Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://de.fast2test.com

Anbieter der Studienmaterialien zur IT-Zertifizierung! Sicher, einfach und schnell. 100%-Pass-Garantie!

Exam : **CEH-001**

Title : Certified Ethical Hacker (CEH)

Vendor : GAQM

Version : DEMO

NO.1 You visit a website to retrieve the listing of a company's staff members. But you can not find it on the website. You know the listing was certainly present one year before. How can you retrieve information from the outdated website?
A. Through Google searching cached files
B. Through Archive.org
C. Download the website and crawl it
D. Visit customers' and prtners' websites
Answer: B
Explanation:
Archive.org mirrors websites and categorizes them by date and month depending on the crawl time. Archive.org dates back to 1996, Google is incorrect because the cache is only as recent as the latest crawl, the cache is over-written on each subsequent crawl. Download the website is incorrect becausethat's the same as what you see online. Visiting customer partners websites is just bogus. The answer is then Firmly, C, archive.org

NO.2 To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic. What type of scan is Winston attempting here?
A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
B. He is utilizing a SYN scan to find live hosts that are listening on your network.
C. This type of scan he is using is called a NULL scan.
D. He is using a half-open scan to find live hosts on your network.
Answer: D

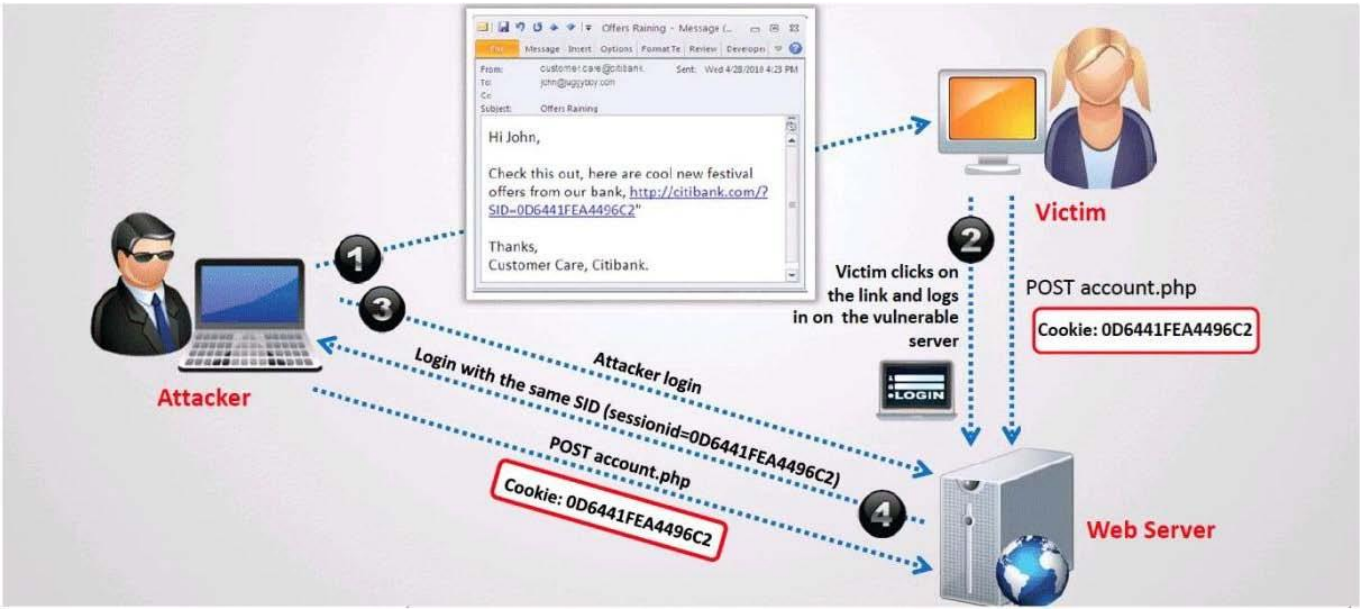
NO.3 What is the proper response for a NULL scan if the port is closed?
A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response
Answer: E
Explanation:
Closed ports respond to a NULL scan with a reset.

NO.4 Which cipher encrypts the plain text digit (bit or byte) one by one?
A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher
Answer: D

NO.5 Information gathered from social networking websites such as Facebook, Twitter and

LinkedIn can be used to launch which of the following types of attacks? (Choose two.)
A. Smurf attack
B. Social engineering attack
C. SQL injection attack
D. Phishing attack
E. Fraggle attack
F. Distributed denial of service attack
Answer: B,D

NO.6 What type of session hijacking attack is shown in the exhibit?



A. Cross-site scripting Attack
B. SQL Injection Attack
C. Token sniffing Attack
D. Session Fixation Attack
Answer: D

NO.7 A digital signature is simply a message that is encrypted with the public key instead of the private key.
A. true
B. false
Answer: B

NO.8 Under what conditions does a secondary name server request a zone transfer from a primary name server?
A. When a primary SOA is higher that a secondary SOA
B. When a secondary SOA is higher that a primary SOA
C. When a primary name server has had its service restarted
D. When a secondary name server has had its service restarted

E. When the TTL falls to zero
Answer: A

NO.9 Rebecca is a security analyst and knows of a local root exploit that has the ability to enable local users to use available exploits to gain root privileges. This vulnerability exploits a condition in the Linux kernel within the execve() system call. There is no known workaround that exists for this vulnerability. What is the correct action to be taken by Rebecca in this situation as a recommendation to management?
A. Rebecca should make a recommendation to disable the () system call
B. Rebecca should make a recommendation to upgrade the Linux kernel promptly
C. Rebecca should make a recommendation to set all child-process to sleep within the execve()
D. Rebecca should make a recommendation to hire more system administrators to monitor all child processes to ensure that each child process can't elevate privilege
Answer: B

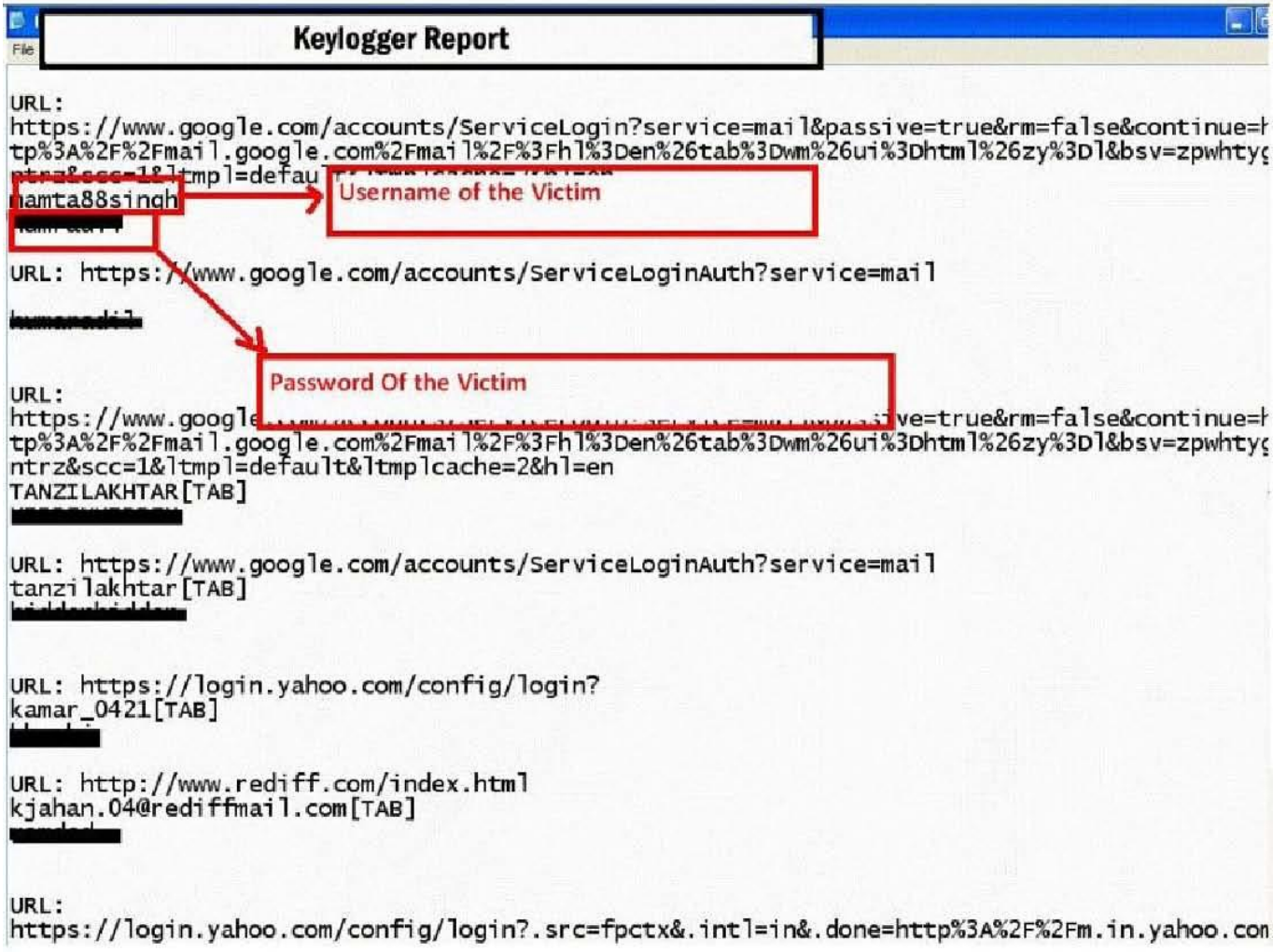
NO.10 Rebecca has noted multiple entries in her logs about users attempting to connect on ports that are either not opened or ports that are not for public usage. How can she restrict this type of abuse by limiting access to only specific IP addresses that are trusted by using one of the built-in Linux Operating System tools?
A. Ensure all files have at least a 755 or more restrictive permissions.
B. Configure rules using ipchains.
C. Configure and enable portsentry on his server.
D. Install an intrusion detection system on her computer such as Snort.
Answer: B
Explanation:
ipchains is a free software based firewall for Linux. It is a rewrite of Linux's previous IPv4 firewalling code, ipfwadm. In Linux 2.2, ipchains is required to administer the IP packet filters. ipchains was written because the older IPv4 firewall code used in Linux
2.0 did not work with IP fragments and didn't allow for specification of protocols other than TCP, UDP, and ICMP.

NO.11 Assuring two systems that are using IPSec to protect traffic over the internet, what type of general attack could compromise the data?
A. Spoof Attack
B. Smurf Attack
C. Man inthe Middle Attack
D. Trojan Horse Attack
E. Back Orifice Attack
Answer: D,E
Explanation:
To compromise the data, the attack would need to be executed before the encryption takes place at either end of the tunnel. Trojan Horse and Back Orifice attacks both allow for potential data manipulation on host computers. In both cases, the data would be compromised either before encryption or after decryption, so IPsec is not preventing the attack.

NO.12 What information should an IT system analysis provide to the risk assessor?
A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis
Answer: C

NO.13 Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.


Account Login
Login
User Name:
Password:
Remember Login
LOGIN
Password Reminder


Keylogger Report
File
URL:
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
Username of the Victim
URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail
Password Of the Victim
URL:
https://www.google
ve=true&rm=false&continue=h
tp%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Den%26tab%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtyg
ntrz&scc=1&ltmpl=default&ltmplcache=2&hl=en
TANZILAKHTAR[TAB]
URL: https://www.google.com/accounts/ServiceLoginAuth?service=mail
tanzilakhtar[TAB]
URL: https://login.yahoo.com/config/login?
kamar_0421[TAB]
URL: http://www.rediff.com/index.html
kjahan.04@rediffmail.com[TAB]
URL:
https://login.yahoo.com/config/login?.src=fpctx&.intl=in&.done=http%3A%2F%2Fm.in.yahoo.con

How will you defend against hardware keyloggers when using public computers and Internet Kiosks? (Select 4 answers)
A. Alternate between typing the login credentials and typing characters somewhere else in the focus window
B. Type a wrong password first, later type the correct password on the login page defeating the keylogger recording
C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
D. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsd". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsd"
E. The next key typed replaces selected text portion. E.g. if the password is "secret", one could type "s", then some dummy keys "asdfsd". Then these dummies could be selected with mouse, and next character from the password "e" is typed, which replaces the dummies "asdfsd"
Answer: A,C,D,E

NO.14 Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?
A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death
Answer: A

NO.15 Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company's largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason's client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.
Without any proof, Jason's company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason's company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.
Jason's supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason's supervisor opens the picture files, but cannot find anything out of the ordinary with them.
What technique has Jason most likely used?
A. Stealth Rootkit Technique
B. ADS Streams Technique
C. Snow Hiding Technique

D. Image Steganography Technique
Answer: D

NO.16 An attacker is attempting to telnet into a corporation's system in the DMZ.
The attacker doesn't want to get caught and is spoofing his IP address.
After numerous tries he remains unsuccessful in connecting to the system.
The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?
A. The firewall is blocking port 23 to that system
B. He needs to use an automated tool to telnet in
C. He cannot spoof his IP and successfully use TCP
D. He is attacking an operating system that does not reply to telnet even when open
Answer: C

NO.17 Joe Hacker is going wardriving. He is going to use PrismStumbler and wants it to go to a GPS mapping software application. What is the recommended and well-known GPS mapping package that would interface with PrismStumbler?
Select the best answer.
A. GPSDrive
B. GPSMap
C. WinPcap
D. Microsoft Mappoint
Answer: A
Explanation:
Explanations: GPSDrive is a Linux GPS mapping package. It recommended to be used to send PrismStumbler data to so that it can be mapped. GPSMap is a generic term and not a real software package. WinPcap is a packet capture library for Windows. It is used to capture packets and deliver them to other programs for analysis. As it is for Windows, it isn't going to do what Joe Hacker is wanting to do. Microsoft Mappoint is a Windows application. PrismStumbler is a Linux application. Thus, these two are not going to work well together.

NO.18 Which type of antenna is used in wireless communication?
A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional
Answer: A

NO.19 Which are true statements concerning the BugBear and Pretty Park worms?
Select the best answers.
A. Both programs use email to do their work.
B. Pretty Park propagates via network shares and email
C. BugBear propagates via network shares and email
D. Pretty Park tries to connect to an IRC server to send your personal passwords.

E. Pretty Park can terminate anti-virus applications that might be running to bypass them.
Answer: A,C,D
Explanation:
Both Pretty Park and BugBear use email to spread. Pretty Park cannot propagate via network shares, only email. BugBear propagates via network shares and email. It also terminates anti-virus applications and acts as a backdoor server for someone to get into the infected machine. Pretty Park tries to connect to an IRC server to send your personal passwords and all sorts of other information it retrieves from your PC. Pretty Park cannot terminate anti-virus applications. However, BugBear can terminate AV software so that it can bypass them.

NO.20 Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page in which also he remains unsuccessful. What is the probable cause of Bill's problem?
A. You cannot use a buffer overflow to deface a web page
B. There is a problem with the shell and he needs to run the attack again
C. The HTML file has permissions of read only
D. The system is a honeypot
Answer: C