Offensive Penetration Testing Glossary

Created By: Somesh K Tiwari, Teaching Assistant

1. **Bash Shell -** Bash (Bourne Again Shell) is the free version of the Bourne shell distributed with Linux and GNU operating systems. Bash is similar to the original, but has added features such as command line editing. A command language script written for the sh shell will also run in the bash shell.
2. **Bind Shell -** Bind shell is a type of shell in which the target machine opens up a communication port or a listener on the victim machine and waits for an incoming connection. The attacker then connects to the victim machine's listener which then leads to code or command execution on the server.
3. **Burp Suite -** Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
4. **DNS Enumeration -** DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.
5. **Exploit -** An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.
6. **HTTP Service -** HTTP service is very beneficial while performing Ethical Hacking related tasks. It can be used to host fake Phishing webpages and website, to transfer files to remote victim servers. With web applications becoming more popular every day, now it's more important to have the knowledge to understand and operate HTTP Servers like Apache.
7. **Hypervisor -** A hypervisor or virtual machine monitor is a computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.
8. **ISO Image -** An ISO image is a disk image of an optical disc. In other words, it is an archive file that contains everything that would be written to an optical disc, sector by

sector, including the optical disc file system. ISO image files bear the .iso filename extension. The name ISO is taken from the ISO 9660 file system used with CD-ROM media, but what is known as an ISO image might also contain a UDF (ISO/IEC 13346) file system (commonly used by DVDs and Blu-ray Discs).

9. **Kali Linux -** Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.
10. **LFI -** An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even Cross-site Scripting (XSS). Typically, LFI occurs when an application uses the path to a file as input.
11. **MSFvenom -** MSFvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance. msfvenom replaced both msfpayload and msfencode as of June 8th, 2015. The advantages of msfvenom are: One single tool. Standardized command line options.
12. **Metasploit Framework -** The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.
13. **Netcat -** Netcat (also known as 'nc' or 'Swiss Army knife') is a networking utility used for reading or writing from TCP and UDP sockets using an easy interface. Netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP. The command is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.
14. **Nmap -** Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.
15. **Open Source Software -** Open-source software is a type of computer software in which source code is released under a license in which the copyright holder grants users the

right to study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

16. **Payload -** A payload refers to the component of a computer virus that executes a malicious activity. Apart from the speed in which a virus spreads, the threat level of a virus is calculated by the damage it causes. Viruses with more powerful payloads tend to be more harmful.
17. **Port Scanner -** A port scanner is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.
18. **RFI -** Remote File Inclusion (RFI) is a type of vulnerability most often found on PHP running websites. It allows an attacker to include a remotely hosted file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation.
19. **Setoolkit -** The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. The Social-Engineer Toolkit (SET) was created and written by the founder of TrustedSec. It is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. It has over 2 million downloads and is aimed at leveraging advanced technological attacks in a social-engineering type environment.
20. **Social Engineering -** Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information.
21. **SSH (Secure Shell) -** Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.
22. **SQL Injection -** SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. To perform different queries that are not allowed by the application.
23. **Vulnerability Scanning -** Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects

and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

24. **Wireshark -** Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.
25. **XSS -** Cross-site scripting is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

- https://www.tutorialspoint.com/
- https://docs.kali.org/
- http://www.linux-magazine.com/