ECSA v4 Exam Study Guide
By Chui Raymond Chan - Do not Distribute

George is performing a security analysis for Hammond and Sons LLC. His next task will be to test the security of the wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus not work for his needs?

A. Nessus is too loud *
B. Nessus cannot perform wireless testing
C. Nessus is not a network scanner
D. There are no ways of performing a "stealthy" wireless scan

Larry is an IT consultant who works for corporations and governments. He is currently working for the city of Denver, Colorado. Larry plans on shutting down the city's network using a number of BGP routers and zombies he has taken control of over the last few months. What type of attack is Larry planning to carry out?

A. DRDoS *
B. DDoS
C. DoS
D. Smurf

You just passed your ECSA exam a couple of months ago and are about to start your first consulting job running security audits for a financial institution. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks you what methodology will you be using to test the company's network.

A. Microsoft Methodology
B. LPT Methodology*
C. Cisco Methodology
D. Google Methodology

You are working as an IT security auditor hired by a law firm to test whether you can gain access to sensitive information about the company's clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing some passive scans against their system. What tool should you use?

A. Netcraft *
B. Nmap
C. Ping sweep
D. Dig

Bill is the accounting manager for Grummon and Sons LLC. On a regular basis, he has to send PDF documents containing sensitive information outside his company through

email. Bill protects the PDF documents with a password and sends them to their intended recipients. When the IT manager of Bill's company discovers that Bill is only using the password protect feature in Adobe Acrobat, he tells Bill that the password is not enough protection. Why is this?

A. PDF passwords can easily be cracked by software brute force tools*
B. PDF passwords are converted to clear text when sent in email
C. PDF passwords are not considered safe by Sarbanes-Oxley
D. When sent in email, PDF passwords are stripped from the document completely

You are an IT security consultant attempting to gain access to the state of New Hampshire's network. After trying numerous routes of attack, you are still unsuccessful. You decide to perform a Google search for ftp.nh.st.us to see if the New Hampshire's network utilized an FTP site. You find information about their FTP site and from there, you are able to perform a thorough scan of the New Hampshire state network. What type of scan have you just performed?

A. FTP bounce scan *
B. FTP backdoor scan
C. SYN scan
D. RPC scan

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without the knowledge of the IT department. George notices that a few managers are using an SFTP program on their computers as he walks by their offices. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 22 and dst port 22 *
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 23 and dst port 23

Jennifer works at a small law firm in Chicago. Jennifer's work duties take up about three hours of her day, so the rest of the day she spends on the Internet. One of Jennifer's favorite sites is Myspace. One day, Jennifer comes into work and tries to access the Myspace page but is met with a "This site has been restricted" message. Jennifer is upset because she really wants to keep using Myspace to stay in touch with her friends. What service could Jennifer possibly use to get around the block on Myspace at her company?

A. Anonymizer *
B. FTP proxy
C. Hping2
D. HTTrack

After passively scanning the network of a Department of Defense company, you decide to move on to actively scanning the network to find which hosts are alive and what operating systems they are running. You know that the company is very large, so there should be a number of hosts that respond to any scans. You start an ICMP ping sweep by sending one IP packet to the broadcast address of the network, but only receive responses from about five hosts; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only Unix and Unix-like systems will reply to this scan *
B. Only Windows systems will reply to this scan
C. A switched network will not respond to packets sent to the broadcast address
D. Only servers will reply to this scan

Terri works for a security consulting firm that is currently performing a penetration test on a financial institution. Terri's duties include bypassing the firewalls and switches to gain access to the network. From an outside address, Terri sends an IP packet to one of the company's switches with the ACK bit and the source address of her machine. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri's computer *
B. Poison the switch's MAC address table by flooding it with ACK bits
C. Crash the switch with a DoS attack since ACK bits cannot be sent by computers, only switches
D. Macof attack

Michael is the senior security analyst of Kimball Construction Company in Miami, Florida. As part of a yearly security audit, Michael is scanning his entire network to check for vulnerabilities, unknown hosts, and open ports that do not need to be open. Using Nmap, Michael performs an XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Open *
B. Closed
C. Stealth
D. Filtered

You are a security analyst working for a private party out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank's security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of SSH packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Ettercap *
B. Snort
C. Airsnort
D. Ethercap

Fran is a systems administrator working for a large electronics company in the Midwest. She wants to scan her network quickly to find all the hosts that are alive using ICMP ECHO Requests. What type of scan is Fran going to perform?

A. ICMP ping sweep *
B. Smurf scan
C. Ping trace
D. Tracert

John works in an office with about one hundred other employees. John works in the Accounting department, but is very technically savvy. His ex-girlfriend, Hillary, works in the Sales department. John wants to find out Hillary's network password so he can take a look at her documents on the file server. While Hillary is at lunch one day, John logs onto her computer and installs LophtCrack and sets the program to sniff all traffic. John sends Hillary an email with a link to \\FileServer1\sales.xls telling her that the file included the sales for last quarter. What information will John be able to gather from this?

A. Hillary's network username and password hash *
B. The SID of Hillary's network account
C. The SAM file from Hillary's computer
D. The network shares that Hillary has permissions for

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish?

A. Perform a zone transfer *
B. Perform DNS poisoning
C. Send DOS commands to crash the DNS servers
D. Enumerate all the users in the domain

You are a security analyst who has compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. After enumerating the network you discover the Domain Controllers of the company's network. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish?

A. Enumerate domain user accounts and built-in groups *
B. Enumerate MX and A records from DNS

C. Establish a remote connection to the Domain Controller
D. Poison the DNS records with false records

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based in HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive.org and view the HTML code of news.com from three years ago. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal:

<img src=http://coolwebsearch.com/ads/pixel.news.com width=1 height=1 border=0>

What have you found?

A. Web bug *
B. CGI code
C. Trojan.downloader
D. Blind bug

Harold is a web designer who completed a website for ghttech.net about a month ago. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure that site has received so far. Harold navigates to google.com and types in the following search

What will this search produce?

A. All sites that link to ghttech.net *
B. All sites that ghttech.net links to
C. All search engines that link to .net domains
D. Sites that contain the code: link:www.ghttech.net

As part of the reconnaissance you are performing on a network, you use dnstracer to find valuable information. You type in the following command:

What information will this return?

A. The PTR record(s) for 164.58.245.134 *
B. The A record(s) for 164.58.245.134
C. The in-addr.arpa record(s) for 164.58.245.134
D. The host file record for 164.58.245.134

Larry is the network administrator of a Windows environment. Larry uses a sniffing tool called WinDump to monitor traffic on his network. Larry's friend, who works as a network administrator for another company, saw Larry use WinDump one day and really liked its functionality. The only problem is that Larry's friend administrates a Linux

network environment. What equivalent tool could Larry's friend use to monitor network traffic?

A. Tcpdump *
B. Pwdump
C. Httport
D. Xdump

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You do a search for IT jobs on Dice.com and find the following information for an open position:

What is this information posted on the job website considered?

A. Information vulnerability *
B. Competitive exploit
C. Social engineering exploit
D. Trade secret

What is the following command trying to accomplish?

A. Verify that UDP port 445 is open for the 192.168.0.0 network *
B. Verify that TCP port 445 is open for the 192.168.0.0 network
C. Verify that Netbios is running for the 192.168.0.0 network
D. Verify that UDP port 445 is closed for the 192.168.0.0 network

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. List weak points in their network *
B. Show outdated equipment so it can be replaced
C. Use attack as a launching point to penetrate deeper into the network
D. Demonstrate that no system can be protected against DoS attacks

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\repair *
B. %systemroot%\system32\drivers\etc
C. %systemroot%\system32\LSA
D. %systemroot%\LSA

Tom is a systems administrator for a Unix network. He needs to run some brute force attacks on the passwords of his users to ensure that they are abiding by the corporate password policy. Where can Tom find these passwords?

A. /etc/passwd *
B. /drivers/etc/shadow
C. /root/hidden
D. /etc/pwd

You are a security analyst performing a penetration test on a company in the Midwest. After some initial reconnaissance, you discover the IP of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. HTTP Configuration Arbitrary Administrative Access Vulnerability *
B. HTML Configuration Arbitrary Administrative Access Vulnerability
C. Cisco IOS Arbitrary Administrative Access Online Vulnerability
D. URL Obfuscation Arbitrary Administrative Access Vulnerability

What is kept in the following directory?

HKLM\SECURITY\Policy\Secrets

A. Service account passwords in plain text *
B. Cached password hashes for the past 20 users
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

A security analyst is setting up a false survey website that will require users to create a username and a strong password. He sends the link to the site to all the employees of a company. What information will he be able to gather?

A. The employees' network usernames and passwords *
B. Bank account numbers and the corresponding routing numbers
C. The IP address of the employees' computers
D. The MAC address of the employees' computers

Why is it essential that security analysts know Cisco routers inside and out?

A. 75% of enterprise routers are Cisco *
B. 90% of enterprise routers are Cisco

C. 75% of Internet core routers are Cisco
D. 90% of Internet core routers are Cisco

30. Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Reciprocation *
B. Scarcity
C. Friendship/Liking
D. Social Validation

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks, you change the Group Policy to force 14 character passwords. The next week you dump the SAM database from a domain controller and run a password cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes *
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked we local accounts on the Domain Controller

Why is it a good idea to perform a penetration test from the inside?

A. Because 70% of attacks are from the inside *
B. It is never a good idea to perform a penetration test from the inside
C. To attack a network from a hacker's perspective
D. Because 90% of attacks are from the inside

What is the smallest possible Windows shellcode?

A. 800 bytes *
B. 1000 bytes
C. 600 bytes
D. 100 bytes

On Linux/Unix based web servers, what privilege should the daemon service be run under?

A. Something other than root *
B. Root
C. You cannot determine what privilege runs the daemon service
D. Guest

Jim has performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify that the vulnerability test was correct. The second utility actually is able to execute five known exploits against his network that the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives *
B. False positives
C. True negatives
D. True positives

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code actually rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Metamorphic *
B. Polymorphic
C. Oligomorhic
D. Transmorphic

After attending a security seminar on the state of network security, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using a utility mentioned at the seminar, Userinfo, you attempt to establish a null session with one of the servers, and are successful. Why is that?

A. RestrictAnonymous must be set to "2" for complete security *
B. RestrictAnonymous must be set to "3" for complete security
C. RestrictAnonymous must be set to "10" for complete security
D. There is no way to always prevent an anonymous null session from establishing

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located in a subnet that resides deep inside his network. After analyzing the sniffer's logs, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk sets all packets with a TTL of one *
B. Firewalk sets all packets with a TTL of zero
C. Firewalk cannot be detected by network sniffers
D. Firewalk cannot pass through Cisco firewalls

Where would you find a list of well known ports on your Windows Server 2003?

A. %systemroot%\system32\drivers\etc\services *
B. %systemroot%\system32\services
C. %systemroot%\system32\WBEM\services
D. %systemroot%\drivers\etc\services

An "idle" system is also referred to as what?

A. Zombie *
B. PC not connected to the Internet
C. PC not being used
D. Bot

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Windows computers are constantly talking *
B. Linux/Unix computers are constantly talking
C. Linux/Unix computers are easier to compromise
D. Windows computers will not respond to idle scans

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port, what will be the response?

A. 31401 *
B. 31402
C. 31399
D. The zombie will not send a response

If an attacker's computer sends an IPID of 31400 to a zombie computer on a closed port, what will be the response?

A. The zombie computer will not send a response *
B. 31401
C. 31400
D. 31402

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using NMAP, of a user connected to his web server. Why will Jonathan not be successful?

A. HTTP does not keep a constant session *
B. Only an HTTPS session can be hijacked
C. Only FTP traffic can be hijacked
D. Only DNS traffic can be hijacked

How many possible sequence number combinations are there?

A. 4 billion *
B. 320 billion
C. 1 billion
D. 32 million

You have SNMP set up in multiple offices of your company. Your SNMP software manager is not receiving data from the other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should be open for SNMP to talk properly? (Select 2)

A. 162 *
B. 161 *
C. 389
D. 445

Harold is the senior security analyst for a law firm on the East coast. He wants to test the security of his company's web pages, so he decides to use Form Scalpel from an outside connection through a proxy server over HTTPS. What will be the results from Harold's test?

A. He will be able to extract all the forms from the pages *
B. Form Scalpel will not work over an HTTPS connection
C. Form Scalpel will not work through a proxy server connection
D. Form Scalpel will extract all javascript and perl code

In Linux, what is the smallest possible shellcode?

A. 24 bytes *
B. 8 bytes
C. 800 bytes
D. 80 bytes

At what layer of the OSI model do routers function on?

A. Three *
B. Four
C. Two
D. Five

A packet is sent to a router that does not have the packet's destination address in its route table, how will the packet get to its proper destination?

A. Gateway of last resort *
B. Border Gateway Protocol
C. Root Internet servers
D. Reverse DNS

Kim is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF *
B. UDP
C. BPG
D. ATM

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf *
B. Trinoo
C. Fraggle
D. SYN flood

You are monitoring your internal network while a security consulting firm attempts various means of network intrusion from the outside. Using ethereal, you notice a large amount of traffic on TCP ports 16660 and 65000. What tool is the consulting firm attempting to use?

A. Stacheldraht *
B. Trinoo
C. TFN 2K
D. Beast

After undergoing an external IT audit, George found out that his network was vulnerable to DDoS attacks. What countermeasure could he take to prevent DDoS attacks?

A. Disable direct broadcasts *
B. Enable direct broadcasts

C. Disable BGP
D. Enable BGP

You are testing to see if your network is susceptible to ARP poisoning. You set this up by redirecting packets between two hosts to travel through your computer. You set up the packets to use your MAC address. After a short time, both hosts become unresponsive and freeze up completely. What do you need to do to prevent this?

A. You must retransmit the packets to their intended destinations *
B. You must force the packets to transmit to the hosts MAC addresses
C. You must force the packets to send to your IP address first, then to the hosts' IP addresses
D. You must retransmit the packets through the broadcast address of your computer first

Your company's network just finished going through a SAS 70 audit. This audit found that overall, your network is secure, but there are some areas that need improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Change the default community string names *
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Block all internal MAC address from using SNMP

Victor, who owns a large ISP in Texas, wants to make sure that his company's infrastructure is as secure as possible. He hires an outside security consulting firm that performs tests on his routers. The first test they perform is an attempted DoS attack against his routers' BGP implementation. Fortunately, the DoS attack is not successful. What attempted attack did the consulting company perform?

A. Fuzzing *
B. Blurring
C. Smurfing
D. Ruffing

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router *
B. More RESET packets to the affected router to get it to power back up

C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Paulette works for an IT security consulting company that is currently performing an audit for the company ACE Unlimited. Paulette's duties include logging in to all the company's network equipment to ensure the IOS versions are up to date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client that changes need to be made. From the screenshot, what changes should the client company make?

A. Remove any identifying numbers, names, or version numbers *
B. The banner should have more detail on the version numbers for the network equipment
C. The banner should not state that only authorized IT personnel may proceed
D. The banner should include the CISCO contact information as well

What technology changes all source IP addresses of every packet with its own address before sending out?

A. NAT *
B. MAC filtering
C. AMT
D. Anonymizer

What will the following command accomplish?

A. Test ability of a router to handle over-sized packets *
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to asses the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. By turning off what feature would eliminate the ability to easily enumerate this information on your Cisco routers?

A. Cisco Discovery Protocol *
B. Border Gateway Protocol
C. Broadcast System Protocol
D. Simple Network Management Protocol

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. CVE *
B. IANA
C. APIPA
D. RIPE

Software firewalls work at which layer of the OSI model?

A. Data Link *
B. Network
C. Transport
D. Application

Why is a static packet filter firewall not as secure as other types of firewalls?

A. They do not look into the packet past the header information *
B. They cannot restrict IP packets based on their source
C. They cannot restrict IP packets based on their destination
D. They cannot look into the packet at all

After attending a security class, William decides to set up a dual-homed proxy for the network of his small business. He installs an extra network card on his computer, creates ACL rules, and enables packet forwarding. William also turns on a sniffer to monitor traffic on his new proxy. He quickly notices that source IPs he added to his ACL are still able to send to his network and through his proxy. Why is William seeing this result?

A. Packet forwarding should be disabled *
B. ACL rules should not be used with a proxy
C. Only one network card should be used for a dual-homed proxy
D. Dual-homed proxies need at least three network cards, two for functionality and one for monitoring

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers in his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold's needs?

A. Application-level proxy firewall *
B. Packet filtering firewall

C. Circuit-level proxy firewall
D. Data link layer firewall

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow in connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Statefull firewall *
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Packet filtering firewall

After undergoing a security audit, it was suggested that a hardened computer be placed in the DMZ to run firewall software. What is this hardened computer called?

A. Bastion host *
B. Perimeter host
C. Bastion firewall
D. Perimeter firewall

At what layer of the OSI model does a screened router function on?

A. Network layer *
B. Session layer
C. Data link layer
D. Physical layer

For security reasons and to conserve the number of public IP addresses owned by his company, Jason uses NAT to translate the private IPs on his internal network to a private IP. Jason decides to use 192.169.0.0 through 192.169.255.255 for his internal IPs. Jason's company decides to pay for a security audit. Why would the security audit company recommend that Jason change his internal IP address scheme?

A. His IP scheme does not fall under RFC 1918 *
B. His IP scheme does not fall under RFC 19872
C. His IP scheme includes too many Class C networks
D. His IP scheme includes too many class B networks

After passing her ECSA exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. NAT does not work with IPSEC *
B. NAT does not work with statefull firewalls

C. IPSEC does not work with packet filtering firewalls
D. Statefull firewalls do not work with packet filtering firewalls

What is the target host IP in the following command?

A. 172.16.28.95 *
B. 10.10.150.1
C. Firewalk does not scan target hosts
D. This command is using FIN packets, which cannot scan target hosts

What operating system would respond to the following command?

A. FreeBSD *
B. Windows 95
C. Windows XP
D. Mac OS X

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Real-time anomaly detection *
B. Pattern matching
C. Signature-based anomaly detection
D. Statistical-based anomaly detection
==========
Tyler is a licensed penetration tester who just signed a contract with Anytime Productions, an entertainment company based out of Hollywood. Tyler has been asked by the company to perform security audits at all of their 15 offices spread throughout the United States. Tyler has no prior knowledge about any of the company's networks. What type of penetration testing is Tyler going to perform?

A. When a penetration tester is not informed or told about a network that will be tested, that test is called a grey-box test
B. Tyler is going to perform a black-box test since he does not know anything about the networks *
C. since Tyler has no information about the company's systems; this would be called a white-box test
D. This method of penetration testing is referred as an orange-book test since Tyler does not know anything about the networks
---

Madison is the IT director for Lincoln Financial, an investment company based out of Seattle. Madison's company just underwent an external information systems audit and they passed every test with flying colors. Since she has proven herself to the executives, she wants to convince them to allow her to implement wireless throughout the office. Their main concern is that the wireless network would be too slow to run all the network-based applications they run. Madison assures the executives that if they use 802.11n, there will be plenty of bandwidth. What is the maximum raw data rate available in 802.11n?

A.100 Mbps is the maximum data rate available when using the wireless standard 802.11n
B. If they choose to use 802.11n, the maximum data rate available is 54 Mbps
C. Since the maximum data rate available in 802.11n is only 2.4 Mbps, Madison should recommend this as a solution
D. The maximum data rate available in 802.11n is 600 Mbps *

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and "zombies". What type of Penetration Testing is Larry planning to carry out?

A. DoS Penetration Testing
B. Firewall Penetration Testing
C. Router Penetration Testing *
D. Internal Penetration Testing

Zane is a licensed penetration tester working as a network administrator for a large car rental company in Miami. Zane is currently performing his annual security audit against the company's entire network. Zane is plugged into a port inside his company and is using Macof to flood the ARP cache of a network switch. If this MAC flooding technique works, what will happen to that network switch?

A. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch
B. Zane should never perform this type of attack on a production switch since it would turn the switch off completely, disrupting network traffic
C. The switch will drop into hub mode if the ARP cache of the switch is successfully flooded *
D. If the ARP cache is flooded the switch will drop into pix mode making it less susceptible to attacks

---

Thompson is a licensed penetration tester working on a two-month contract for Tyler Associates, a marketing firm based out of Dallas. Thompson was asked to first examine and audit the company's website to see how secure it is. Thompson performs searches and research on the Internet for records referring to the company. Thompson was able to find an article on a national news website that pointed back to the company's site. From the article's title, it appeared that there was a data leak at the company a couple of months

ago that led to customer information being stolen. When Thompson clicked on the link, it said that the page could not be found. Where can Thompson go to that might have an old record of what the company's website used to look like?

A. Thompson can perform the following search on Google: rewind.org:"name of company's website" to see past versions of the website
B. Thompson can go to archive.org to see past versions of the website *
C. Whois.com is a very useful website when looking for past versions of a website
D. If Thompson wants to see past versions of the website; he can go to the Library of Congress since they archive websites as well as books

---

George passed his ECSA/LPT exam about 6 months ago and now is about to start his first external penetration test for a company. Before any testing can begin, the company has asked George to sign an agreement that outlines the framework for his external and internal testing. This agreement ensures that there is a common understanding of the limitations, constraints, liabilities, and indemnification considerations prior to the tests. What has the company asked George to sign?

A.George has to sign a non-disclosure clause, which creates the common understanding of limitations, constraints, and liabilities between George and the company
B. George has been asked by the company to sign a mea culpa clause, outlining the limitations, constraints, and liabilities of the test
C. The company has asked George to sign the rules of behavior *
D. The ISO 27002 title clause is what the company has asked George to sign, outlining all restrictions to the test

---

Kyle is the chief network security analyst for Yertas Shipping, a logistics company based out of San Francisco. Kyle is also a licensed penetration tester. Kyle is working from a laptop at a WiFi hotspot performing Nessus scans against his company's network trying to see where any weaknesses might be. Kyle finds that the built-in tests are not enough, so he wants to create his own custom security tests with Nessus. What can Kyle use to create his own custom tests for Nessus?

A. Kyle can use NASL, the scripting language built into Nessus, to create his own custom scripts *
B. There is a built-in Nessus scripting language called STAR that will allow Kyle to create his own custom scripts
C. Nessus-Perl is a scripting language that can be used to create custom Nessus scripts
D. Kyle should use the scripting language NSPT, which is a built-in native language for Nessus

---

To test your website for vulnerabilities, you type in a quotation mark (') for the username field. After you click Ok, you receive the following error message window:

Comments

What can you infer from this error window?

A. The user for line 3306 in the SQL database has a weak password
B. The quotation mark (‘) is a valid username
C. SQL Injection is not possible
D. SQL Injection is possible *

Cylie is a licensed penetration tester currently working on contract for Greyson Team Builders, a building contractor company based out of Dallas. Cylie has set up a network probe on the network perimeter to analyze traffic coming into and going out of their network. Cylie looks at the log files and notices an enormous amount of ICMP traffic with the type field of 8.

What does this ICMP type field indicate?

A.The type 8 field in the ICMP packet means that the host is saying whether it is open or closed
B. From this type field, Cylie can infer that the Ping packet is performing an echo reply
C. It indicates that the host keep-alive message is being sent
D. The type 8 field means the ICMP packet is performing an echo request *

Gerald is a pen tester working on contract to audit and test the network of the New York Lottery. Under new state laws, the lottery must undergo an external audit at least once a year. According to the lottery, the most important function they carry out is the nightly drawing of numbers for all their games. This process must measure up to the most stringent set of guidelines and rules; otherwise all players would loose faith in the lottery itself. One way the lottery accomplishes this is with the use of MD5 checksums. Reports are printed out before each drawing to ensure that all numbers balance. On these pre-draw reports there is a checksum number. This checksum must exactly match the checksum on the report that is ran after the drawing to ensure that nothing was tampered with or changed.

What principle is being used here by the lottery to ensure reliability?

A. Since the drawings are such a vital function to the lottery, they must ensure the availability of the reports by using the checksums
B. The authorization of those with access to the reports is being verified by using MD5 checksums before and after the drawings
C. The MD5 checksums ensure the confidentiality of the data being used
D.The principal of integrity is being used here, verifying that no data has been changed *

Lyle is a licensed penetration tester working as a network administrator for Jacobson & Associates. Lyle has been asked by his supervisor to audit the network of a partner company on the other side of town. Through some Nessus scans, Lyle is able to see that the company is running an FTP, web, and email server on a publicly accessible IP subnet. Through vulnerabilities on the web server, Lyle is able to execute some arbitrary code and gain administrative access on the server. Lyle then tries to find other workstations or servers on the same subnet, but the scans do not turn up any results.

What scheme has the partner company implemented to separate the FTP, web, and email servers?

A. An implementation of NAT was used to hide internal IP's and separate the public facing computers
B. An RRAS solution was used to route the networks separately to keep the internal IP's hidden
C. The partner company has implemented a DMZ which separates the public facing computers from the internal ones *
D. The scheme used by the partner company was to implement PAT to hide internal IP's and separate the public facing computers

---

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room.

What type of attack has the technician performed?

A. Tailgating *
B. Man trap attack
C. Fuzzing
D. Backtrapping

Simon is a licensed penetration tester working under contract for the state of Oregon. He has been hired on to perform network audits for every state agency. Through some social engineering, Simon was able to discover that the Oregon department of transportation uses a Citrix server to connect remote users to their main office. If Simon wanted to scan the agency's network for servers using Citrix, how could he accomplish that?

A. Simon needs to search for port 5900 to find servers running Citrix

B.Since Citrix runs on TCP port 389, Simon would need to scan the servers for that port to see which ones are running that service
C. Simon can tell which servers are running Citrix if he can successfully connect to their IPs on port 6250
D.To scan the agency's network for Citrix servers, Simon needs to search for port 2598 *

Heather is a licensed penetration tester working on contract for the city of Miami for 6 months. Heather has performed a number of tests against their network and now is reviewing their IT policies and procedures. Heather has commended them for their procedures when it comes to logging and backing up their log files. She has noticed that they have automatic processes that backup their SQL databases and transaction log files on a production server and restore them onto a standby server. What is this process called?

A.Backing up SQL databases and log files and restoring them to a standby server is called log shipping *
B. Log parsing is what this process is called
C. This process is called transact-restore
D. This procedure when carried out in this manner is called backlogging

---

Blake is a licensed penetration tester working as the chief information officer for the California Lottery. Blake has been asked to set up an internal IIS web server on a Windows 2003 Server machine to host an Intranet for the agency. When Blake sets up IIS with the default configuration, where will the log files be sent to for the web service?

A. C:\Windows\system32\LogFiles\W3SVC1 is the default logging directory for IIS *
B. The log files will be saved to C:\Windows\inetsrv\LogFiles\W3SVC1 which is the default for IIS
C. As with all events on Windows 2003 server, the log files will be sent to C:\Windows\system32\inetsrv\W3SVC1
D.Blake will need to look for the IIS log files in C:\Program files\inetsrv\LogFiles\W3SVC1 since that is the default

---

Jayson is the chief network security analyst for Simonton Incorporated, a large investment form with offices all over the world. Jayson is using a tool that simulates an attack against his company's website. Jayson runs Wireshark to capture and display the traffic to and from the website. If Jayson wants to display just HTTP request packets, what filter should he use in Wireshark?

A.There is no specific filter in Wireshark that will only display HTTP request packets. He must sort those packets out by hand.
B.The tshark.timerequest filter is the correct filter to use if he wants to display HTTP request packets
C. Jayson should use the http.request filter to see HTTP request packets *
D. The filter in Wireshark that will display HTTP request packets is the get.request filter

---
Xavier is a licensed penetration tester who works for Getright Technologies, an IT security consulting firm based out of Boston. Xavier and a team of consultants have flown to St. Louis to perform a complete external audit on a company. This company, before any testing can begin, asks that Xavier and his team sign a legal document that prevents them from talking about any sensitive information they might find in the testing process. What has the company asked Xavier and his team to sign?

A. In order to proceed with the tests, Xavier and his team were asked to sign an ascension clause
B. A FERPA document, otherwise known as a closed-lip agreement, was what the company asked Xavier and his team to sign
C. Xavier has been asked by the company to sign a Habeas corpus document, specifying how Xavier and his team cannot release the sensitive information found in the test
D. The company has asked Xavier and his team to sign a NDA document *

What does the following command trying to accomplish?

C:\> nmap -sU -p445 192.168.0.0/24

A.Verify that UDP port 445 is closed on 192.168.0.0 network
B.Verify that TCP port 445 is open on 192.168.0.0 network
C.Verify that NETBIOS is running on 192.168.0.0 network
D.Verify that UDP port 445 is open on 192.168.0.0 network *

Travis is the owner of an IT security company and is also a licensed penetration tester. Travis' company has been contracted by the city of Cleveland to audit the networks of every school in the city's district. Travis and his company usually base their testing on the different regulations that a hiring company falls under. What regulatory act should Travis' company use to measure the schools against?

A. If Travis' company wants to base their testing on the specific regulation that applies to this school district, they should use the FERPA act *
B.Since Travis' company will be testing schools, the SOX act is the primary regulation that they should be measured against
C.Travis' company needs to use the Gramm-Leach-Bliley act to measure the schools against
D.The HIPPA act, which regulates education and educational institutions, should be followed when testing the schools
---
Travis is the chief security analyst for a large construction company in Memphis. After undergoing a recent IT security audit, Travis' company was told to implement more security measures if they wanted to become ISO certified. Travis was told that he needed a network-based IPS to monitor and block traffic if needed. Travis does not have money

in his budget for any commercial products, so he decides to use Snort. What Snort mode should Travis run to block traffic coming into his network?

A. Travis should run Snort in inline mode to block traffic coming into his network *
B If Travis wants to block traffic and he wants Snort to be network based, he should run Snort in NIDS mode
C.Travis would have to run Snort in core-wall mode
D.Snort's pass-through mode would be able to accomplish what Travis needs

---

You are performing a security analysis of a company's website, running on IIS 6.0, which contains over 200 web pages. You use HTTrack to pull all the pages and files to your local computer for examination. After examining all the images and javascript files, you pour through the html code on each and every page. On a contact page, you find the following code that you believe should not be there:

<a href="shell:cache\..\..\Local Settings\temp\install.exe">

What is the purpose of this code?

A.Open up a command shell that allows install.exe to run from the web server ***
B. Execute install.exe in the profile of any user that clicks on the link
C. This code will do nothing since IIS 6.0 will stop this from executing
D.Copy install.exe from the company's web server to the local user that clicks on the link

---

Bill is a licensed penetration tester working as the chief security analyst for On The Move Incorporated, a car rental company based out of Kansas City. Bill is currently performing an audit on all company networks in each office throughout the United States. Bill did not let any of the Network Administrators of the offices know that this audit was occurring so he could get a better measure of their network's security. Bill begins scanning what appears to be a DMZ of the office in Kansas City. From the scan, Bill can see ports listening for SFTP, web, and email traffic which is normal. But Bill also finds another machine listening on port 3389, which infuriates him since he has told all the Network Administrators that this port is not allowed to be open.

Why would Bill be angry about finding out this information?

A. Bill is most likely angry because TFTP runs on port 3389
B.Windows Messaging runs on port 3389, which transfers data in clear text
C. Port 3389 is used by SNMP which is inherently insecure, especially when used in a DMZ
D.Bill is angry because RDP runs on port 3389 and it is not secure to have that open in a DMZ *

Cindy is an IT consultant currently working on-site at Hesterman & Associates, a large law firm in Dallas. Hesterman & Associates has hired Cindy to perform an external IT audit so that they can become ISO 27001 certified. After performing some footprinting and passive scanning steps, she is able to log on to one of the company's servers to find out some more information.

What should Cindy do to find out all the ports the server is listening on?

A. Cindy should open a command window and type in: netstat –an *
B. Cindy needs to open a telnet session and type in: netcat –an
C. She should open a command window and type in: finger –an
D. On the company's servers, Cindy needs to type in CMD at the Run line and type in: tracert –r

---

Henry is a network administrator for Teryson Incorporated, a shipping company based out of Chicago. Henry is preparing his network for an external audit that will take place in one month. Henry's company uses VoIP phones throughout the office which are very feature-rich, but pose a security threat if not protected. Henry decides to shut off all ports from his internal subnet to another subnet that contains his servers, except for the standard SIP ports. After doing this, all the IP phones are not able to download the custom configuration that was set up and available on the VoIP server. Henry checks his firewall logs and sees that the phones are trying to connect to the VoIP server using TFTP to get the configurations.

What must Henry do to allow traffic to pass between the subnets so that the phones can download the necessary configuration files?

A. He needs to disable NAT on the border firewall so the subnets can talk to each other
B. Henry must open UDP port 69 on his firewall in order for the phones to get the configuration files *
C. An IPSEC tunnel using UDP port 23 needs to be created
D.UDP port 21 needs to be open on the firewall so the configuration files can get to the phones

---

Sharon is about to begin penetration tests against a manufacturing company's network that hired her on for a one year contract. Throughout each step of her test, she must document meticulously what actions she takes. Sharon attempts to break into some of the network's devices using an SNMP hack. In her documentation, what TCP/IP layer should she write down as being attacked by this SNMP hack?

A. SNMP exists on the transport layer, so that is the layer she should write down the attack as occurring
B. SNMP normally uses the application layer, but SNMP hacks must occur on the Internet layer

C. Sharon should document that this attack occurs on the application layer *
D. She should write that the attack occurs on the network access layer

---

Simon is studying for his ECSA/LPT test and is having difficulty with certain topics. Simon is a network administrator at his job and thus does not have to write or program at all. The ECSA/LPT section on exploits has a large amount of coding and scripting languages, so Simon is struggling. Simon cannot figure out or understand why it repeatedly states that Linux is easier to write exploits for than Windows. Why is it easier to write exploits for Linux?

A. It is easier to write exploits for Linux because the shellcode for Linux can be as small as 24 bytes *
B.Shellcode for Windows is only written in a proprietary Microsoft language, thus making it harder to exploit than Linux
C. The larger the shellcode, the easier and operating system is to exploit. Since Linux shellcode can be as large as 800 bytes, it is easier to exploit than Windows
D.Since the shellcode for Linux is only written in C++, it is easier to exploit

---

Michael is a certified penetration tester working on contract with the US Department of Defense. Michael has been hired on to test all the internal and external websites that the department hosts. Michael performs a number of Google searches against their sites. When Michael tries to navigate to the specific pages he finds, he keeps getting an HTTP/1.1 error page with message code of 407.

What does this specific error message mean?

A. Michael can see from the error message that the website cannot be found
B. This means that proxy authentication is required *
C. This error means that the page requires a client certificate
D. This tells Michael that the page must be displayed with a high-security web browser

---

Rita is a licensed penetration tester working as the senior security analyst for Mytime Incorporated, an ISP based out of Seattle. Rita has been asked to travel to one of the company's branch offices to perform a network security audit. Rita takes her laptop and plugs it into a port inside the office. Right away she is able to get an IP address apparently from the office's DHCP server. Rita starts up Wireshark and is immediately able to sniff large amounts of traffic. Rita stops the capture, examines the logs, and is able to see numerous packets being sent around to the MAC address 01:00:0C:CC:CC:CC. What can she deduce from this MAC address?

A. She can tell that they are using Cisco routers *
B.Routers running in hub mode normally use this specific MAC address
C.If network equipment such as routers and switches are seen sending out packets with the source MAC address as seen here, they are susceptible to ARP cache poisoning
D.From this specific MAC address, Rita can deduce that they are using Juniper routers

---

Tyler is a licensed penetration tester who just signed a contract with Anytime Productions, an entertainment company based out of Hollywood. Tyler has been asked by the company to perform security audits at all of their 15 offices spread throughout the United States. Tyler has no prior knowledge about any of the company's networks. What type of penetration testing is Tyler going to perform?

A.When a penetration tester is not informed or told about a network that will be tested, that test is called a grey-box test
B. Tyler is going to perform a black-box test since he does not know anything about the networks *
C. Since Tyler has no information about the company's systems; this would be called a white-box test
D. This method of penetration testing is referred as an orange-book test since Tyler does not know anything about the networks

---

Madison is the IT director for Lincoln Financial, an investment company based out of Seattle. Madison's company just underwent an external information systems audit and they passed every test with flying colors. Since she has proven herself to the executives, she wants to convince them to allow her to implement wireless throughout the office. Their main concern is that the wireless network would be too slow to run all the network-based applications they run. Madison assures the executives that if they use 802.11n, there will be plenty of bandwidth. What is the maximum raw data rate available in 802.11n?

A. 100 Mbps is the maximum data rate available when using the wireless standard 802.11n
B. If they choose to use 802.11n, the maximum data rate available is 54 Mbps
C. Since the maximum data rate available in 802.11n is only 2.4 Mbps, Madison should recommend this as a solution
D. The maximum data rate available in 802.11n is 600 Mbps *

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are constantly talking
B. Windows computers are constantly talking *
C. Windows computers will not respond to idle scans
D. Linux/Unix computers are easier to compromise

Victor is a licensed penetration tester working on contract for a large financial institution in Miami. After signing the legal agreements for the testing he will perform, Victor examines the security policies that are currently in place at the company. To his surprise, the company actually has an Internet and remote users policy, but it is the most lax he has ever seen. The policy states that there are no restrictions on Internet usage and that anyone in the company can gain remote access. What is this type of policy called?

A. A permissive policy, as seen here, is essentially wide open
B. This type of policy is called an all-inclusive policy
C. This is called a promiscuous policy since it is essentially wide open *
D. Many smaller companies without the financial resources choose to use this type of policy; a prudent policy

---

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and "zombies". What type of Penetration Testing is Larry planning to carry out?

A. DoS Penetration Testing
B. Firewall Penetration Testing
C. Router Penetration Testing *
D. Internal Penetration Testing

Sally is a licensed penetration tester that is about to begin auditing the network security for a bank in central Michigan. Sally has to make a presentation to the Executives explaining what tasks will be carried out and why. Sally also shows them the risk involved when referring to information and assets. The formula she shows them is:

R = A X T X V

In this formula, what does the "T" stand for?

A.The vulnerable time span of an information asset in regards to risk
B. Perceived targets is represented by the "T" when calculating risk
C. The "T" stands for perceived threat *
D. A company or organization's information assets

Jacob is the network administrator for his company, a large investment firm based out of Miami. Jacob wants to ensure that his company is as secure as possible, so he decides to hire an outside IT consulting firm to perform some penetration tests next month. Before that company performs their tests, Jacob wants to secure the network as much as possible, according to industry standards.

What standard for information security management could Jacob follow to help prepare for the upcoming penetration test?

A.There is no defacto standard for information management security, so he should rely entirely on the external company
B. Jacob should read and follow the ISO 27002 standard for information management to prepare for the upcoming penetration test ***
C.The ISO 27000 regulation is what Jacob needs to adhere to in order to prepare for the tests

D.If Jacob wants to prepare his company; he should purchase the ISO 9000 standard which is the blanket standard for all information systems

---

Lori is a pen tester working for Yertas Associates, an IT consulting firm out of Austin, Texas. Lori is currently working on contract at a manufacturing company in Dallas, ensuring that they are compliant with all necessary regulations and standards. The first step that Lori carries out in a pen test is to ensure the company has all the processes in place that properly recognize the identity of an individual when he or she attempts to gain access to any systems.

What is this first process that Lori checks on?

A. The first process that Lori checks is the authentication of individuals before access to systems is granted *

B.She checks to make sure that the users are authorized to gain access to the company's systems

C.Lori checks the confidentiality of the users' IDs to ensure that sensitive information is not leaked

D. The availability of a users' account, whether it is active or locked

---

Tyler is a licensed penetration tester helping a company write signatures for a Snort node they placed internally that captures all mirrored traffic from their border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?

alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg: "BACKDOOR SIG - SubSseven 22"; flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;)
alert

A. Packets that contain the payload of BACKDOOR SIG - SubSseven 22 will be flagged

B. The payload of 485 is what this Snort signature will look for

C. Snort will look for 0d0a5b52504c5d3030320d0a in the payload *

D.From this snort signature, packets with HOME_NET 27374 in the payload will be flagged

---

You are an IT security consultant attempting to gain access to State of New Hampshire's network. After trying numerous routes of attack, you are still unsuccessful. You decide to perform a Google search for ftp.nh.st.us to check if the New Hampshire's network utilized an FTP site. You find information about their FTP site and from there; you are able to perform a thorough scan of their network. What type of scan have you just performed?

A. SYN scan

B. FTP bounce scan *
C. RPC scan
D. FTP backdoor scan

Why is it important to mention ROI when presenting executive report findings of a security analysis?

A. ROI has nothing to do with a thorough security analysis report
B. Executives will not spend money unless there is a return on their investment
C. There is no need to mention ROI in an executive report since that should be reserved for a financial report
D. There is no need to mention ROI in an executive report since that should be reserved for a technical report

---

Jennifer works for a small law firm in New York city. Jennifer spends too much time on the Internet. Jennifer's favorite sites are Myspace and YouTube. One day, Jennifer comes to work and tries to access Myspace page but is met with "This site has been restricted" message. Jennifer is upset because she really wants to keep using Myspace to stay in touch with her friends.

What service could Jennifer possibly use to get around the block on Myspace at her company?

A. Hping2
B. Anonymizer *
C. HTTrack
D. FTP proxy

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked *
C. Port Unreachable
D. Protocol Unreachable
