



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Hacker Tools, Techniques, Exploits, and Incident Handling (Security 504)"  
at <http://www.giac.org/registration/gcih>

## INCIDENT HANDLING

**1 What is the most common error committed by incident handlers?**

- A Failure to document adequately
- B Not acting quickly enough
- C Calling a false alarm
- D

**A CORRECT ANSWER**

**Book 4.1 Page 10**

**2 How would you determine if a NIC is in promiscuous mode on an NT host?**

- A Ifconfig
- B Ipconfig
- C Iputil
- D TCPconfig

**B CORRECT ANSWER**

**Book 4.1 Page 142**

**3 Toneloc is an example of what type of reconnaissance tool?**

- A Sniffer
- B Port scanner
- C War dialer
- D Enumerator

**C CORRECT ANSWER**

**Book 4.1 Page 118**

**4 Outbound traffic to ports 666/6667 on a Unix system is a potential sign of the presence of a:**

- A Sniffer
  - B Trojan horse
  - C Root kit
  - D Back Orifice
- C** CORRECT ANSWER

Book 4.1 Page 113

**5** Which of the following is an example of malicious code?

- A Virus
- B Trojan horse
- C Easter egg
- D All of the above

**D** CORRECT ANSWER

Book 4.1 Page 118

**6** Why would a SysAd perform a backup immediately after a successful restore and operational test?

- A In case of reinfection
- B Appease management
- C For evidence
- D Just cuz' you're paranoid doesn't mean they're not out to get you

**A** CORRECT ANSWER

Book 4.1 Page 90

**7** What generally occurs when you delete a file in most operating systems?

- A Space overwritten
- B Entry is deleted in file system database
- C Drive location is formatted
- D File is erased

**B** CORRECT ANSWER

Book 4.1 Page 205

**8** What is likely the most overlooked phase of the 6-step incident handling process?

- A Containment
- B Lessons Learned
- C Note taking
- D Eradication

**B** CORRECT ANSWER

Book 4.1 Page ??

**9 What is CIRT?**

- A Computer Incident Response Team
- B Computer Incident Recovery Tactics
- C Common Incident Recovery Techniques
- D Computer Inquiry and Response Team

**A** CORRECT ANSWER

Book 4.1 Page 46

**10 Developing and implementing effective computer security policy falls under which of the primary incident handling phases?**

- A Containment
- B Preparation
- C Identification
- D Eradication

**B** CORRECT ANSWER

Book 4.1 Page 34

**11 Which of the following is a critical component of a good contingency plan?**

- A Policy
- B Transportation
- C Documentation
- D All of the above

**D** CORRECT ANSWER

Book 4.1 Page 34

**12 When are the most damaging mistakes typically made in the incident handling process?**

- A Very shortly after identification of an incident
- B During containment
- C In Recovery
- D Eradication

**A** CORRECT ANSWER

Book 4.1 Page 45

**13** Which of the following is critical to preparing successfully for handling incidents?

- A Developing an emergency communications plan
- B Establishing a command center
- C Compiling a jump kit
- D All of the above

**D** CORRECT ANSWER

Book 4.1 Page 52-55

**14** Choose the correct order for the following incident handling activities:

- A Dispatch team – validate incident - secure area – perform backup
- B Secure area – dispatch team – perform backup – validate incident
- C Dispatch team – secure area – validate incident – perform backup
- D Secure area – validate incident – dispatch team – perform backup

**C** CORRECT ANSWER

Book 4.1 Page 75

**15** During recovery, and incident handler should pay keen attention to minimizing the chance for:

- A Reinfection
- B
- C
- D

**C** CORRECT ANSWER

Book 4.1 Page

**16** When is the best time to begin writing a follow-up report for an incident:

- A After the system has been restored and operational for a short period
- B Immediately after recovery
- C Before the next internal audit
- D After validating the incident

**CORRECT ANSWER**

**Book 4.1 Page**

**17 What are the primary phases of incident handling?**

- A Identification-Team Deployment-Containment-Eradication-Recovery
- B Preparation-Identification-Containment-Eradication-Recovery-Lessons Learned
- C Identification-Containment-Recovery-Testing-Lessons Learned
- D Preparation-Team Deployment-Containment-Eradication-Recovery-

**B CORRECT ANSWER**

**Book 4.1 Page 32**

**18 Malicious code exploits can accomplish which of the following?**

- A Capture user IDs and passwords
- B Destroy data
- C Modify audit logs
- D All of the above

**D CORRECT ANSWER**

**Book 4.1 Page 104**

**19 Which of the following would be classified as an incident?**

- A Being probed
- B Opening an infected mail attachment
- C Receiving DoS attack
- D All of the above

**D CORRECT ANSWER**

**Book 4.1 Page Various – focus on importance of probes, 117**

**20 Why would an incident handler run an identified exploit on her/his own system?**

- A To determine what information was gained by the would-be attacker
- B To tests the effectiveness of the exploit
- C Never would, under any circumstances
- D None of the above

**A** CORRECT ANSWER

Book 4.1 Page 121

**21 Information espionage typically is carried out by?**

- A Casual hackers or ankle-biters
- B Insiders
- C Random attackers
- D The competition

**B** CORRECT ANSWER

Book 4.1 Page 129

**22 System audit trails can serve to:**

- A Detect intrusion
- B Identify system errors
- C Assess incident damage
- D All of the above

**D** CORRECT ANSWER

Book 4.1 Page B-2

**23 Expert Witness is:**

- A An intrusion detection system
- B A firewall application
- C A forensics tool
- D A vulnerability scanner

**C** CORRECT ANSWER

Book 4.1 Page 185

**24 Which of the following is a key to success in an Emergency Action Plan?**

- A Documenting thoroughly
- B Act swiftly and decisively
- C Utilize out-of-band communication channels
- D A and B
- E A and C

**E** CORRECT ANSWER

Book 4.1 Page 12-15

**25** In the Detect-React-Defend-Recover emergency action model, at what point should forensics commence?

- A Detect
- B React
- C Defend
- D Recover

**B** CORRECT ANSWER

Book 4.1 Page 26

**26** In the six phase incident handling model, at which point would decisions about notifying law enforcement be made?

- A Containment
- B Eradication
- C Preparation
- D Identification

**C** CORRECT ANSWER

Book 4.1 Page 38

**27** Which of the following are signs of an incident?

- A Numerous unsuccessful logon attempts
- B Denial of service
- C System performance degradation
- D All of the above
- E A and B only

**D** CORRECT ANSWER

Book 4.1 Page 62-63

**28** The initial assessment phase of handling an incident can be likened to what medical procedure?



- A Surgery
- B Triage
- C Pre-Op
- D None of the above

**B** CORRECT ANSWER

Book 4.1 Page 64

**29** At what point in the six-phase incident handling model is the first team deployed?

- A Preparation
- B Identification
- C Eradication
- D Containment

**D** CORRECT ANSWER

Book 4.1 Page 67

**30** Which of the following is a good backup option during containment?

- A Safeback
- B WinZip
- C Drive Duplicator
- D All of the above
- E A and C only

**E** CORRECT ANSWER

Book 4.1 Page 71

**31** What should be the final steps in the containment phase?

- A Changing passwords
- B Definition/certification of trust model
- C Reinstallation of OS
- D All of the above
- E A and B only

**E** CORRECT ANSWER

Book 4.1 Page 80

**32** What should be the first step in the eradication phase?

- A System backup
- B Reinstallation of OS
- C Determine cause of incident
- D None of the above

**C** CORRECT ANSWER

Book 4.1 Page 82

**33** What should be the final step in the eradication phase?

- A System backup
- B Diagnose symptoms
- C Remove cause of incident
- D None of the above

**E** CORRECT ANSWER

Book 4.1 Page 12-15

**34** Who should make decision about restoring affected systems?

- A Incident handler
- B System administrator
- C System owner
- D IS manager

**C** CORRECT ANSWER

Book 4.1 Page 90

**35** Which of the following are key components of follow-up report?

- A Lessons learned
- B Detailed index of forensic evidence
- C Recommended changes
- D A and B
- E A and C

**E** CORRECT ANSWER

Book 4.1 Page 94

**36** Which of the following is a potential sign of espionage?

- A Off-hours access
- B Access violation patters in audit logs
- C Excessive drive space consumption
- D All of the above
- E A and B only

**E** CORRECT ANSWER

Book 4.1 Page 132

**37** Which of the following is a source of audit information?

- A Firewall logs
- B Intrusion Detection System logs
- C Registry
- D All of the above
- E A and B only

**D** CORRECT ANSWER

Book 4.1 Page 228-230

**38** Which of the following is a potential sign of sniffer infection?

- A New port in use
- B NIC in promiscuous mode
- C Disk flashes to rhythm of net
- D All of the above
- E A and C only

**D** CORRECT ANSWER

Book 4.1 Page 142

**39** What potential purposes do system audits service?

- A Identification of intrusion
- B Reducing vulnerability to intrusion
- C Evidence collection
- D All of the above
- E A and C only

**E** CORRECT ANSWER

Book 4.1 Page A7

**40** The Caligula virus locates what key data in the registry?

- A User ID and password
- B Browser security setting
- C PGP key ring
- D All of the above
- E A and B only

**C** CORRECT ANSWER

**Book** 4.1 **Page** 204

© SANS Institute 2000 - 2002, Author retains full rights.

## HACKER EXPLOITS – Part 1

1 What are the three main areas of security that can fall under attack?

- A Confidentiality, Integrity, Availability
- B Confidentiality, Integrity, Access
- C Concurrency Integration Availability
- D Concurrency Integrity Authentication

**A** CORRECT ANSWER

Book 4.2 Page 9

2 A Denial of Service exploit is an example of an attack against:

- A Integrity
- B Availability
- C Authentication
- D Confidentiality

**B** CORRECT ANSWER

Book 4.2 Page 12

3 A tool utilized to gain re-entry to a compromised system is called a:

- A Sniffer
- B Back door
- C Port scanner
- D Root kit

**B** CORRECT ANSWER

Book 4.2 Page 25

4 Taking control of an existing session is an example of what kind of exploit?

- A IP spoofing
- B War dialing
- C Session hijacking
- D Buffer overflow

**C** CORRECT ANSWER

Book 4.2 Page 31

5 How frequently should users change passwords?

- A Monthly
- B Every login
- C Less than the time to brute force-crack the password
- D Whenever an internal audit is scheduled

**C** CORRECT ANSWER

Book 4.2 Page 36

**6** An exploit to gain debug access on an NT system process is:

- A Sechole
- B Fraggle
- C Campas
- D GetAdmin

**A** CORRECT ANSWER

Book 4.2 Page 103

**7** Limiting the processor usage for system users would *help* prevent which of the following exploits?

- A Red Button
- B aglimpse
- C CPU Hog
- D Distributed DoS

**C** CORRECT ANSWER

Book 4.2 Page 117

**8** Blocking port 139 on an NT network would *help* prevent which of the following exploits?

- A WinNuke
- B Red Button
- C Both of the above
- D Neither of the above

**C** CORRECT ANSWER

Book 4.2 Page 129, 135

**9** The only way to restore service to a machine exploited to run at 100% CPU utilization is:

- A Block ports 135, 139
- B Reboot the machine
- C Disconnect from the network
- D Restore system binaries

**B** CORRECT ANSWER

Book 4.2 Page 116, 147

**10** Several attacks exploit CGI. For what does it stand?

- A Computer Generated Imagery
- B Common Gateway Interface
- C Computer Gateway Integration
- D Commonly Generated Information

**B** CORRECT ANSWER

Book 4.2 Page 177

**11** A denial of service attack utilizing large numbers of half-open TCP/IP connections:

- A Win Nuke
- B SYN Flood
- C aglimpse
- D IRIX wrap

**B** CORRECT ANSWER

Book 4.2 Page 269

**12** CVE stands for:

- A Common Vulnerabilities and Exposures
- B Computer Vulnerability Enumeration
- C Common Vulnerability Enumeration
- D Computer Vulnerabilities and Exposures

**A** CORRECT ANSWER

Book 4.2 Page 93

**13** GetAdmin takes advantage of a hole in the Win login process to:

- A Grant debug access to any user on a system process
- B Add a normal user to the administrators group
- C Allow a hacker to authenticate improperly
- D None of the above

**A** CORRECT ANSWER

Book 4.2 Page 93

**14** This exploit causes a Denial of Service attack by manipulating application priority levels:

- A WinNuke
- B Red Button
- C CPU Hog
- D sechole

**C** CORRECT ANSWER

Book 4.2 Page 116

**15** Attacks involving out-of-band data are successful because of:

- A A lack of proper data validation procedures
- B OS simply cannot process all kinds of data
- C Login security holes
- D All of the above

**A** CORRECT ANSWER

Book 4.2 Page 124

**16** Red Button exploits what operating system vulnerability?

- A The Windows login process
- B A hole in the Windows registry
- C Default NT Everyone group permissions
- D Storage of clear text passwords on the server

**C** CORRECT ANSWER

Book 4.2 Page 135

**17** Blocking port 135 on a network's firewall would help prevent what attack(s)?



- A Win Nuke
- B RPC Locator
- C Red Button
- D CPU Hog

**B** CORRECT ANSWER

Book 4.2 Page 146

**18** How does a buffer overflow compromise processing?

- A By sending the wrong data type to a system program
- B By sending too much data to a system program
- C By consuming all the drive space on a server
- D All of the above

**B** CORRECT ANSWER

Book 4.2 Page 160

**19** A flaw in the msconf.dll library in NT allows for which of the following exploits?

- A Win Nuke
- B NetMeeting buffer overflow
- C campas
- D None of the above

**B** CORRECT ANSWER

Book 4.2 Page 159

**20** The following attacks exploit weaknesses in CGI:

- A aglimpse
- B campas
- C IRIX wrap
- D All of the above
- E A and B only

**D** CORRECT ANSWER

Book 4.2 Page 180-217

**21** Which of the following would likely be an effective defense against ToolTalk?

- A Implement a packet-filtering firewall
- B Remain current with OS patches
- C Implement AntiSniff
- D All of the above
- E A and B only

**E** CORRECT ANSWER

Book 4.2 Page 204

**22** IMAPD is what?

- A A backdoor usually in the form of a Trojan horse
- B A remote email service
- C A loadable kernel module
- D All of the above
- E B and C only

**B** CORRECT ANSWER

Book 4.2 Page 208

**23** The IMAPD exploit utilizes which of the following methods?

- A Covert installation as a Trojan horse
- B Buffer overflow
- C Packet sniffing
- D A and C
- E A and B

**B** CORRECT ANSWER

Book 4.2 Page 209

**24** Which of the following would likely be an effective defense against the IMAPD exploit?

- A Implement Intrusion Detection System
- B Filter external IMAP port access utilizing a firewall
- C Strong authentication
- D All of the above
- E B and C

**E** CORRECT ANSWER

Book 4.2 Page 214

**25** IMAPD connects over what port?

- A 53
- B 143
- C 135
- D 139
- E 6667

**B** CORRECT ANSWER

Book 4.2 Page 215

**26** The IRIX wrap exploit utilizes which technique?

- A SYN flood
- B ACK storm
- C Buffer overflow
- D Packet sniffing

CORRECT ANSWER

Book 4.2 Page

**27** Which of the following would likely be an effective defense against the IRIX wrap exploit?

- A Maintain current vendor patches
- B Implement packet-filtering firewall
- C Remove Outbox software from server
- D All of the above
- E A and C only

**E** CORRECT ANSWER

Book 4.2 Page 223

**28** What is ICMP?

- A Internet CounterMeasure Protocol
- B Internet Control Message Protocol
- C Integrated Control Message Protocol
- D Integrated CounterMeasure Protocol

**E** CORRECT ANSWER

Book 4.2 Page 235

**29** The Ping of Death exploit works in what way?

- A Sends out of band data to execute program code
- B Sends an oversized ping packet causing the OS to crash
- C Installs covertly as a Trojan Horse

**B** CORRECT ANSWER

Book 4.2 Page 234

**30** Which of the following would likely be an effective defense against the Ping of Death exploit?

- A Implement Intrusion Detection System
- B Implement packet-filtering firewall or router
- C Maintain current vendor patches
- D All of the above
- E B and C

**E** CORRECT ANSWER

Book 4.2 Page 240

**31** How does the SSPing exploit work to deny service?

- A Sends out of band data to execute program code
- B Sends multiple serial pings causing the OS to crash
- C Installs covertly as a Trojan Horse
- D Sends a series of fragmented, oversized ICMP packets
- E B and C

**D** CORRECT ANSWER

Book 4.2 Page 243

**32** What primary operating system does SSPing affect?

- A Solaris
- B Windows NT
- C Linux
- D OpenVMS
- E AIX

**B** CORRECT ANSWER

Book 4.2 Page 243

**33** How does the Land denial of service attack work?

- A Sends oversized ping packet causing OS to hang
- B Overflows buffer with fragmented data
- C Sends SYN packet with identical target and source address and port numbers
- D A and B

**C** CORRECT ANSWER

Book 4.2 Page 2251

**34** Which of the following might be effective in defending against the Land DoS attack?

- A Implement Intrusion Detection System
- B Implement router filters
- C Maintain current vendor patches
- D All of the above
- E B and C only

**E** CORRECT ANSWER

Book 4.2 Page 256

**35** How does the Smurf DoS attack work?

- A Sends oversized ping packet causing OS to hang
- B Sends ICMP pings to broadcast addresses
- C Sends SYN packet with identical target and source address and port numbers
- D A and B
- E None of the above

**B** CORRECT ANSWER

Book 4.2 Page 259

**36** How does the Fraggle DoS attack work?

- A Broadcasts UDP echo packets
- B Sends ICMP pings to broadcast addresses
- C Sends SYN packet with identical target and source address and port numbers
- D A and B
- E None of the above

**A** CORRECT ANSWER

Book 4.2 Page 263

**37** Which of the following is a symptom of a Smurf DoS attack?

- A Network degradation
- B Large number of ICMP replies
- C Large number of UDP replies
- D All of the above
- E B and C only

**E** CORRECT ANSWER

Book 4.2 Page 264

**38 Hack A Tack utilizes what exploit techniques?**

- A Trojan horse installation
- B Remote machine control
- C Buffer overflow
- D A and B
- E B and C

**D** CORRECT ANSWER

Book 4.2 Page 279

**39 Which of the following is an example of social engineering?**

- A Cracking an encrypted password file
- B Dumpster diving
- C Call help desk for new password
- D All of the above
- E B and C

**E** CORRECT ANSWER

Book 4.2 Page

**40 Which of the following is an encryption technique?**

- A Symmetric
- B Salt
- C Hash
- D A and B
- E A and C

**E** CORRECT ANSWER

Book 4.2 Page 39

## HACKER EXPLOITS – Part 2

1 ARIN, whois, and DNS interrogation are methods for conducting what stage of an exploit?

- A Scanning
- B Enumeration
- C Reconnaissance
- D Covering tracks

**C** CORRECT ANSWER

Book 4.3 Page 15

2 A war dialer allows a would-be hacker to:

- A Enumerate an organization's phone directory
- B Identify modems on a target network
- C Authenticate to a target network
- D All of the above

**B** CORRECT ANSWER

Book 4.3 Page 18

3 Nmap, strobe, and probe are examples of what kind of hacking tool?

- A Port scanners
- B Sniffers
- C Trojan horses
- D War dialers

**C** CORRECT ANSWER

Book 4.3 Page 25

4 Firewalk utilizes which field to walk open ports through a firewall?

- A SYN
- B ACK
- C TTL
- D FIN

**C** CORRECT ANSWER

Book 4.3 Page 32

5 SATAN and Nessus are examples of what kind of security tool?

- A Firewall
- B Port scanner
- C Vulnerability scanner
- D Sniffer

**C** CORRECT ANSWER

Book 4.3 Page 38

**6** Which of the following are types of IP spoofing?

- A Changing IP address
- B Exploiting trust
- C Source routing
- D All of the above

**D** CORRECT ANSWER

Book 4.3 Page 50-55

**7** Island hopping sniffer attacks involve?

- A Using multiple machines to sniff network traffic
- B Moving from machine to machine to find a good place to sniff
- C Accessing off-shore network to direct attacks
- D Sniffing with mobile PCs

**A** CORRECT ANSWER

Book 4.3 Page 67

**13** DNS, used to map internet site names to addresses, stands for:

- A Domain Name System
- B Domain Nomenclature Service
- C Differentiated Naming Service
- D None of the above

**A** CORRECT ANSWER

Book 4.3 Page 81

**14** The TCP handshake process consists of the following steps:



- A SYN-ACK-SYN-ACK
- B SYN-ACK-FIN
- C SYN-ACK-SYN
- D SYN-ACK-ACK-SYN

**A** CORRECT ANSWER

Book 4.3 Page 49

**15** Why is a simple change of address type of IP spoof limited in its potential as an exploit:

- A Responses from target machine will go to the real address used, not the spoofing machine, preventing completion of the TCP connection
- B It does not truly hide the attacker's IP address
- C It is a highly sophisticated technique that is difficult to perform correctly
- D It is not limited, but, rather, allows the hacker easily to establish an interactive session

**A** CORRECT ANSWER

Book 4.3 Page 50

**16** An attacker can accomplish IP spoofing by which of the following means?

- A Exploiting trust relationships between machines
- B Changing her/his IP address manually
- C Source routing
- D All of the above

**D** CORRECT ANSWER

Book 4.3 Page 53-56

**17** An exploit particularly useful in avoiding the attention of IDSs is:

- A DNS zone transfer
- B Session hijacking
- C IP fragmentation
- D Denial of service

**C** CORRECT ANSWER

Book 4.3 Page 59

**18** Probably the single best method of defending against sniffers is:

- A Deploying switched ethernet at key network points
- B Establishing a DMZ
- C Tweak firewall settings
- D Use a packet-filtering router

**A** CORRECT ANSWER

Book 4.3 Page 69

**18** An attacker can prevent an ACK storm when hijacking a session by::

- A Remotely rebooting the source machine in the hijacked session
- B Sending a DoS attack to the source machine
- C Installing a sniffer on the network
- D Cannot be prevented

**B** CORRECT ANSWER

Book 4.3 Page 74

**19** Two excellent defenses against session hijacking exploits are:

- A Session encryption and proxy-based firewalls
- B Proxy-based firewall and packet-filtering router
- C Session encryption and strong authentication
- D Strong authentication and a packet-filtering router

**C** CORRECT ANSWER

Book 4.3 Page 79

**20** A DNS cache poisoning exploit has what effect?

- A Allows attacker to take over an existing session
- B Redirects traffic to an IP address not associated with the URL indicated
- C Causes denial of service
- D All of the above

**B** CORRECT ANSWER

Book 4.3 Page 83

**21** A distributed denial of service attack involves:

- A Denying service to multiple hosts from the same source machine
- B Commandeering numerous machines to deny service on a host
- C Launching a denial of service from an intermediary machine
- D Denying service on a distributed processing system

**B** CORRECT ANSWER

Book 4.3 Page 106

**21** Good defense against distributed denial of service attacks involves:

- A Implement Intrusion Detection Systems
- B Develop good working relationship with ISP
- C Maximize redundancy for critical systems
- D All of the above

**D** CORRECT ANSWER

Book 4.3 Page 115

**22** Which of the following is NOT a denial of service exploit?

- A Syn Flood
- B Smurf
- C WinNuke
- D NetCat

**D** CORRECT ANSWER

Book 4.3 Page 100-103

**23** What kind of exploit brought down Yahoo and Amazon.com recently?

- A Distributed denial of service
- B Back Orifice
- C Worm virus
- D Trojan horse

**A** CORRECT ANSWER

Book 4.3 Page 106

**24** Which of the following exploits can be carried out using Tribe Flood Network 2000?

- A UDP Flood
- B Targa
- C ICMP Flood
- D All of the above

**D** CORRECT ANSWER

Book 4.3 Page 110

**25** Which of the following is NOT a repository for tracking state for authentication in web applications?

- A URL session tracking
- B Cookies
- C Hidden form elements
- D ipconfig

**D** CORRECT ANSWER

Book 4.3 Page 120-121

**26** With Back Orifice, is the Server program component installed on the Victim or the Attacking machine?

- A Victim
- B Attacking
- C Neither – Back orifice has no server component
- D Both

**A** CORRECT ANSWER

Book 4.3 Page 129

**27** What was the infamous port number associated with original Back Orifice?:

- A 135
- B 80
- C 6667
- D 31337

**D** CORRECT ANSWER

Book 4.3 Page 137

**28** Back Orifice is, essentially:

- A An effective enumeration tool
- B A highly sophisticated general utility remote administration tool
- C Usually distributed surreptitiously and installed as a back door
- D ALL of the above

**D** CORRECT ANSWER

Book 4.3 Page 127-140

**29** Though a cross-platform tool, RootKits were originally spied on what operating system?

- A Windows NT
- B AIX
- C SunOS
- D Cp/m

**C** CORRECT ANSWER

Book 4.3 Page 142

**30** Which of the following is NOT likely to be an effective defense against or contingency for RootKits?

- A Known good MD5 hashes of key system files
- B Maximizing root security
- C Tripwire
- D Deploying an application proxy firewall

**D** CORRECT ANSWER

Book 4.3 Page 140-145

**31** RootKits perform which of the following exploits:

- A Backdoor access,
- B Network sniffing
- C Replace key system binaries with modified substitutes
- D All of the above
- E A and B

CORRECT ANSWER

Book 4.3 Page 141

**32** Knark is a RootKit specifically designed for which operating system

- A Windows NT/2000
- B Linux
- C Solaris
- D B and C
- E A and B

**B** CORRECT ANSWER

Book 4.3 Page 152

**33** Unlike traditional RootKits, Knark is a LKM, which means what?

- A That it's a Linux Kernel Module, allowing it to operate specifically on that OS
- B That it's a Loadable Kernel Module, allowing it to operate at the kernel level rather than the application level
- C That it's a Learning Kernel Module, allowing it to replicate itself, replacing good applications
- D None of the Above

**B** CORRECT ANSWER

Book 4.3 Page 151

**34** Which of the following would likely be an effective defense against/contingency for Knark infection?

- A Maximizing root access security
- B Implement Intrusion Detection System
- C Build a monolithic kernel on sensitive systems
- D All of the above
- E A and B only

**D** CORRECT ANSWER

Book 4.3 Page 159-160

**35** Which of the following would likely be an effective defense against/contingency for the ability of attackers to cover their tracks?

- A Use WORM media for logging and auditing
- B Encrypt auditing and logging files
- C Implement Intrusion Detection System
- D All of the above
- E A and B only

**E** CORRECT ANSWER

Book 4.3 Page 171

**36** Reverse WWW Shell utilizes what protocol command to avoid caching to cover its tracks?

- A HTTP Put
- B HTTP Post
- C ICMP echo
- D HTTP Get

**B** CORRECT ANSWER

Book 4.3 Page 173

**37** What is POLP?

- A Principle of Least Privileges – assign only whatever functionality and access is necessary
- B Principle of Lateral Privacy – maintain tight anonymity at all times
- C Policy of Lean Production – deploy only those systems that can be maintained securely

**A** CORRECT ANSWER

Book 4.3 Page 174

**38** Loki pings over which port?

- A 53
- B 6667
- C 21
- D 31337

**A** CORRECT ANSWER

Book 4.3 Page 175

**39** What is the general state of computer security today?

- A The defense is rapidly catching up with the advanced hacker community
- B The hacker community is rapidly catching up with advanced security measures
- C The hacker community is dwindling, attacks getting less frequent
- D The defense is barely keeping ten steps behind the hacker community

**D** CORRECT ANSWER

**Book** 4.3 **Page** 193-195

**40** Which of the following is a contributing factor to the state of system security today?

- A Lack of comprehensive testing prior to implementation
- B Not enough R&D budget
- C Lack of understanding of the severity of the threat
- D All of the above
- E A and C only

**E** CORRECT ANSWER

**Book** 4.3 **Page** 193-195

© SANS Institute 2000 - 2002, Author retains full rights.



# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
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
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
Mentor Session - SEC504	Columbia, SC	Oct 10, 2017 - Nov 21, 2017	Mentor
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	Live Event
Mentor Session - SEC504	Dayton, OH	Oct 23, 2017 - Nov 27, 2017	Mentor
Community SANS Columbus SEC504	Columbus, OH	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Des Moines SEC504*	Des Moines, IA	Oct 30, 2017 - Nov 04, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, Italy	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS New York SEC504*	New York, NY	Nov 06, 2017 - Nov 11, 2017	Community SANS
Mentor Session AW - SEC504	Houston, TX	Nov 06, 2017 - Jan 29, 2018	Mentor
SANS Amsterdam 2017	Amsterdam, Netherlands	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Nov 08, 2017 - Nov 15, 2017	Community SANS
Community SANS Toronto SEC504	Toronto, ON	Nov 13, 2017 - Nov 18, 2017	Community SANS
Community SANS Charlotte SEC504	Charlotte, NC	Nov 13, 2017 - Nov 18, 2017	Community SANS
Pen Test Hackfest Summit & Training 2017	Bethesda, MD	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Detroit SEC504**	Detroit, MI	Nov 27, 2017 - Dec 02, 2017	Community SANS