Certified Ethical Hacker V8

1. Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack. What should Peter do to prevent a smurf attack?

A. He should disable unicast on all routers

B. Disable multicast on the router

C. Turn off fragmentation on his router

D. Make sure all anti-virus protection is updated on all systems

E. Make sure his router won't take a directed broadcast

Answer(s): E

---

2. This is an example of whois record.

A. Search engines like Google,Bing will expose information listed on the WHOIS record

B. An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record

C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record

D. IRS Agents will use this information to track individuals using the WHOIS record information

Answer(s): B,C

---

3. You have just installed a new Linux file server at your office. This server is going to be used by several individuals in the organization, and unauthorized personnel must not be able to modify any data.

A. Network Based IDS (NIDS)

B. Personal Firewall

C. System Integrity Verifier (SIV)

D. Linux IP Chains

Answer(s): C

---

4. Carl has successfully compromised a web server from behind a firewall by exploiting a vulnerability in the web server program. He wants to proceed by installing a backdoor program. However, he is aware that not all inbound ports on the firewall are in the open state.

A. 53

B. 110

C. 25

D. 69

Answer(s): A

---

5. Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

A. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network

B. Victim's Operating System versions,services running and applications installed will be published on Blogs and Forums

C. Victim's personally identifiable information such as billing address and credit card details,may be extracted and exploited by the attacker

D. Once infected,the computer will be unable to boot and the Trojan will attempt to format the hard disk

Answer(s): C

---

6. You receive an email with the following message:

A. 222.173.190.239

B. 233.34.45.64

C. 54.23.56.55

D. 199.223.23.45

Answer(s): A

---

7. John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module.

A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.

B. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel after it has been recompiled and the system rebooted.

C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.

D. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation.

Answer(s): D

---

8. A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from

A. Follow proper legal procedures against the company to request payment.

B. Tell other customers of the financial problems with payments from this company.

C. Threaten to publish the penetration test results if not paid.

D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Answer(s): A

---

9. While scanning a network you observe that all of the web servers in the DMZ are responding to ACK packets on port 80.

A. They are using Windows based web servers.

B. They are using UNIX based web servers.

C. They are not using an intrusion detection system.

D. They are not using a stateful inspection firewall.

Answer(s): D

---

10. Which are true statements concerning the BugBear and Pretty Park worms?

A. Both programs use email to do their work.

B. Pretty Park propagates via network shares and email

C. BugBear propagates via network shares and email

D. Pretty Park tries to connect to an IRC server to send your personal passwords.

E. Pretty Park can terminate anti-virus applications that might be running to bypass them.

Answer(s): A,C,D

---

11. One of the better features of NetWare is the use of packet signature that includes

A. 0 (zero)

B. 1

C. 2

D. 3

Answer(s): D

---

12. After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

A. IUSR_

B. acmr,dns

C. nobody,dns

D. nobody,IUSR_

Answer(s): C

---

13. A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.

A. Kernel level privileges

B. Ring 3 Privileges

C. User level privileges

D. System level privileges

Answer(s): A

---

14. You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.

A. Sequence number: 17768729 Acknowledgement number: 82980070

B. Sequence number: 82980010 Acknowledgement number: 17768885

C. Sequence number: 87000070 Acknowledgement number: 85320085

D. Sequence number: 82980070 Acknowledgement number: 17768885

Answer(s): D

---

15. Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

A. By using the pictures to hide information,the employee utilized picture fuzzing

B. The employee used steganography to hide information in the picture attachments

C. The method used by the employee to hide the information was logical watermarking

D. The Kiley Innovators employee used cryptography to hide the information in the emails sent

Answer(s): B

---

16. The SYN flood attack sends TCP connections requests faster than a machine can process them.

A. Micro Blocks. Instead of allocating a complete connection,simply allocate a micro record of 16-bytes for the incoming SYN object

B. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall

C. Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection

D. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point,the server knows the client is valid and will now accept incoming connections from that client normally

E. SYN cookies. Instead of allocating a record,send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address,port number,and other information. When the client responds with a normal ACK,that special sequence number will beincluded,which the server then verifies. Thus,the server first allocates memory on the third packet of the handshake,not the first.

Answer(s): A,C,D,E

---

17. NSLookup is a good tool to use to gain additional information about a target network. What does the following command accomplish?

A. Enables DNS spoofing

B. Loads bogus entries into the DNS table

C. Verifies zone security

D. Performs a zone transfer

E. Resets the DNS cache

Answer(s): D

---

18. While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor. How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.

B. Do not scan the broadcast IP.

C. Spoof the source IP address.

D. Only scan the Windows systems.

Answer(s): B

---

19. Exhibit: Given the following extract from the snort log on a honeypot, what do you infer from the attack?

A. A new port was opened

B. A new user id was created

C. The exploit was successful

D. The exploit was not successful

Answer(s): D

---

20. War dialing is a very old attack and depicted in movies that were made years ago.

A. It is cool,and if it works in the movies it must work in real life.

B. It allows circumvention of protection mechanisms by being on the internal network.

C. It allows circumvention of the company PBX.

D. A good security tester would not use such a derelict technique.

Answer(s): B