

Lecture 6

System Hacking

Mohd Zaki Mas'ud

You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk.

Kevin Mitnick

Warning: Critical WinRAR Flaw Affects All Versions Released In Last 19 Years

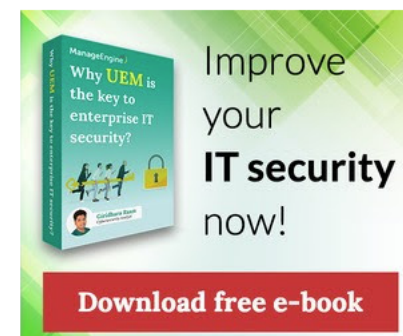
📅 February 21, 2019 👤 Swati Khandelwal



Beware Windows users... a new dangerous remote code execution vulnerability has been discovered in the WinRAR software, affecting hundreds of millions of users worldwide.

Cybersecurity researchers at Check Point have disclosed technical details of a critical vulnerability in WinRAR—a popular Windows file compression application with 500 million users worldwide—that affects all versions of the software released in last 19 years.

The flaw resides in the way an old third-party library, called UNACEV2.DLL, used by the software handled the extraction of files compressed in ACE data compression archive file format.



Popular News



540 Million Facebook User
Records Found On Unprotected
Amazon Servers

Over 1 Million **ASUS** Computers Hacked

Remember the [CCleaner hack](#)?

CCleaner hack was one of the largest supply chain attacks that infected more than [2.3 million users](#) with a [backdoored](#) version of the software in September 2017.

Security researchers today revealed another massive supply chain attack that compromised over 1 million computers manufactured by Taiwan-based tech giant ASUS.

SPONSORED SEARCHES

[Verify an Email Address](#)

[AntiVirus Sophos](#)

[Managed Server](#)

[VPN for Computer](#)

A group of state-sponsored hackers last year managed to hijack ASUS Live automatic software update server between June and November 2018 and pushed malicious updates to install backdoors on over one million Windows computers worldwide.

According to cybersecurity researchers from Russian firm [Kaspersky Lab](#), who discovered the attack and dubbed it **Operation ShadowHammer**, Asus was informed about the ongoing supply chain attack on Jan 31, 2019.

AT&T Business + AlienVault join forces.

The new AT&T Cybersecurity

[Learn More](#)

Improve
your
IT security
now!

[Download free e-book](#)

Popular News



540 Million Facebook User
Records Found On Unprotected
Amazon Servers



Facebook Caught Asking Some
Users Passwords for Their
Email Accounts



NSA Releases GHIDRA Source
Code — Free Reverse
Engineering Tool



Hackers Could Turn Pre-
Installed Antivirus App on



Trending:

[Article 13 >](#)

[Huawei P30 Pro >](#)

[Google Stadia >](#)

[AMD Ryzen 3000 >](#)

[Galaxy S10 >](#)

Security

US service provider hit by 'record-breaking' 1.7Tbps DDoS attack

Just five days after Github was whacked by massive 1.35Tbps attack



Carly Page

[@CarlyPage_](#)

06 March 2018



Pornhub has been hacked, but the hackers aren't...



iPhone 11 release date, specs and price: Leaked...



iPhone 11 release date, specs and price: Chassis...

System Hacking

- the information gathered from the information gathering and scanning can now be used for next phase:
- In this chapter, show how the information gathered can be used to “kick down the door” of a system and carry out the attack goal.
- information such as usernames, groups, passwords, permissions, and other system details, let attacker to see a reasonably accurate picture of the target.
- The more information gathered, the better, and the easier to locate the points that are vulnerable to attack.

- **Footprinting**

- Namespaces
- Employee information
- Phone numbers
- Facility information
- Job information






- **Scanning**

- locating active hosts
- identify hosts
- information about services running on each host.

- **Enumeration**

- Usernames
- Group information
- Passwords
- Hidden shares
- Device information
- Network layout
- Protocol information
- Server data
- Service information

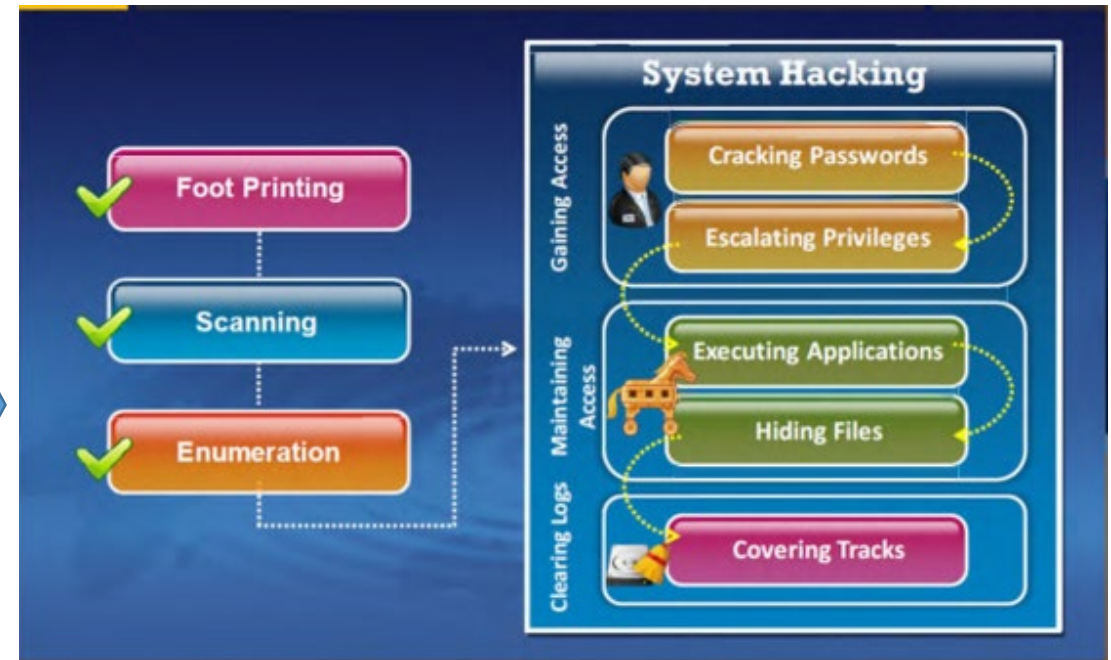
System Hacking Goals

Hacking-Stage	Goal	Technique/Exploit Used
 Gaining Access	To collect enough information to gain access	Password eavesdropping, brute forcing
 Escalating Privileges	To create a privileged user account if the user level is obtained	Password cracking, known exploits
 Executing Applications	To create and maintain backdoor access	Trojans
 Hiding Files	To hide malicious files	Rootkits
 Covering Tracks	To hide the presence of compromise	Clearing logs

The goal of an attacker at different hacking stages and the technique used to achieve that goal

System Hacking involves several malicious stages:-

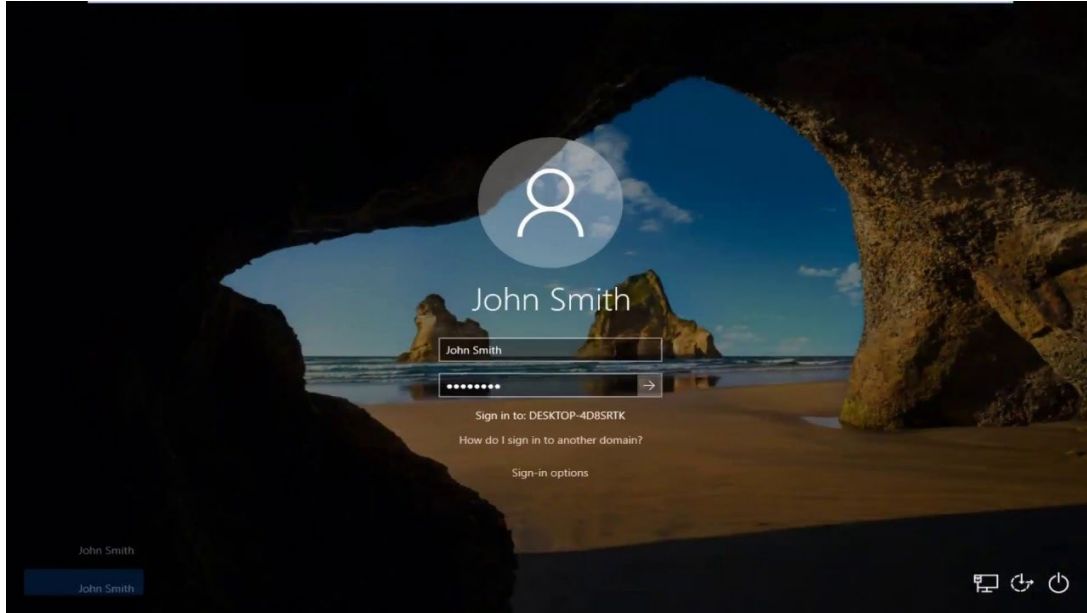
- Gaining access via cracking passwords or exploits
- escalating privileges,
- executing applications,
- hiding files,
- covering tracks,



System Hacking stages

Gaining Access via password cracking

Cracking Password



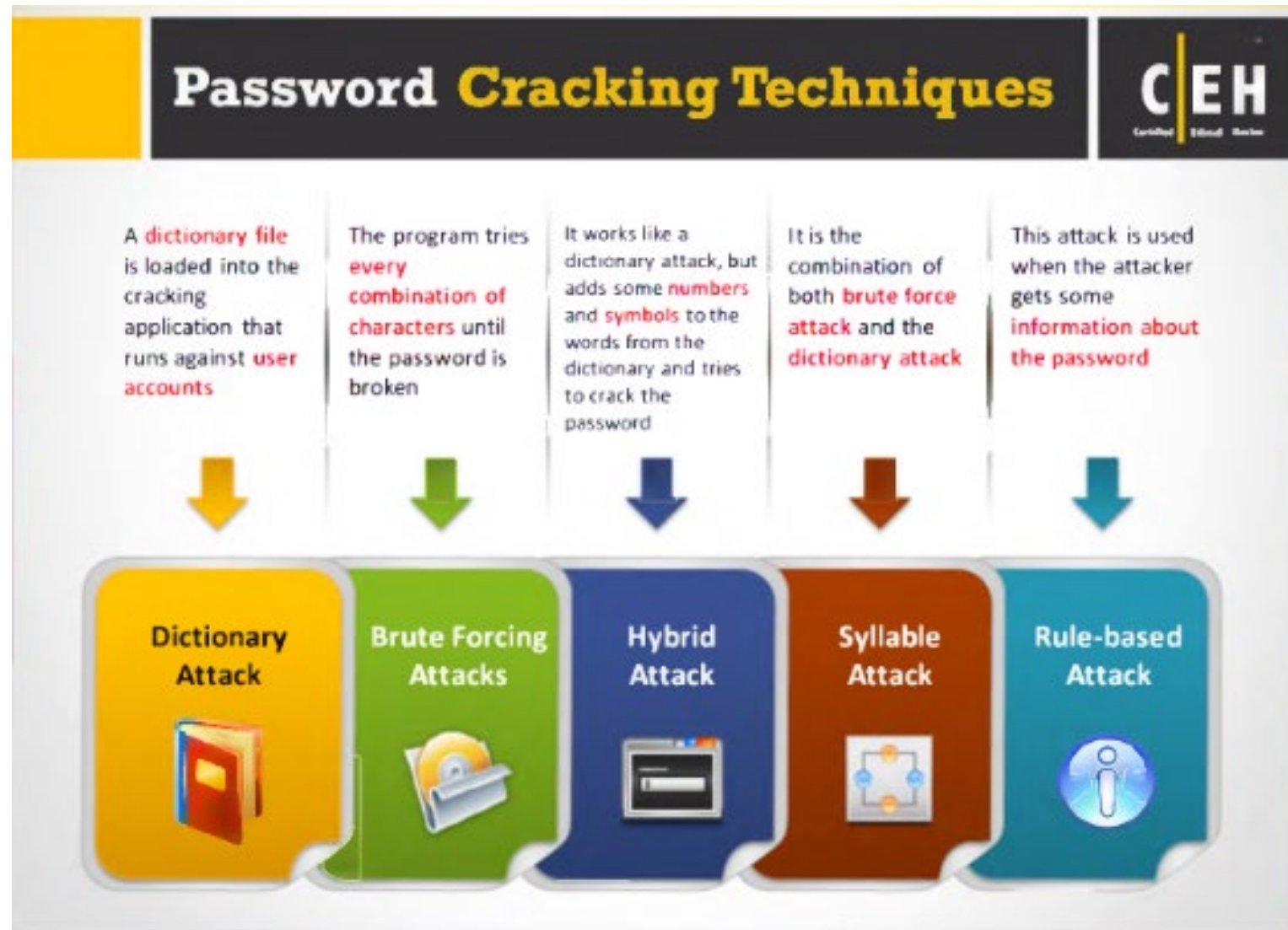
Ophcrack, cain and abel,
Jack the ripper, hydra,
crunch

- Password cracking is the process of recovering passwords from the data that has been transmitted by a computer system or stored in it
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system
- Most of the password cracking techniques are successful due to weak or easily guessable passwords

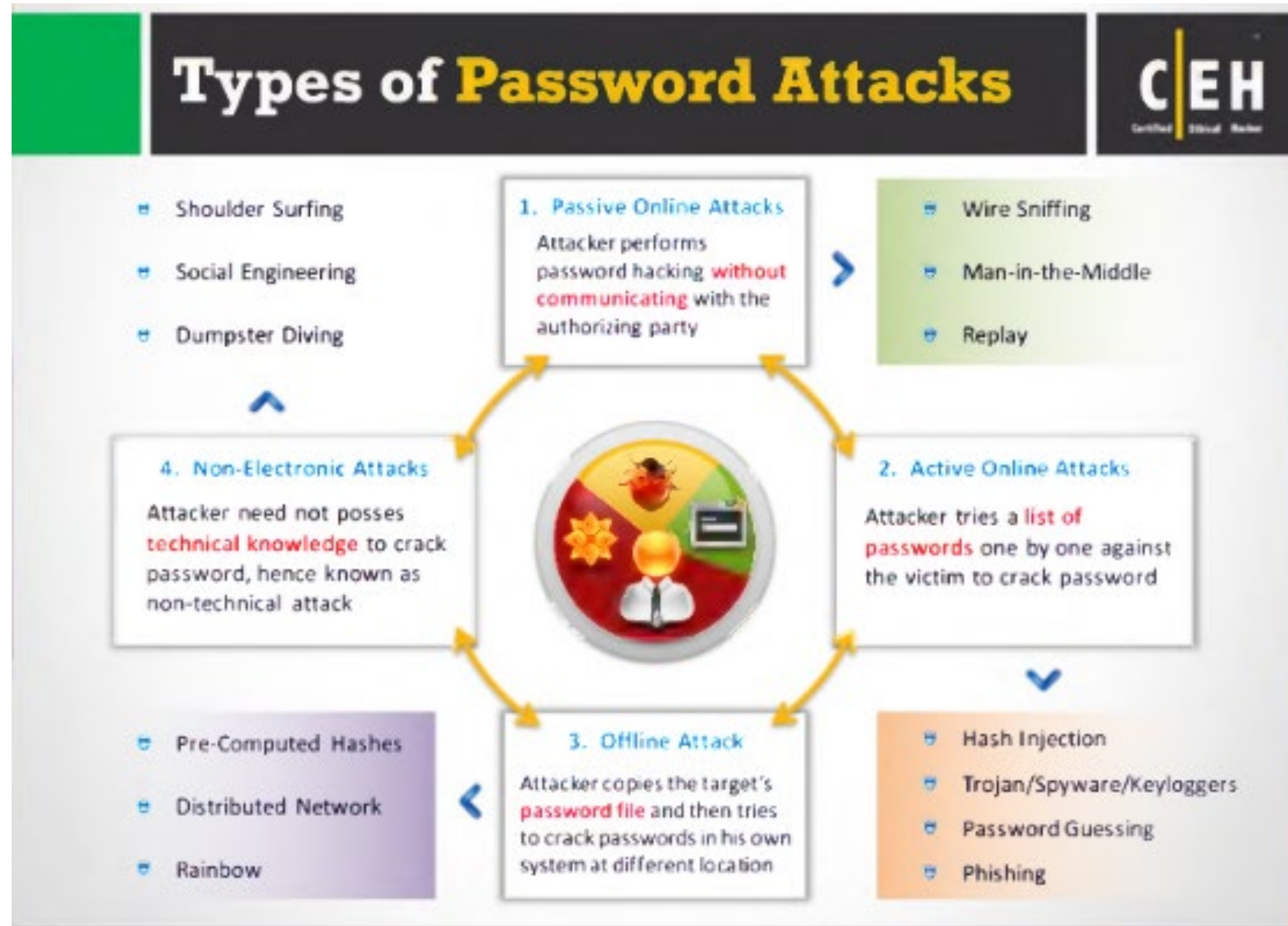
How complex is your Password

- Password should not be simple since simple passwords are prone to attacks
- complexity requirements policy setting help user create a good password
- should be a combination of alphanumeric characters such as letters, numbers, punctuation marks, and mathematical and other conventional symbols
- Conveniently people will try to use thier personal info in creating password but it can be exposed.
- A password should contain :-
 - letters, special characters, and numbers: apl@52
 - numbers: 23698217
 - special characters: &*#@!(%)
 - letters and numbers: meetl23
 - letters: POTHMYDE
 - letters and special characters: bob@&ba
 - characters and numbers: 123@\$4

How can password is break

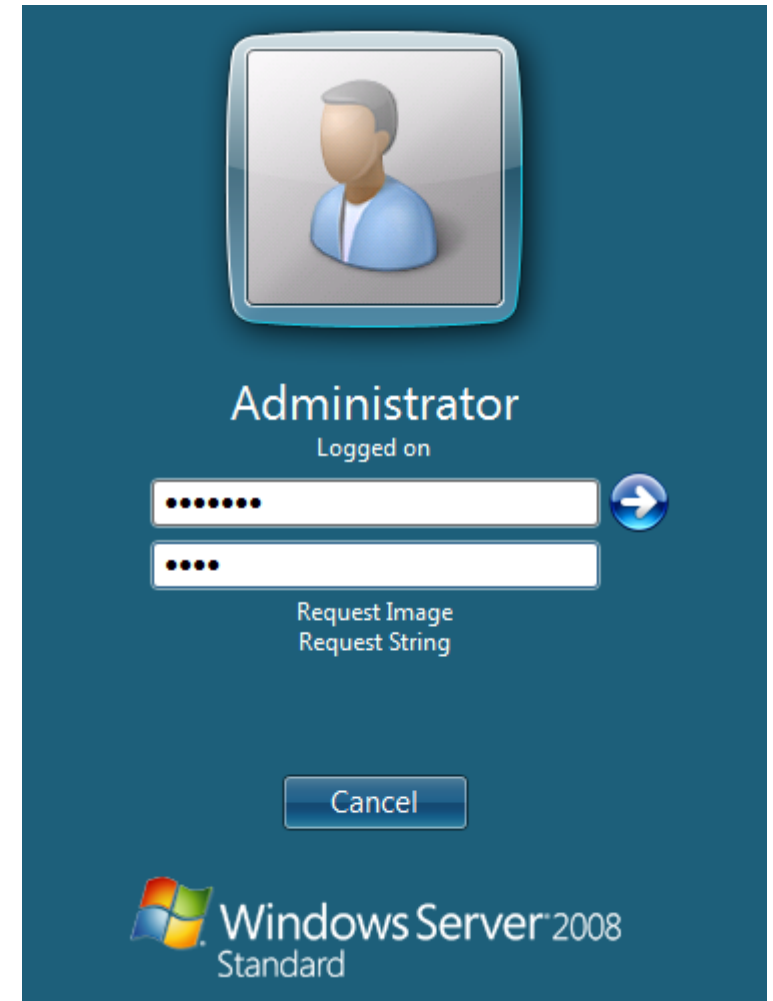


Password Attack type

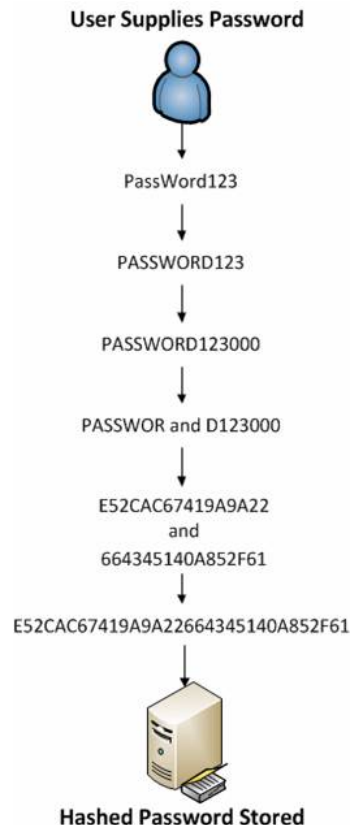
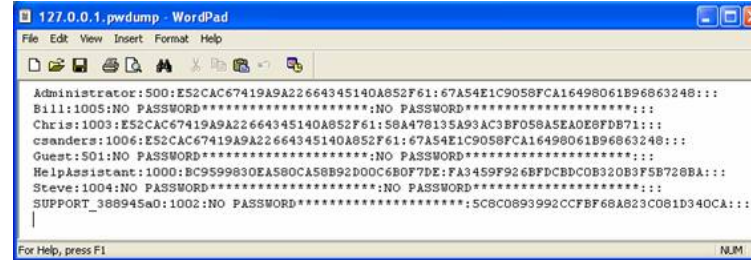


Microsoft Authentication

- Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM
- The NTLM authentication protocol types:
 - 1. NTLM authentication protocol
 - 2. LM authentication protocol
 - These protocols store user's password in the SAM database using different hashing methods
- Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM

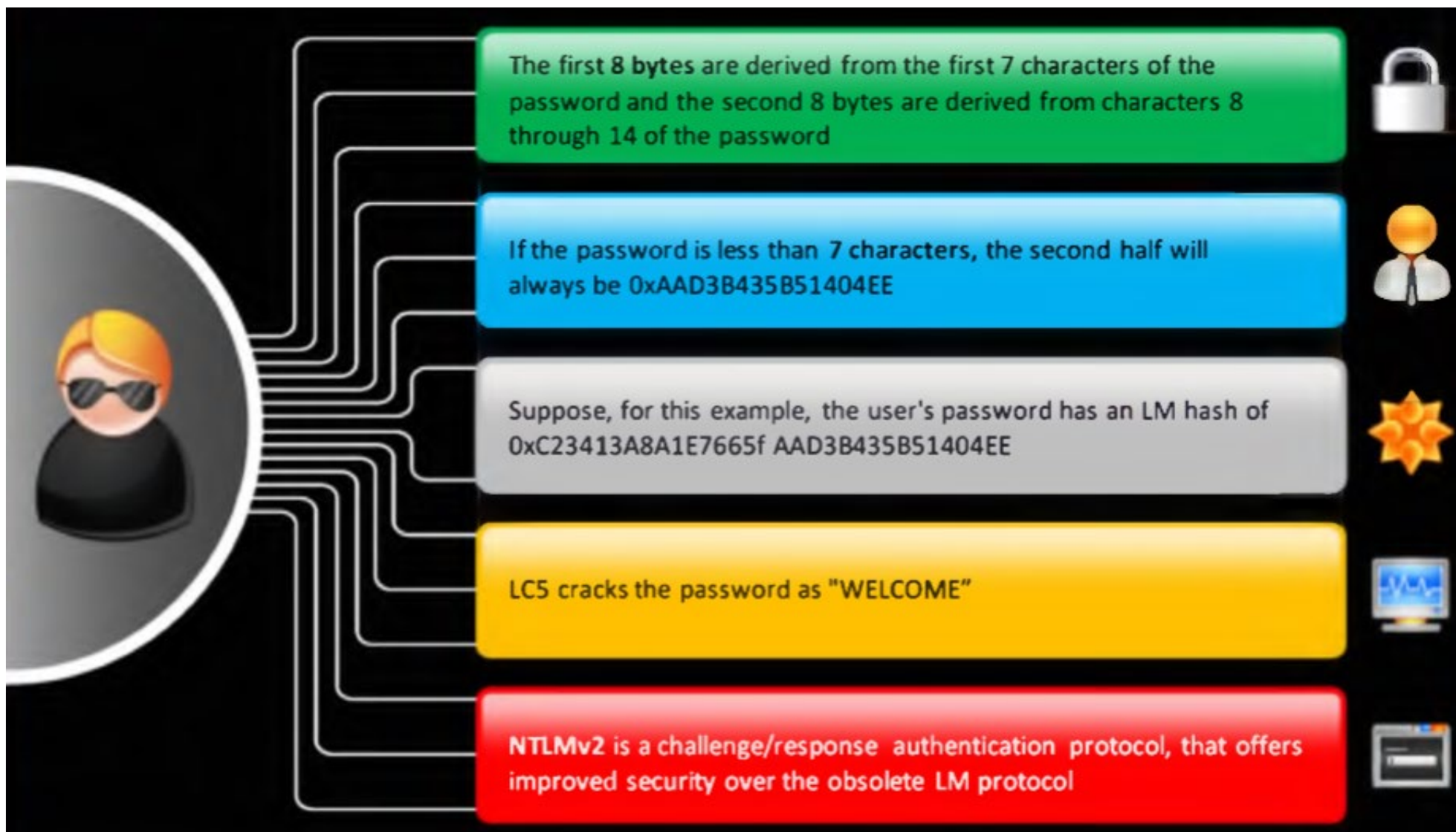


Password stored as hash



The LM hash of a password is computed using a six-step process:

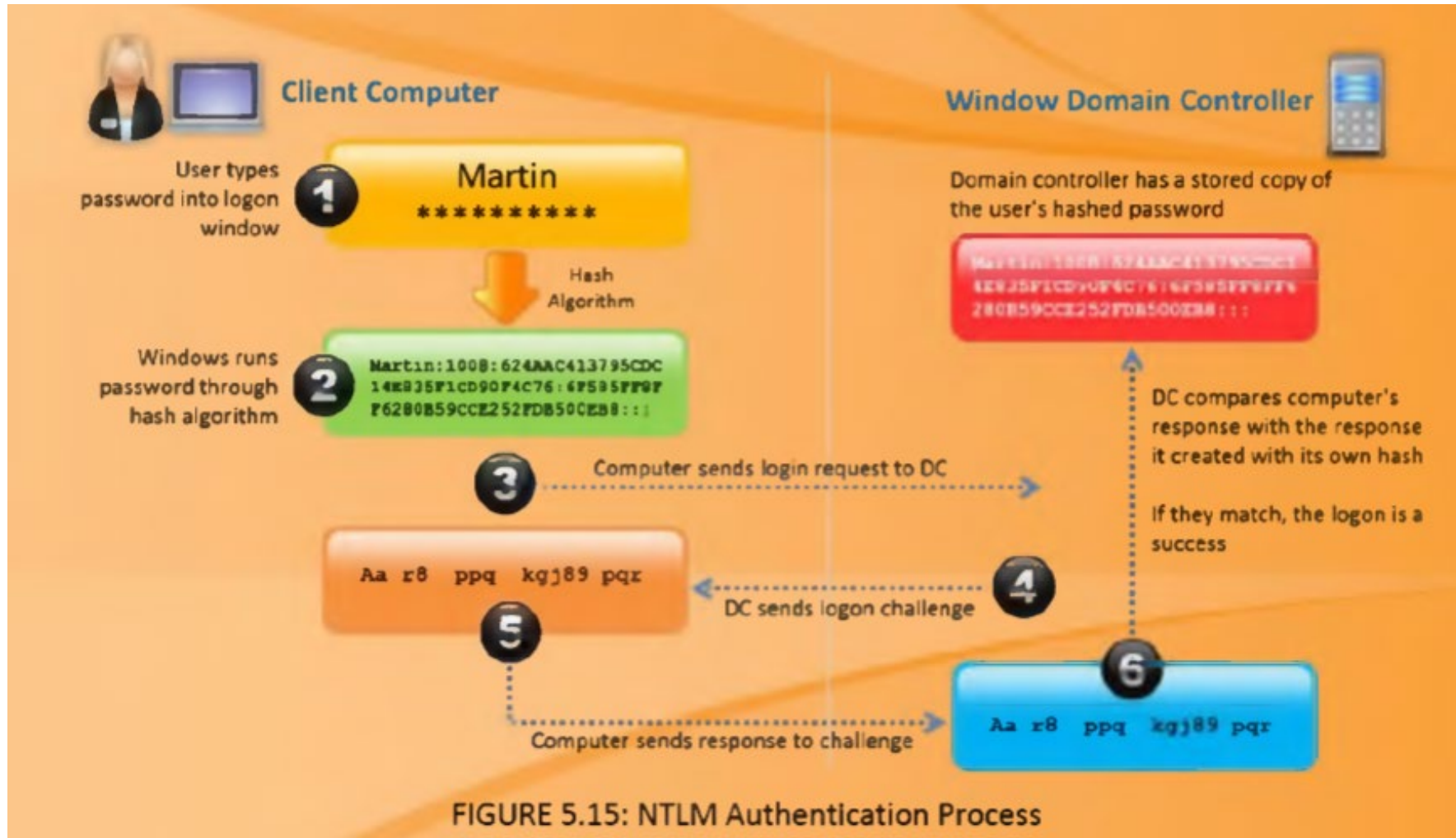
- The user's password is converted into all uppercase letters
- The password has null characters added to it until it equals 14 characters
- The new password is split into two 7 character halves
- These values are used to create two DES encryption keys, one from each half with a parity bit added to each to create 64 bit keys.
- Each DES key is used to encrypt a preset ASCII string (KGS!@#\$%), resulting in two 8-byte ciphertext values
- The two 8-byte ciphertext values are combined to form a 16-byte value, which is the completed LM hash



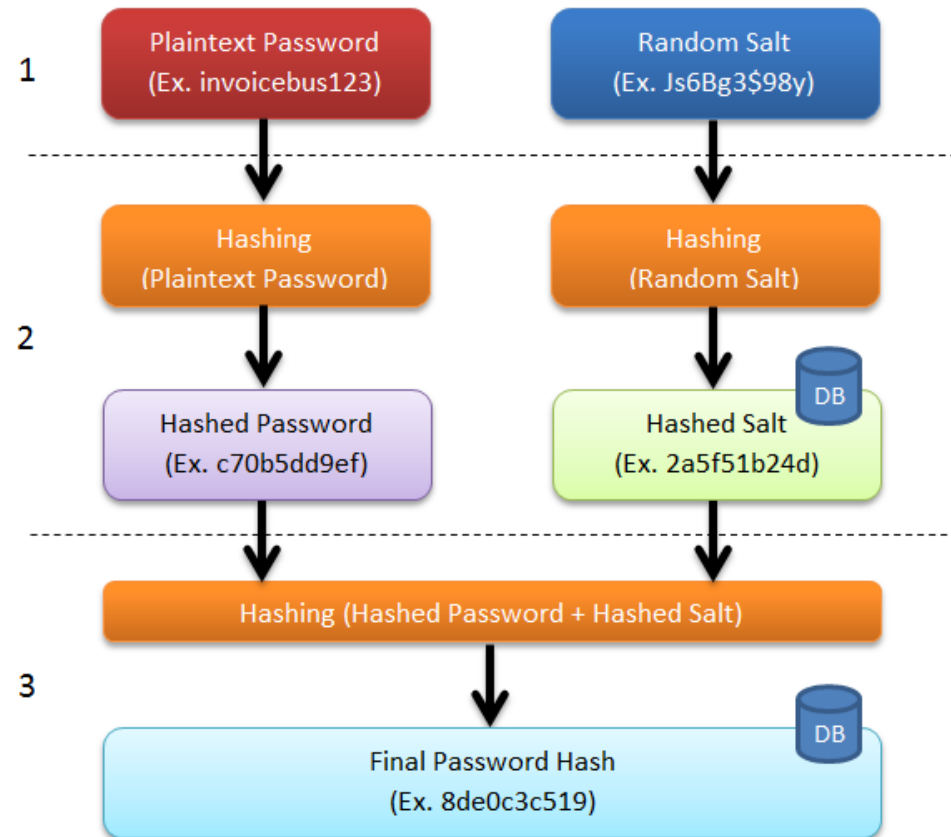
To address the problems in NTLM 1, Microsoft introduced NTLM version 2, and advocated its use wherever possible

Attribute	LM	NTLMv1	NTLMv2	
Password Case Sensitive	No	YES	YES	✓
Hash Key Length	56bit + 56bit	-	-	✓
Password Hash Algorithm	DES (ECB mode)	MD4	MD5	✓
Hash Value Length	64bit + 64bit	128bit	128bit	✓
C/R Key Length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	✓
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	✓
C/R Value Length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	✓

NTLM Authentication Process



Salting



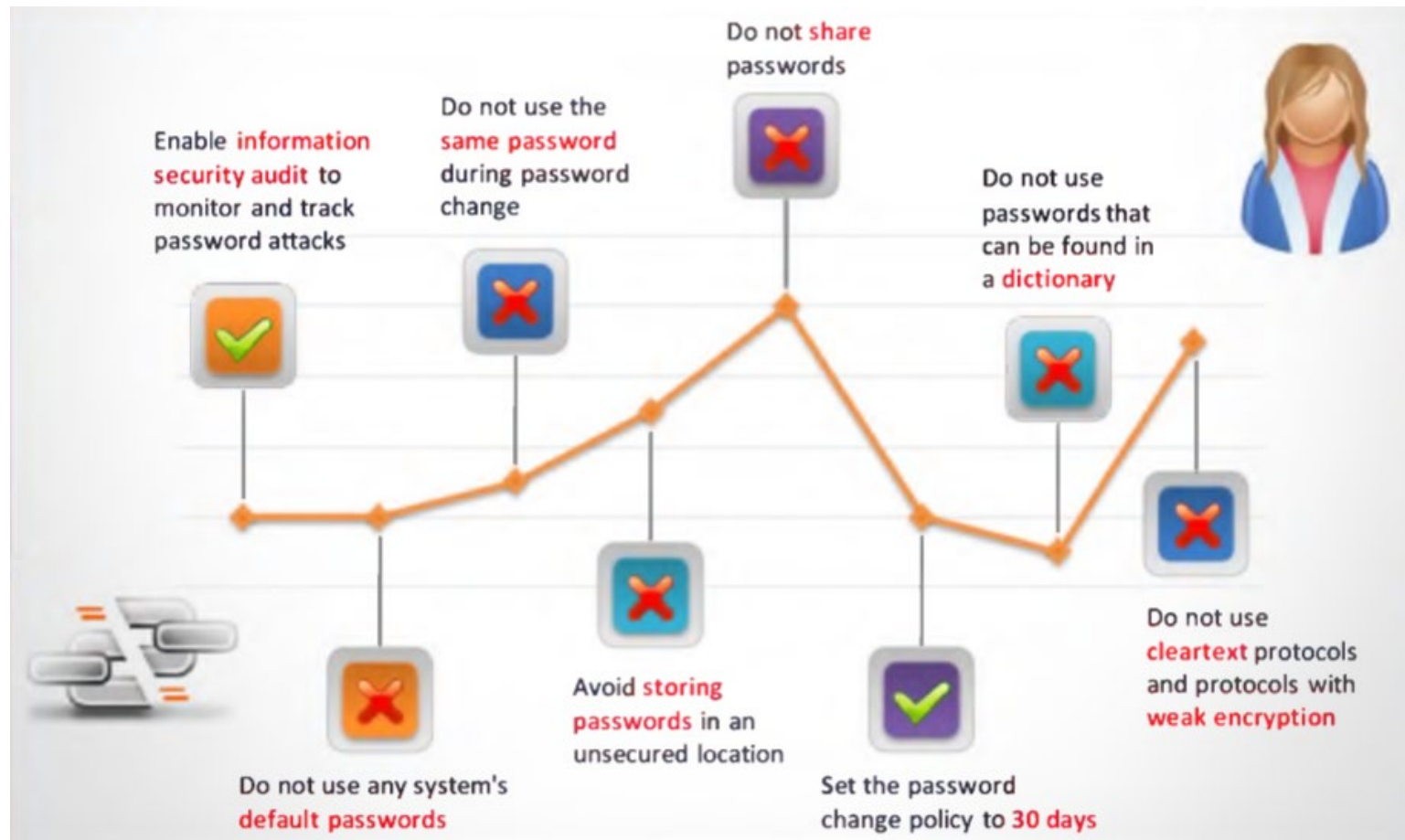
- Salting is a way of making passwords more secure by adding random strings of characters to passwords before their md5 hash is calculated.
- This makes cracking passwords harder.
- The longer the random string, the harder it becomes to break or crack the password.

Password cracking tool

- pwdump 7 and fgdump
- L0pthCrack
- Cain & Abel
- Ophcrack
- RainbowCrack



Defend from Password Cracking



Escalating Privileges

Escalating Privileges

- An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges
- The attacker gains access to the networks and their associated data and applications by taking the advantage of defects in design, software application and poorly configured operating systems.
- These privileges allows attacker to view private information, delete files, or install malicious programs such as viruses, Trojans, worms.
 - Vertical escalation
 - Horizontal escalation



Offline NT Password & Registry Editor

<http://pogostick.net>



Windows Password Recovery Bootdisk

<http://www.rixler.com>



Windows Password Reset Kit

<http://www.reset-windows-password.net>



PasswordLastic

<http://www.passwordlastic.com>



Windows Password Recovery Tool

<http://www.windowspasswordsrecovery.com>



Stellar Phoenix Password Recovery

<http://www.stellarinfo.com>



ElcomSoft System Recovery

<http://www.elcomsoft.com>



Windows Password Recovery Personal

<http://www.windows-passwordrecovery.com>



Trinity Rescue Kit

<http://trinityhome.org>



Windows Administrator Password Reset

<http://www.systoolsgroup.com>

Privilege Escalation countermeasures

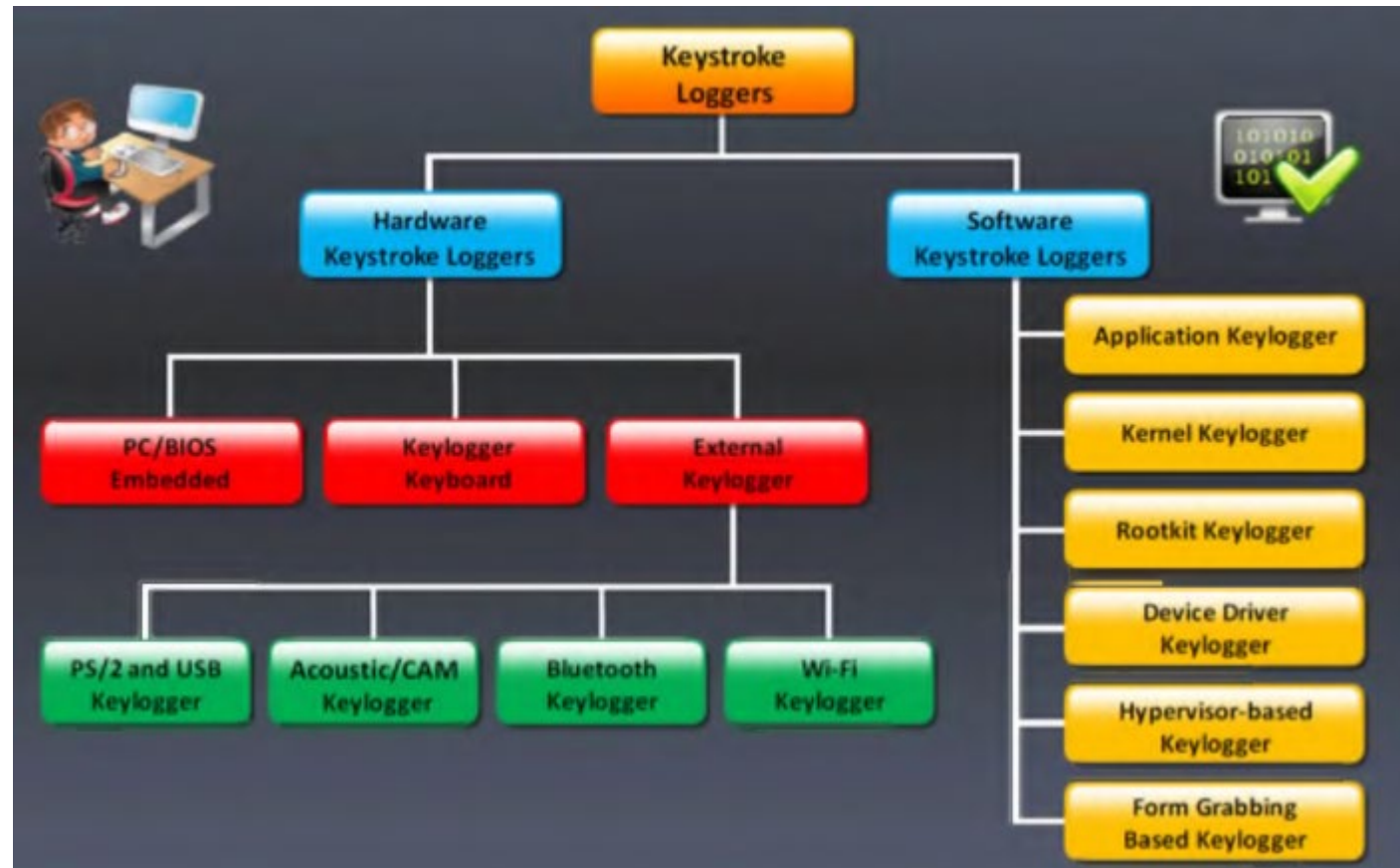
- Restrict the interactive logon privileges
- Run users and applications on the least privileges
- Implement multi-factor authentication and authorization
- Run services as unprivileged accounts
- Use encryption technique to protect sensitive data
- Implement a privilege separation methodology to limit the scope of programming errors and bugs
- Reduce the amount of code that runs with particular privilege
- Perform debugging using bounds checkers and stress tests
- Test operating system and application coding errors and bugs thoroughly
- Patch the systems regularly

Executing Applications










Executing Applications

- execute malicious applications in this stage. This is called "owning " the system.
- execute some of his or her own malicious programs remotely on the victim's machine to gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources, crack passwords, capture screenshots, install a backdoor to maintain easy access
- The malicious programs that the attacker executes on victim's machine may be:
 - Backdoor
 - Cracker
 - Keyloggers
 - Spyware

Type of Keylogger



Keylogger Tool

 Ultimate Keylogger http://www.ultimatekeylogger.com	 Powered Keylogger http://www.mykeylogger.com
 Advanced Keylogger http://www.mykeylogger.com	 StaffCop Standard http://www.staffcop.com
 The Best Keylogger http://www.thebestkeylogger.com	 iMonitorPC http://www.imonitorpc.com
 SoftActivity Keylogger http://www.softactivity.com	 PC Activity Monitor Standard http://www.pcacme.com
 Elite Keylogger http://www.widestep.com	 KeyProwler http://keyprowler.com

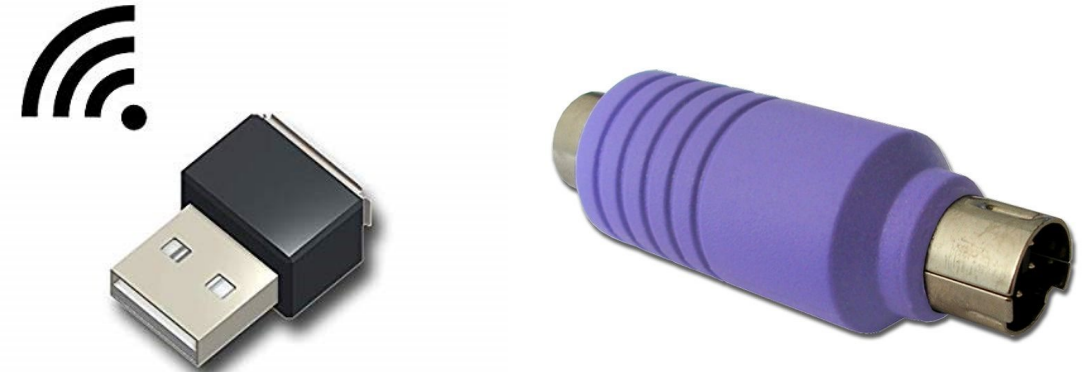
 Aobo Mac OS X KeyLogger http://www.keylogger-mac.com	 KidLogger for MAC http://kidlogger.net
 Perfect Keylogger for Mac http://www.blazingtools.com	 MAC Log Manager http://www.keylogger.in
 Award Keylogger for Mac http://www.award-soft.com	 logkext https://code.google.com
 Mac Keylogger http://www.award-soft.com	 Keyboard Spy http://alphaomega.software.free.fr
 REFOG Keylogger for MAC http://www.refog.com	 FreeMacKeylogger http://www.hwsuite.com

Hardware Keylogger

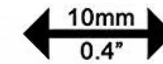


Last year, a white hat hacker developed a cheap Arduino-based device that looked and functioned just like a generic USB mobile charger, but covertly logged, decrypted and reported back all keystrokes from Microsoft wireless keyboards.

Dubbed [KeySweeper](#), the device included a web-based tool for live keystroke monitoring and was capable of sending SMS alerts for typed keystrokes, usernames, or URLs, and work even after the nasty device is unplugged because of its built-in rechargeable battery.



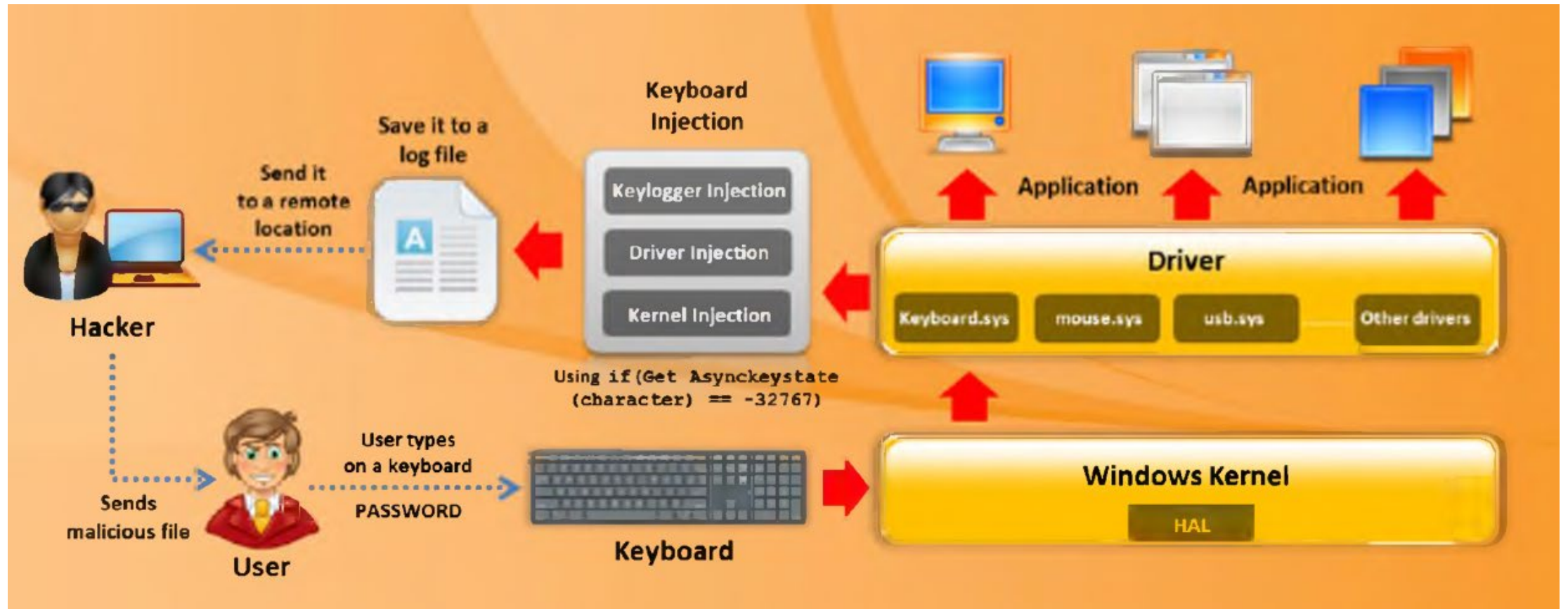
Features:



Possible features:



How Keylogger assist Hacker.



How to Defend Against Keyloggers

- Install anti-spyware/antivirus programs and keeps the signatures up to date
- Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
- Install good professional firewall software and anti-keylogging software
- Recognize phishing emails and delete them
- Keep your hardware systems secure in a locked environment and frequently v check the keyboard cables for the attached connectors
- Choose new passwords for different online accounts and change them frequently
- Use software that frequently scans and monitors the changes in the system or network

Defend from Spyware

- Perform web surfing safely and download cautiously
- Do not use administrative mode unless it is necessary
- Do not use public terminals for banking and other sensitive activities
- Do not download free music files, screensavers, or smiley faces from Internet
- Beware of pop-up windows or web pages. Never click anywhere on these windows
- Permanently delete cookie, cache, URLs history, and temporary files on the computer when done web surfing
- Do not store personal information on any computer system that is not totally under your control

Hiding files

Rootkits

- Rootkits are programs that hide their presence as well as attacker's malicious activities, granting them full access to the server or host at that time and also in future
- Rootkits replace certain operating system calls and utilities with its own modified versions of those routines that in turn undermine the security of the target system causing malicious functions to be executed

- An attacker places a rootkit by:
 - Scanning for vulnerable computers and servers on the web
 - Wrapping rootkit in a special package like games
 - Installing rootkit on the public computers or corporate computers through social engineering
 - Launching zero day attack (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)
 - Means of a link and a bot from IRC, ICQ
- Attackers use rootkits to:
 - Root the host system and gain remote backdoor access
 - Mask attacker tracks and presence of malicious applications or processes
 - Gather sensitive data, network traffic, etc. from the system to which attackers might be restricted or possess no access
 - Store other malicious applications and act as a server resource for bot updates and so on

Types of Root kits

- Hypervisor - level Rootkit
 - Hypervisor-level rootkits are usually created by exploiting hardware features such as Intel VT and AMD-V.
- Kernel - level Rootkit
 - The kernel is the core of the operating system.
 - These cover backdoors on the computer and are created by writing additional code or by substituting portions of kernel code with modified code via device drivers in Windows or loadable kernel module in Linux.
- Application - level Rootkit
 - Application-level rootkit operates inside the victim's computer by replacing the standard application files with rootkits
- Hardware/Firmware Rootkit
 - Hardware/firmware rootkits use devices or platform firmware to create a persistent malware image in hardware, such as a hard drive, system BIOS, or network card.
- Boot - loader - level Rootkit (Bootkit)
 - Boot-loader-level (bootkit) rootkits function either by replacing or modifying the legitimate boot loader with another one.
- Library - level Rootkits
 - Library-level rootkits work higher up in the OS and they usually patch, hook, or supplant system calls with backdoor versions to keep the attacker unknown.

Detecting Rootkits

- Signature-based Detection
 - Signature-based detection methods work as a rootkit fingerprints.
 - compare the sequence of bytes from a file compared with another sequence of bytes that belong to a malicious program.
- Heuristic Detection
 - Heuristic detection works by identifying deviations in normal operating system patterns or behaviors
- Integrity-based Detection
 - Integrity-based detection functions by comparing a current file system, boot records, or memory snapshot with a known, trusted baseline.
- Cross-view-based Detection
 - Cross-view-based detection techniques function by assuming the operating system has been subverted in some way.
- Runtime Execution Path Profiling
 - The Runtime Execution Path Profiling technique compares runtime execution path profiling of all system processes and executable files.

Defend against rootkit

- defend against rootkits are listed as follows:
- Reinstall OS/applications from a trusted source after backing up the critical data
- Staff with ill-defined responsibilities
- Well-documented automated installation procedures need to be keep
- Install network and host-based firewalls
- Use strong authentication
- Store the availability of trusted restoration media
- Harden the workstation or server against the attack
- Update the patches for operating systems and applications

Covering Tracks

Covering Tracks

- Erasing evidence is a requirement for any attacker who would like to remain obscure.
- This is one method to evade trace back.
- This starts with erasing the contaminated logins and possible error messages that may have been generated from the attack process.
- There are several ways to clear online tracks:
 - Private browsing
 - History in the address field
 - Disable stored history
 - Delete private data
 - Clear cookies on exit
 - Clear cache on exit
 - Delete downloads
 - Disable password manager
 - Clear data in password manager
 - Delete saved sessions
 - Delete user JavaScript
 - Set up multiple users
 - Remove Most Recently Used (MRU)
 - Clear Toolbar data from the browsers
 - Turn off AutoComplete

Summary

- System hacking is the phase where penetration to the target are happening
- Vulnerabilities of the target is exploited to gain access to the target system
- Several malicious stages are generally executed during this phase, namely, gaining access, escalating privileges, executing applications, hiding files and covering tracks
- Each step have it owns specific method and tool.

End of System Hacking