



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Hacking Ethically!!!



Advanced Cybersecurity (ACCB6000)

Applied Computing - WISA



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

VM Download

\\192.168.135.200\ACCB6000\$

Previous sessions...

- **Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience**
- **Purpose and role of Hackers, Penetration Testing, Various Laws and Standards**
- **Understanding Footprinting and Reconnaissance Concepts, Methodology.**
- **Using various Tools, Taking Countermeasures**
- **Network Scanning, Tools and Techniques**
- **Banner Grabbing**
- **Scanning – PenTesting**
- **Enumeration Concepts, Techniques, Countermeasures**

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.



Previous sessions...

Understanding and Assessing Vulnerabilities

- **What is Vulnerability? How is it classified?**
- **Assessing Vulnerabilities.**
- **Managing Vulnerabilities**

Social Engineering

- **Understand Social Engineering Concepts, Techniques**
- **Understanding Threats, Impersonation**
- **Countermeasures**

Lab/ Tutorials

- **Activity 1 Getting Ready**
- **Activity 2 Information Gathering**
- **Activity 3 Scanning and Enumeration**
- **Activity 4- Vulnerability Assessment**
- **Activity 5 – Social Engineering**

Continuing the earlier lectures, we discussed on Network Scanning, different tools and methodologies used like Banner Grabbing and mitigation methods etc. following that enumeration concepts, its different tools and techniques were discussed. we continued focusing on assessing vulnerabilities within a network (either it is our target to attack or defend), different tools used to assess and techniques

During the tutorials, under isolated lab environment you might have practiced different Footprinting, scanning, enumerating methods using various tools and assessed the vulnerabilities.

Gaining access and escalating privileges

- ***Hacking Methodology (Based on CEH)***
- ***Understanding techniques to gain access to the system***
- ***Techniques to escalate privileges***

Lab/ Tutorials

- ***Activity 6 – Exploiting Network***

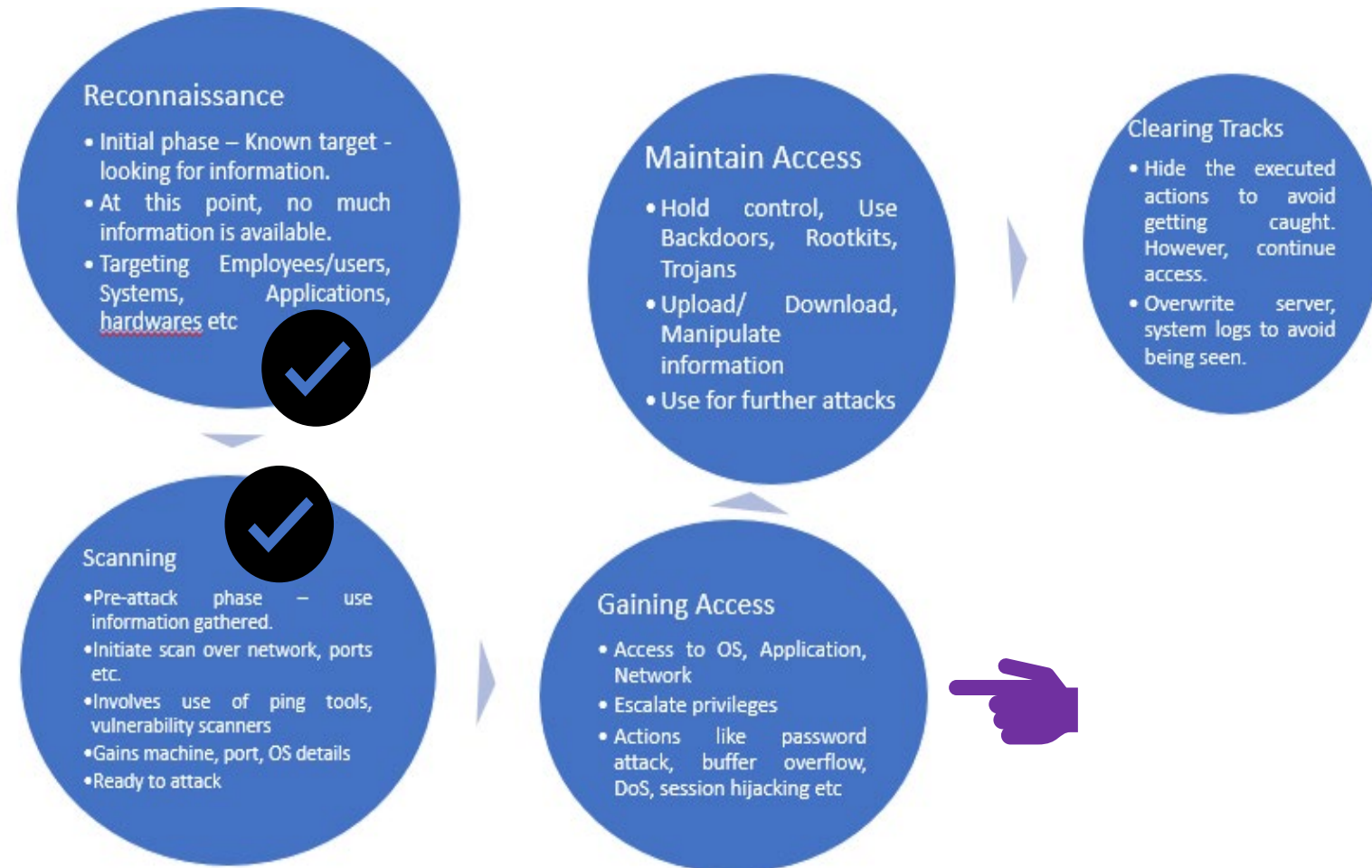
During this week, with applied knowledge and understanding on Footprinting, Network Scanning, Enumerating the target, and assessing vulnerabilities, we shall move forward focusing on the hacking methodology. We shall understand various techniques to gain access, escalate privileges, create and maintain remote access to the target.

During the tutorials, under isolated lab environment you will be using different techniques to gain access and escalate privileges.

Hacking - Methodology

○ Do you remember the process?

- ✓ Footprinting and Reconnaissance
- ✓ Scanning
- ✓ Enumeration
- ✓ Vulnerability Analysis
- Gaining Access
- Maintaining Access
- Clearing Logs



Hacking - Methodology

- Do you remember the process?
 - ✓ Footprinting and Reconnaissance
 - ✓ Scanning
 - ✓ Enumeration
 - ✓ Vulnerability Analysis
 - Gaining Access
 - Maintaining Access
 - Clearing Logs

Gaining Access

Cracking Passwords ∞ Escalate Privileges

Maintaining Access

Executing Applications ∞ Hiding Files

Clearing Logs

Cover your tracks

Hacking - Methodology

- Gaining Access
 - To bypass the access control systems and gain access into the target system
 - Techniques like Password cracking, Social Engineering helps to gain access
- Privilege Escalation
 - To get rights of a legitimate user or administrator
 - Techniques like vulnerability exploitation helps to escalate privileges
- Execute Application
 - To create and maintain remote access to the target system
 - Trojans, Spywares, Backdoors, Keyloggers help to execute applications
- Hiding Files
 - To hide your presence in the target system
 - To hide the attackers' malicious activities and data theft
 - Rootkits, Steganography helps to hide files
- Covering Tracks
 - To hide the evidences
 - Clearing the logs

Gaining Access – Password Cracking

- Gaining Access

- To bypass the access control systems and gain access into the target system
- Techniques like Password cracking, Social Engineering helps to gain access
- The primary intention of cracking passwords is to recover them. However, it could be used on a wrong intention to gain unauthorized access to the target system
- Password Cracking won't be always successful. It depends on the strength and nature of passwords been placed on a system

- Types

- ✓ Non – Electronic Attacks
- ✓ Online Attacks
 - ✓ Active
 - ✓ Passive
- ✓ Offline Attacks

Gaining Access – Password Cracking

- **Non – Electronic Attacks**
 - Social Engineering Attacks
 - Shoulder Surfing
 - Dumpster Diving

- **Active Online Attacks**
 - **Default Passwords**
 - Password Guessing
 - Trojans, Spyware, Keylogger
 - LLMNR/NBT-NS Poisoning

Default Passwords

Search Passwords

531 vendors, 2117 passwords

[@passdb on Twitter](#) / [Firefox Search](#)

1. Fortinet - FortiGate	
Method	Serial Console
User ID	maintainer
Password	pbcpbn(add-serial-number)
Level	Administrator
Doc	
Notes	You must have physical access to the system.

2. Fortinet - FortiGate	
Method	Serial Console
Password	bcpb(serial number of the firewall)
Level	Administrator

[Home](#) > [Brocade](#) > Fabric OS - All

🔍 Brocade - Fabric OS - All

Default username, password, ip...

	User name	Password	Description
🙄	root	show me!	- Gigabit SAN (by Nicolas Gregoire)n- Admin access (Multi)

Username root

Password fivranne

Notice - Gigabit SAN (by Nicolas Gregoire)n- Admin access (Multi)

👍 Its working!

Not working 🗑️

Gaining Access – Password Cracking

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- **Password Guessing**
- Trojans, Spyware, Keylogger
- LLMNR/NBT-NS Poisoning



More time required.
Probability of success
is very less.



Target a User

Create a list of passwords

Rank the passwords

Test the password

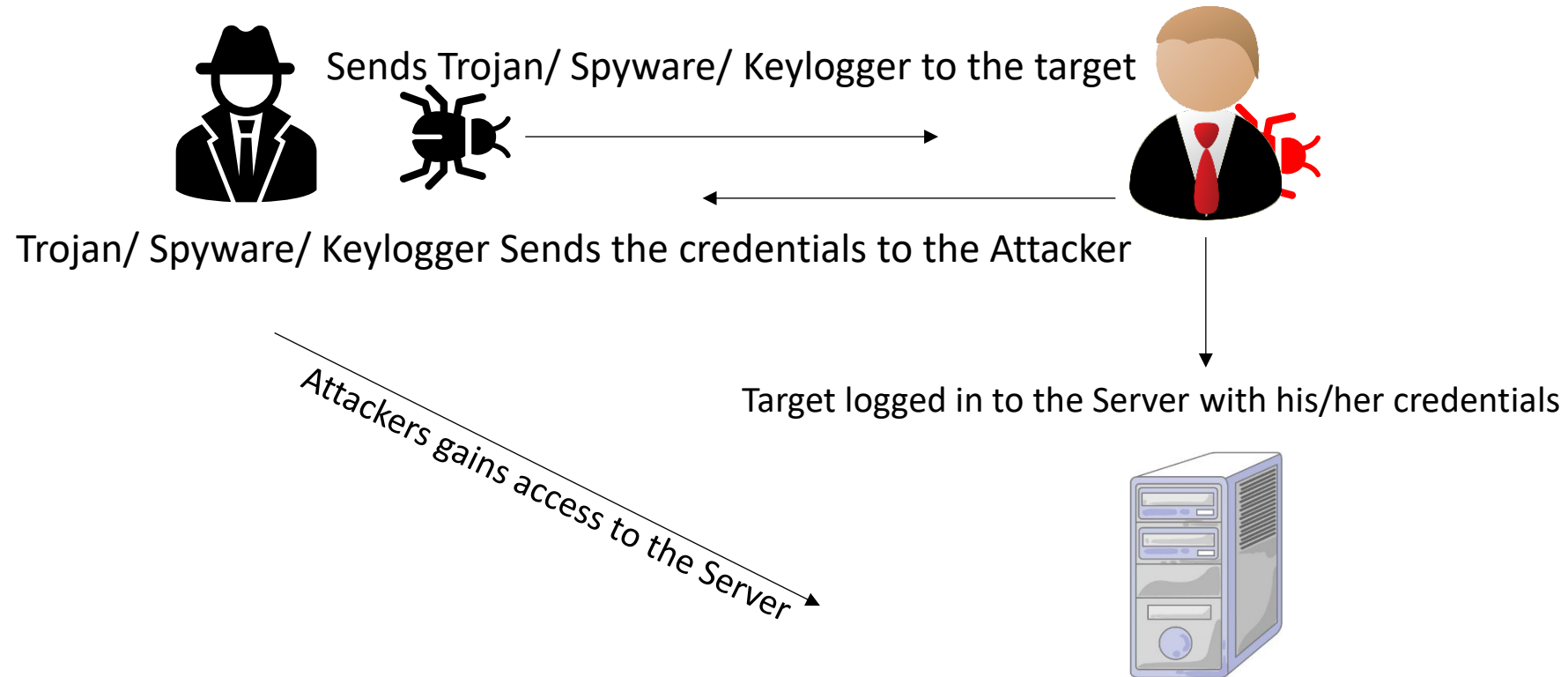
Gaining Access – TSK

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- Password Guessing
- **Trojans, Spyware, Keylogger**
- LLMNR/NBT-NS Poisoning



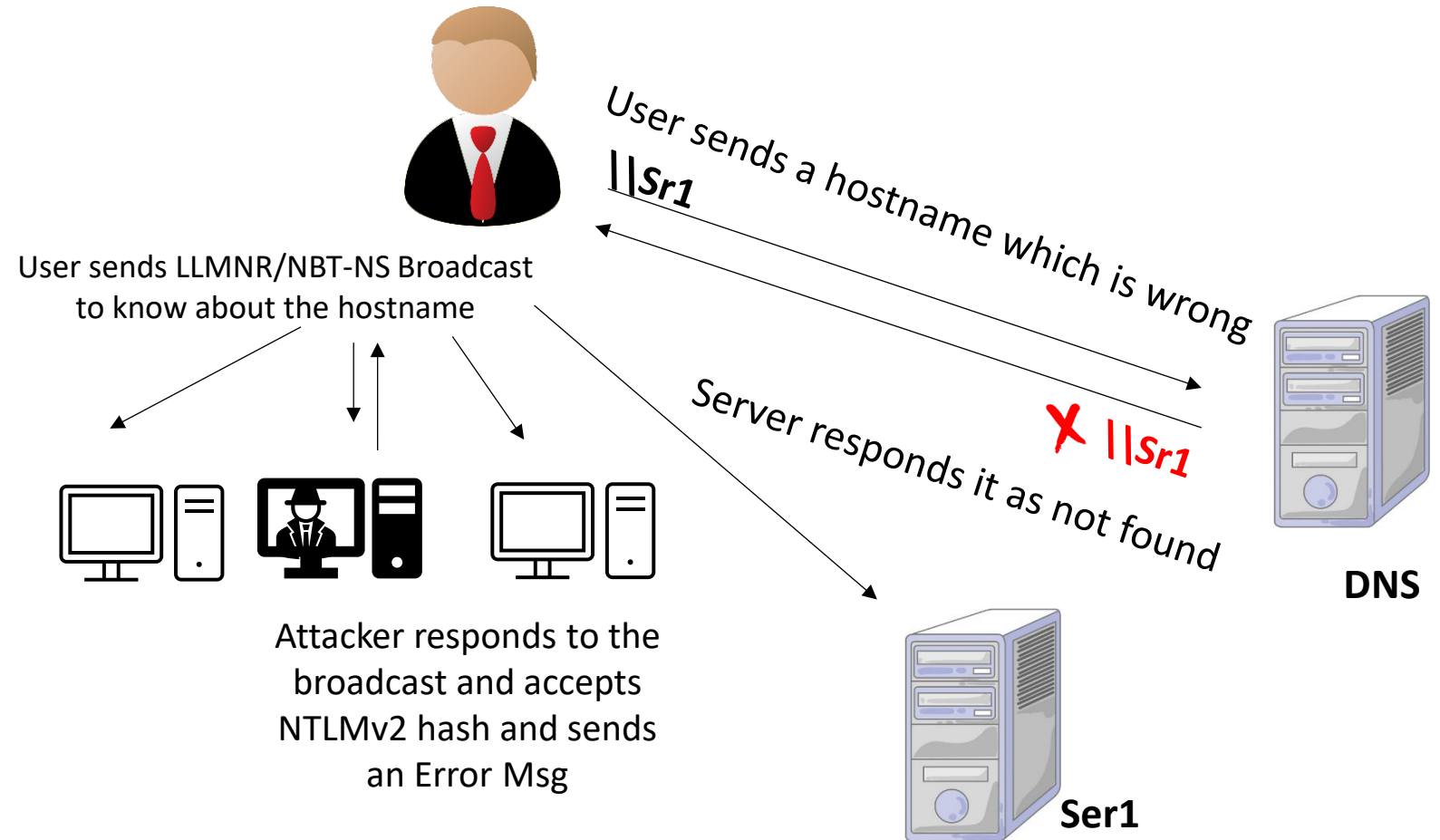
Gaining Access – Name Resolution Services

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

- Default Passwords
- Password Guessing
- Trojans, Spyware, Keylogger
- **LLMNR/NBT-NS Poisoning**



Gaining Access – Passive Attacks

- **Non – Electronic Attacks**

- Social Engineering Attacks
- Shoulder Surfing
- Dumpster Diving

- **Active Online Attacks**

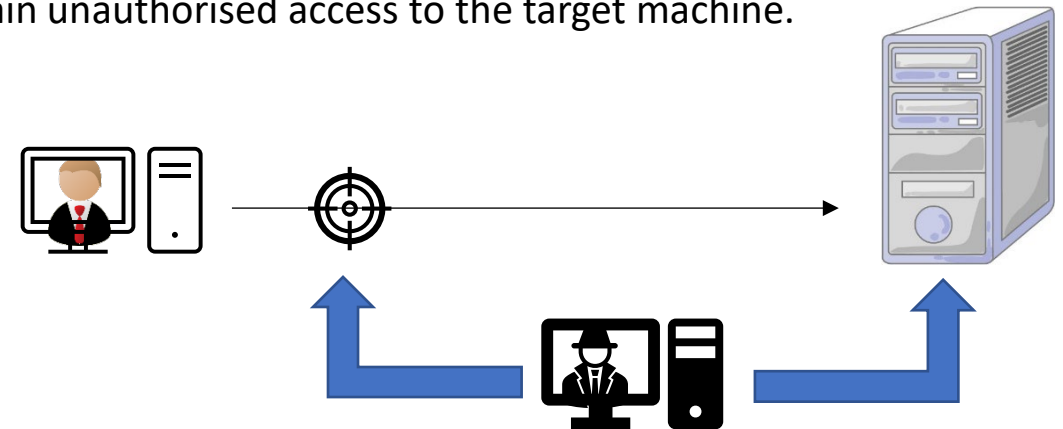
- Default Passwords
- Password Guessing
- Trojans, Spyware, Keylogger
- LLMNR/NBT-NS Poisoning

- **Passive Online Attacks**

- **Wire Sniffing**
- **Man-in-the-Middle and Replay Attack**



- ❑ Attacker uses packet sniffing tools to gain access and observe the traffic within the network.
- ❑ Sensitive data traffic (FTPs, rlogins, passwords etc) are later used to gain unauthorised access to the target machine.



- ❑ Attacker gains access to the communication channels between victim and target server to gather information.
- ❑ With gathered information, a replay attack may be initiated using the tokens to gain access to the network.

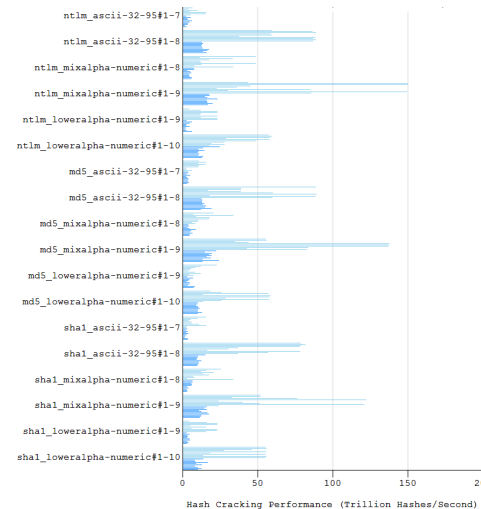
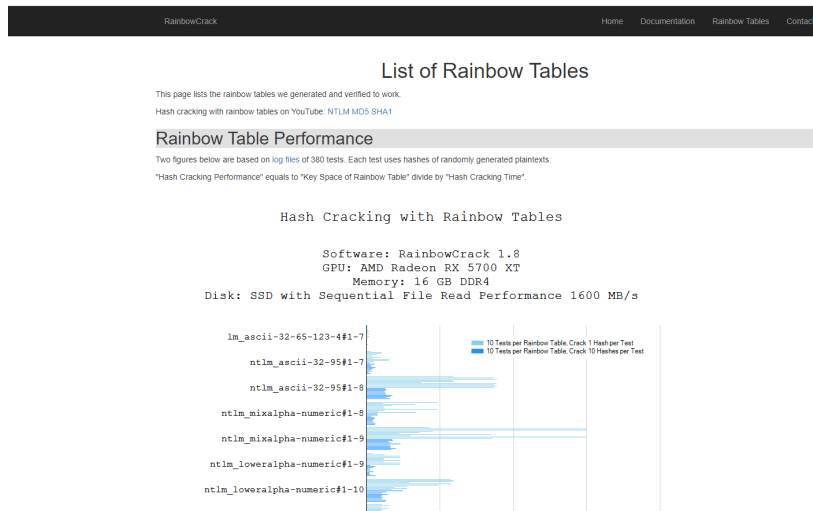
Gaining Access – Offline Attacks

- **Rainbow Table Attack**

- Using the pre-computed hash table values, compare the hash values of passwords that are gathered during the earlier phases and match the password.

- **Distributed Network Attack**

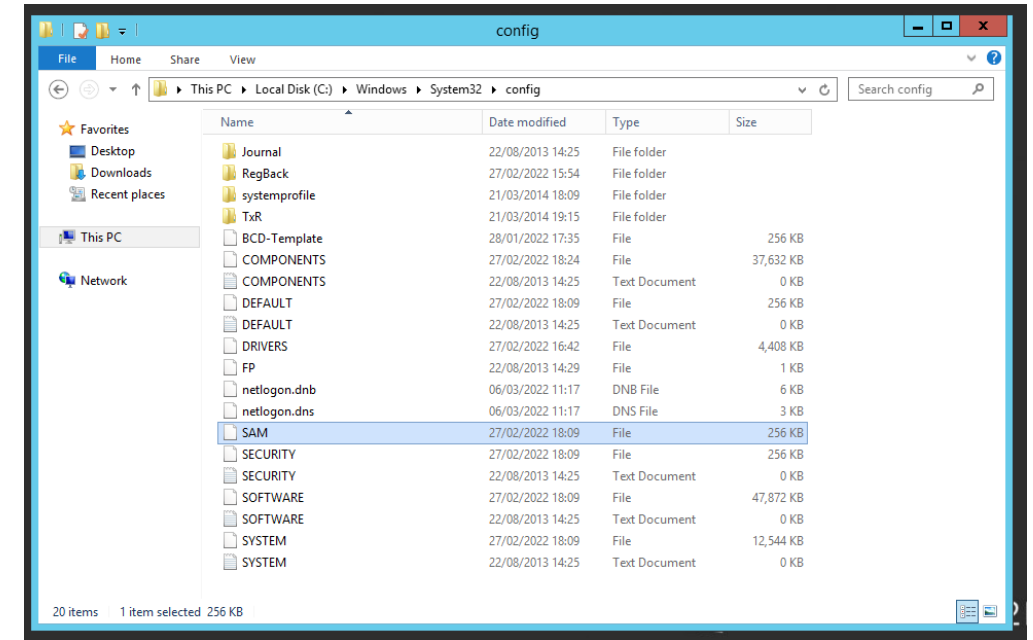
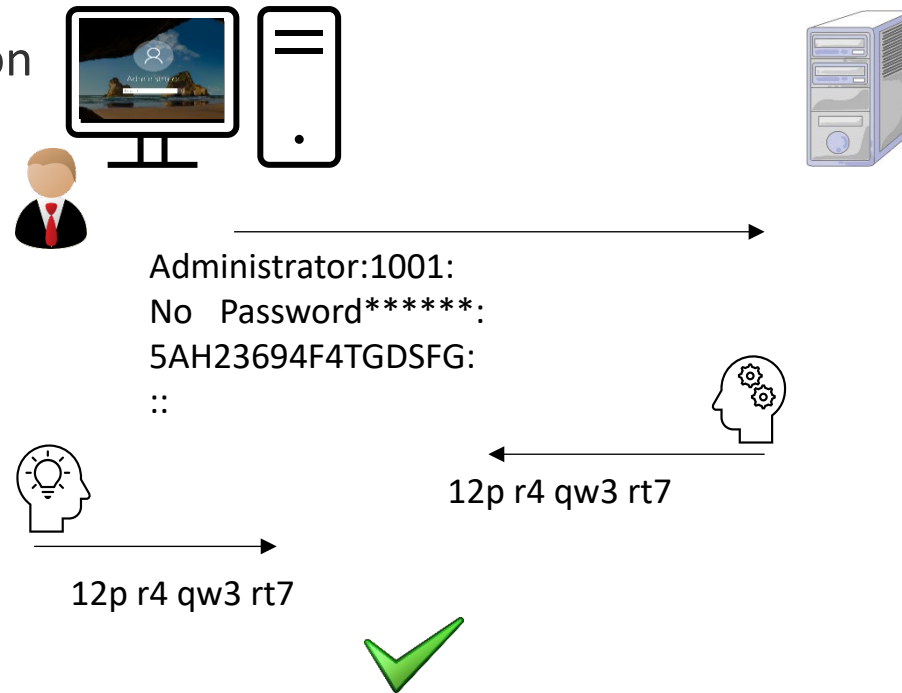
- A technique used to recover passwords from hashes and (or) password protected files.
- This technique uses the unused processing power of machines across the network to decrypt the passwords.



Gaining Access – Authentication Mechanism

- Security Accounts Manager (SAM) Database: *It has Username, User ID, LM Hash, NTLM Hash.*

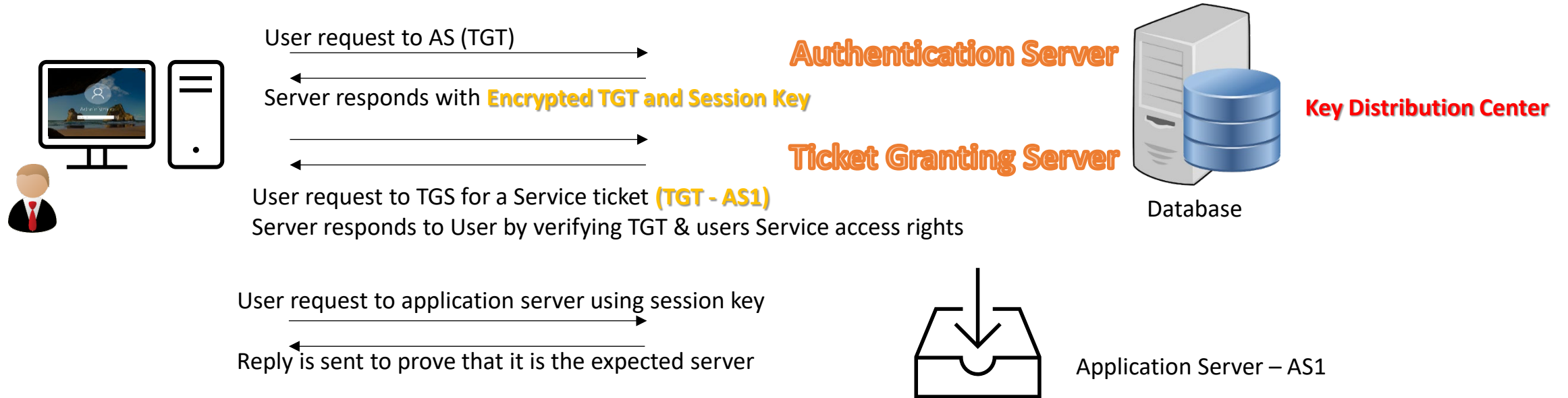
- NTLM Authentication



- Kerberos Authentication: Windows has made Kerberos as its default authentication protocol.
- Other protocols like Oauth, OpenID Connect etc are also used

Gaining Access – Authentication Mechanism

- Kerberos Authentication: Windows has made Kerberos as its default authentication protocol.



Gaining Access – Salting

- It is a technique where random string of characters are added to the password before calculating the hash.
- This makes reverse hashing more complex.
- This could overcome pre-computed hash attacks.

Gaining Access – Defending Password Cracking

- **How to defend against password cracking?**

- With reference to our lecture so far.... Could you state ways to defend against password cracking?

- **Disable LMBNR, NBT-NS**

- Turn off multicast name resolution

- Disable NetBIOS over TCP/IP

Privilege Escalation

- Escalating privileges

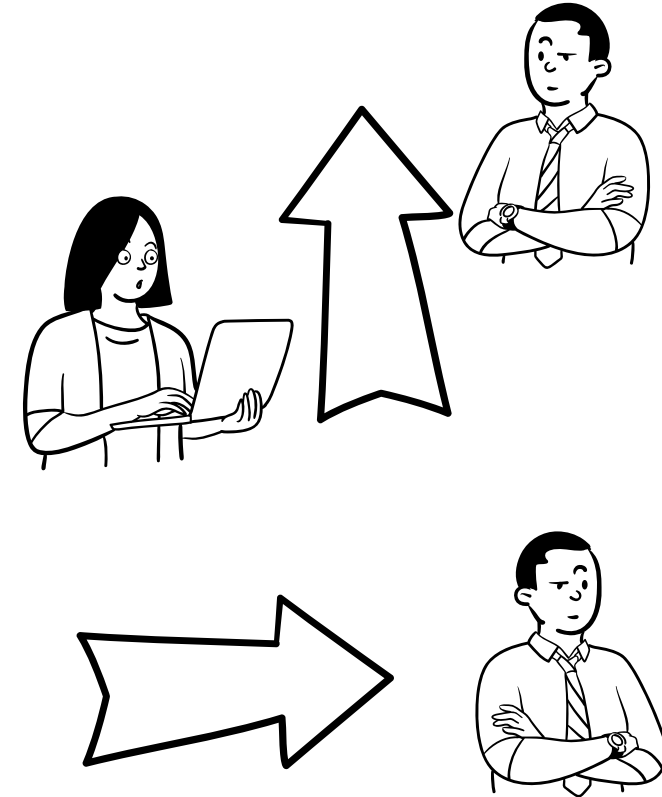
- After gaining access to the network, the attacker would need to have privileges to execute the intended tasks.
- To acquire the privileges, the attacker looks for **design flaws, configuration errors, code weaknesses** etc in Operating Systems and available Software Applications.

- Types



✓ Vertical Privilege Escalation

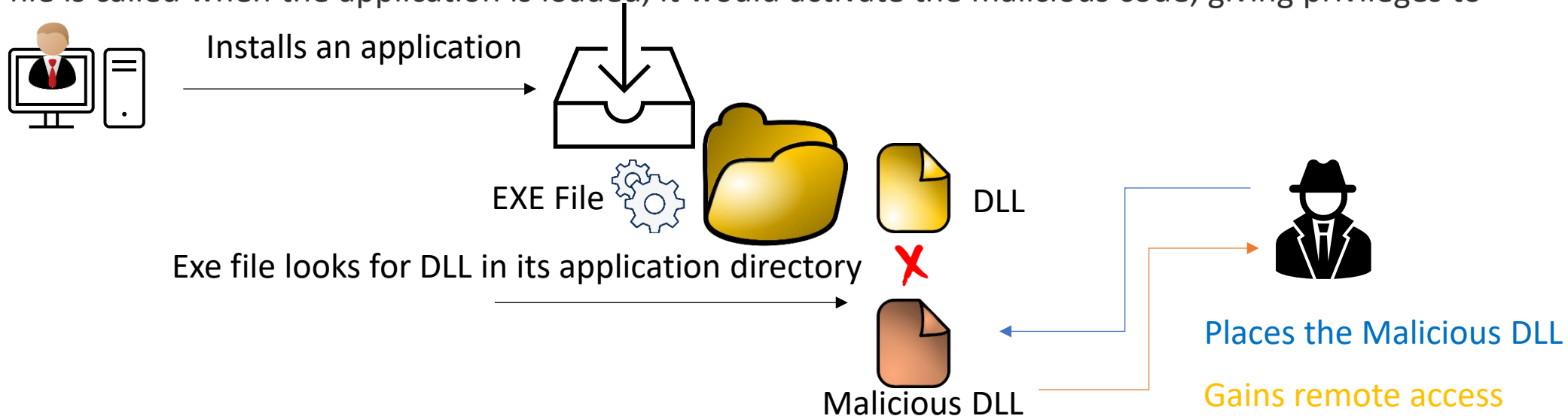
✓ Horizontal Privilege Escalation



Privilege Escalation – Methods

○ DLL Hijacking

- By injecting malicious code in the form of DLL file into an application, DLL Hijacking could be executed.
- Once the DLL file is called when the application is loaded, it would activate the malicious code, giving privileges to the attacker.



○ Dylib Hijacking

- In Apple Computers, OS X, it searches for dylib in multiple directories.
- Attacker can inject a malicious Dylib in its directories. Once the Dylib file is called when the application is loaded, it would activate the malicious code, giving privileges to the attacker.

Privilege Escalation – Methods

- Attackers **exploit** software vulnerabilities using its flaws in the program code, services, even in Kernel.
- Then, execute malicious code.
- They find out the exploit using various web sources.

(From our previous lectures, could you list out few exploit database sites?)

- Exploiting software applications helps attackers to execute commands or binary to gain higher privileges.
- They desperately need to escalate privileges to bypass security and achieve their goals.

Privilege Escalation – Vulnerabilities

- **Spectre Vulnerability**

- **Using SV**

- ✓ Attackers *read adjacent memory locations of a process and access information for which they are not authorized.*
 - ✓ Attackers can read the kernel memory or perform a web-based attack using JavaScript

- **Meltdown Vulnerability**

- **Using MV**

- ✓ Attackers escalate privileges by *forcing an unprivileged process to read other adjacent memory locations* such as kernel memory and physical memory.
 - ✓ Attackers can access system's critical information like credentials, private keys etc.

- **Access Token Manipulation, Application Shimming, File System Permissions Weakness, Path Interception, Scheduled Tasks, Launch Daemon, Plist Modification, Setuid and Setgid, Web Shell etc are similar kind of Privilege escalation techniques**

Privilege Escalation – Defending them

- Restrict **Privileges**
- **Encrypt** Sensitive data
- Implement **MFA** and **Authorization**
- Run services as **unprivileged accounts**
- **Test** for coding errors and bugs
- Implement a **privilege separation methodology** to limit the scope of programming errors and bugs
- **Patch and Update** regularly
- Restrict **users**
- Continuously **monitor file system permissions** using auditing tools
- Reduce the privileges of users and groups, so that **only legitimate administrators can make service changes**
- Use **whitelisting tools** to identify and block malicious software.
- Use **fully qualified paths** in all the windows applications
- **Block** unwanted system utilities or software

Module Feedback

VM Download



\\192.168.135.200\ACCB6000\$

Any Questions?

References

- **EC-Council CEH**
- **Cisco Networking Academy**
- **Tevel Cyber Corps**
- **Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition**
- **Wikipedia**
- **Other website sources given in this presentation**
- *** The intension of usage is for Educational Purpose Only**