cve-2016-10229

Password Cracking in Linux (Slide 1 of 2)

- Originally stored in cleartext in /etc/passwd.
- Now stored as hash values in /etc/shadow.
  - Hashing algorithm depends on the distro.

Attack Method	Tools
Brute force login passwords for services such as SSH, telnet, FTP, HTTP, Samba, VNC, etc.	• John the Ripper • Medusa • Hydra • Ncrack • Crowbar • Metasploit auxiliary/scanner modules
Copy the /etc/passwd and /etc/shadow files, unshadow (combine) the copies, and send them to a password cracker.	• John the Ripper • Medusa • Hydra • Ncrack • Crowbar

Password Cracking in Linux (Slide 2 of 2)

Attack Method	Tools
Dump the hashes from a compromised machine and send them to a password cracker.	• Metasploit module post/linux/gather/hashdump • John the Ripper, etc. • RainbowCrack • Hashcat
Dump cleartext passwords currently stored in memory.	Mimipenguin—https://github.com/huntergregal/mimipenguin
Pass the hash if the passwords take too long to crack. Works particularly well against Samba with LM or NTLM authentication.	Metasploit module auxiliary/scanner/smb/smb_login
Install a physical or software-based keylogger.	• Meterpreter `keyscan_start` and `keyscan_dump` commands • USB keyloggers
Use social engineering to obtain user passwords.	• Kali Social Engineering Toolkit (SET) • WiFi-Pumpkin
Boot the target computer into single user mode to reset the root password.	• Reboot and edit GRUB to enter single user mode, then change the root password.

Linux Service and Protocol Configurations

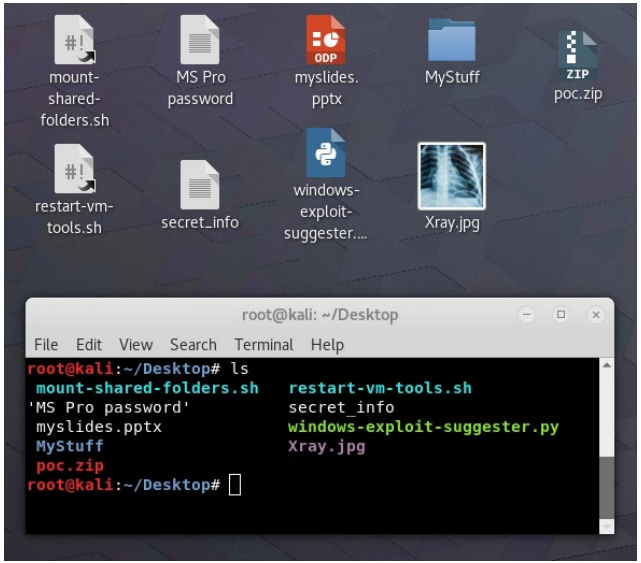
Exploit	Description
GHOST **CVE-2015-0235**	• Exploits how the popular EXIM mail server uses the gethostbyname function in the GNU C library (glibc). • Can give an attacker remote control over the entire system. • Affects nearly all distros that have EXIM installed. • Metasploit module exploit/linux/smtp/exim_gethostbyname_bof
Shellshock **CVE-2014-6271, CVE-2014-6278**	• Exploits a vulnerability in how the Bash shell handles external environment variables. • **Exploit-db.com** lists 15 exploits. • Metasploit has 10 exploit modules; `search shellshock`.
Heartbleed **CVE-2014-0160**	• A platform-independent information disclosure vulnerability in the OpenSSL encryption library. • When exploited properly, it can induce the server to also echo back random data from memory, including login credentials and session cookies. • Metasploit module auxiliary/scanner/ssl/openssl_heartbleed, https://gist.github.com/eelsivart/10174134
POODLE **CVE-2014-3566, CVE-2014-8730**	• A platform-independent MITM attack that forces web servers and browsers to negotiate down from the stronger TLS to the weaker SSL 3.0. • https://github.com/mpgn/poodle-PoC

Linux File Systems (Slide 1 of 2)

- Virtual tree structure
- Base level is / (root)
- Top-level directories for most distros:
  - bin—binaries
  - boot—system boot files
  - dev—a virtual directory of device files (like USB sticks, webcams)
  - etc—config files
  - home—users' personal directories
  - lib—libraries (application code snippets)
  - media—where inserted removable media is mounted
  - mnt—(legacy) where storage or partitions are manually mounted
  - opt—where software you compile often ends up
  - proc—a virtual directory that contains information about running processes
  - root—home directory of the root superuser
  - usr—shared application files
  - sbin—applications only the superuser can run
  - srv—data for servers
  - sys—virtual directory about connected devices
  - tmp—temporary files
  - var—logs

Linux File Systems (Slide 2 of 2)

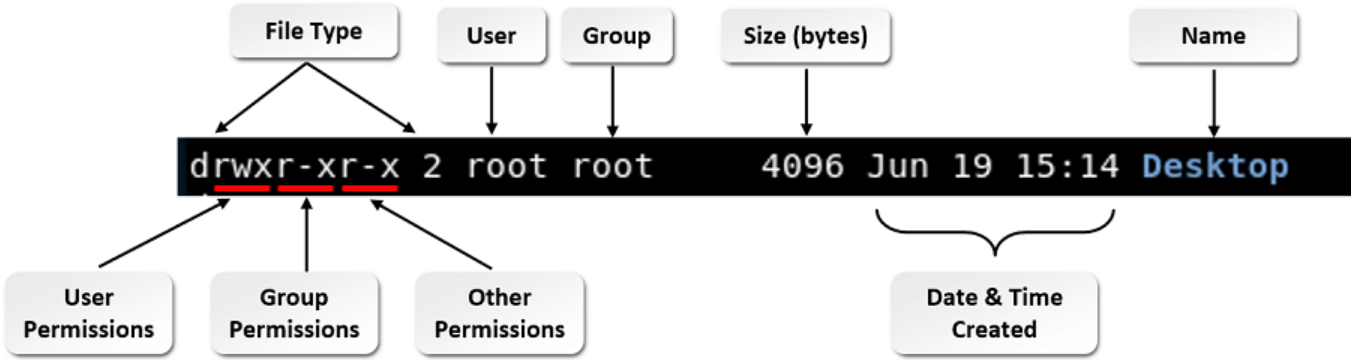
- Linux Bash is case sensitive with different commands from MS-DOS.
- Use a forward slash (/) to separate path levels.
- Everything, including running processes, is treated as a file.
- Files with spaces in their names are enclosed in quotes.
- Bash uses colors for different file types.



Linux Permissions (Slide 1 of 2)

- File types:
  - - = Regular File
  - d = Directory (folder)
  - l = Symbolic Link
  - b = Block Special Device
  - c = Character Device
  - s = Unix Socket
  - p = Named Pipe

- To view permissions, enter `ls -l`
  - Entities: u, g, o
  - Permissions: r, w, x, -
  - Octal permissions: 4, 2, 1, 0



Linux Permissions (Slide 2 of 2)

- To assign permissions, use `chmod`
  - `chmod 777 myfile`
  - `chmod 644 myfile`
  - `chmod 740 myfile`
- Special permission bits
  - setuid/SUID
  - setgid/SGID
  - Sticky bit

```
drwxrwxrwt  18 root root  4096 Jun 27 06:29 tmp
```

Sensitive Linux Files (Slide 1 of 2)

File	Description
GRUB (/boot/grub)	Most commonly used bootloader package that loads the Linux kernel.
/etc/passwd	List of all local accounts.
/etc/shadow	Password hashes for all local accounts.
/etc/group	List of all local groups.
/etc/gshadow	Password hashes for local groups.
/proc/cmdline	Kernel parameters.
/etc/rc.*	Run commands.

Sensitive Linux Files (Slide 2 of 2)

File	Description
/etc/profile	Sets system-wide environment variables on user shells.
/etc/hosts	Host-name-to-IP mappings—checked before DNS for name resolution.
/etc/resolv.conf	Lists DNS servers for system to use.
/etc/pam.d	Password and lockout policies.
~/.bash_profile, ~/.bash_login, ~/.profile, /home/user/.bashrc, /etc/bash.bash.rc, /etc/profile.d	Possible locations to insert a script that will run when the shell starts.

Privilege Escalation in Linux (Slide 1 of 2)

Vulnerability/ Technique	Description
/etc/passwd, /etc/shadow	Obtain a copy of these files to crack root or privileged user passwords.
Weak process permissions	Find processes with weak controls and see if you can inject malicious code into those processes.
User application compromise	• Compromise end user applications and plug-ins such as OpenOffice, VNC, and Adobe Flash Player. • Some require social engineering to get the end user to open a file or browser page.
SetUID binaries	Locate applications you can run as root.
Services running as root	Locate services that are owned by (running as) root and see if you can compromise them.

Privilege Escalation in Linux (Slide 2 of 2)

Vulnerability/ Technique	Description
Shared folders	Search for sensitive information in Samba shared folders, as it is common for them to have few or no restrictions.
Kernel and service exploits	Find exploits that target the kernel and privileged services.
Meterpreter upgrade	If you have a Bash shell from Metasploit, try to upgrade it to the more versatile Meterpreter.
Netcat upgrade	If you have a Netcat shell, try to upgrade it to a fully interactive TTY or Meterpreter.
Exploit cron jobs	Exploit badly configured cron jobs to gain root access.
Missing patches and misconfigurations	Search for missing patches or common misconfigurations that can lead to privilege escalation.

Default Accounts in Linux (Slide 1 of 2)

- root—superuser account that can do anything
- adm—used for diagnostics and monitoring
- mail—handles email; used by sendmail and postfix daemons
- news—used for Usenet news
- www-data—default website user
- nobody—assigned by the NFS daemon to a mounted NFS share whose owner is not a local user
- sshd—used for unprivileged operations by the SSH daemon
- lp—used for the printer system
- ftp—used for anonymous FTP access
- uucp—controls ownership of serial ports

Default Accounts in Linux (Slide 2 of 2)

To Do This:	Run This Command:
See all local accounts	`cat /etc/passwd`
See all password hashes	`sudo cat /etc/shadow`
Search for a particular account	`grep jason /etc/passwd`
See who has UID 0 (root)	`getent passwd 0`
See who is in the root group	`getent group root`
See who is in the wheel group (able to run the `su` command to change to root)	`getent group wheel`
See who is in the adm group (able to monitor the system and read log files)	`getent group adm`
See who is in the admin group (an administrative group in older distributions)	`getent group admin`
See who has the right to run the `su` command	`sudo cat /etc/sudoers`

Default Configurations in Linux

- User home permissions.
  - Default permission is 775.
- World-readable and world-writable directories and files.
  - Default permission is 644.
- Insecure mount or export options.
  - Default mount points include rw, suid, dev, exec, auto, nouser, and async.
- Services and applications with weak defaults.
  - Communication protocols that are not secure.
  - Default passwords.
  - Many open ports.

Android Vulnerabilities (Slide 1 of 3)

- Android is a mobile OS based on Linux.
- Apps are packaged as APKs.
- Users can install apps from Google Play or other sources.
- Easily as susceptible to compromise as laptops and desktop computers.

Android Vulnerability	Description
Physical theft	Their small size makes Android devices especially vulnerable to theft and loss.
Weak or no passwords	Many users do not enable passwords or use weak passwords on their device.
Lack of data encryption	Many apps, including those that use the SQLite database, store data in cleartext.
Ability to side-load apps	Android allows users to install unsigned apps from any source, even on devices that are not rooted.
Rooted device	Many Android users root their devices to have more control over their phones. Unfortunately, this makes it easier to compromise the phones, as users now have root level privileges.
SQL injection	The SQLite database, which is the most commonly used database in mobile devices, is vulnerable to a SQL injection attack.

Android Vulnerabilities (Slide 2 of 3)

Android Vulnerability	Description
Unauthorized access or excessive permissions by apps	Many apps either request more permissions than they actually need, or do not request permissions at all to access resources such as contacts, microphone, camera, location services, etc.
Data leakage from syncing	Security vulnerabilities in cloud-based services could expose the Android device to attack, especially if the user uses the same password for multiple websites.
Lack of antivirus/malware protection	Most users do not install endpoint protection on their devices. This leads to virus infections, unsafe surfing, malicious downloads, SMShing, etc.
Missing updates and patches	Android and its apps need periodic patching. This often does not happen, or users roll back the updates to recover disk space or improve performance.
QuadRooter vulnerabilities	A set of four vulnerabilities affecting devices that use Qualcomm chipsets (about 900 million devices). Any of the four could escalate privilege and grant an attacker root access. CVE-2016-2503.
Certifi-Gate mRST flaw	A flaw in mobile remote support tools. Allows an attacker to install a malicious app and gain control of the device. Affects versions up to 5.1 (Lollipop). No CVE number.

Android Vulnerabilities (Slide 3 of 3)

Android Vulnerability	Description
Stagefright MMS flaw	Considered the most serious Android flaw to date. Allows an attacker to send a malicious video message that can be processed by the native media playback library without user knowledge. Permits escalation of privilege and remote arbitrary code execution. Affects versions up to 5.1. CVE-2015-3864.
Android Installer hijacking	Allows attackers to replace legitimate APK with malicious one. Affects older devices up to v4.1 (Jelly Bean). No CVE number.
Android FakeID flaw	Allows a malicious app to hijack the trusted status of a legitimate app by forging its digital signature, thus escaping sandboxing. Affects versions 2.1 (Eclair) to 4.3 (Jelly Bean). No CVE number.
TowelRoot	A kernel-level flaw allows a user or attacker to quickly root older devices, up to version 4.4 (KitKat).
Janus vulnerability	An attacker could add malicious code in the form of a DEX file to an APK without changing the APK digital signature. CVE-2017-13156.
Cross-platform protocol vulnerabilities	As a Linux variant, Android is susceptible to exploits that affect common protocols or features, such as POODLE, KRACK, and Dirty COW.

Apple macOS and iOS Vulnerabilities (Slide 1 of 2)

- Apple has a reputation for good security.
- OSs based on BSD Unix and subject to common OS vulnerabilities.
- Jailbreaking a device introduces more vulnerabilities.

macOS and iOS Vulnerability	Description
Kernel Memory Corruption	Allows attackers to execute arbitrary code or cause a DoS. Affects iOS versions prior to 11.3, and macOS prior to 10.13.4. CVE-2018-4150.
Graphics Driver vulnerability	Allows attackers to execute arbitrary code or cause a DoS. Affects iOS versions prior to 11.2.5. CVE-2018-4109.
IOMobileFrameBuffer vulnerability	A weakness in the kernel extension used to manage the screen frame buffer allows attackers to execute arbitrary code. Affects iOS prior to 11.2. CVE-2017-13879.
High Sierra Bug	Allows anyone to log in to macOS High Sierra as root with no password.
Mactans	Plugging your iPhone into this malicious USB charger will inject persistent malware into your device.

Apple macOS and iOS Vulnerabilities (Slide 2 of 2)

macOS and iOS Vulnerability	Description
Jailbroken iPhone	Jailbreaking overwrites the firmware, bypassing security controls. This gives users root privilege so they can install unauthorized applications. But malware can also be installed.
Thunderstrike	A hardware-based bootkit that overwrites OS X firmware. Spreads through maliciously modified peripheral devices that plug into the Thunderbolt interface. CVE-2014-4498.
iCloud API vulnerability	A series of iCloud attacks ("Celebgate") resulted in the theft of about 500 private celebrity photos and uncovered a weakness in the iCloud API that would allow unlimited password brute forcing.
MaControl Backdoor	An APT backdoor that has had several variations and delivery mechanisms. When installed, it connects to a Command and Control (CnC) in China to receive instructions.

Hardware Attacks (Slide 1 of 2)

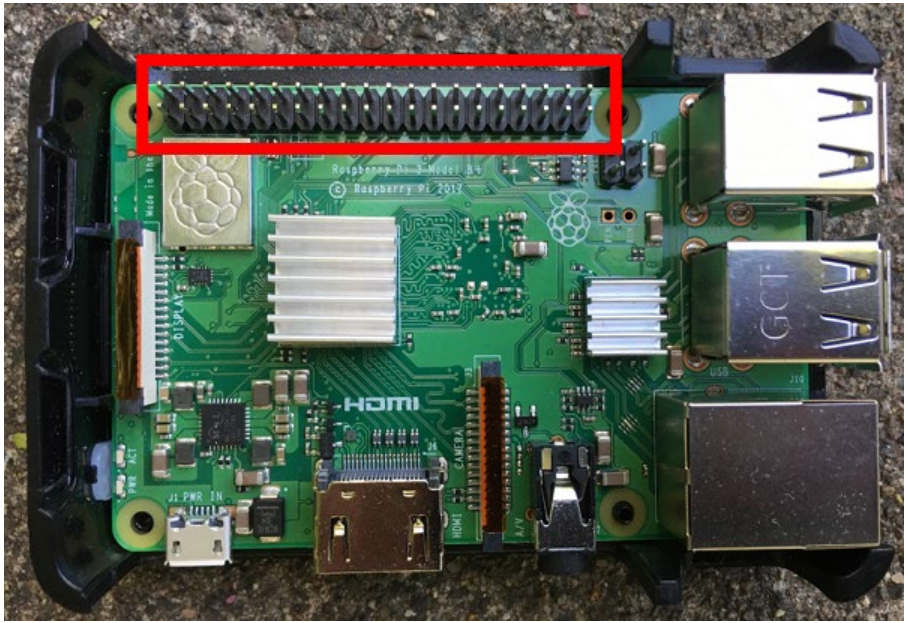
Cold boot attack: An attack where an attacker with physical access to a computer that contains an encrypted drive may be able to retrieve encryption keys after starting the computer from its off state.

Serial console: A connection made through the RS-232 or USB serial port that provides a person direct administrative access to a computer or network device.

JTAG connector: (Joint Test Action Group connector) A simple hardware interface that enables a computer to communicate directly with chips on a board.

JTAG debugging: (Joint Test Action Group debugging) A troubleshooting methodology used by hardware manufacturers to test printed circuit boards, and used to hack a device such as a home router.

Hardware Attacks (Slide 2 of 2)



Guidelines for Exploiting *nix-Based Vulnerabilities (Slide 1 of 2)

- If you are less experienced with Linux, refer to Windows vulnerabilities and exploits to help you understand the Linux equivalents.
- In addition to finding exploits online or in Metasploit, consider using common Linux features in your exploits.
- When cracking passwords in Linux, consider using a combination of techniques.
  - Cracking offline copies of /etc/passwd and /etc/shadow, dumping hashes, brute forcing network services, and using SMB exploits against the Samba service.
- Use Nmap and online research to identify vulnerable services and protocols.
- Use sticky bits, SUID, and SGID to attack Linux file systems.
  - Target directories that contain sensitive information or have weak permissions.

Guidelines for Exploiting *nix-Based Vulnerabilities (Slide 2 of 2)

- After compromising a low-level Linux account, use password cracking, kernel exploits, SUID binaries, shared directories, weak permissions, poorly configured cron jobs, and suggested Metasploit modules to escalate privilege.
- Check to see which privileged default and service-added Linux accounts you can target for password cracking or hash dumping.
- Look for service and protocol versions, weak directory permissions, and weak mount points you can target.
- When attacking mobile devices, use physical access, social engineering/app side-loading, lack of basic security practices, and software exploits to compromise the target.
- If applicable, consider using hardware-based attacks against devices if you have physical access to them.

Reflective Questions

1. Which Windows exploits have you found to be the most effective? Have you found some operating systems to be easier targets than others?

2. Which *nix-based exploits have you found to be the most effective? Which systems are you likely to target in your own pen tests?