Global Information Assurance Certification Paper

Section 1: Incident Handling

1. The first phase of incident handling is:
    a. Containment
    b. Preparation
    c. Identification
    d. Eradication
    e. All of the Above
    f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 32

2. The establishment of _____ is an important part of the Preparation stage.
    a. a security policy
    b. alternate communication methods
    c. a chain of communication
    d. proper backups
    e. All of the Above
    f. None of the Above

answer: e
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 34

3. The posting of warning banners on computer terminals is part of:
    a. establishing communications
    b. monitoring the systems
    c. a security policy
    d. a command center
    e. All of the Above
    f. None of the Above

answer: c
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 37

4. Which of the following people should *not* be in a secured area during an incident:
    a. Floor Manager
    b. Witnesses
    c. CIRT team members
    d. law enforcement agents
    e. All of the Above
    f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 43

5. Conducting "War Games" is a part of which phase of incident handling:
    a. Identification
    b. Eradication
    c. Containment
    d. Recovery
    e. All of the Above

f. None of the Above

answer: f (Preparation phase is correct)
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 44

6. An incident handling "jump bag" is:
   a. a collection of software/hardware/supplies that is kept for emergencies
   b. a software program designed to collect data from the network
   c. a piece of hardware designed to duplicate data on hard drives
   d. a personal collection of documents describing security incidents
   e. All of the Above
   f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 52

7. Which of the following items is a sign of an incident:
   a. Unsuccessful logon attempts
   b. Poor system performance
   c. Intrusion detection software sends an alarm
   d. System crashes
   e. All of the Above
   f. None of the Above

answer: e
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 62-63

8. Determining if an event is an actual incident is part of which phase of incident handling:
   a. Preparation
   b. Identification
   c. Eradication
   d. Follow-up
   e. All of the Above
   f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 64

9. The first phase in which the incident handler will begin to modify the affected systems is:
   a. Preparation
   b. Identification
   c. Recovery
   d. Containment
   e. All of the Above
   f. None of the Above

answer: d
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 65

10. Incidents are best handled by:
   a. a single individual

b. a single individual with an assistant handler
c. three individuals working as a hierarchy
d. the entire CIRT team simultaneously
e. All of the Above
f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 61, 75

11. Securing an area should begin in which phase of incident handling:
a. Containment
b. Eradication
c. Recovery
d. Identification
e. All of the Above
f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 67

12. The legal implications of handling computer and data evidence is known as:
a. Chain of Custody
b. Possession and Prosecution
c. React and Defend
d. Proper Backups
e. All of the Above
f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 69

13. An example of a program that copies a bit-by-bit image of a hard drive is:
a. NT Backup
b. Nessus
c. WinAT
d. Ghost
e. All of the Above
f. None of the Above

answer: d
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 70

14. A drive duplicator is:
a. A software package that copies files from hard drives
b. A hardware device that makes image copies of hard drives.
c. A vendor that recovers lost data from hard drives
d. A program that replays an attack
e. All of the Above
f. None of the Above

answer: b

source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 72

15. In order to expedite the handling of an incident, you may have to coordinate closely with:
    a. Help Desk personnel
    b. Internet Service Providers
    c. Law Enforcement Agencies
    d. System Administrators
    e. All of the Above
    f. None of the Above

answer: e
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 45-46, 57, 73

16. Encouraging users to alert the CIRT *early* to an incident increases the speed of which phase of incident handling:
    a. Preparation
    b. Identification
    c. Containment
    d. Eradication
    e. All of the Above
    f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 61

17. Which phrase is commonly used in conjunction with the Containment phase of incident handling:
    a. "watch and learn"
    b. "backup, backup, backup"
    c. "stop the bleeding"
    d. "if the data doesn't fit, you must acquit"
    e. All of the Above
    f. None of the Above

answer: c
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 62-63

18. Which item would be considered "best evidence":
    a. Image copy of a hard drive
    b. Tape backup from a hard drive
    c. The original hard drive
    d. File printouts of the hard drive
    e. All of the Above
    f. None of the Above

answer: c
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 70

19. At what point does the incident handler *always* lose control of the incident investigation:
    a. When law enforcement becomes involved
    b. When corporate legal department becomes involved
    c. When legal department becomes involved

d. When senior management becomes involved
e. All of the Above
f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 74

20. What phase of incident handling immediately follows the Containment phase:
a. Recovery
b. Intensification
c. Follow-up
d. Eradication
e. All of the Above
f. None of the Above

answer: d
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 81

21. The "initial assessment" occurs during which phase of incident handling:
a. Preparation
b. Identification
c. Containment
d. Eradication
e. All of the Above
f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 64

22. Software applications such as Cybercop, ISS, NetSonar, SAINT and NMAP can be used to:
a. Locate and save forensic data from compromised systems
b. Detect vulnerabilities in computer systems
c. Create image copies of files and hard drives
d. Keep logs of incident handler activities during an investigation
e. All of the Above
f. None of the Above

answer: b
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 84

23. A system designed to attract and collect information about an attacker is known as a:
a. Honeypot
b. Tiger pit
c. Trip mine
d. Border guard
e. All of the Above
f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 83

24. A useful tool in locating "trojan horse" applications in a computer would be:
    a. personal firewall software
    b. anonymizer software
    c. encryption software
    d. anti-virus software
    e. All of the Above
    f. None of the Above

answer: d
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 86

25. Which method of recovering the system would provide the highest confidence level in the resulting OS after an incident:
    a. replacing only affected files from a known good backup and applying all current patches
    b. restoring the OS from a known good backup and applying all current patches
    c. reinstalling the OS from original installation disks and applying all current patches
    d. copying an installation from a known good system and applying all current patches
    e. All of the Above
    f. None of the Above

answer: c
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 88

26. Why is validating a system during the recovery phase important:
    a. To verify that the system is back in its original working condition
    b. To verify that the system has not been re-compromised during the recovery
    c. To assure the users of the computer and restore the confidence level associated with its use
    d. To verify that you did not introduce any instabilities that will affect the computer's operation
    e. All of the Above
    f. None of the Above

answer: e
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 89

27. To help prevent a system from being compromised a second time, you should:
    a. Change the IP address and name of the computer
    b. Load all current vender patches for both the OS and applications
    c. Increase logging for at least 72 hours after the initial incident
    d. Use software tools such as Tripwire and ISS to monitor activity on the computer
    e. All of the Above
    f. None of the Above

answer: e
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 83, 88, 91

28. During the Follow-up phase of incident handling, you should create:
    a. a CIRT
    b. CD's with known good binaries and boot files
    c. a Command Center
    d. an incident report
    e. All of the Above
    f. None of the Above

answer: c
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 93

29. A "Lessons Learned" or "Post-mortem" meeting is part of which phase of incident handling:
    a. Follow-up
    b. Containment
    c. Recovery
    d. Preparation
    e. All of the Above
    f. None of the Above

answer: a
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 94

30. Which of the following should *not* be a member of a CIRT team:
    a. System Administrator
    b. Corporate security officer
    c. Public relations representative
    d. Senior Manager
    e. All of the Above
    f. None of the Above

answer: f
source: Incident Handling: Step-by-Step and Computer Crime Investigation, p. 41-43

Section 2: Hacker Exploits 1

1. The three main areas of computer security are:
    a. Speed, Control and Power
    b. Confidentiality, Integrity and Availability
    c. Public, Personal and Corporate
    d. Local, Regional and National
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 9

2. An exploit is:
    a. Anything a person can use to gain access or make gaining access easier
    b. Formatting a hard drive using a remote access tool
    c. Distribution of offensive materials
    d. Creating and using a pseudonym on the internet
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 8

3. Attackers will always look for:
    a. expensive vulnerability scanning software such as Cybercop or ISS
    b. corporate credit cards to finance their activities
    c. the path of least resistance
    d. financial and market data to sell to the highest bidder
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 13

4. HTTP traffic is typically found on port:
    a. 21
    b. 25
    c. 51
    d. 80
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 21

5. Which of the following *cannot* be exploited on a computer system:
    a. Ports
    b. Services
    c. Passwords
    d. Third party software
    e. All of the Above
    f. None of the Above

answer: f
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 20

6. Indirect information gathered from surrounding events is referred to as:
    a. Social Engineering
    b. Covert Channels
    c. Inference Channels
    d. Back Doors
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 25

7. Gathering information by using a network sniffer would be an example of using:
    a. Social Engineering
    b. Covert Channels
    c. Inference Channels
    d. Back Doors
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 28

8. Taking over a TCP/IP connection that is already established is known as:
   a. Session Hijacking
   b. Sniffing
   c. Smurfing
   d. Surfing
   e. All of the Above
   f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 31

9. An attack that renders a computer unusable by legitimate users is known as:
   a. Buffer Overflow
   b. Password Cracking
   c. Session Hijacking
   d. Denial of Service
   e. All of the Above
   f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 32

10: L0phtcrack and Crack are examples of programs that perform what kind of exploit:
   a. Network Sniffing
   b. Trojan Horse
   c. Password Cracking
   d. Social Engineering
   e. All of the Above
   f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 34

11. A random string that is attached to a password before it is encrypted and stored is known as:
   a. Spice
   c. Salt
   d. Pepper
   e. Crust
   e. All of the Above
   f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 44

12. Which operating system has uncrackable passwords:
   a. Windows NT
   b. Solaris

c. Linux
d. OS-2
e. All of the Above
f. None of the Above

answer: f (all passwords can be cracked)
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 44

13. The current version of L0phtcrack is:
a. 1.5
b. 1.52
c. 2.5
d. 2.52
e. All of the Above
f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 46: http://l0pht.com/l0phtcrack/

14. The Dictionary/Brute Hybrid setting in the Tools>Option menu tells L0phtcrack to:
a. Perform both the dictionary and brute force attacks
b. Concatenate numbers to the dictionary words while running the dictionary attack
c. Reverse the order of the dictionary and brute force attacks
d. Run the dictionary and brute force attacks simultaneously
e. All of the Above
f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 53

15. Passwords for a Unix system, if they are *not* shadowed, are stored in:
a. /etc/passwd
b. /etc/password
c. /usr/passwd
d. /usr/password
e. All of the Above
f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 75

16. The utility used to view the output of Crack is called:
a. Seer
b. Repeater
c. Show
d. Reporter
e. All of the Above
f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 75

17. Passwords for Unix systems, if they are shadowed are stored in:
    a. /etc/shadow
    b. /tmp/shadow
    c. /usr/shadow
    d. /sdw/shadow
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 85

18. The NT process that "GetAdmin" exploits is:
    a. DebugActiveProcess
    b. NtOpenProcessToken
    c. Inetinfo
    d. msconf.dll
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 94

19. The NT process that "SecHole" exploits is:
    a. DebugActiveProcess
    b. NtOpenProcessToken
    c. Inetinfo
    d. msconf.dll
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 104

20. An example of a Denial of Service exploit would be:
    a. GetAdmin
    b. SecHole
    c. Win Nuke
    d. Red Button
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 123

21 An exploit that takes advantage poor program management of input data size is:
    a. Denial of Service
    b. Spoofing
    c. Smurfing
    d. Buffer Overflow
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 160

22. The "aglimpse", "campas", "tooltalk" and "imapd" exploits are an example of which type of exploit:
    a. Denial of Service
    b. Buffer Overflow
    c. Session Hijacking
    d. Password Cracking
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 178

23. The "aglimpse" and "campas" programs are what type of service:
    a. CGI scripts
    b. PERL scripts
    c. RPC locators
    d. Telnet scripts
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 178, 188

24. The attack characterized by sending ICMP-echo request packets with a spoofed address to several machines in order to flood a machine with ICMP-echo replies is known as:
    a. Land
    b. Smurf
    c. SYN Flood
    d. Ping of Death
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 259

25. The "Ping of Death" attack works by sending:
    a. a SYN packet to a target computer, and not responding to the SYN-ACK package that is returned
    b. ICMP-echo request packets with a spoofed address to several machines in order to flood a machine with ICMP-echo replies
    c. an IP packet with the source and destination address and port set to the same value
    d. an oversized ICMP-echo request packet
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 235

26. A "SYN Flood" exploit is an example of which type of attack:
    a. Denial of service
    b. Buffer Overflow
    c. Back Door
    d. Session Hijacking
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 269

27. "Hack a'Tack" is an example of a _____ attack:
    a. Password Cracker
    b. Trojan Horse
    c. Buffer Overflow
    d. Denial of Service
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 279

28. Altering data is an attack against:
    a. Confidentiality
    b. Availability
    c. Integrity
    d. Responsibility
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 11

29. The "Fraggle" attack works in the same manner as a "Smurf" attack, except:
    a. it uses UDP packets instead of ICMP packets
    b. it uses IPX/SPX protocol instead of TCP/IP protocol
    c. it uses port 21 instead of port 20
    d. it is named after the hacker that wrote the tool
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 263

30. Large, highly fragmented ICMP packets are a sign of which attack:
    a. Land
    b. Ping of Death
    c. Snort
    d. SSping
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 1, p. 259

Section 2: Hacker Exploits 2

1. The first step in the flow of an attack is:
    a. Exploit Systems
    b. Keeping Access
    c. Reconnaissance
    d. Scanning
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 3

2. A popular online "whois" service is:
    a. ORIS
    b. ACORN
    c. L0PHT
    d. ARIN
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 15

3. "ToneLoc" and "THC-Scan" are examples of what type of program:
    a. war dialers
    b. network sniffers
    c. trojan horses
    d. DDOS
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 19

4. "NMAP" scans for:
    a. services
    b. ports
    c. computers
    d. vulnerabilities
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 27

5. A tool to use to determine open ports on a firewall is:
    a. Firewalk
    b. Frag Router
    c. NMAP
    d. Nessus
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 32

6. A freeware vulnerability scanner is:
    a. NMAP
    b. NetCat
    c. Sniffit
    d. Nessus
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 35

7. A feature of "NMAP" is:
    a. war dialing
    b. password guessing
    c. TCP stack fingerprinting
    d. changing SNMP community names
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 28

8. The third step in the flow of an attack is:
    a. Exploit Systems
    b. Covering the Tracks
    c. Reconnaissance
    d. Scanning
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 45

9. An attacker that uses tools written by a hacker without fully understanding how it functions is often called:
    a. Internet Idiot
    b. Script Kiddie
    c. Tool Timer
    d. Dead Cow
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 11

10. A standard term that a hacker uses once he has taken control of the machine, is that the computer "is _____":
    a. "hosed"
    b. "owned"
    c. "rented"
    d. "toasted"
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 3

11. The ability of a computer to specify the path that a packet should take to come back to the requesting computer is known as:
    a. IP fragmentation
    b. tunneling
    c. source routing
    d. DNS cache poisoning
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 55

12. The act of making your computer appear to be another computer by changing the IP address is known as:
    a. Smurfing
    b. Sniffing
    c. Spoofing
    d. Snorting
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 47

13. A defense against DNS Cache Poisoning is:
    a. Use SSL with server-side authentication
    b. Use split-split DNS
    c. Use digitally signed DNS records
    d. Use the latest version of DNS software (i.e. BIND)
    e. All of the Above
    f. None of the Above

answer: e
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 88-89

14. A DOS tool is:
    a. Targa
    b. NetBus
    c. NetCat
    d. Hobbit
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 104

15. The first fragment of a fragmented TCP packet in a "Tiny Fragment" attack does not contain:
    a. TCP port number
    b. IP address
    c. Source IP address
    d. SYN flag
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 61

16. A TCP tool that uses the same methodology as Firewalk is:
    a. NSLOOKUP
    b. WHOIS
    c. TRACEROUTE
    d. FINGER
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 34

17. "Hunt" is a software tool that performs:
    a. vulnerability scanning
    b. session hijacking
    c. backdoor access
    d. DDOS
    e. All of the Above
    f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 75

18. Port 20034 is a known port used by:
    a. Portal of Doom
    b. Back Orifice
    c. NetBus 2 Pro
    d. Telecommando
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 165

19. A DDOS tool that uses ICMP-echo replies to tunnel communication is:
    a. Targa
    b. Trin00
    c. TFN
    d. Back Orifice
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 111

20. The protocol that "Hunt" uses to undermine a session is:
    a. RARP
    b. ICMP
    c. ARP
    d. NetBIOS
    e. All of the Above
    f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 76

21. A tool used to move data between systems on any specified port is:
    a. NetCat
    b. NMAP
    c. Snort
    d. Trin00
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 92

22. A feature of NetCat is it can be used:
    a. as a port scanner
    b. to replay attacks
    c. as a relay to other NetCat installations
    d. as a backdoor access point
    e. All of the Above
    f. None of the Above

answer: e
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 100

23. The hacker group Cult of the Dead Cow created what program:
    a. Back Orifice
    b. Trin00
    c. TFN

d. NetBus
e. All of the Above
f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 127

24. DOS is an acronym for:
a. a well known hacker group
b. Distributed Operating System
c. Denial Of Service
d. Differential Offset Sockets
e. All of the Above
f. None of the Above

answer: c
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 102

25. A method to hijack a web session that maintains state can be accomplished by:
a. using a tool like "HTTP Tunnel"
b. typing in an URL such as "https://www.bank.com/acctbal.asp?sid=34112323"
c. requesting state information from the DNS server
d. create a duplicate application and use this application to capture state information
e. All of the Above
f. None of the Above

answer: b
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 121

26. An way to limit the effectiveness of sniffers is:
a. allow source routing
b. intrusion detection systems (IDS's)
c. firewalls
d. switched ethernet
e. All of the Above
f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 66

27. The "BOSOCK32" plug-in for Back Orifice gives which capability to the program:
a. Streaming Video
b. 32-bit encryption of data
c. Graphical file viewer and registry editor
d. ICMP tunneling
e. All of the Above
f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 135

28. The second step in the flow of an attack is:
    a. Exploit Systems
    b. Keeping Access
    c. Reconnaissance
    d. Scanning
    e. All of the Above
    f. None of the Above

answer: d
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 16

29. Knark uses which Linux capability in order to function:
    a. Loadable Kernal Module (LKM)
    b. Programmable Access Module (PAM)
    c. Volume Manager Daemon (VOLD)
    d. Kernal Dependency Module (KDM)
    e. All of the Above
    f. None of the Above

answer: a
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 16

30. "Nessus" runs on which platform(s):
    a. Solaris
    b. NT
    c. Linux
    d. FreeBSD
    e. All of the Above
    f. None of the Above

answer: e
source: Computer and Network Hacker Exploits: Step-by-Step, Part 2, p. 41

Last Updated: July 25th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event