6- Types of Ethical Hacking

1. IDS stands for ________
   Ans: intrusion detection system.

2. A ________ can take down your Internet Connection or even you entire network.
   Ans: DoS attack

3. A hacker using a ________ can steal confidential information in e-mails and files being transferred.
   Ans: network analyzer

4. Network Testing and port scanning tools are ____________
   a. Sam Spade
   b. SuperScan
   c. NetScan
   d. Nmap or NmapWin
   e. Netcat
   f. WildPacketsEtherPeek

5. ________ is a software tool that basically scans the network to see who’s there.
   Ans: port scanner

6. ________ help to identify unauthorized hosts or applications and network host configuration errors that can cause serious vulnerabilities.
   Ans: port scanner

7. ________ tests can be performed very quickly without having to touch individual network hosts.
   Ans: Post-scan

8. As an ethical hacker, you should scan all _____UDP and _______TCP ports on each network host that’s found by your scanner.
   Ans: 65,535 UDP, 65,535 TCP

9. Commonly Hacked Ports:

<table>
<thead>
<tr>
<th>Ports No.</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Echo</td>
</tr>
<tr>
<td>19</td>
<td>Chargen</td>
</tr>
<tr>
<td>20</td>
<td>FTP (File Transfer Protocol)</td>
</tr>
<tr>
<td>21</td>
<td>FTP control</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
</tr>
<tr>
<td>25</td>
<td>SMTP(Simple Mail Transfer Protocol)</td>
</tr>
<tr>
<td>37</td>
<td>Daytime</td>
</tr>
<tr>
<td>53</td>
<td>DNS(Domain Name System)</td>
</tr>
<tr>
<td>69</td>
<td>TFTP(Trivial File Transfer Protocol)</td>
</tr>
<tr>
<td>79</td>
<td>Finger</td>
</tr>
<tr>
<td>80</td>
<td>HTTP(HyperText Transfer Protocol)</td>
</tr>
<tr>
<td>110</td>
<td>POP3(POST OFFICE PROTOCOL Version 3)</td>
</tr>
<tr>
<td>111</td>
<td>SUN RPC(Remote Procedure Calls)</td>
</tr>
<tr>
<td>135</td>
<td>RPC/DCE end point mapper for Microsoft networks</td>
</tr>
<tr>
<td>137,138,139</td>
<td>NetBIOS ove TCP/IP</td>
</tr>
<tr>
<td>161</td>
<td>SNMP(Simple Network Management Protocol)</td>
</tr>
<tr>
<td>220</td>
<td>IMAP(Internet Message Access Protocol)</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS(HTTP over SSL)</td>
</tr>
<tr>
<td>512,513,514</td>
<td>Berkeley r commands</td>
</tr>
<tr>
<td>1214</td>
<td>Kazaa and Morpeus</td>
</tr>
<tr>
<td>1433</td>
<td>Microsoft SQL Server</td>
</tr>
<tr>
<td>1434</td>
<td>Microsoft SQL Monitor</td>
</tr>
<tr>
<td>3389</td>
<td>Windows Terminal Server</td>
</tr>
</tbody>
</table>
10. __________ is a great tool for general network information, such as the number of unique IP addresses, NetBIOS names, and MAC addresses found.
   Ans: NetScanTools
11. ________ is executed through the searching of a single host for open ports.
   Ans: Port Scanning
12. ________ is executed through the searching of multiple hosts in order to target just one specific open port.
   Ans: Port Sweeping
13. Protection from port scanning is often achieved through the use of a __________.
   Ans: Firewall
14. A _____ monitors incoming and outgoing connections through one’s personal computer.
   Ans: Firewall
15. _______ deny outside access to an individual’s personal computer.
   Ans: Firewall
16. ICMP stands for ____________
   Ans: Internet Control Message Protocol.
17. ______ software helps you to monitor the performance of any IP-based device and helps businesses remotely visualize their system performance and monitor network services bandwidth utilization, switches, routers and traffic flow.
   Ans: Network monitoring
18. ____________ is the act of capturing the information provided by banners, configurable text-based welcome screens from network hosts that generally display system information.
   Ans: Banner Grabbing
19. ____________ is often used for white hat hacking endeavors like vulnerability analysis and penetration testing as well as gray hat activities and black hat hacking.
   Ans: Banner Grabbing
20. ____________ is a tool that allows you to look into a network and analyze data going across the wire for network optimization, security, and/or troubleshooting purposes.
   Ans: Network Analyzer
21. ____________ are often generically referred to as sniffers.
   Ans: Network Analyzer
22. An excessive amount of ARP requests can be a sign of an ______ on your network.
   Ans: ARP poisoning/ARP spoofing
23. SNMP stands for ________________
    Ans: Simple Network Management Protocol
24. Name of the Network analyzer ________

<table>
<thead>
<tr>
<th>Name of Network Analyzer</th>
<th>Supporting Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>EtherPeek by WildPackets</td>
<td>Windows</td>
</tr>
<tr>
<td>Ethereal</td>
<td>Windows and UNIX</td>
</tr>
<tr>
<td>Ettercap</td>
<td>Windows and UNIX</td>
</tr>
<tr>
<td>Dsniff</td>
<td>UNIX</td>
</tr>
</tbody>
</table>

25. ____________ is one in which a mobile user can connect to a local area network through a wireless (radio) connection.
   Ans: Wireless LAN (WLAN)
26. The ______ group of standards specify the technologies for wireless LANs.
   Ans: IEEE 802.11
27. Common Wireless LANs threats are _______________________
   Ans: Rogue Access Points/Ad-Hoc Networks, Denial of Service, Configuration Problems, Passive Capturing
28. Wireless Network Attacks are _________________________________
   Ans: Encrypted traffic, rogue Networks, Physical security problems, vulnerable wireless workstations, default configuration setting.
29. ________________ has its own weakness that allows hackers to crack the encryption keys and decrypt the captured traffic.
   Ans: 802.11 encryption protocol(Wired Equivalent Privacy(WEP))
30. _____________ watch out for unauthorized access points and wireless clients attached to your network that are running in ad-hoc mode.
   Ans: Rogue Networks
31. Using _____, you can test for Access Points that don’t belong on your network.
   Ans: NetStumbler or client manager software
32. _______________ stores encrypted WEP keys in the Windows Registry even for multiple networks.
   Ans: Orinoco Client Manager
33. _______________ is a program that acts as an interface between the software and the computer hardware.
   Ans: Operating System
34. ___________ is an integrated set of specialized programs used to manage overall resources and operations of the computer.
   Ans: Operating System
35. ____________ is specialized software that controls and monitors the execution of all other programs that reside in the computer, including application programs and other system software.
   Ans: Operating System
36. Some of the common vulnerabilities found in all versions of windows are_______
37. _________________ are those e-mail and instant messaging(IM) applications that we depend on are often hacked within a network.
   Ans: Messaging System
38. _____________ can crash a server and provide unauthorized administrator access.
   Ans: Email Bombs
39. An Email bomb is also known as _____________.
   Ans: letter bomb
40. ________________ is form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.
   Ans: Email bombs
41. An attacker can create an _____________ by sending hundreds or thousands of email with very large attachments.
   Ans: attachment-overloading attack
42. The whole email server may be targeted for a complete interruption of service with these failures like _________________.
   Ans: storage overload and bandwidth blocking
   ________is an interesting attack to find two or more users on the same or different e-mail systems.
   Ans: Autoresponders attack
43. _______________ is that annoying automatic email response you often get back from random users when you are subscribing to a mailing list.
Ans: Autoresponders attack
44. An attacker can crash your email service or bring it to a crawl by filling the incoming Internet connection with junk is known as _______________.
   Ans: Bandwidth blocking
45. When a basic telnet connection is made on port 25(SMTP) ______________displayed on an email server.
   Ans: Banner
46. Web application security vulnerabilities are _______________
47. ______________ allows an attacker to alter backend SQL statements by manipulating the user supplied data.
   Ans: SQL injection
48. Cross Site Scripting is also shortly known as ___________.
   Ans: XSS
49. __________ target scripts embedded in a page that are executed on the client side.
   Ans: XSS
50. Attacker can use ______ to execute malicious scripts on the users browsers.
   Ans: XSS
51. __________is an attack which allows the attacker to execute the scripts on the victim’s browser.
   Ans: XSS
52. ______________ attack is browsing a site and looking for clues about the server’s directory structure.
   Ans: Directory Traversal
53. ______________ is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.
   Ans: Directory Traversal or Path Traversal
54. Web servers provide two main levels of security mechanisms_______________
   a. Access Control Lists(ACLs)
   b. Root directory
55. SNMP stands for _________________
   a. Simple Network Messaging Protocol
   b. Simple Network Mailing Protocol
   c. Simple Network Management Protocol
   d. Simple Network Master Protocol
56. Banner grabbing is often used for
   a. White Hat Hacking
   b. Black Hat Hacking
   c. Gray Hat Hacking
   d. Script kiddies
57. A attacker can create an __________attack by sending hundreds or thousands of e-mails with very large attachments.
   a. Connection attack
   b. Auto responder attack
   c. Attachment overloading attack
   d. All of the above
58. Which of the following tool is used for Network Testing and Port Scanning
   a. NetCat
   b. SuperScan
   c. NetScan
   d. All of above