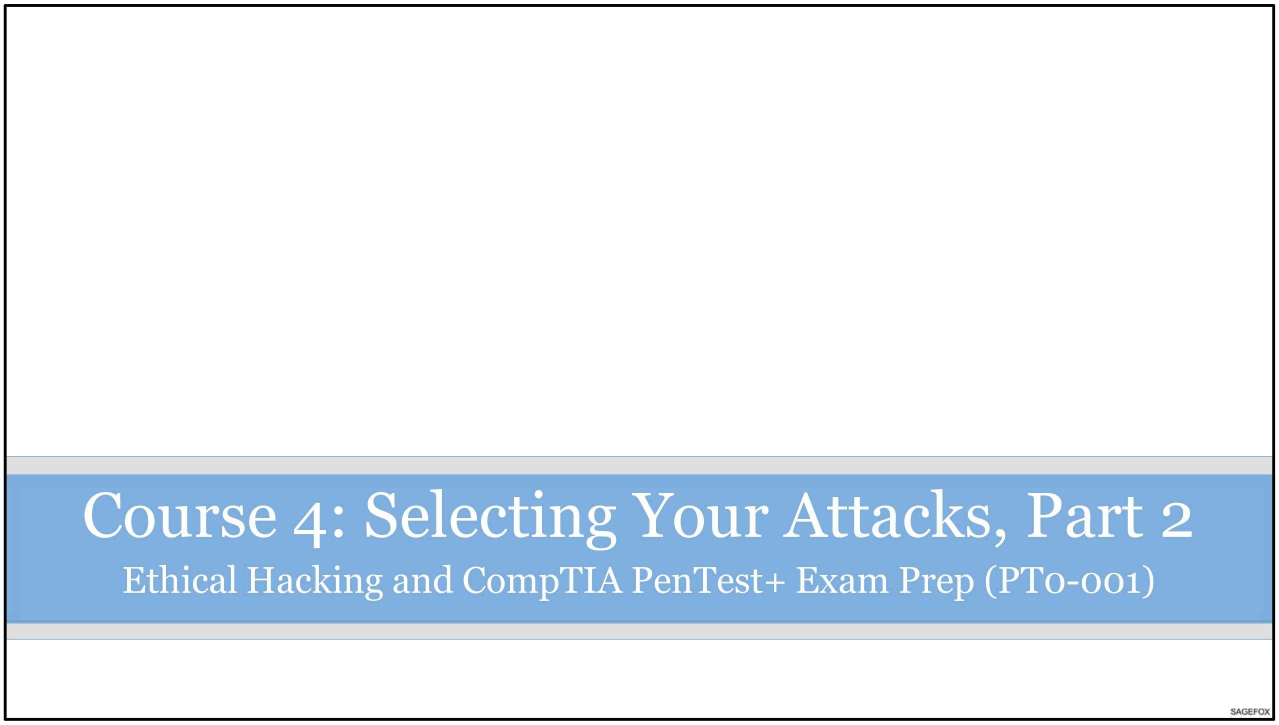


Course 4: Selecting Your Attacks, Part 2

Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001)

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Cross-Site Scripting Demo

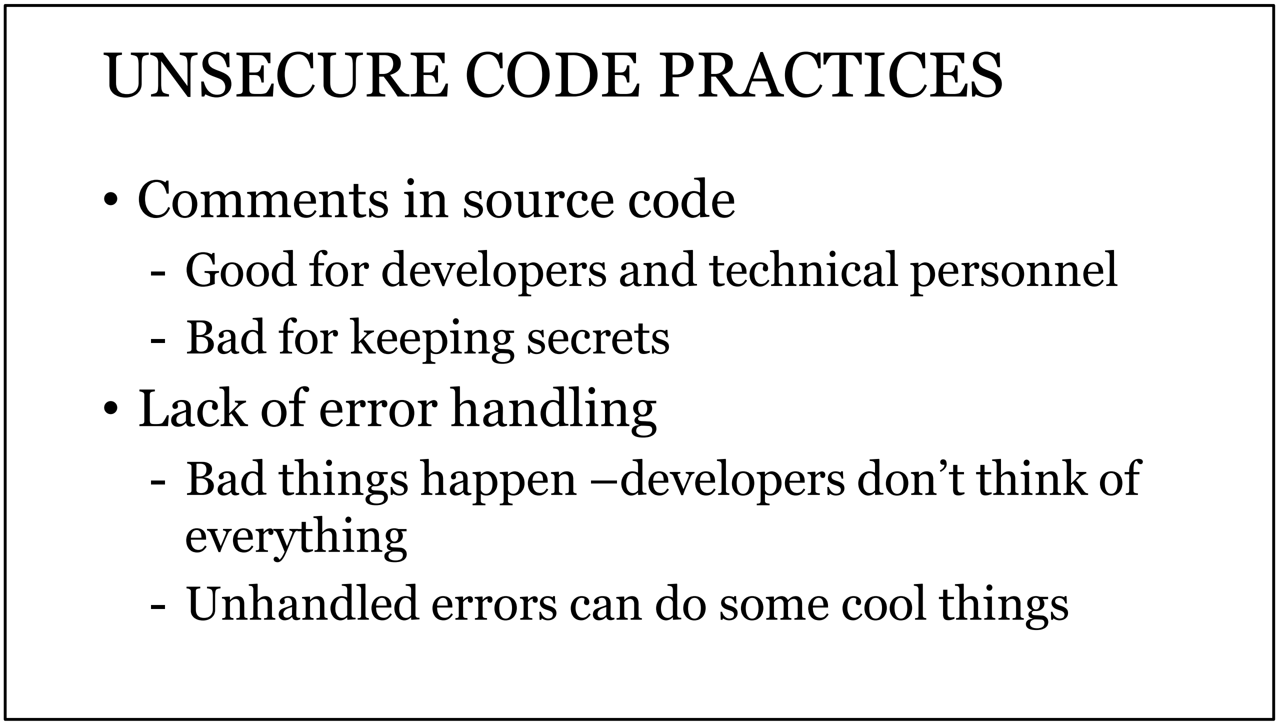
Episode 1

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

Code Vulnerabilities

Episode 2

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

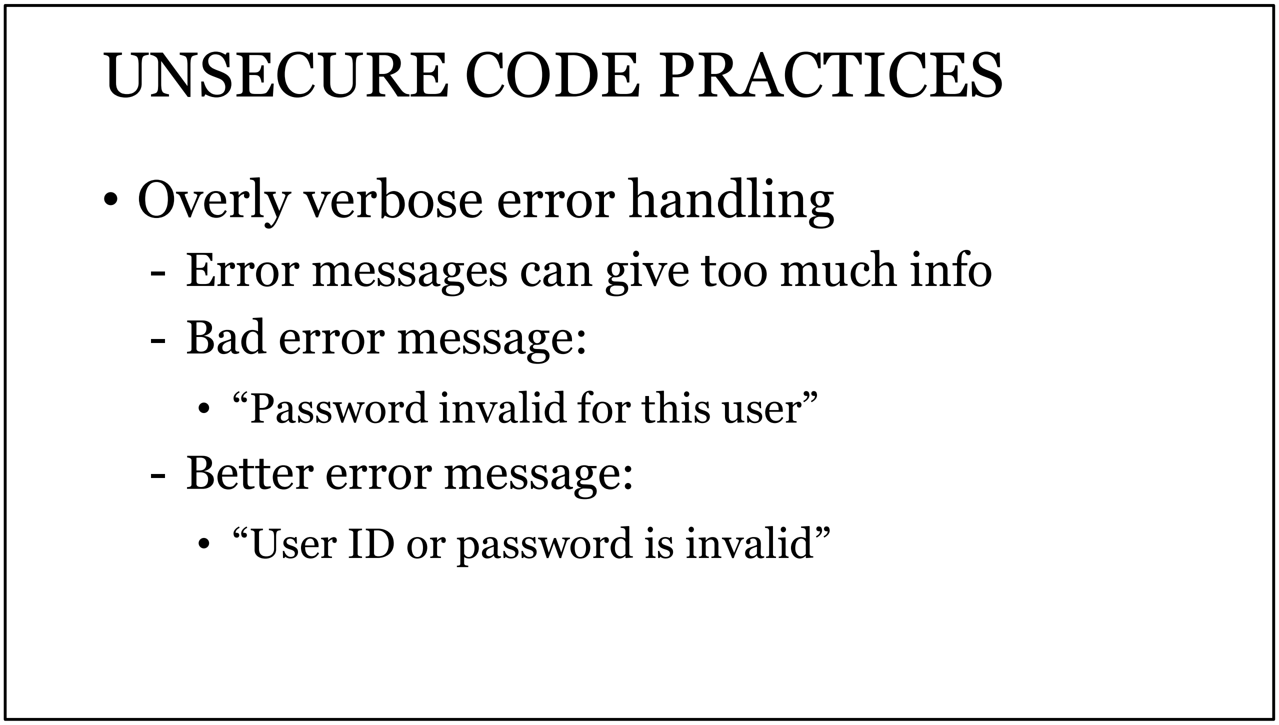


UNSECURE CODE PRACTICES

- Comments in source code
  - Good for developers and technical personnel
  - Bad for keeping secrets
- Lack of error handling
  - Bad things happen –developers don’t think of everything
  - Unhandled errors can do some cool things

3.4.9 Unsecure code practices
3.4.9.1 Comments in source code
3.4.9.2 Lack of error handling
3.4.9.3 Overly verbose error handling

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

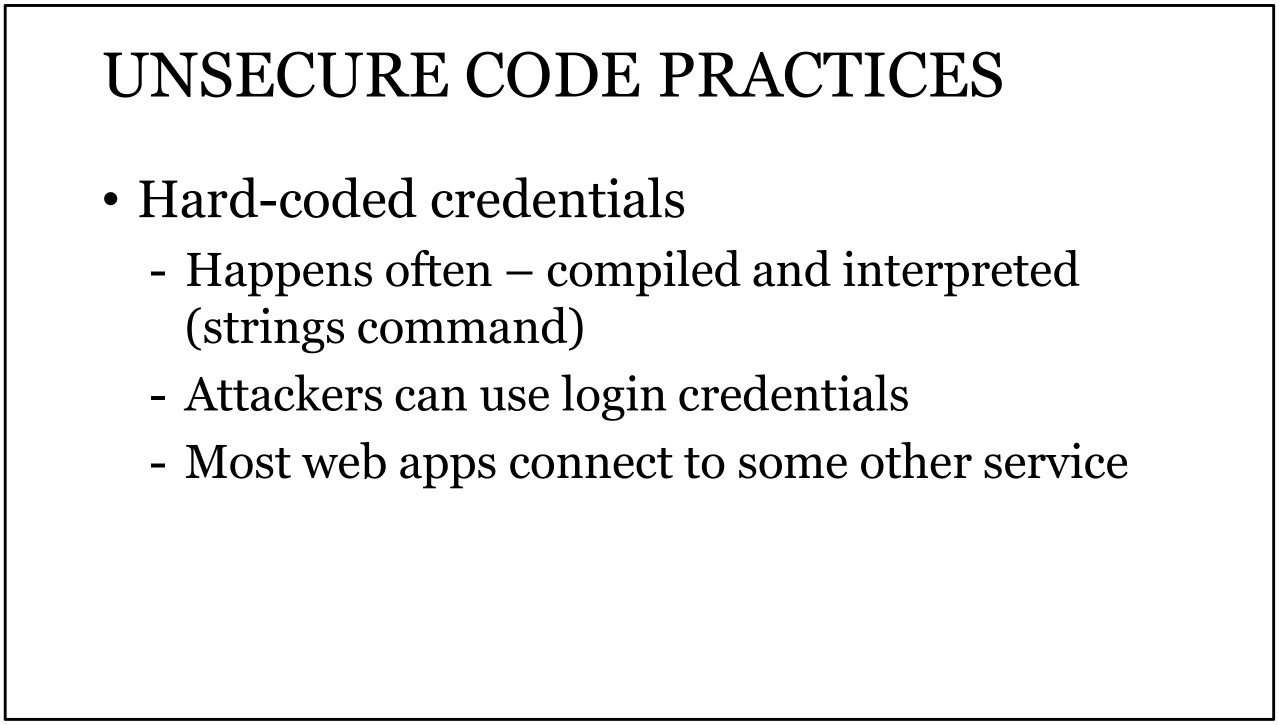


UNSECURE CODE PRACTICES

- Overly verbose error handling
  - Error messages can give too much info
  - Bad error message:
    - “Password invalid for this user”
  - Better error message:
    - “User ID or password is invalid”

3.4.9 Unsecure code practices
3.4.9.1 Comments in source code
3.4.9.2 Lack of error handling
3.4.9.3 Overly verbose error handling

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

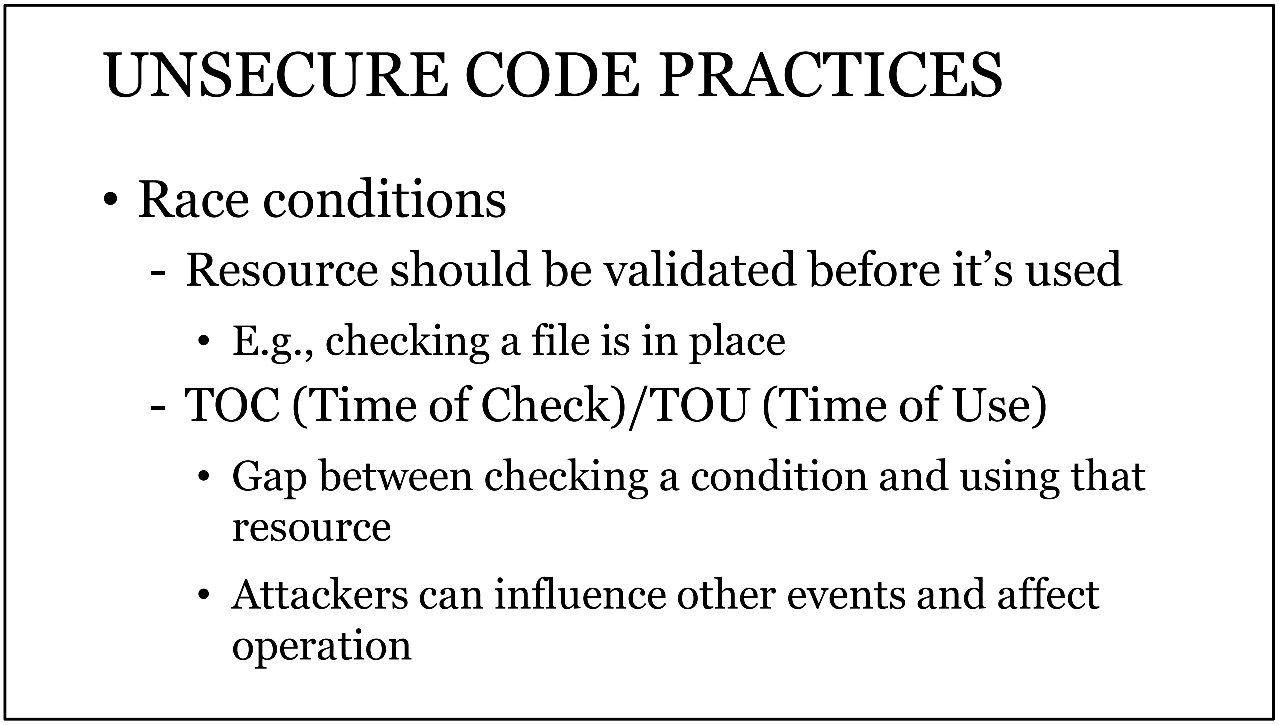


UNSECURE CODE PRACTICES

- Hard-coded credentials
  - Happens often – compiled and interpreted (strings command)
  - Attackers can use login credentials
  - Most web apps connect to some other service

3.4.9.4 Hard-coded credentials
3.4.9.5 Race conditions

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

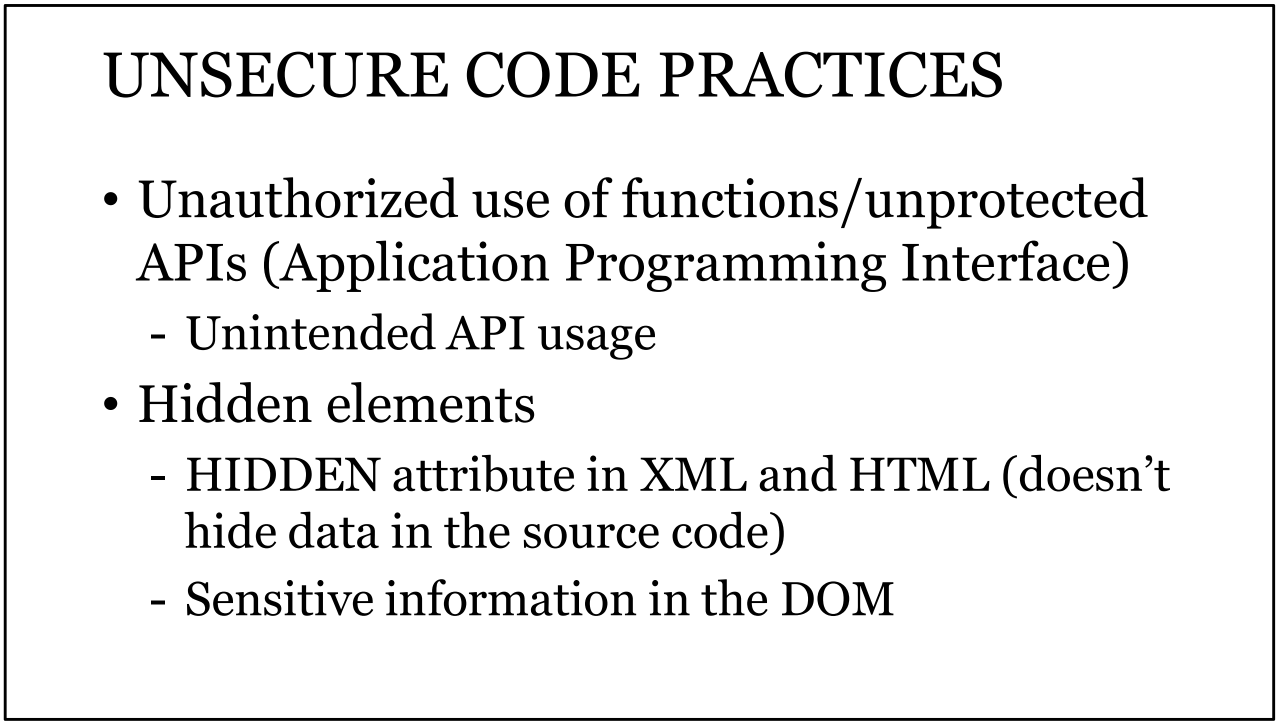


UNSECURE CODE PRACTICES

- Race conditions
  - Resource should be validated before it’s used
    - E.g., checking a file is in place
  - TOC (Time of Check)/TOU (Time of Use)
    - Gap between checking a condition and using that resource
    - Attackers can influence other events and affect operation

3.4.9.4 Hard-coded credentials
3.4.9.5 Race conditions

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

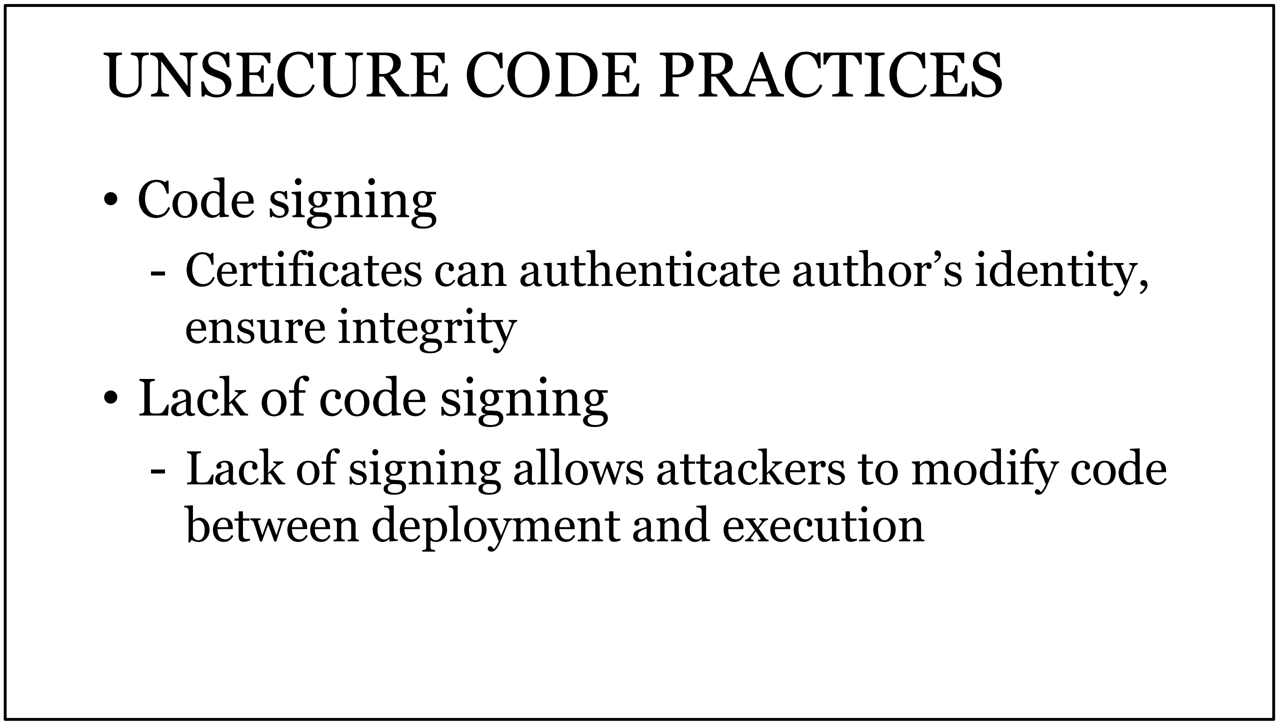


UNSECURE CODE PRACTICES

- Unauthorized use of functions/unprotected APIs (Application Programming Interface)
  - Unintended API usage
- Hidden elements
  - HIDDEN attribute in XML and HTML (doesn't hide data in the source code)
  - Sensitive information in the DOM

3.4.9.6 Unauthorized use of functions/unprotected APIs
3.4.9.7 Hidden elements
3.4.9.7.1 Sensitive information in the DOM
3.4.9.8 Lack of code signing

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



UNSECURE CODE PRACTICES

- Code signing
  - Certificates can authenticate author’s identity, ensure integrity
- Lack of code signing
  - Lack of signing allows attackers to modify code between deployment and execution

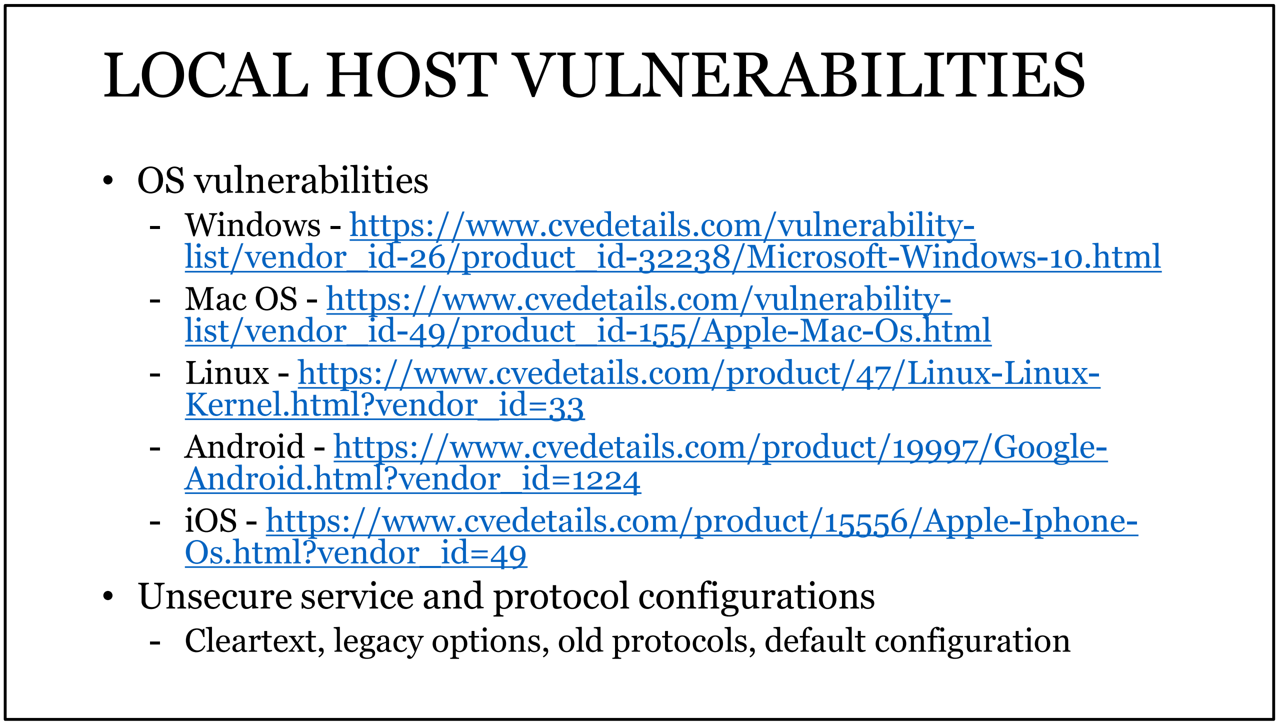
3.4.9.6 Unauthorized use of functions/unprotected APIs
3.4.9.7 Hidden elements
3.4.9.7.1 Sensitive information in the DOM
3.4.9.8 Lack of code signing

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Local Host Vulnerabilities

Episode 3

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon



LOCAL HOST VULNERABILITIES

- OS vulnerabilities
  - Windows - https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html
  - Mac OS - https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-155/Apple-Mac-Os.html
  - Linux - https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33
  - Android - https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
  - iOS - https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
- Unsecure service and protocol configurations
  - Cleartext, legacy options, old protocols, default configuration

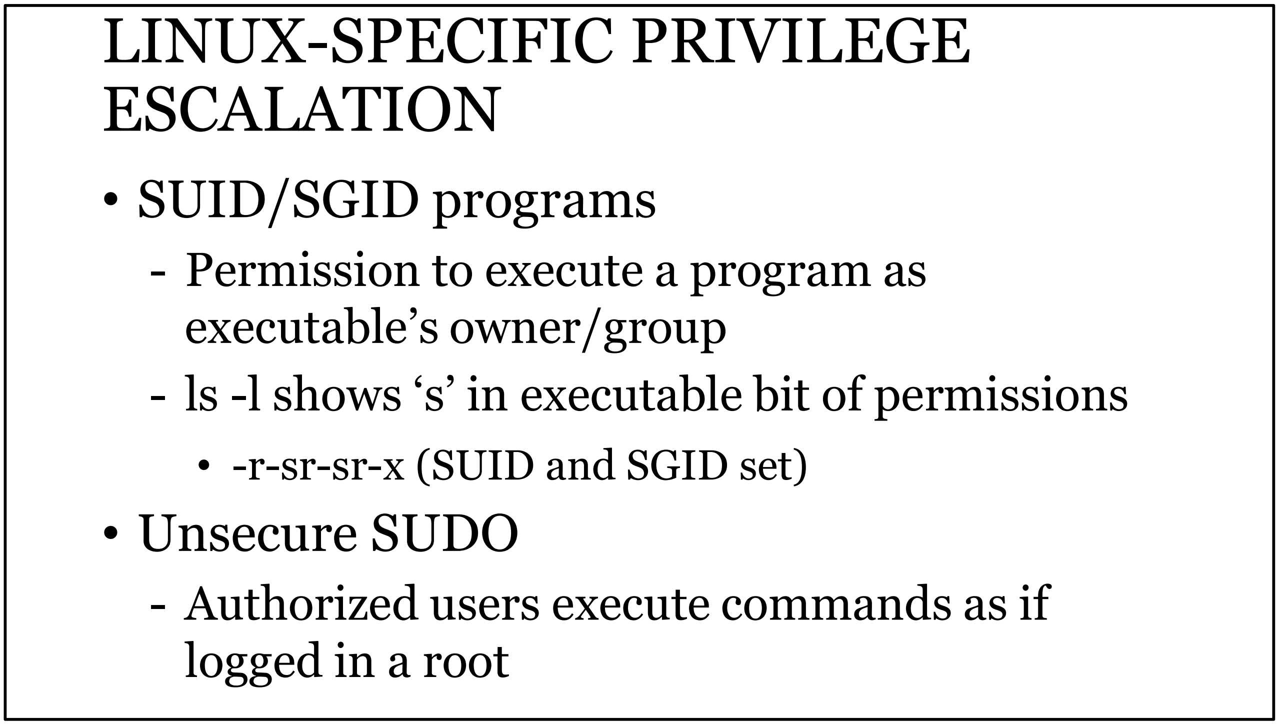
3.5 Given a scenario, exploit local host vulnerabilities
3.5.1 OS vulnerabilities
3.5.1.1 Windows
3.5.1.2 Mac OS
3.5.1.3 Linux
3.5.1.4 Android
3.5.1.5 iOS
3.5.2 Unsecure service and protocol configurations

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

Privilege Escalation (Linux)

Episode 4

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

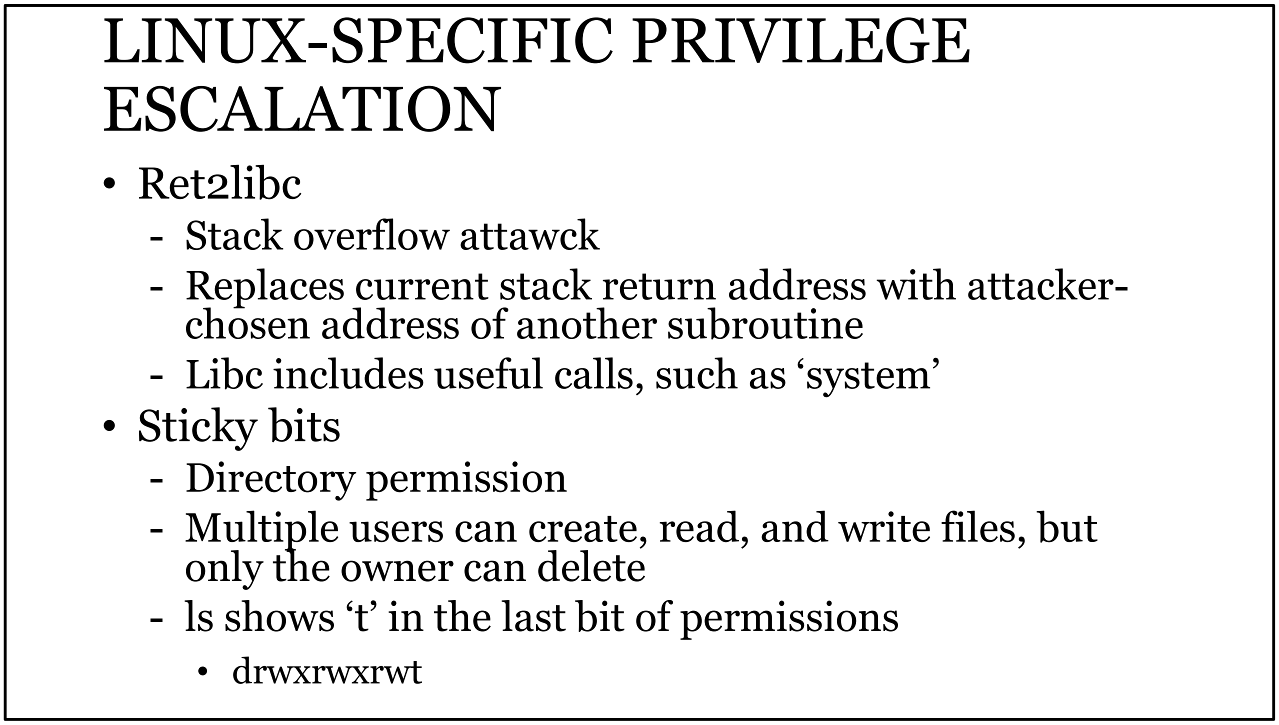


LINUX-SPECIFIC PRIVILEGE ESCALATION

- SUID/SGID programs
  - Permission to execute a program as executable's owner/group
  - ls -l shows 's' in executable bit of permissions
    - -r-sr-sr-x (SUID and SGID set)
- Unsecure SUDO
  - Authorized users execute commands as if logged in a root

3.5.3 Privilege escalation
3.5.3.1 Linux-specific
3.5.3.1.1 SUID/SGID programs
3.5.3.1.2 Unsecure SUDO
3.5.3.1.3 Ret2libc
3.5.3.1.4 Sticky bits

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

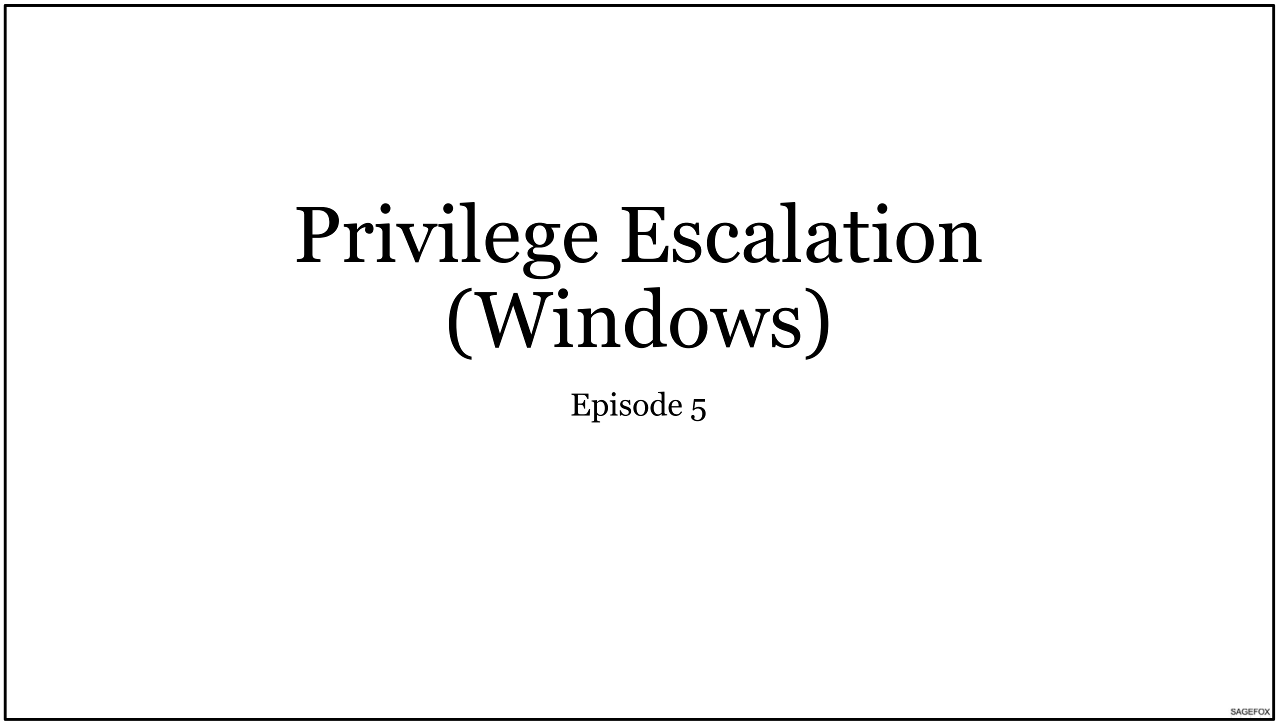


LINUX-SPECIFIC PRIVILEGE ESCALATION

- Ret2libc
  - Stack overflow attawck
  - Replaces current stack return address with attacker-chosen address of another subroutine
  - Libc includes useful calls, such as ‘system’
- Sticky bits
  - Directory permission
  - Multiple users can create, read, and write files, but only the owner can delete
  - ls shows ‘t’ in the last bit of permissions
    - drwxrwxrwt

3.5.3 Privilege escalation
3.5.3.1 Linux-specific
3.5.3.1.1 SUID/SGID programs
3.5.3.1.2 Unsecure SUDO
3.5.3.1.3 Ret2libc
3.5.3.1.4 Sticky bits

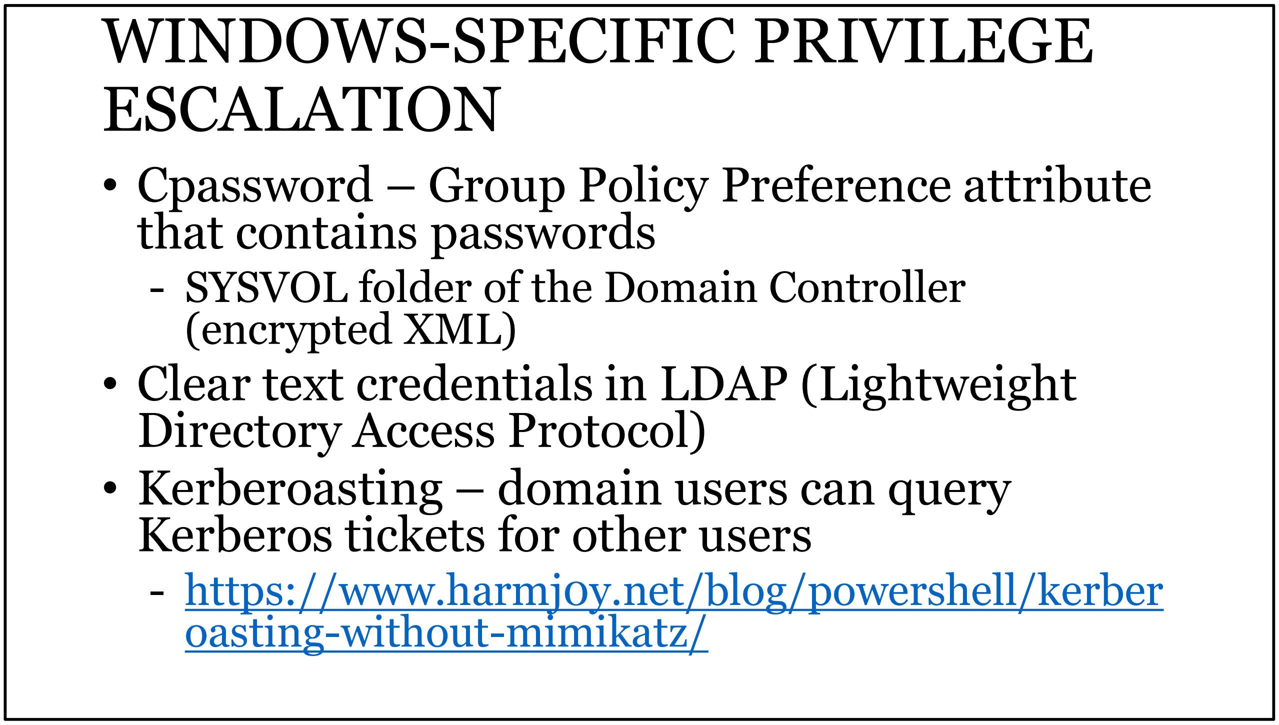
Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



Privilege Escalation (Windows)

Episode 5

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



WINDOWS-SPECIFIC PRIVILEGE ESCALATION

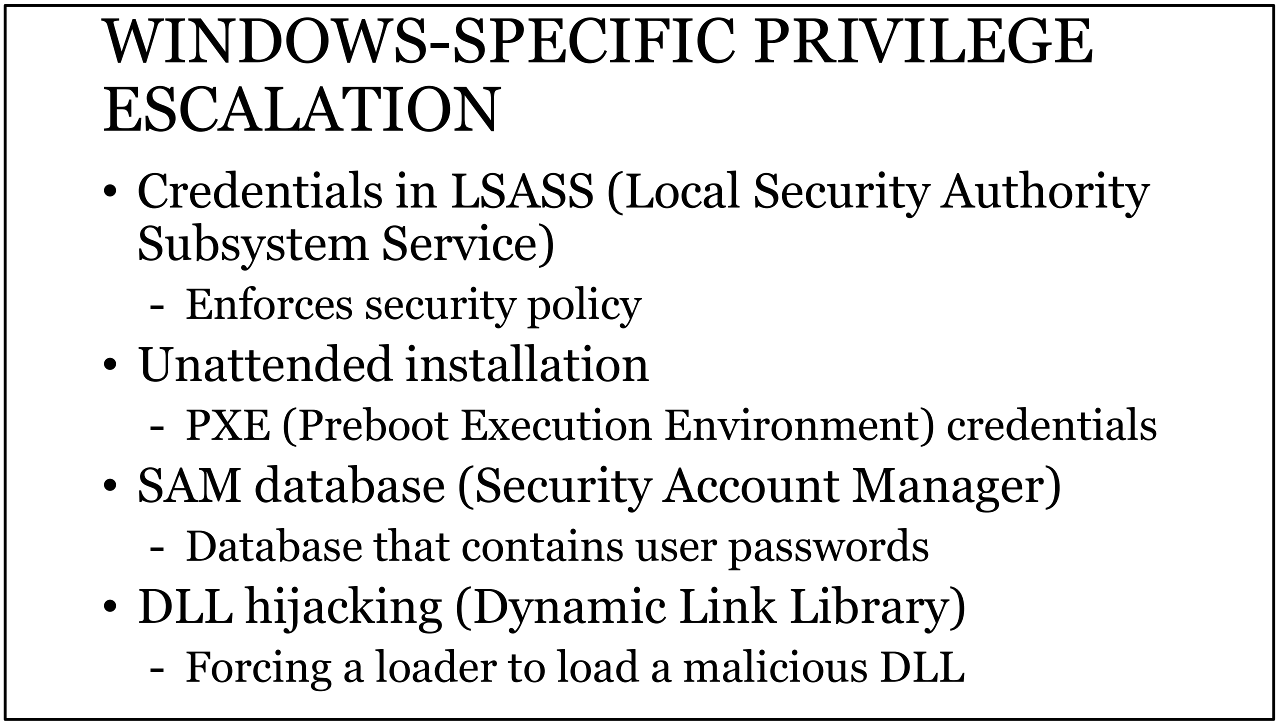
- Cpassword – Group Policy Preference attribute that contains passwords
  - SYSVOL folder of the Domain Controller (encrypted XML)
- Clear text credentials in LDAP (Lightweight Directory Access Protocol)
- Kerberoasting – domain users can query Kerberos tickets for other users
  - https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

3.5.3.2 Windows-specific
3.5.3.2.1 Cpassword
3.5.3.2.2 Clear text credentials in LDAP
3.5.3.2.3 Kerberoasting

https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

3.5.3.2.4 Credentials in LSASS
3.5.3.2.5 Unattended installation
3.5.3.2.6 SAM database
3.5.3.2.7 DLL hijacking

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon



WINDOWS-SPECIFIC PRIVILEGE ESCALATION

- Credentials in LSASS (Local Security Authority Subsystem Service)
  - Enforces security policy
- Unattended installation
  - PXE (Preboot Execution Environment) credentials
- SAM database (Security Account Manager)
  - Database that contains user passwords
- DLL hijacking (Dynamic Link Library)
  - Forcing a loader to load a malicious DLL

3.5.3.2 Windows-specific
3.5.3.2.1 Cpassword
3.5.3.2.2 Clear text credentials in LDAP
3.5.3.2.3 Kerberoasting

https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

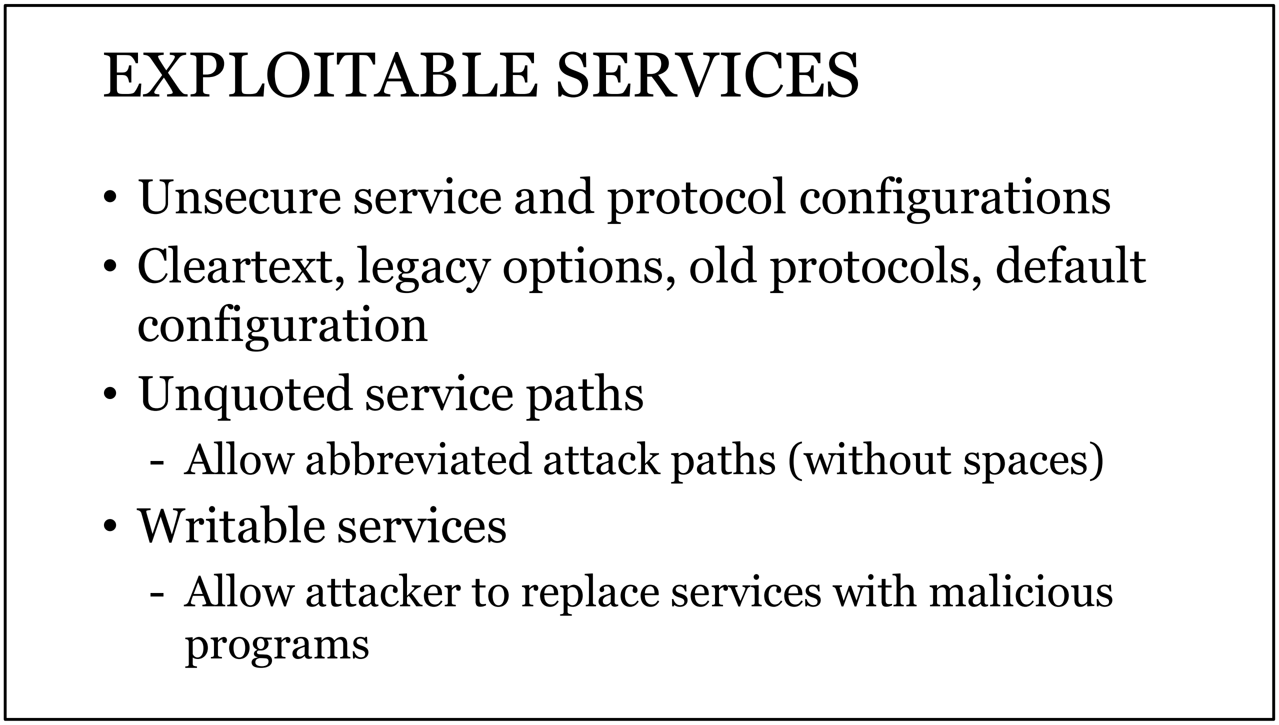
3.5.3.2.4 Credentials in LSASS
3.5.3.2.5 Unattended installation
3.5.3.2.6 SAM database
3.5.3.2.7 DLL hijacking

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

Misc. Privilege Escalation

Episode 6

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



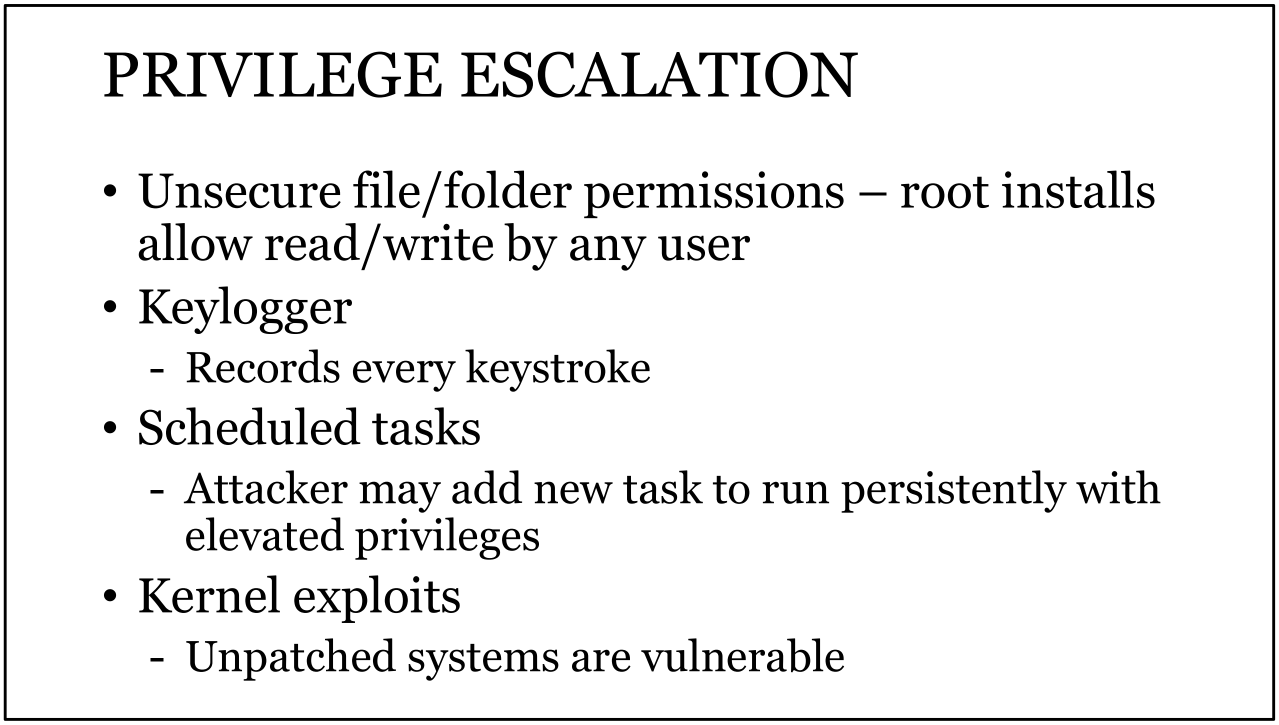
EXPLOITABLE SERVICES

- Unsecure service and protocol configurations
- Cleartext, legacy options, old protocols, default configuration
- Unquoted service paths
  - Allow abbreviated attack paths (without spaces)
- Writable services
  - Allow attacker to replace services with malicious programs

3.5.3.3 Exploitable services
3.5.3.3.1 Unquoted service paths
3.5.3.3.2 Writable services
3.5.3.4 Unsecure file/folder permissions
3.5.3.5 Keylogger
3.5.3.6 Scheduled tasks
3.6.3.7 Kernel exploits

https://pentestlab.blog/2017/04/24/windows-kernel-exploits/

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



PRIVILEGE ESCALATION

- Unsecure file/folder permissions – root installs allow read/write by any user
- Keylogger
  - Records every keystroke
- Scheduled tasks
  - Attacker may add new task to run persistently with elevated privileges
- Kernel exploits
  - Unpatched systems are vulnerable

3.5.3.3 Exploitable services
3.5.3.3.1 Unquoted service paths
3.5.3.3.2 Writable services
3.5.3.4 Unsecure file/folder permissions
3.5.3.5 Keylogger
3.5.3.6 Scheduled tasks
3.6.3.7 Kernel exploits

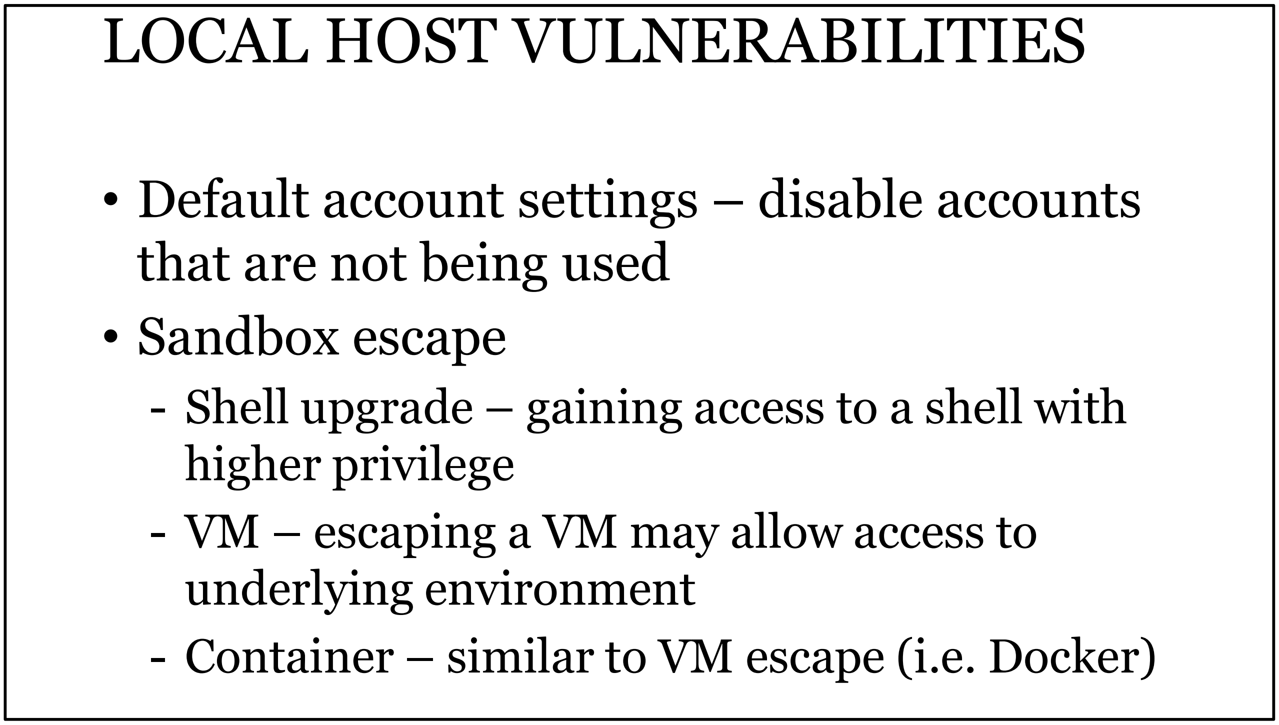
https://pentestlab.blog/2017/04/24/windows-kernel-exploits/

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

Misc. Local Host Vulnerabilities

Episode 7

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



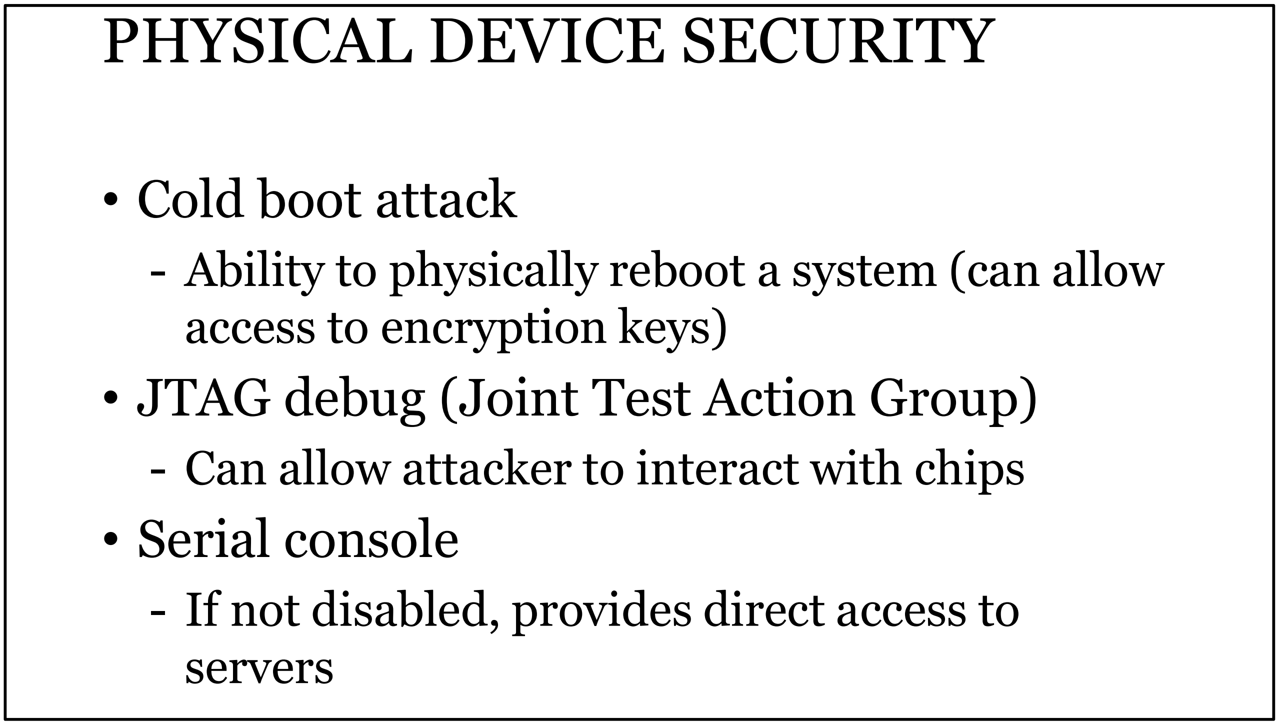
LOCAL HOST VULNERABILITIES

- Default account settings – disable accounts that are not being used
- Sandbox escape
  - Shell upgrade – gaining access to a shell with higher privilege
  - VM – escaping a VM may allow access to underlying environment
  - Container – similar to VM escape (i.e. Docker)

3.5.4 Default account settings
3.5.5 Sandbox escape
3.5.5.1 Shell upgrade
3.5.5.2 VM
3.5.5.3 Container
3.5.6 Physical device security
3.5.6.1 Cold boot attack
3.5.6.2 JTAG debug
3.5.6.3 Serial console

https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
https://4sysops.com/archives/reset-a-windows-10-password

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



PHYSICAL DEVICE SECURITY

- Cold boot attack
  - Ability to physically reboot a system (can allow access to encryption keys)
- JTAG debug (Joint Test Action Group)
  - Can allow attacker to interact with chips
- Serial console
  - If not disabled, provides direct access to servers

3.5.4 Default account settings
3.5.5 Sandbox escape
3.5.5.1 Shell upgrade
3.5.5.2 VM
3.5.5.3 Container
3.5.6 Physical device security
3.5.6.1 Cold boot attack
3.5.6.2 JTAG debug
3.5.6.3 Serial console

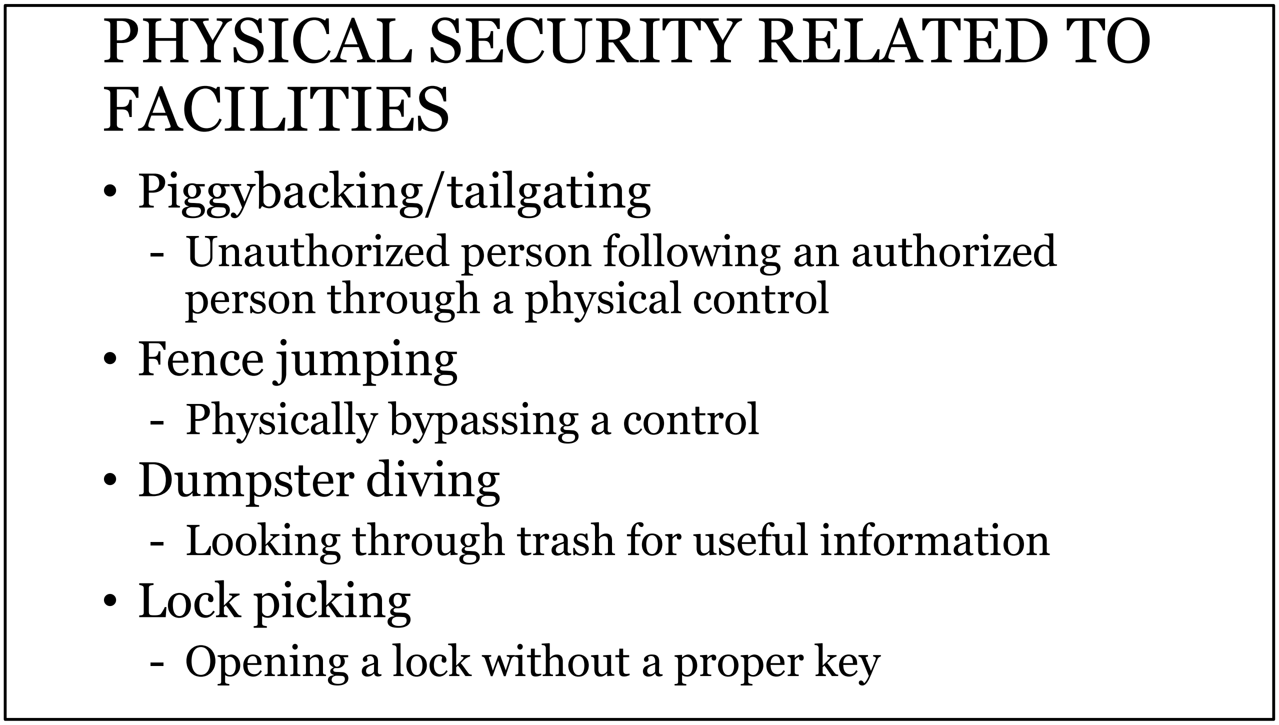
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise
https://4sysops.com/archives/reset-a-windows-10-password

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Physical Security

Episode 8

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



PHYSICAL SECURITY RELATED TO FACILITIES

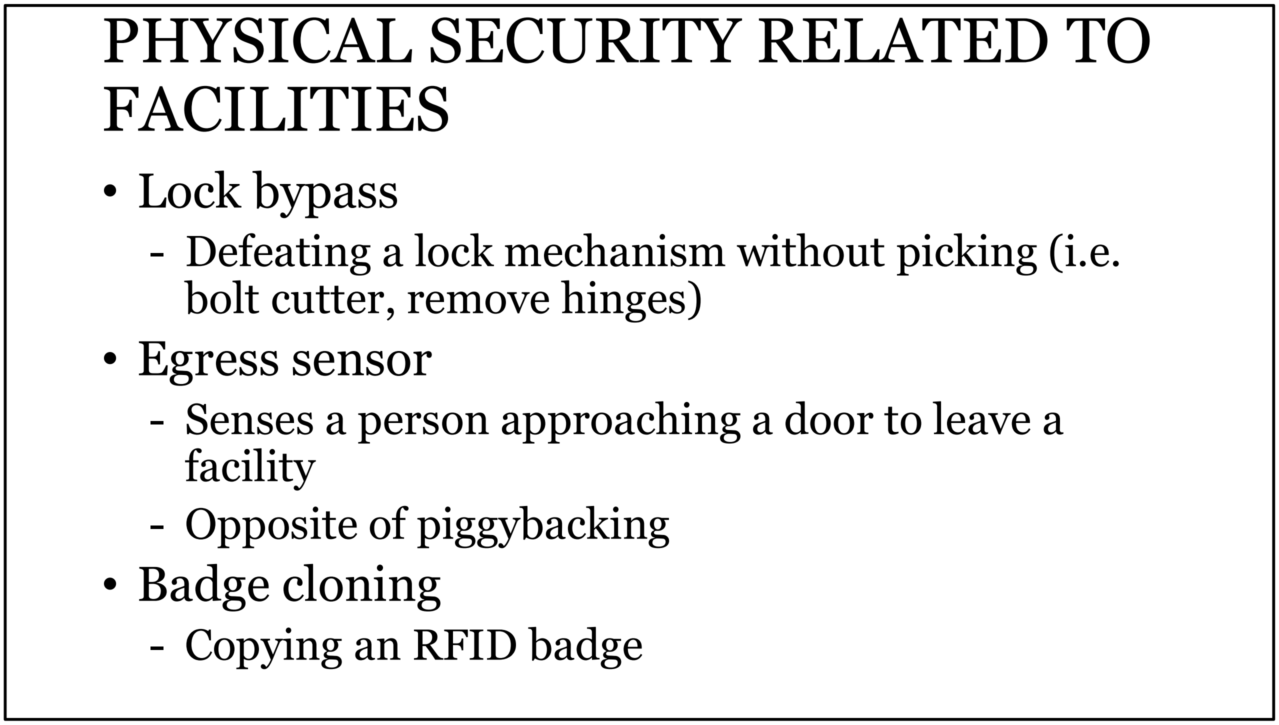
- Piggybacking/tailgating
  - Unauthorized person following an authorized person through a physical control
- Fence jumping
  - Physically bypassing a control
- Dumpster diving
  - Looking through trash for useful information
- Lock picking
  - Opening a lock without a proper key

3.6 Summarize physical security attacks related to facilities
3.6.1 Piggybacking/tailgating
3.6.2 Fence jumping
3.6.3 Dumpster diving
3.6.4 Lock picking

https://www.scribd.com/doc/205665803/Lockpicking-Detail-Overkill

3.6.5 Lock bypass
3.6.6 Egress sensor
3.6.7 Badge cloning

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon



PHYSICAL SECURITY RELATED TO FACILITIES

- Lock bypass
  - Defeating a lock mechanism without picking (i.e. bolt cutter, remove hinges)
- Egress sensor
  - Senses a person approaching a door to leave a facility
  - Opposite of piggybacking
- Badge cloning
  - Copying an RFID badge

3.6 Summarize physical security attacks related to facilities
3.6.1 Piggybacking/tailgating
3.6.2 Fence jumping
3.6.3 Dumpster diving
3.6.4 Lock picking

https://www.scribd.com/doc/205665803/Lockpicking-Detail-Overkill

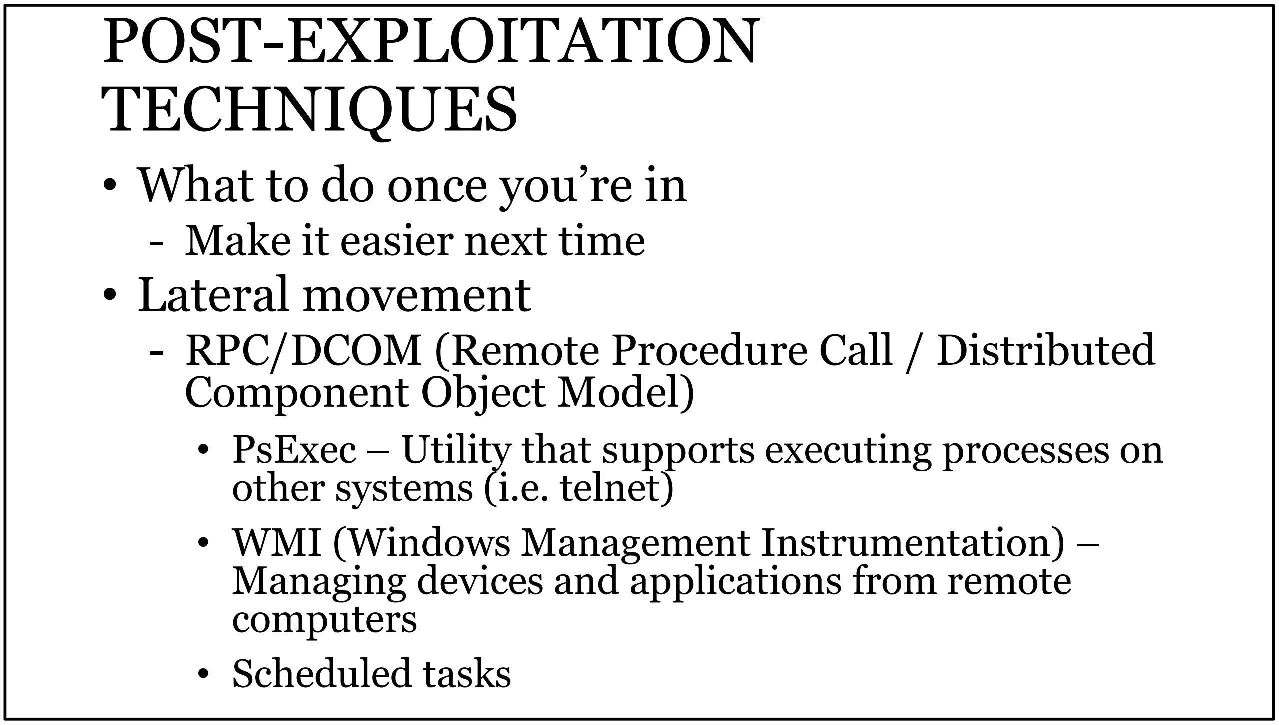
3.6.5 Lock bypass
3.6.6 Egress sensor
3.6.7 Badge cloning

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon

Post-Exploitation Techniques

Episode 9

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

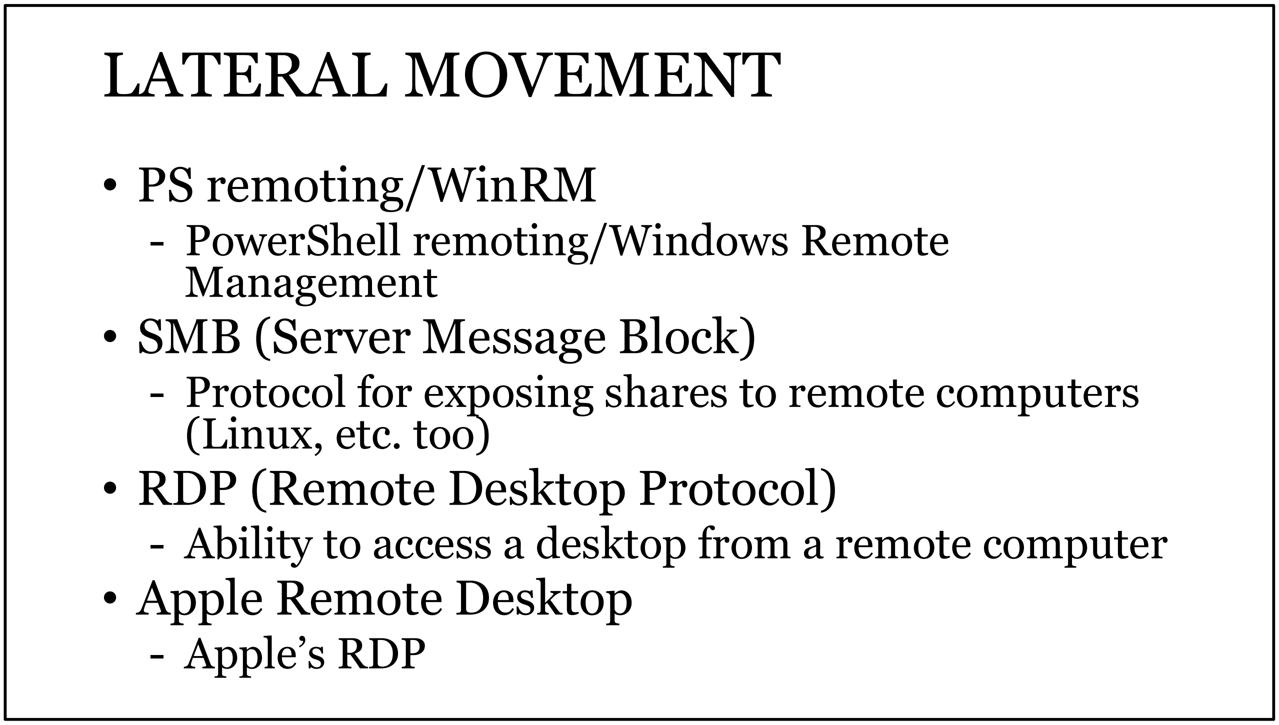


POST-EXPLOITATION TECHNIQUES

- What to do once you’re in
  - Make it easier next time
- Lateral movement
  - RPC/DCOM (Remote Procedure Call / Distributed Component Object Model)
    - PsExec – Utility that supports executing processes on other systems (i.e. telnet)
    - WMI (Windows Management Instrumentation) – Managing devices and applications from remote computers
    - Scheduled tasks

3.7 Given a scenario, perform post-exploitation techniques
3.7.1 Lateral movement
3.7.1.1 RPC/DCOM
3.7.1.1.1 PsExec
3.7.1.1.2 WMI
3.7.1.1.3 Scheduled tasks
3.7.1.2 PS remoting/WinRM
3.7.1.3 SMB
3.7.1.4 RDP
3.7.1.5 Apple Remote Desktop

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

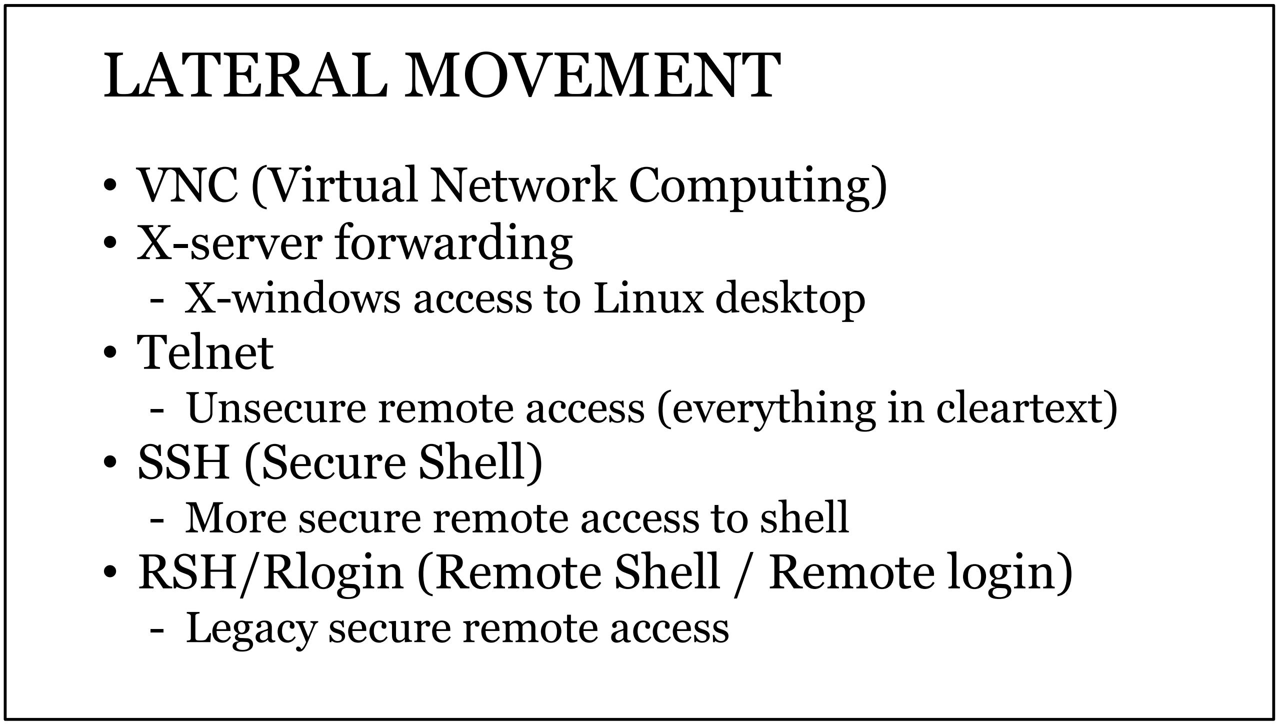


LATERAL MOVEMENT

- PS remoting/WinRM
  - PowerShell remoting/Windows Remote Management
- SMB (Server Message Block)
  - Protocol for exposing shares to remote computers (Linux, etc. too)
- RDP (Remote Desktop Protocol)
  - Ability to access a desktop from a remote computer
- Apple Remote Desktop
  - Apple’s RDP

3.7 Given a scenario, perform post-exploitation techniques
3.7.1 Lateral movement
3.7.1.1 RPC/DCOM
3.7.1.1.1 PsExec
3.7.1.1.2 WMI
3.7.1.1.3 Scheduled tasks
3.7.1.2 PS remoting/WinRM
3.7.1.3 SMB
3.7.1.4 RDP
3.7.1.5 Apple Remote Desktop

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon



LATERAL MOVEMENT

- VNC (Virtual Network Computing)
- X-server forwarding
  - X-windows access to Linux desktop
- Telnet
  - Unsecure remote access (everything in cleartext)
- SSH (Secure Shell)
  - More secure remote access to shell
- RSH/Rlogin (Remote Shell / Remote login)
  - Legacy secure remote access

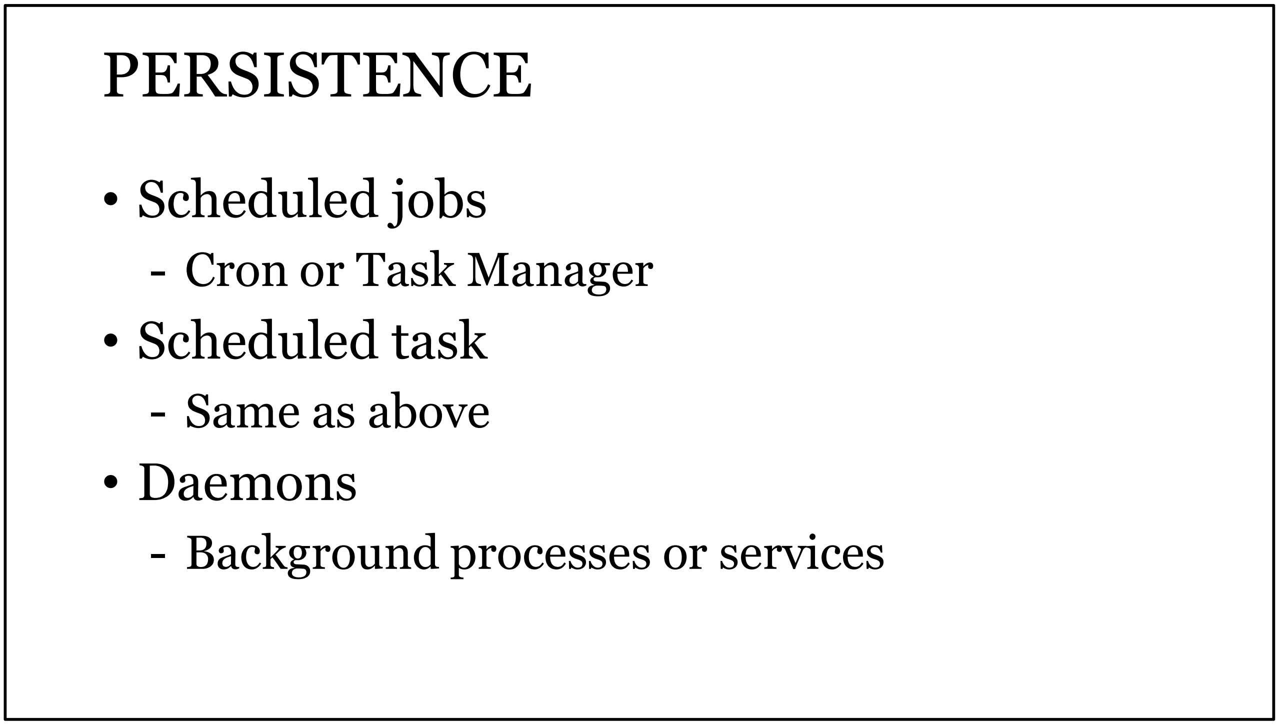
3.7.1.6 VNC
3.7.1.7 X-server forwarding
3.7.1.8 Telnet
3.7.1.9 SSH
3.7.1.10 RSH/Rlogin

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

Persistence and Stealth

Episode 10

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

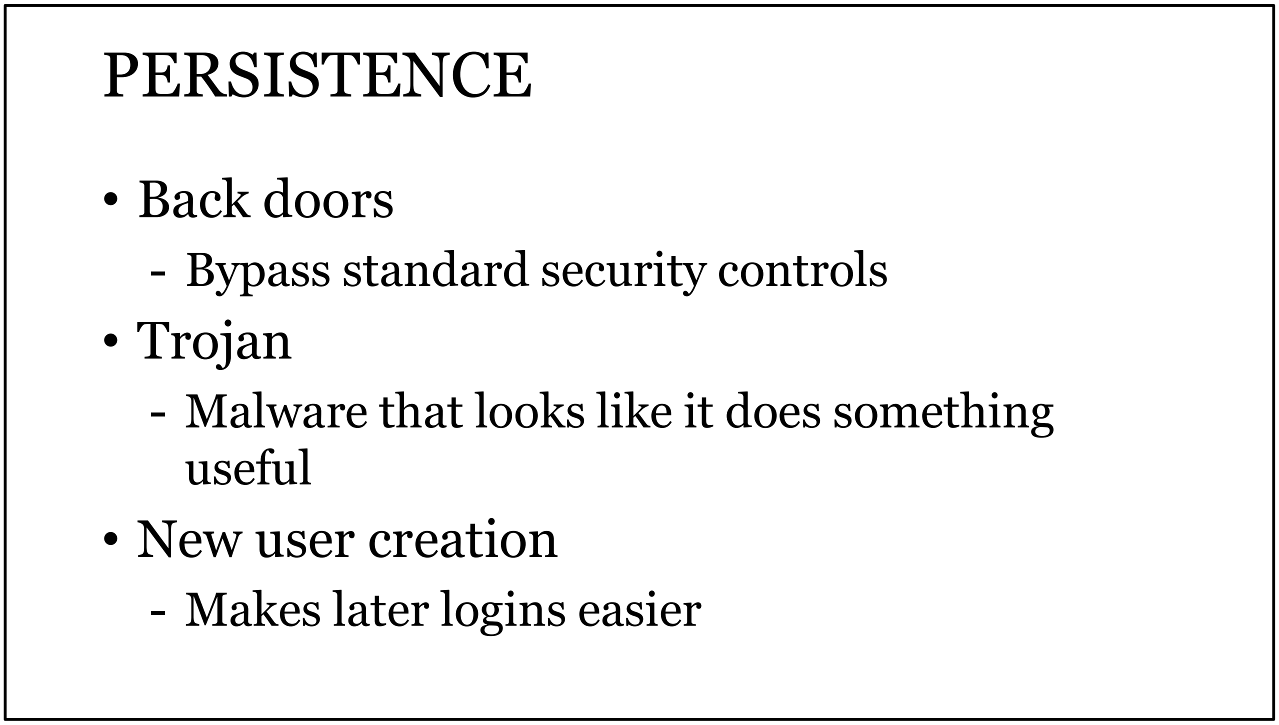


PERSISTENCE

- Scheduled jobs
  - Cron or Task Manager
- Scheduled task
  - Same as above
- Daemons
  - Background processes or services

3.7.2 Persistence
3.7.2.1 Scheduled jobs
3.7.2.2 Scheduled tasks
3.7.2.3 Daemons
3.7.2.4 Back doors
3.7.2.5 Trojan
3.7.2.6 New user creation

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon

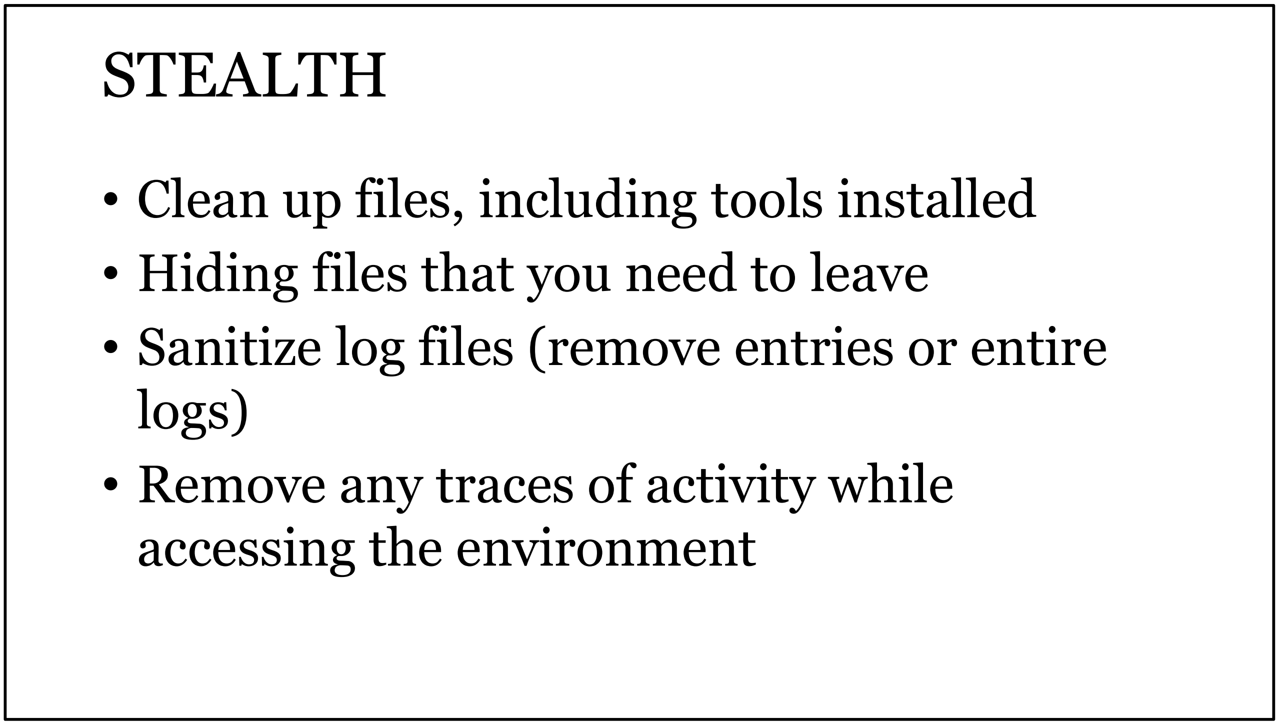


PERSISTENCE

- Back doors
  - Bypass standard security controls
- Trojan
  - Malware that looks like it does something useful
- New user creation
  - Makes later logins easier

3.7.2 Persistence
3.7.2.1 Scheduled jobs
3.7.2.2 Scheduled tasks
3.7.2.3 Daemons
3.7.2.4 Back doors
3.7.2.5 Trojan
3.7.2.6 New user creation

Source: Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001) with Michael Solomon



STEALTH

- Clean up files, including tools installed
- Hiding files that you need to leave
- Sanitize log files (remove entries or entire logs)
- Remove any traces of activity while accessing the environment

3.7.3 Covering your tracks

Source: Ethical Hacking and CompTIA
PenTest+ Exam Prep (PT0-001) with Michael
Solomon