Created by Surendra Pander {@technical surendra}

Junior Pentester level Interview Question

By Surendra Pander {@technical surendra}

1. What is XPath Injection in penetration testing?

XPath injection is a type of vulnerability in which malicious input is used to inject unintended commands into an XML document. This can be done by injecting any user-supplied string directly into an XPath expression, or even by using specially crafted elements and attributes. Injection attacks are one of the most common methods used to exploit software vulnerabilities because they allow attackers to run arbitrary code as part of the attack payload.

2. Explain Web Application Scanning with w3af in pen-testing?

w3af is versatile and can be used for a number of purposes in pen-testing. For example, it can be used to identify vulnerabilities in web applications before conducting a full attack, to check for signs of malware and phishing attacks, and to monitor for security issues. In addition, w3af can be used to identify vulnerabilities in outdated or insecure web applications.

3. Explain reflected XSS Vulnerability.

Reflected XSS vulnerability occurs when data entered in a web form is accessed by an unpatched web browser and interpreted by the application. The data entered in the form is then displayed on the web page as if it was coming from the user's web browser. This vulnerability is exploited when an attacker sends a specially crafted input to a web form that is then reflected in the web page. This allows the attacker to inject malicious code into the web page and to run the code without being detected.

4. What is Hijacking Execution in pen-testing?

Hijacking execution in penetration testing is a technique that attackers use to gain access to systems or networks. Hijacking execution takes advantage of the privileges and permissions granted to an intruder by default on compromised machines, which can then be used for malicious purposes. Attackers may also leverage user accounts created specifically for reconnaissance or attack tasks, as well as preexisting administrative rights on target machines. By taking advantage of these vulnerabilities, hijackers can bypass common security controls and compromise systems without being detected.

5. Write a few points about SEH Overwrite Exploits?

SEH Overwrite Exploits are a type of security exploit that allows an attacker to execute code on a target system in memory, even if the target process has normal read, write, and execute permissions.
These exploits take advantage of security vulnerabilities in the operating system or application. They can be used to run malicious code on a targeted system, steal data, or implant malware. A lot of remote code execution (RCE) exploits are available for the Server Executable Hypervisor, or SEH.

6. What is POP POP RET in penetration testing?

POP POP RET is a tool that can be used to detect and exploit vulnerable applications. To use this tool, you will first need to scan the target network for vulnerable applications. Once you have identified the vulnerable applications, you can use POP POP RET to exploit them. By exploiting the vulnerabilities, you can gain access to the systems and data that are protected by the vulnerable applications.

7. What is meant by DNS Reconnaissance in penetration testing?

When we conduct a penetration test, the most important task is understanding the internal network structure and DNS configuration. This is done through various forms of DNS reconnaissance, also known as DNS sniffing. DNS reconnaissance can be used to gather information about hosts and name servers, as well as their associated configuration. This can include things such as the type of DNS server used, the name server addresses, the primary and secondary name servers, and the A, AAAA, and CNAME records.

8. What are porting public exploits?

Porting public exploits is a process by which an attacker takes advantage of vulnerabilities in public applications or systems so that they can be used to exploit other vulnerable systems. Porting means taking the exploits and making them work on different versions of the application, system, operating system, etc. It could also mean adopting these exploits to carry out attacks against new targets or finding alternative ways to deliver payloads from the exploited target(s). Port scanning is a reconnaissance technique employed during exploitation whereby attacking computers are scanned for open ports using network protocols.

9. What is XAMPP?

XAMPP is a completely free and open-source development platform for hosting websites, accessible through a web browser. It is an easy-to-use platform that has a lot of features for web developers. It also has a variety of modules and templates that make it easy to set up a website.

Moreover, XAMPP can be used for creating databases, e-commerce solutions, and more. This is also useful for penetration testers, it can be used in web application testing.

10. What is SSL Stripping in penetration testing?

SSL Stripping is a process that removes the SSL/TLS encryption from an HTTP request before it is sent to the webserver. This allows an attacker to view and modify the data that is being sent in cleartext.SSL stripping can be used by attackers as part of a denial-of-service attack or for other nefarious purposes such as spying on user activity.

11. What is John the ripper tool and how penetration testers are using it?

John the Ripper is a computer security tool used by penetration testers to test the security of a computer system. It is a command-line tool that can be used to test the security of various file formats. It can also be used to extract data from a target computer.

12. What is token Impersonation?

In penetration testing, token impersonation is a technique that is used to gain access to resources or systems that are protected by authentication methods such as passwords or tokens. Token impersonation is used to access these resources by pretending to be someone other than the user who is supposed to be accessing them. Token Impersonation can also be used as part of social engineering attacks or phishing exercises.

13. What is Pass the Hash in penetration testing?

Pass the Hash is a popular cyber security testing practice used to find vulnerable systems and test whether they can be exploited by attackers. It works like an attacker tries different passwords on a target system in order to see if any of them are valid – or, more accurately, triggers the authentication process required for access to that system. By doing this, the tester can then gain access to the account without having to actually break into the system.

14. What is SSHExec?

SSHExec is a remote shell interface implemented in the SSH protocol. It allows an attacker to run commands on the target machine over SSH without having to be physically present on that system. SSHExec works by establishing a connection between the attacker’s system and the target system. Once the connection is established, the attacker can run commands or scripts on the target system.

15. What are Socks4a and Proxy Chains?

A socks4a and proxy chains are two types of network analysis tools that are used for penetration testing. socks4a works as a proxy and can intercept packets leaving and entering your targeted systems. It can be used to map the flows of traffic and can be used to examine protocols and handshake data. On the other hand, proxy chains can be used to combine socks4a with various command-line tools to perform various actions on the proxy such as injecting packets, capturing packets, and mangling packets.

16. What is Local File Inclusion (LFI)?

Local file inclusion (LFI) is a technique used by attackers to include malicious files in the request packets sent to vulnerable systems. This can allow an attacker to access privileged information, or even execute arbitrary code on the target system. LFI vulnerabilities are particularly prevalent in web applications and can be exploited remotely by attacking users who visit affected websites. By including specially crafted requests within HTTP requests, an attacker can inject scripts into pages served up by the application, giving them full control over those pages and any data stored within them.

17. What is Remote File Inclusion (RFI)?

Remote File Inclusion (RFI) is an exploit technique used in penetration testing whereby a malicious user includes files on the target server that are not actually part of the web application or system being tested. These files can be stored anywhere, but they must exist outside of the document root. This allows attackers to inject arbitrary script code into pages served up by vulnerable servers – potentially allowing them to steal data, execute commands as privileged users or even take over entirely compromised systems.

18. Explain Leveraging XSS with the Browser Exploitation Framework?

Exploiting XSS in web applications is a common technique used by hackers. XSS, or Cross-Site Scripting, is an attack where a malicious user injects scripts into a website to inject malicious code into the user’s browser. These scripts can inject any script or HTML into a document, which when viewed by a user, can execute without their consent or knowledge. Browser Exploitation Framework (BFX) is a tool used by hackers to exploit XSS in web applications.

19. What is War-FTP?

War-FTP is a program used in penetration testing which allows users to FTP through an insecure network. FTP is an application used to transfer files between computers. War-FTP is a command-line tool and can be used for emulators such as Wireshark, Carrier Grade NAT (CGNAT), or TAP devices.

20. What is the method of Finding the Attack String in Memory?

An attack string is important in understanding the process of finding an attack string in memory. An attack string is a set of characters that can be used to breach the security of a system. The term is used in many different ways, but the important thing is that it is a set of characters that can be used to violate the security of a system.

21. What is Data Execution Prevention in penetration testing?

Data Execution Prevention, or DEP, is a technique used to help prevent malicious code from running on a computer. DEP helps protect against specific types of attacks, such as code injection and cross-site scripting. Many penetration testing engagements require the use of DEP to mitigate potential risks. However, some tests may still require the execution of unprotected code to execute properly.

22. What is the Smartphone Pentest Framework?

A smartphone penetration testing framework is a software tool used by security auditors and hackers to test the vulnerabilities of mobile devices, typically smartphones. A typical penetration testing process begins with scanning for known exploits on target systems in order to identify any exploitable deficiencies. Once vulnerabilities have been identified, the attack surface can be analyzed to determine which areas may be vulnerable to exploitation. In many cases, forensic analysis will also be carried out in an attempt to locate sensitive data or evidence that could be used for criminal purposes should unauthorized access occur.

23. What is USSD Remote Control?

USSD Remote Control is an amazing tool that can be used during penetration testing. USSD Remote Control uses the unique signaling protocol of USSD over GPRS. This can be used to communicate with various devices over GPRS. The benefits of using USSD Remote Control in penetration testing are manifold. USSD Remote Control allows the penetration tester to control various devices remotely. This includes devices that are not always connected to the internet. USSD Remote Control is a very efficient tool and can be used to control a large number of devices. It also allows the penetration tester to perform various tasks remotely. For example, the penetration tester can use USSD Remote Control to scan devices for vulnerabilities.

24. What is EternalBlue SMB Remote Windows Kernel Pool Corruption?

EternalBlue is a Windows remote code execution vulnerability that was published by Microsoft in March of 2017. EternalBlue exploits an SMB protocol memory corruption issue and allows attackers to gain control of vulnerable systems. This exploit can be used against both Server 2008 R2 SP1 and later versions, as well as Windows 10 Anniversary Update and earlier releases. EternalBlue has been exploited in attacks on Linux machines, macOS devices, Android phones/tablets, iOS devices (including the Apple Watch), routers, car drivers' computers running firmware from Juniper Networks Inc., smart TVs from Sony Corp.

25. Explain Incognito attacks with Meterpreter?

An Incognito attack is an effective way to test the security of a system without the fear of being detected. By using Meterpreter to execute an Incognito attack, you can test the security of a system without the victim knowing about it.

26. What is Broken Access Control Vulnerability?

Broken access control is an attack vector used in penetration testing. It refers to the situation when an intruder gains unauthorized access to a system or network by exploiting a vulnerability that has been identified and fixed, but where some entry point remains unpatched. Broken Access Control (BAC) attacks can be carried out through exploit kits, phishing emails with embedded malicious attachments, weak passwords on systems and websites, social engineering tricks such as getting users to reveal their password on-demand or via chatbots, or even simple bypass of employee self-protection measures like two-factor authentication.

For more details, you can refer to the following article – How to Prevent Broken Access Control?

27. Explain Cryptographic Failures in penetration testing?

Cryptographic failures are common in penetration testing. They can result in the compromise of sensitive information, as well as unauthorized access to systems. Lessons learned from cryptographic failures in penetration testing can be applied to avoid them in the future. Proper cryptography ensures that data transmissions are secure, preventing attackers from eavesdropping on or manipulating any messages being sent between two systems. Cryptographic failures in penetration tests can have serious consequences for organizations because they allow unauthorized individuals access to sensitive information and networks.

28. What is Insecure Design Vulnerability?

Insecure design vulnerability is a type of security vulnerability that can be found in web and application designs. These vulnerabilities make it possible for attackers to gain access to the system and exploit its weaknesses, which could result in data loss or other malicious activities. Website administrators are encouraged to use OWASP Top 10 Secure Coding Guidelines when designing their sites and applications, as these provide a basic foundation upon which more specific defensive measures may be layered.

29. What is a Security Misconfiguration vulnerability?

A security misconfiguration vulnerability in OWASP is an exposure of the organization’s sensitive information through a weakness in system configuration or user behavior. In general, any flaw that allows unauthorized access to data can be labeled as a security misconfiguration vulnerability. Examples include vulnerabilities found in web applications, networks, and even computer systems themselves. A common misconception among many organizations is that

they are not at risk for breaches because their network protocols and application configurations are up-to-date. Any exposed service on your network could be exploited by malicious entities seeking to exploit known vulnerabilities for gainful purposes stealing proprietary data, breaching trust relationships with customers or employees, conducting denial-of-service attacks, etc.

30. What is an Outdated Component's vulnerability?

A vulnerable component can be defined as any software or hardware element that might be used by an attacker to exploit vulnerabilities in other components and access unauthorized data or systems. Any part of the architecture, design, implementation, operation, administration, or support of the organization could potentially become compromised if not properly protected against attacks. The aim of this paper is to provide readers with a comprehensive understanding of vulnerability concepts followed by providing some practical tips on how organizations can protect their critical infrastructure from cyber-attacks.

31. What is Identification and Authentication Failures vulnerability?

An identification and authentication failure vulnerability is a weakness in an identification or authentication process that allows unauthorized access to information. Identification and authentication failures vulnerabilities can be caused by tampering with the data, use of stolen credentials, or errors during user registration. In some cases, these weaknesses may also lead to fraudulent activities such as identity theft or credit card fraud.

32. What is Software and Data Integrity Failures vulnerability?

Software and data integrity failures vulnerability (SDF) is a type of security vulnerability that can occur when software or data are not properly protected from unauthorized access. SDFs arise when an attacker gains access to sensitive information, such as passwords or user account details, by exploiting one of the vulnerabilities in the system. When these confidential records are compromised, it could lead to serious consequences for the users involved. A breach involving personal data can have devastating effects on individuals' careers and social lives.

33. What is Server-Side Request Forgery vulnerability?

Server-Side Request Forgery (SSRF) is a vulnerability in web applications that allows an attacker to inject illegitimate requests into the application, resulting in unauthorized access or modification of data. An attacker can exploit this vulnerability by tricking the user into submitting a specially crafted request to the server. SSRF attacks are typically used as part of cross-site scripting (XSS) attacks and can be very successful if executed against privileged accounts with admin rights on target websites.

34. What is Frame Injection vulnerability?

Frame injection vulnerability is a type of security flaw that allows an attacker to inject arbitrary frames into the flow of traffic passing through a website or application. This can be accomplished by injecting frames into the response sent from the server to the browser, or by manipulating elements in an HTTP request header. Frames are small pieces of HTML or XML that make up document content and are displayed within a web page as if they were part of the document itself. By inserting malicious frames into these responses, attackers may be able to inject code directly onto websites and applications users' screens-causing them serious personal loss of injury, data theft, and even loss of revenue for businesses online.

35. What is URL Redirection vulnerability?

URL Redirection vulnerability is a type of security vulnerability that allows an attacker to redirect the user's browser to a different website than was intended. This attack can be performed by tricking the victim into clicking on a malicious link or opening an illegitimate file. Redirections may also occur when users attempt to access pages that have been moved from their original location, due not only to human error but also to intentional manipulation by hackers and/or cybercriminals. URL redirection vulnerabilities are often used in malware attacks because they allow attackers to install infected files on targeted machines without the user ever knowing about it. You can also refer to the article Unvalidated Redirects and Forwards.

36. What is penetration testing dropbox?

Penetration testing dropbox is a security tool that can be used by security professionals to collect logs, artifacts, and other information from targets. It is important to note that the penetration testing dropbox is not a vulnerability scanner. Instead, it collects and stores data related to the target machines and applications. This data can be used to conduct further penetration tests on the target machines.

37. Explain How Data is Protected During and after Penetration Testing?

Security professionals refer to data protection as its own discipline unto itself – protecting confidential personal information, sensitive company files, and secure network communications. Protecting data involves ensuring confidentiality, integrity, and accessibility. Confidentiality ensures that data is kept secret from unauthorized parties who might try to steal or otherwise misappropriate the information, either personally or via the organization. Information security specialists have traditionally protected systems using access controls, firewalls, passwords, encryption/decryption techniques, intrusion detection software, etc.

38. Explain How Risk Analysis and Penetration Testing Are Different from Each Other?

Risk Analysis and Penetration Testing are both important aspects of information security, however, they have some key differences. Risk Analysis is the process of identifying, quantifying, and assessing the potential risks associated with a security vulnerability, system, or

process. Penetration Testing is the process of testing a system's vulnerability to attack by trying to exploit discovered vulnerabilities. Penetration Testing can be used to find vulnerabilities that could be harmful if exploited.

39. Does Penetration Testing Break a System?

In a penetration testing scenario, an exploit may be used to gain access to a system or to elevate privileges on the system. This may then be used to explore the target system in order to identify other vulnerabilities. Once vulnerabilities have been identified, penetration testers often use them to exploit systems to further assess the level of risk involved.

40. Is Penetration Testing Important If the Company Has a Firewall?

A firewall is a device that helps protect computer systems from unauthorized access. It does this by blocking or preventing traffic from entering and leaving the system. In most cases, firewalls are installed on servers, networks, and individual workstations in order to protect these devices against attacks by outside malicious parties such as hackers or cyberspies.

41. Why Should Penetration Testing Be Carried out by a Third Party?

When it comes to security, many organizations have a tendency of neglecting the perimeter. While this is understandable in the vast majority of cases, due to breaches that often originate from outside sources such as phishing and malware attacks, failing to properly secure your internal network can be shut down. A third-party penetration testing firm can help alleviate some of these problems by providing reliable and accurate information about vulnerabilities present in your organization's systems or networks. Additionally, they can provide guidance on how best to address them – whether through vulnerability assessment or remediation.

42. What Are the Legal Steps Involved in Penetration Testing?

There are many different types of tests that a penetration tester might do. These include:

Vulnerability scanning is the practice of scanning systems for potentially exploitable vulnerabilities.
IQ scanning is the use of intrusive and often automated methods to determine the security of systems.
Social engineering is the practice of exploiting human factors to gain access to systems.
Physical access is the attempt to gain unauthorized access to systems through direct or remote access.

43. Can Penetration Testing Be Automated?

One of the key challenges in Penetration Testing is automated scanning and gathering of data. And this is where automation comes into the picture. Automation allows a penetration tester to automate the tasks that help in data gathering. This way, data is captured and analyzed in a systematic and efficient manner. Automation also allows for a quicker turnaround of reports, as well as saves time, and manpower.

44. Explain the benefits and drawbacks of Linux OS and Microsoft Windows for web application Testing?

Factors -

Cost

All kinds of distributions are available for free in Linux.

Microsoft Windows is Paid Operating system.

Utilization

Linux is Difficult for beginners.

Microsoft Windows is User-friendly for beginners.

Trusted or Reliable

Linux is more reliable and secure for users.

Windows is Less reliable and secure.

Softwares

Free and paid both kinds of software are available for Linux.

Most of the software is paid in Microsoft Windows.

Hardware

Initially, hardware compatibility was a problem, the bulk of physical appliances now supports Linux.

Windows has never had a problem with hardware compatibility.

Security

Linux Operating System that is extremely safe for users.

Because inexperienced users utilize this OS so Windows is vulnerable to attackers.

Support
Online community support is available to help with any problem.

Microsoft support is available online, and there are numerous publications available to help you diagnose any problem.

45. What are the commonly targeted ports during penetration testing?

FTP (port 20, 21)
SSH (port 22)
Telnet (port 23)
SMTP (port 25)
HTTP (port 80)
NTP (port 123)
HTTPS (port 443

46. What kind of penetration testing can be done with Diffie Hellman exchange?

DH exchange (Diffie-Hellman Exchange) is a cryptographic protocol that is used to create secure communications. It uses the same key every time two communicating parties use it to encrypt data. The protocol is named after two mathematicians, named Diffie and Hellman. The protocol works by generating two public keys and two secret keys. The public keys are made available to anyone who wants to send secure messages to the corresponding secret keys.

47. What are the Methods of detecting and defending against Rootkits?

How do you detect a rootkit: There is no single detection method that is guaranteed to work for every rootkit. However, some common methods used to detect a rootkit include scans with anti-malware programs, looking for unusual program behavior, and checking for modified files.
How do you protect yourself from a rootkit attack: There is no foolproof way to prevent a rootkit attack, but there are several steps that can be taken to protect oneself. These steps include ensuring that the computer is installed with up-to-date antivirus software, not downloading unknown software, and using caution when using unknown or unverified applications.
You can also refer to the article – Detecting and Checking Rootkits with chkrootkit and rkhunter Tool in Kali Linux.

48. What is Hail Mary function (Armitage) in penetration Testing?

The hail Mary function can be used in penetration testing to move files or streams to and from servers. The hail Mary function can be used to perform a variety of tasks, such as copying files, transferring files over a network, authenticating to a server, moving files to and from a target, and performing other tasks.

49. What are the functions of a full-fledged Windows Rootkit?

A Windows Rootkit is a type of malware that infects and runs undetected within the Operating System (OS) of a computer. Once installed, it allows the creator or installer to perform various tasks on behalf of the rootkits' user without being detected by normal security measures. A full-fledged Windows Rootkit can allow hackers access to sensitive information like passwords, banking details, emails, and other personal data stored on the infected machine.

50. What are the functions of the Java applet popup in penetration testing?

The process of creating a Java applet popup is simple. First, the tester must create a Java program that will be used as the popup. Next, the tester must create a file with the .html extension and place it in the same directory as the Java program. The file must have the same name as the Java program, but with the .html extension. The file should be divided into two parts. The first part contains the code that will be used to create the Java applet popup, and the second part contains the HTML code that will be used to display the Java applet popup.

My social medial accounts -

Twitter — https://twitter.com/technicalSure

YouTube —
https://www.youtube.com/channel/UCZq87M0I0-zEfLuyy

Instagram —
https://www.instagram.com/surendra_choudhary1241/

Linkedin —
https://www.linkedin.com/in/surendra-pander-4066761b7/