Cheat Sheets, Resources

Penetration Testing Interview Questions Cheat Sheet

March 5, 2021 | by Stefano Lanaro | Leave a comment

Introduction

When interviewing for a penetration testing job, you will most probably be required to answer a number of technical questions so that the interviewer can get a good understanding of your current level of knowledge and skill.

This guide will try to cover the most common questions that you are likely to come across during a pentesting interview. If you are already a penetration tester or have been studying pentesting for a while, most of these concepts and techniques should already be very familiar to you.

General

The interviewer might start by asking some general questions in relation to the high level processes that involve penetration testing, the various types of penetration tests that can be conducted, the types of teams that can conduct penetration tests and

some of the overall concepts used in the field.

Question	Answer
What are the phases in the penetration testing lifecycle	The main phases are planning & reconnaissance, where the goals, timeline and scope are defined and initial information is gathered, Enumeration where active scans and tests are performed to identify any vulnerabilites, exploitation, where access is gained through vulnerabilities discovered while performing enumeration, post-exploitation where there is an effort in order to maintain the access previously gained through new users or backdoors and elevate the current privileges and reporting, where all of the findings, risk ratings and relevant remediations are added to a final report. Afterwards a cleanup is necessary to remove any new user accounts, backdoors or exploits
What types of penetration testing assessments are there	Some of the most common types of penetration tests are external, which is usually done off-site against an external network, internal where the assessment is conducted from within the target network, web application tests which objective is to find security vulnerabilities in web-based applications through both manual and automated tests, social engineering which tries to exploit to weak link in most organisation i.e. its employees, through phishin, vishing, tailgating, phyisical testing, media drops etc.
Difference between active and passive reconnaissance	During active reconnaissance, the attacker will perform scans or tests that will interact with the target machine, potentially triggering alarms or creating logs, whereas during passive reconnaissance the attacker makes use of open source intelligence to gather information about the target.

How are penetration tests classified	There are mainly three types of penetration tests: black box, white box and grey box. In black box assessments, the tester tries to simulate a real attack, and is provided with very little to no knowledge of the target application or network. In white box assessments, the tester is given full access to things like application source code, network diagram and even authentication credentials to privileged accoutns, this increases drastically the amount of tests that can be performed. In grey box assessments, the tester will have some prior knowledge and documentation of the target system, but wonÃ¢Â€Â™t necessarily have high privileged access to it.
What types of penetration testing teams are there and what are their responsibilities	The main teams are red, blue and purple. Read teams try as best as humanly possible to simulate a real attack using tools and technique used by cyber criminals. Blue teams are respoonsible for defending systems from attacks by red teams or real attackers, through various countermeasures such as firewalls, SIEM systems, honey pots etc. Purple teams use real life techniques and tools to identify vulnerabilites and apply blue team frameworks in order to protect the organisation from real attacks, it is often a combination of red and blue teams, rather than a team of its own.
What are some of the types of attackers	Script kiddie: an unskilled individual who uses scripts or programs developed by others to attack applications, networks or devices. Advanced persistent threat: a skilled and stealthy threat individual, typically a nation state or state-sponsored group, which manages to gain unauthorized access to a system and remains undetected for long periods of time. Malicious insider: a malicious individual who poses a threat to an organization from within the organization, such as an employee, a former employee or a contractor, it may potentially have inside information concerning the organizationÃ¢Â€Â™s security practices, data and computer systems.

What are the most common types of malware	The most common types of malware are viruses, which are self-replicating and can spread to other systems, trojan which are disguised as legitimate software, worms are like viruses but do not require a host program to spread, spyware such as keyloggers are used to sensitive information such as credentials, adware which are used to display advertisement and are usually harmless, ransomware which are designed to lock users out of their systems and demand a ransom, logic bombs which are activated at a specific time or when a specific event has occurred and rootkits which are backdoors that allow an attacker to maintain remote control over a system and are particularly hard to identify and remove
What are some of the most common vulnerability databases	National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), Exploit Database, VulDB, Packetstorm, Microsoft Security Bulletins.
What is the Common Vulnerability Scoring System	The Common Vulnerability Scoring System (CVSS) is an open framework to categorize the characteristics and severity of software vulnerabilities. It consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics.Ã‚Â
How would you rate vulnerabilities during a penetration test	In order to rate a vulnerability, a risk matrix is used and a risk level is calculated based on the likelihood and consequence of a given issue.
At what point of an assessment would you start performing testing	Only once a clear scope of work and timeline has been defined and agreed to by all parties, and once authorization to start the testing has been received.
What are some of the most common vulnerabilities	Some of the most common vulnerabilities are injection, deserialization, file inclusion, weak encryption, security misconfigurations, weak password policies.

What is the principle of least privilege	The principle of least privilege (PoLP), requires that in a given system, application or network, a user must be able to access only the information and resources that are necessary for its legitimate purpose.

Infrastructure/Operating Systems

This section covers general questions about infrastructure, for example networking, services and protection mechanisms, and specific operating systems and their security vulnerabilities.

Question	Answer
What is the OSI model and what are its layers	The Open Systems Interconnection model is used to break down what happens behind the scens in a network system in seven layers: Physical (the cables), Data Link (network cards and switches), Network (the router), Transport (TCP/IP), Session, Presentation and Application (end-user)
What is the difference between TCP and UDP	TCP is a connection-oriented protocol and it uses a three-way handshake (SYN, SYN-ACK and ACK). UDP is a connectionless protocol and its speed is much faster than TCP.
What are some of the most common services and what ports do they run on	Some of the most common services are HTTP on port 80, HTTPS on port 443, DNS on port 53, FTp on port 21, SSH on port 22, Telnet on port 23 and+B60 SMTP on port 25.
What is DNS	The Domain Name System (DNS) is a service used to translate domain names to the numerical IP addresses needed for locating and identifying computer services, for example 142.250.69.196 is translated to www.google.com. It runs on port 53.
What is ARP	The Address Resolution Protocol (ARP) is used for discovering the MAC address associated with a given internet layer address, typically an IPv4 address.
What is RDP	The Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. It runs on port 3389.

What is a MAC address	The media access control (MAC) address is a unique identifier assigned to a network interface that is required to be able to communicate with the rest of the network.
What is a firewall and how does it work	A firewall is a network security device that has the ability to either monitor or filter incoming or outgoing network traffic based on pre-defined rules.
What is the difference between an IDS and an IPS	The main difference between them is that IDS is a monitoring system, while IPS is a control system. IDS doesnÃ¢Â€Â™t alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.
What are honeypots	Honeypots are hardware or software mechanisms designed to detect and potentially help to prevent attempts at unauthorized use of a given network, application or device.
What is the difference between encoding, hashing and encrypting	Encoding takes a clear-text string and turns it into an encoded string, which can easily be decoded, it is used to preserve the usability of the information, an example is base64. Hashing takes a clear-text string and turns it into a hash, which will always be the same length, regardless of the clear text string used, it is a one-way operation and therefore it cannot be reversed, it is used to validate the integrity of information or to store sensitive data, an example is MD5. Encryption takes a clear-text string and turns it into an encrypted string through the use of a key, it can be reverse by knowing the algorighm used and the key, it is used to secure confidential information, an example is RSA.
Name a few type of encoding, hash and encryption	Encoding: ASCII, HEX, Base64, URL. Hashing: MD5, SHA-512, NTLM. Encryption: AES, RSA, 3DES.Ã,Â
What is salting and what is it used for	Salting is a technique used to add random data that is used as an additional input when hashing data. Salting makes it harder for attackers to crack a hash as the is appended to the password before it is hashed, creating a much longer hash.

What is the fastest way to crack hashes	The easiest way to crack hashes is through rainbow tables, which are precomputed tables of hashes that cache the output of hashing functions. The hashes stored in these tables are then compared to the target hash, in order to identify itÃ¢Â€Â™s corresponding clear-text value without the need of hashing a list of clear-text strings and comparing them to the hash.
Difference between symmetric and asymmetric encryption	Symmetric encryption only uses one key for encryption as well as decryption. Asymmetric Encryption two keys, one to encrypt the information and one to decrypt it. These keys are called Public Key and Private Key.
In what format are Windows and Linux hashes stored	Windows hashes are stored using NTLM and they used to be stored with LM. Linux passwords are normally hashed using the SHA-256 or SHA-512, in older versions they are hashed with Blowfish or DES.
Where are Windows and Linux hashes stored, how can you retrieve them	Linux hashes are stored in /etc/shadow, they used to be stored under /etc/passwd and they can still be stored there if required. In Windows, NTLM hashes are stored in the SAM hive, the boot key which is stored in the SYSTEM hive is required to obtain them. These are stored in C:\Windows\System32\config\.
What are cron jobs/scheduled tasks	Cron jobs or scheduled tasks give users the ability to schedule the launch of programs or scripts at pre-defined times or after specified time intervals.
Where are cron jobs stored in Windows and Linux	Scheduled tasks in Windows are stored in %WINDIR%\System32\Tasks. Cron jobs in Linux are stored in /etc/crontab, /var/spool/cron, /var/spool/cron/crontabs/root, /etc/cron.d, /etc/cron.daily, /etc/cron.hourly etc.

What are the different package managers used in Linux and where are they used	For Debian-based operating systems, the most common package manager is Advanced Packaging Tool (APT), which uses .deb packages. For RedHat-based operating systems, the most common package manager is Yellowdog Updater, Modified (YUM), which uses .rpn packages. For Arch-based operating systems, the most common package manager is Pacman Package Manager. For OpenSUSE-based operating systems, the most common package manager is Zypper Package Manager (ZYpp).
Describe the permission system used in Linux file systems	Linux file systems divide their permissions in three categories: read, write and execute. When looking at a file or directory, the permissions are mentioned three times, the first time refers to the owner of the file, the second one to users belonging to the group of the file and the third one to everyone else.
What are SUID and sudo	SUID is a Unix file permission that can allow users to run a command or a script with the as the owner of the file, rather than as the user executing it. sudo is Unix feature that allows users to run scripts or commands as another user, by default the root user.
What is Kerberos and how does it perform authentication	Kerberos is an authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. When authenticating, Kerberos uses symmetric encryption and a trusted third party which is called a Key Distribution Center (KDC). At the moment of the authentication, Kerberos stores a specific ticket for that session on the users machine and any Kerberos aware service will look for this ticket instead of prompting the user to authenticate through a password.

What is the difference between WEP, WPA and WPA2	WEP uses the RC4 (Rivest Cipher 4) stream cipher for authentication and encryption. The standard originally specified a 40-bit, pre-shared encryption key, later on a 104-bit key became available. WPA is also based on RC4, although it introduced Temporal Key Integrity Protocol (TKIP), which uses 256-bit keys to encrypt data, along with other key features such as per-packet key mixing which make it a much better option. WPA2 replaced RC4 and TKIP with two stronger encryption and authentication mechanisms: Advanced Encryption Standard (AES) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), respectively. Also meant to be backward-compatible, WPA2 supports TKIP as a fallback if a device cannot support CCMP. AES comprises three symmetric block ciphers. Each encrypts and decrypts data in blocks of 128 bits using 128-, 192- and 256-bit keys.
What is WPS Why is it insecure	Wi-Fi Protected Setup (WPS) is a feature supplied with many routers which is designed to make the process of connecting to a wireless network from a device easier. In order to make a connection, WPS uses a eight-digit PIN that needs to be entered on the device, which already makes this a lot easier to crack than any other encryption. Furthermore, rather than check the entire eight-digit PIN at once, the router checks the first four digits separately from the last four digits, which makes it even easier to crack as tehre are only 11,000 possible four-digit codes, and once the brute force software gets the first four digits right, the attacker can move on to the rest of the digits. Many routers come with WPS enabled by default. A way manufacturers use to mitigate this attack is to add a time out period after a number of attempts. Reaver can be used to crack WPS PINs.

Common Techniques & Attacks

The interviewer might ask questions about specific techniques or attacks that a penetration test might need to carry out as part of their day-to-day responsibilities.

Even if you donÃ¢Â€Â™t know how to perform some of these attacks, it is crucial that

you understand how these attacks occur, what is the potential consequence and how these can potentially be remediated.

Question	Answer
How can DNS and ARP be exploited by attackers	ARP spoofing or ARP cache poisoning is an attack by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attackerÃ¢Â€Â™s MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead. The attack can only be used on networks that use ARP, and requires attacker have direct access to the local network segment to be attacked. DNS spoofing, also referred to as DNS cache poisoning, is a form of of attack in which corrupt Domain Name System data is introduced into the DNS resolverÃ¢Â€Â™s cache, causing the name server to return an incorrect IP address, it can be exploited by attackers and allow them to receive information that was not intended for them.
What is DDoS	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, application or network by overwhelming the target with an amount of traffic that it is unable to handle. This attack targets availability rather than confidentiality or integrity.
What is buffer overflow	Buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the bufferÃ¢Â€Â™s boundary and overwrites adjacent memory locations. Attackers can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code, therefore executing arbitrary code on the target system. There are two main types of buffer overflows: stack based, more common and easier to perform and heap based, less common and harder to perform.Ã‚Â

What is packet inspection	Packet inspection is a technique that inspects in detail the data being sent over a computer network, and it is often used to detect malicious activity or to identify sensitive information.
What is privilege escalation Provide a few examples	Privilege escalation allows an attacker, through the exploitation of a vulnerability or misconfiguration, to elevate their privileges and gain access to unauthorized resources on the system. An example could be through a clear-text password stored in a history file or through a vulnerable application installed on the target system.
What is the difference between bruteforce and dictionary attacks	Bruteforce attacks tries a list of possible passwords that are generated during the attack based on pre-defined rules, whereas dictionary attack use a list of known or commonly used passwords stored in a file.
What is a golden ticket attack	A golden ticket attack allows an attacker to create a Kerberos authentication ticket from a compromised service account, called krbtgt. By using the NTLM hash of the compromised account an attacker can create fraudulent golden tickets. These tickets appear pre-authorized to perform whatever action the attackers want without any real authentication.
What is a common misconfiguration of FTP and SMB	A common misconfiguration of FTP is the anonymous login, which if enabled can allow any user to authenticate to the server without the need to enter credentials. A common misconfiguration of SMB is null session authentication , which can allow any user to authenticate to an SMB share by providing a null username and password.

Web Application Vulnerabilities & Attacks

Nowadays most applications run on web browsers and are hosted in the cloud, and due to this the need to perform tests against web application has increased drastically.

Therefore, it is crucial for a successful penetration to be very familiar with all of the main vulnerabilities and misconfigurations that can affect web applications, the possible consequences and remediation.

Question	Answer
what is XSS, what types of XSS are there, what are the consequences of a successful attack and how do you prevent XSS	Cross-site scripting is a security vulnerability that can allow attackers to inject client-side scripts or code into web pages viewed by other users. The types of XSS are: Reflected, which means the malicious code is within the current HTTP request, Stored, which means the malicious code is stored in the websiteÃ¢Â€Â™s database or in the webpage itself and DOM-based, meaning the vulnerability lies on the client-side rather then in the server-side application code. It can result in an attacker accessing sensitive data such as the userÃ¢Â€Â™s session or credentials, or taking full control of the target application. It can be prevented by filtering the input before the request is made, encoding the output in the HTTP response, use the Content-Type and X-Content-Type-Options headers or escaping certain special characters.
What is SQL Injection, different types and examples, how to prevent	SQL injection is a vulnerability that allows an attacker to interfere with the queries that an application makes to its database and to inject custom queries to retrieve unintended data or perform unintended actions. There are three main types of SQL injection: In-Band, meaning the attacker uses the same platform to both perform the attack and gather its output, Blind, where the attacker perform the attack in one platform although said platform does not return any output which makes it harder to ascertain whether the vulnerability actually exists, therefore it is indispensable to rely on the response time or certain patterns of the application in order to exploit it. Out-of-band SQL injection is performed when the attacker cant use the same platform to perform the attack and gather the output, or when a server is too slow or unstable for these actions to be performed. SQL injection can be prevented by using input validation, character whitelisting, encoding or escaping.

Secure and HTTPOnly flags	Secure and HTTPOnly are flags that can be set against session cookies. The secure flag ensures that cookie information is only transmitted over an HTTPS channel. The HTTPOnly flag ensures that cookie information can only be accessed by the web server and not by client-side scripts, this limits the damage that XSS could to to a victim user.
What is CSRF, what does it entail and how can it be prevented	Cross-site request forgery (CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform by using maliciously crafted web requests. It can allow an attacker to cause a victim user to carry out an unintended action, for example changing their email address, password or transferring funds. This can result in a full compromise of the victimÃ¢Â€Â™s account. CSRF attacks can be prevented through the use of CSRF tokens, which ensures the request made by the end user is genuine and makes it impossible for attackers to craft a malicious HTTP request for the end user to execute. To be effective, CSRF tokens need to be unpredictable, tied to the userÃ¢Â€Â™s session and validated upon every user action is executed.
What is IDOR, what are its consequences and how can you prevent it	Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. If present, they can allow attackers to access unintended data on the database, including sensitive information such as passwords, potentially gaining full access to the web server. It can be prevented through input validation or by using indirect references.

What are LFI and RFI and what are the consequences of these attacks How can they be prevented	Local file inclusion and remote file inclusion occur when a web application includes a file within its code in order to use functions within it and when proper input validation is not in place. Through local file inclusion, attackers can potentially access files within the web server that were not meant to be publicly available, whereas through remote file inclusion, attackers can include remote files, and therefore potentially execute malicious scripts hosted on a web server. The easiest way to prevent LFI and RFI attacks is to simply not include files in a way that they can be manipulated by users, otherwise input sanitization can be used.
How can you secure data in transit	The HTTPS protocol on port 443 can be used to secure data in transite between a client and a server, through TLS or SSL encryption.

Penetration Testing Tools

Knowing the most common penetration testing tools and how to use them is a key skill for any penetration tester, as these tools will help greatly in automating attacks and enumerations, as well as performing manual testing.

Question	Answer
What tool would you use to perform a port scan	The most popular tool to perform port scans is Nmap. Port scans can also be done through scripting, for example using Python.
What tools would you use to inspect network packets	The most common tools for packet inspection are Wireshark and Dig.
What tool would you use to bruteforce passwords, online and offline	Hydra and Patator are used for online cracking, where as John the Ripper and Hashcat are used for offline cracking.
What tool would you use to automate SQL injection attacks	SQLMap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection attacks.
What tool would you use to perform an ARP spoofing attack	The main tools used for ARP spoofing are Arpspoof, Ettercap and Responder.

What tools would you use to perform testing against WiFi networks	Aircrack-ng is a complete suite of tools used to assess WiFi network security and test for various vulnerabilities.
What tool can help generate malicious executables	The Metasploit MSFvenom tool is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance. It allows to generated encoded malicious payloads.
What tools would you use to scan a network for known vulnerabilities	Tools like Nessus or OpenVAS can be used to scan networks for known vulnerabilities.
What tool would you use to inspect the route between a host and a destination	Traceroute, or tracert, is a network diagnostic tool used to identify the exact route and hops is used for a host to connect to a given destination, and to measure any packet transit delays.

Scenario-Based

The interviewer will most likely ask some scenario-based questions, which will test your critical thinking in situations where you may need to exploit a certain vulnerability or suggest a remediation but the answer may not be as straightforward. There isnÃ¢Â€Â™t necessarily a right or wrong answer to these, as long as you can come up with a creative way that works it will prove you have what it takes.

Try to think of other scenarios you may come across during a penetration test that may need extra thinking.

Question	Answer
How would you remotely access a service that can only be accessed from within an internal network	Port forwarding is a technique used to redirect a communication request from one address and port number combination to another. For example, if port 80 is only accessible from within the internal network but port 443 is accessible remotely, a port forward rule can be created to forward all incoming traffic on port 443 to port 80.

How would you allow regular users to run bash scripts as root and which way is most secure	The best way would be to use cron jobs, as long as the user does not have access to modify the script that is being run, alternatively a SUDO rule can be added to allow the user to run the script as sudo.
If you were able to obtain an NTLM hash but could not decrypt it, how would you use this knowledge to obtain access to the target host	Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server by using the NTLM or LM hash of a userÃ¢Â€Â™s password, instead of requiring the plaintext password.
What measures would you put in place to prevent brute forcing	Password bruteforcing can be prevented through the use of account lockout mechanisms, CAPTCHA, multi-factor authentication and IP-based restrictions.

Conclusion

When participating in a penetration testing or cyber security interview, try to look calm and donÃ¢Â€Â™t panic. Your answers should be thorough but concise, keep in mind that as a penetration tester you need to be able to explain difficult concepts in simple terms to a non-technical audience.

Although the interviewer will not expect you to know all of the questions as doing research is also part of being a penetration tester, it is natural that the more you can answer, the better..

If you donÃ¢Â€Â™t know the answer to some of the questions, try to think outside the box and come up with your own answers and solutions to the problem, rather than not answering at all. This will show you have the right mindset and attitude for the job.