Global Information Assurance Certification Paper

Author: Dustin Anders
Date: 05/21/2000
Advanced Incident Handling and Hacker Exploits Practical Assignment
Chosen Assignment: Create a Test that demonstrates your knowledge of the subject area

---

Section I: 30 Questions from Incident Handling

1: Which of the following is NOT a step of accomplishing Triage?
A. Identifying critical functions
B. Testing & revising
C. Identifying less critical functions
D. Implementing the strategies

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 4
Correct Answer: C

2: It's very important to take notes during an incident. What should you document so that your notes hold up in court as evidence?
A. Names of any analysts working with you on the incident
B. Times and hostnames that you saw unusual activity
C. The Who, What, When, and Where.
D. Time, IP Addresses, hostnames compromised

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 12
Correct Answer: C

3: As you execute the Emergency Action Plan, you should NOT tell the user which of the following:
A. Please turn on full logging until we get there
B. Please take your hands off the keyboard and move away from the computer
C. Disconnect the network/modem connection to the machine
D. Don't touch anything, we'll be right there

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 17
Correct Answer: A

4: What type of backup should you make of the infected machine(s)?
A. Full System Backup
B. Bit-by-bit Backup
C. Only backup the infected files
D. Partial Backup

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 18
Correct Answer: B

5: What information should be contained in your warning banners?
A. Disclaimer of system use
B. Warning to intruders that the system is unauthorized and they will be prosecuted
C. Your organization's policy on the resumption of privacy
D. Your system administrator's contact information

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 37
Correct Answer: C

6: What does it mean when a company is escrowing passwords?
A. The company hires an external company to maintain all superuser passwords in case of an incident
B. Passwords are kept in sealed envelopes in locked containers in case of an incident
C. A manager or supervisor keeps all system passwords for incidents
D. A analyst is chosen to have complete access to all systems

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 49
Correct Answer: B

7: Which of the following is NOT necessary to have ready for an incident?
A. Small tape recorder
B. Small hub
C. Cell phone
D. Wiretap

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 52
Correct Answer: D

8: All of the following are signs of an intrusion EXCEPT:?
A. Door knob rattling
B. Unusual time of usage
C. Unusually good system performance
D. System crashes

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 63
Correct Answer: C

9: Which of the following instantly copies and clones entire hard drives?
A. Drive Duplicator
B. Safeback
C. Ghost
D. Expert Witness

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 72
Correct Answer: A

10: Which tool should be used to find out information about an intruder?
A. Ping
B. Nslookup
C. Telnet
D. None of the above

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 76
Correct Answer: D

11: When establishing quarantine boundaries, all of the following must be done EXCEPT:
A. Change passwords on all systems
B. Change passwords on affected systems
C. Determine and certify trustmodel
D. If a sniffer is detected or suspected, expand the password change order

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 80
Correct Answer: A

12: What is a honeypot?
A. A system that sniffs all network data for unusual activity.
B. A system that contains no real data but is locked down very tightly to see if the current security loads are sufficient.
C. A system that is designed to collect information about an attacker without yielding any useful data.
D. None of the above

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 83
Correct Answer: C

13: Which of the following is NOT an example of malicious code?
A. Virus
B. Root kit binaries
C. Easter Eggs
D. Visual Basic Scripts

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 106
Correct Answer: D

14: Trojans traditionally do which of the following?
A. E-mail system information off to the attacker
B. Sit on the system listening and waiting for the attacker to connect
C. Delete all files on the system
D. Run sniffing software to collect network data

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 111
Correct Answer: B

15: What is a common way to identify that a root kit is installed on a system?
A. Look for outbound traffic on port 6667
B. Look at the file permissions on all system files
C. Perform a 'netstat –an' to see what ports are listening for connections
D. Look at the owners of system binaries

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 113
Correct Answer: A

16: Smurf is an example of what type of attack?
A. Denial of Service
B. Buffer Overflow
C. Virus
D. Trojan

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 125
Correct Answer: A

17: Fraggle makes use of what protocol?
A. TCP
B. ICMP
C. UDP
D. None of the above

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 125
Correct Answer: B

18: The best method of preventing sexually explicit web surfing is:
A. Creating a policy with the organization to not allow going to sexually explicit sites
B. Blocking all traffic to such sites using software on your firewalls
C. Search for requests in the log files and take appropriate actions against those employees
D. Run software on the clients to prevent unauthorized surfing

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 168
Correct Answer: B

19: ntlast –f –r –n 25 Does what?
A. Gets the last 25 failed remote logon attempts
B. Gets the last 25 interactive logon attempts
C. Gets the last 25 successful logon attempts

D. None of the above

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 180
Correct Answer: A

20: What does tripwire do?
A. Looks into the kernel to see if a loadable module has been installed on Linux
B. Listens on a number of ports to help detect port scans
C. Looks at system files to see if they have been altered
D. Sniffs network traffic

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 183
Correct Answer: C

21: When handling evidence, you should do all the following EXCEPT:
A. Make 2 backups of all evidence
B. Original drive should go in access controlled safe
C. Make copies of all notes taken
D. Use a backup drive for your investigation

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 187
Correct Answer: C

22: Which of the following is NOT a forensics tool?
A. nmap
B. NAI's Guard Dog
C. Expert Witness
D. Safeback

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Pages 186-189
Correct Answer: A

23: What keystroke shows history in DOS?
A. F7
B. F10
C. F1
D. F8

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 200
Correct Answer: A

24: The Caligula virus performs what action?
A. E-mails system information off the infected system
B. Pulls the user's PGP key ring and sends it to a website
C. Trojans the system and waits for a connection
D. Deletes all filesystems

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 204
Correct Answer: B

25: All of the following are methods to hide data EXCEPT:?
A. Change header information inside TCP packets
B. Steganography
C. Marking cluster as bad on the disk
D. Hidden inside TCP header fields crossing a network

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 215
Correct Answer: A

26: Steganography is the process of:
A. Hiding files within other files
B. Encrypting files
C. Hiding data in unused file streams on NTFS partitions
D. Sending hidden data in ftp transmissions

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 215
Correct Answer: A

27: What does the following command do: find / -perm –2000 –o –perm –4000 -print?
A. Prints all files that have been modified in the past 20 days
B. Prints all files with suid and sgid
C. Prints all files modified today
D. Prints all files with the extension of pl

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page 227
Correct Answer: B

28: What command shows the listening services?
A. df
B. nbtstat
C. netstat -an
D. ls

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page A - 5
Correct Answer: C

29: All of the following are true concerning a good audit EXCEPT:
A. You want to collect as much data as possible in your baseline
B. Do not log successful logons, only failed logons in your baseline
C. Burn your tools to a CD
D. Create a written procedure outlining scope, frequency, and responsibility

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page A-9 … A-11
Correct Answer: B

30: What does the global.exe program do?
A. Shows all local and domain groups for a user
B. Shows all members of a specified domain group
C. Shows all members of a specified local group
D. Shows all users and groups on a specified system

Location Found: SANS GIAC 4.1 – Computer Security Incident Handling Page A-26
Correct Answer: B

Section II: 30 Questions from Hacker Exploits Day 1

1: The three main areas of security are:
A. Confidentiality, Privacy & Integrity
B. Integrity, Privacy, & Availability
C. Confidentiality, Integrity, & Availability
D. Confidentiality, Privacy, & Integrity

Location Found: SANS GIAC 4.2 – Computer and Network Hacker Exploits: Page 9
Correct Answer: C

2: Session hijacking is defined as:
A. Causing a loss of service by overwhelming a system with traffic.
B. Taking over a legitimate session and gaining access to a system.
C. Convincing another system that you are a different IP address.
D. Going through multiple systems to either change your identity or gain additional access.

Location Found: SANS GIAC 4.2 – Computer Security Incident Handling Page 14

Correct Answer: B

3: Spoofing is defined as:
A. Causing a loss of service by overwhelming a system with traffic.
B. Taking over a legitimate session and gaining access to a system.
C. Convincing another system that you are a different IP address.
D. Going through multiple systems to either change your identity or gain additional access.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 14
Correct Answer: C

4: Relaying is defined as:
A. Causing a loss of service by overwhelming a system with traffic.
B. Taking over a legitimate session and gaining access to a system.
C. Convincing another system that you are a different IP address.
D. Going through multiple systems to either change your identity or gain additional access.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 14
Correct Answer: D

5: Social engineering involves:
A. Creating robots to infiltrate corporate premises to gain information
B. Convincing people to give you information they normally would not give you
C. Breaking into a company and gaining information
D. Gaining physical access to company premises to gain information

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 19
Correct Answer: B

6: A system has ports 20, 21, 23, 80, 110 running. Which of the following protocols is running on this system:
A. SMTP
B. Finger
C. FTP
D. IRC

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 21
Correct Answer: C

7: Which of the following is NOT true regarding passwords?
A. Most passwords are changed on a bi-monthly basis
B. Most passwords are trivial to guess
C. Most passwords are rarely changed
D. Most systems have accounts with no passwords

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 24
Correct Answer: A

8: What is a buffer overflow?
A. A program that installs on the victim host and waits for instructions from a remote host
B. Sending data to a program that it is not expecting
C. Causing a loss of service by overwhelming a system with traffic.
D. Taking over a legitimate session and gaining access to a system.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 33
Correct Answer: B

9: L0phtcrack, John the ripper, and Cracker Jack are used to do what?
A. Denial of Service
B. Perform buffer overflows
C. Exploit passwords
D. Hijack sessions

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 34
Correct Answer: C

10: Brute force password attacks involve:
A. Using a predetermined list of passwords.
B. Using people's usernames, first and last names to guess passwords
C. Using a dictionary file to guess passwords
D. Trying every possible password until a successful login

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 36
Correct Answer: D

11: Three basic methods of encryption are:
A. symmetric, asymmetric, hash
B. symmetric, asymmetric, cipher
C. stegnagraphic, hash, symmetric
D. crypt, hash, asymmetric

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 39
Correct Answer: A

12: Which of the following is NOT a method of password cracking?
A. Dictionary attack
B. Hybrid attack
C. Crypt attack

D. Brute force attack

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 42
Correct Answer: C

13: L0phtrack can do all of the following EXCEPT:
A. Crack Unix/Windows passwords
B. Dump password registry
C. Sniff passwords off of the network
D. Has brute force as well as dictionary cracking capabilities

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 45
Correct Answer: A

14: Passfilt.dll provides what type of functionality?
A. Checks passwords to see if they are "crackable"
B. Password checking
C. Password cracking
D. Strong Passwords

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 63
Correct Answer: D

15: Syskey provides what capabilities?
A. Allows 128 bit "strong" encryption
B. Allows for automatic check of bad passwords in the SAM database
C. Verifies passwords are following defined security policy
D. Enforces password policy

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 66
Correct Answer: A

16: The Getadmin exploit is:
A. A denial of service attack that causes an NT machine to crash by using up all of the resources.
B. An attack that performs a very sophisticated set of steps that allow a non-admin. User to gain debug-level access on a system process.
C. An attack that grants normal users administrative rights by adding them to the Administrators group.
D. A denial of service attack that involves sending out of band data to a Windows machine.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 93
Correct Answer: C

17: The Sechole exploit is:

A. A denial of service attack that causes an NT machine to crash by using up all of the resources.
B. An attack that performs a very sophisticated set of steps that allow a non-admin. User to gain debug-level access on a system process.
C. An attack that grants normal users administrative rights by adding them to the Administrators group.
D. A denial of service attack that involves sending out of band data to a Windows machine.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 103
Correct Answer: B

18: The Win nuke exploit is:
A. A denial of service attack that causes an NT machine to crash by using up all of the resources.
B. An attack that performs a very sophisticated set of steps that allow a non-admin. User to gain debug-level access on a system process.
C. An attack that grants normal users administrative rights by adding them to the Administrators group.
D. A denial of service attack that involves sending out of band data to a Windows machine.

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 123
Correct Answer: D

19: How do you protect against the Win Nuke exploit?
A. Change a Windows registry setting
B. Apply appropriate service pack and apply a patch from Microsoft
C. Format hard drive and start over
D. Download and install virus scanning software on the machine

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 129
Correct Answer: B

20: Red button works by using which ports?
A. 137-139
B. 135-139
C. 109-110
D. 20-21

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 136
Correct Answer: A

21: RPC Locator is what type of attack?
A. Denial of Service
B. Buffer Overflow
C. Session hijacking
D. Spoofing

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 146
Correct Answer: A

22: All of the following are UNIX exploits except:
A. Aglimpse
B. Tooltalk
C. Campas
D. Sec hole

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 175
Correct Answer: D

23: What is a CGI?
A. An exploit that runs against web servers
B. A specification for interfacing server executed programs with WWW pages
C. A form of vulnerability found on Unix and NT machines
D. A scripting subset that is executed by the browser and delivered by the server

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 178
Correct Answer: B

24: Which of the following is untrue concerning CGIs?
A. Script is executed by web browser
B. Requested by (usually) unauthenticated client
C. Process has all privileges of the web server that called it
D. Can be a compiled program or script written in a multitude of languages including Perl and C

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 189
Correct Answer: A

25: Snort and tcpdump are examples of what type of program?
A. CGI vulnerabilities
B. Denial of Service tools
C. Sniffers

D. Password crackers

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 222
Correct Answer: C

26: Which is NOT a denial of service attack?
A. Phf
B. Ping of death
C. Land
D. Smurf

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 233
Correct Answer: A

27: ICMP of the TCP/IP protocol suite works at what layer in the OSI model?
A. Transport
B. Data Link
C. Session
D. Network

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 235
Correct Answer: D

28: The following is the signature for what type of attack?

```
10:03:14..6900000 192.168.15.1 > 192.168.20.10: icmp: echo request (frag 11267:1480@0+)
10:03:14..6900000 192.168.15.1 > 192.168.20.10: (frag 11267:1480@1480+)
10:03:14..6900000 192.168.15.1 > 192.168.20.10: (frag 11267:1480@5920+)
10:03:14..6900000 192.168.15.1 > 192.168.20.10: (frag 11267:1480@7400+)
10:03:14..6900000 192.168.15.1 > 192.168.20.10: (frag 11267:1480@8880+)
…..
10:03:14..7400000 192.168.15.1 > 192.168.20.10: (frag 11267:1480@65527)
```

A. Smurf Attack
B. Ping of Death
C. SSPing
D. Land

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 239
Correct Answer: B

29: Which of the following is the three-way handshake for TCP connections?
A. Syn, Ack, Syn-ack
B. Syn, Ack, Fin
C. Syn, Syn-ack, Ack
D. Syn, Syn-ack, Fin

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 270
Correct Answer: C

30: An unusually high amount of half-open sessions is an indicator of what type of attack?
A. Syn flood
B. Fin flood
C. Ack storm
D. None of the above

Location Found: SANS GIAC 4.2 – Computer And Network Hacker Exploits: Page 273
Correct Answer: A

Section III: 30 Questions from Hacker Exploits Day 2

1: All of the following are great ways to gather information EXCEPT:
A. ARIN and whois
B. nslookup
C. ping
D. Search engines

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 15
Correct Answer: C

2: THS-Scan 2.0 is a:
A. Port scanner
B. Sniffer
C. War dialer
D. Password cracker

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 19
Correct Answer: C

3: UDP can best be described as:
A. a stateful, connection-oriented protocol
B. a stateless, connectionless protocol
C. a slow, large protocol
D. a lightweight protocol

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 25
Correct Answer: B

4: Nmap is a:
A. Port scanner

B. Sniffer
C. War dialer
D. Password cracker

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 26
Correct Answer: A

5: Nmap is capable of performing the following types of scans:
A. Syn scans
B. Udp scans
C. RPC scans
D. All of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 27
Correct Answer: D

6: TCP stack fingerprinting is defined as what?
A. Depending on the response from a system, nmap can identify what OS is running
B. Depending on the response from a system, nmap can identify what patch level the TCP/IP stack is
C. The process of traversing the TCP/IP stack to identify any vulnerabilities
D. None of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 29
Correct Answer: A

7: Firewalk is based on what other widely-used utility?
A. Ping
B. Traceroute
C. Nslookup
D. Nmap

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 32
Correct Answer: B

8: Firewalk uses what field in the IP header to traverse the network and determine what ports are open?
A. Sequence Number
B. TTL
C. Fragment offset
D. Options field

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 32
Correct Answer: B

9: Which file do you need to edit on Unix systems to disable services?

A. /etc/inetd.conf
B. /etc/inet.conf
C. /etc/services
D. /usr/local/etc/inetd.conf

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 44
Correct Answer: A

10: To successfully spoof another address, one needs to:
A. Send a syn packet to the destination host, perform a host redirect to receive the syn/ack packet and send the ack packet to the destination host.
B. Send a syn packet to the destination host, perform a denial of service on the real host, and send the Ack packet to the destination host with the correct sequence number.
C. Send a syn packet to the destination host with real ip, destination responds with a syn/ack, and send a ack packet with the spoofed ip address.
D. None of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 53
Correct Answer: B

11: What is source routing?
A. It is an option in IP that allows the source of a packet to specify the path it will take on the network.
B. It is the process of routing IP packets with their source addresses.
C. It is the process of routing IP packets to the source address.
D. None of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 55
Correct Answer: A

12: The following are true about IP fragmentation EXCEPT:
A. One can bypass packet filters in firewalls
B. One can send packets through proxying firwalls
C. One can bypass packet filters in routers
D. One can avoid being discovered by intrusion detection systems

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 59
Correct Answer: B

13: Which of the following are types of fragmentation attacks?
A. Tiny fragment attack
B. Fragment overlap attack
C. Large fragment attack
D. B & C Only
E. A & B Only

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 60
Correct Answer: E

14: Which of the following is a way to prevent IP fragmentation attacks?
A. Install packet filters on all routers and firewalls
B. Install application proxy firewalls
C. Install intrusion detection systems
D. Employ an ICMP ingress packet filter

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 64
Correct Answer: B

15: Using switches in your network is the best method to fight against which tools?
A. Denial of Service Tools
B. Frag Routers
C. Password crackers
D. Sniffers

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 68
Correct Answer: D

16: Hunt is what type of tool?
A. Sniffer
B. Session Hijacker
C. Password Cracker
D. Port Scanner

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 71
Correct Answer: B

17: Which of the following are defenses to session hijacking?
A. SSh or a VPN
B. Use a random sequence number
C. Strong authentication
D. A & B
E. A & C

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 79
Correct Answer: E

18: All of the following are true about DNS cache poisoning EXCEPT?
A. Jizz is a tool to implement DNS cache poisoning
B. Upgrading bind is a good defense to poisoning
C. Split DNS is another good defense to poisoning

D. DNS cache poisoning can cause requests for your website to be redirected to someone else's server

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Pages 82-83, 88
Correct Answer: C

19: What are the following commands accomplishing?
Server: `nc -l -p 4444 < filename`
Client: `nc server 4444 > filename`

A. Downloading a file from the server to the client
B. Uploading a file from the client to the server
C. Creating a port listener on the server on port 4444 which displays the contents of filename and redirects it to the client.
D. None of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 93
Correct Answer: A

20: Which of the following is false concerning netcat?
A. Can scan from any source port
B. Can send malformed ICMP packets
C. Performs TCP and UDP port scanning
D. Performs linear scans or random scans

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 94
Correct Answer: B

21: All of the following are distribute denial of service (Ddos) tools EXCEPT:
A. Targa
B. HTC
C. TFN
D. Trin00

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Pages 104, 107, 113
Correct Answer: B

22: What mechanism is often used to determine session for a user in web applications?
A. Cookies with a session variable
B. Database entries on the web server in conjunction with cookie variables

C. Hidden form elements
D. Http get requests
E. All of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 120
Correct Answer: E

23: All of the following are capabilities of Back Orifice 2000 EXCEPT:
A. Allows for remote control of Windows
B. Gather passwords
C. Packet redirection
D. Create user accounts

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Pages 131-132
Correct Answer: D

24: What is BOTOOL?
A. Reliable ICMP tunneling for BO2K traffic
B. Graphical file viewer and registry editor
C. Allows encryption of BO2K traffic
D. Scripting language for both client and server automation

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 135
Correct Answer: B

25: What is a rootkit?
A. A collection of tools that allow an attacker to gain backdoor access into a system.
B. A tool that allows an attacker to gain root access.
C. A shim that sits off the kernel to collect password information.
D. A program that monitors logins for password information.

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 141
Correct Answer: A

26: Which of the following is true about Knark?
A. Replaces kernel with trojan kernel
B. Replaces system binaries with trojan versions
C. Knark is installed as a loadable kernel module and runs at the kernel level

D. Knark listens on various ports for commands remotely

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 152
Correct Answer: C

27: Remove.c is used to do what?
A. Remove entries in the password file on Unix hosts
B. Remove entries in the /var/run/utmp, /var/log/wtmp, and /usr/adm/lastlog files
C. Reconfigure syslog
D. None of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 168
Correct Answer: B

28: Reverse WWW Shell is an example of what?
A. Denial of service
B. Buffer overflow
C. Trojan
D. Session hijacking

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 172
Correct Answer: C

29: Loki uses what protocol?
A. ICMP
B. DNS
C. UDP
D. All of the above

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 175
Correct Answer: D

30: Reverse WWW Shell uses what protocol?
A. SSL
B. Telnet
C. HTTP
D. UDP

Location Found: SANS GIAC 4.3 – Computer And Network Hacker Exploits II: Page 173
Correct Answer: C

Last Updated: May 29th, 2017

Upcoming Training

SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
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
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event