CEH v9

Exam A

QUESTION 1
This kind of malware is installed by criminals on your computer so they can lock it from a remote location. This malware generates a popup window, webpage, or email warning from what looks like an official authority such as the FBI. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again. Which term best matches this definition?

A. Riskware
B. Adware
C. Ransomware
D. Spyware

Correct Answer: C
Section: Malware
Explanation

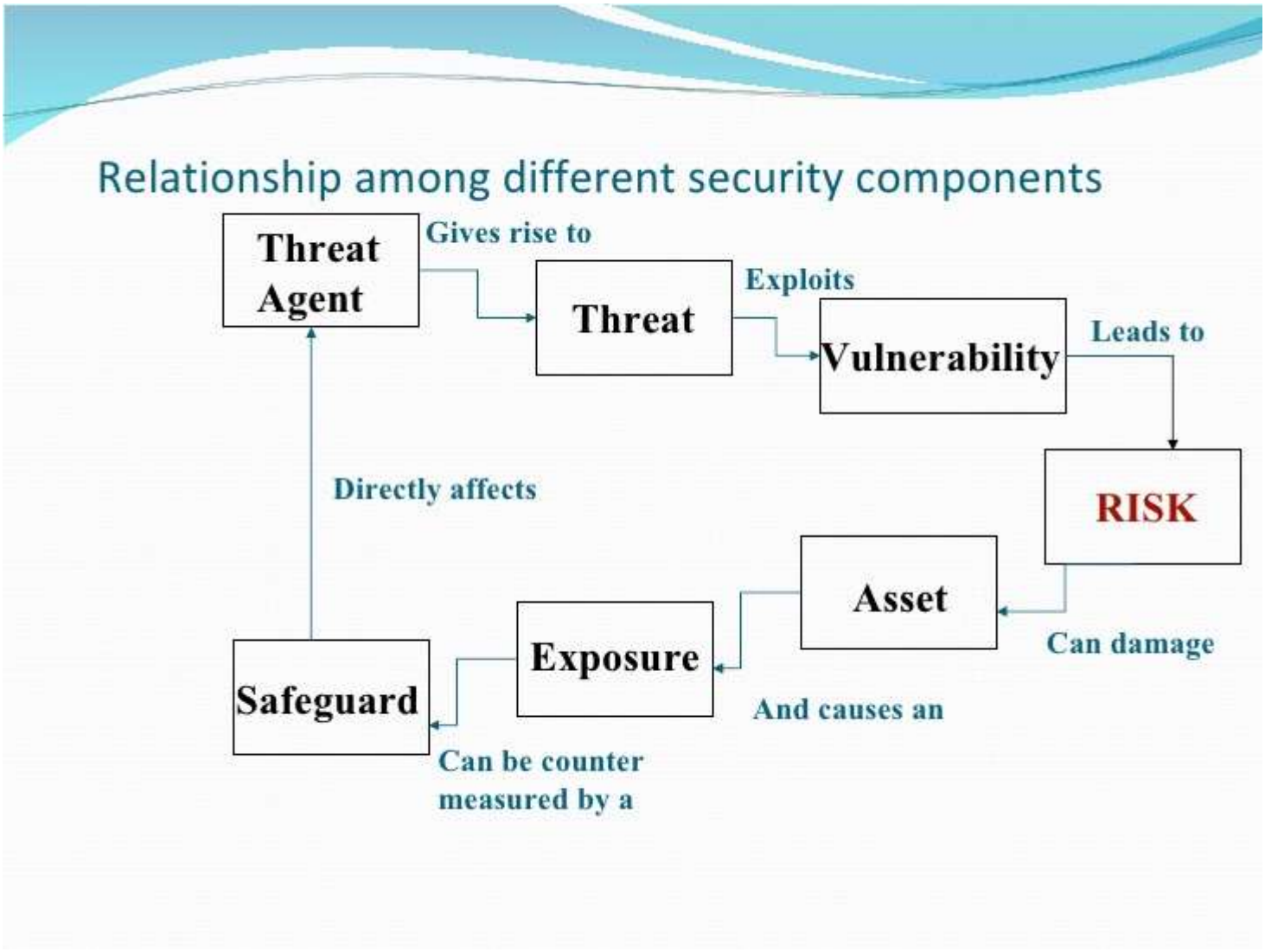
Explanation/Reference:
Ransomware stops you from using your PC. It holds your PC or files for "ransom". This page describes what ransomware is and what it does, and provides advice on how to prevent and recover from ransomware infections.
You can also read our blog about ransomware: The 5Ws and 1H of ransomware.

QUESTION 2
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

A. Likelihood is a possible threat-source that may exploit a vulnerability.
B. Likelihood is the likely source of a threat that could exploit a vulnerability.
C. Likelihood is the probability that the threat-source will exploit a vulnerability.
D. Likelihood is the probability that a vulnerability is a threat source.

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:



QUESTION 3
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from the command line. Which command would you use?

A. c:\compmgmt.msc
B. c:\ncpa.cpl
C. c:\gpedit
D. c:\services.exe

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Old tool replaced by MMC on all Windows syst
can type it into the run prompt as well

QUESTION 4
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web sites's user login page that the software's designers did not expect to be entered. This is an example of what

kind of software design problem/issue?

A. Insufficient exception handling
B. Insufficient security management
C. Insufficient input validation
D. Insufficient database hardening

Correct Answer: C
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
Often related to SQL injection attacks.

QUESTION 5
To determine if a program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program. This is commonly referred to as what type of testing?

A. Randomizing
B. Fuzzing
C. Mutating
D. Ballin, like a Big Baller

Correct Answer: B
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
Fuzzing basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated .
DIfferent inputs are tried agains any input field to see if an error that could result in a vulnerability is found.

QUESTION 6
You have successfully gained access to your client's internal network and successfully compromised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled. Which port would you see listening on these Windows machines in the network?

A. 1433
B. 3389
C. 161
D. 445

Correct Answer: D
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
1433- SQL
3389- RDP-Terminal Services
161- SNMP
445- CIFS/SMB

QUESTION 7
An attacker changes the profile information of a particular user on a target website (the victim). The attacker

uses this string to update the victim's profile to a text file and then submit the data to the attackers database.

< iframesrc=http://www.vulnweb.com/updateif.php style="display:none" > </iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Browser Hacking
B. Cross-Site Scripting
C. Cross-Site Request Forgery
D. SQL Injection

Correct Answer: B
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
The question isn't great, but the idea is that the code will be executed when the victim logs back in. The code will execute on the client's machine.
It doesn't take advantage of the victim being authenticated elsewhere, so it is an example of cross site scripting.

Fundamental difference is that CSRF (Cross-site Request forgery) happens in authenticated sessions when the server trusts the user/browser, while XSS (Cross-Site scripting) doesn't need an authenticated session and can be exploited when the vulnerable website doesn't do the basics of validating or escaping input.

In case of XSS, when the server doesn't validate or escapes input as a primary control, an attacker can send inputs via request parameters or any kind of client side input fields (which can be cookies, form fields or url params). These can be written back to screen , persisted in database or executed remotely. For CSRF, consider an example when you are logged in into your banking site and at the same time logged into Facebook in another tab in same browser. An attacker can place a malicious link embedded in another link or zero byte image which can be like yourbanksite.com/transfer.do?
fromaccnt=youraccnt&toaccnt=attackersAccount&amt=2500. Now, if you accidentally click on this link , in the background transfer can happen though you clicked from the Facebook tab.

This is because your session is still active in browser and browser has your session id. This is the reason the most popular CSRF protection is having another server supplied unique token generated and appended in the request. This unique token is not something which is known to browser like session id. This additional validation at server (i.e whether the transfer request also contains the correct CSRF token) will make sure that the attacker manipulated link (I.e the CSRF attack) in above example will never work.

QUESTION 8
You want to perform a technical assessment on your network. What is the best approach for discovering vulnerabilities on a Windows based computer?

A. Use the built-in Windows Update tools
B. Create a disk image of a clean installation
C. Use a scan tool like Nessus
D. Check mitre.org for the latest list of CVE findings.

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

QUESTION 9
Keatron calls you and tells you that his wireless router increases in temperature noticeably after 7 PM every

night. What tool could you use to view network traffic being sent and received by Keatron's wireless router?

A. Netcat
B. Wireshark
C. Netstat
D. Nessus

Correct Answer: B
Section: Wireless
Explanation

Explanation/Reference:

QUESTION 10
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing. What document describes the specifics of the testing, the associated violations, and essentially protects both the organizations interest and your liabilities as a tester?

A. Service Level Agreement
B. Project Scope
C. Non-Disclosure Agreement
D. Terms of engagement

Correct Answer: D
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 11
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
C. Overwrites the original MBR and only executes the new virus code.
D. It is related to the Arkanis sector from Star Wars.

Correct Answer: B
Section: Malware
Explanation

Explanation/Reference:

QUESTION 12
Which of the following parameters describe LM hashes?

A. It's a simple algorithm so 10,000,000 hashes can be generated per second.
B. Maximum password length is 14 characters
C. There is no distinctions between upper and lower case.
D. All choices are correct

Correct Answer: D

Section: Cryptography
Explanation

Explanation/Reference:
LM Hashing is the default used by older windows system.
It was a simple hashing tool, but it was limited by separating a password into two parts and then converting to uppercase.
All passwords were "padded" to 14 characters
Maximum was 14 characters, which meant that longer passwords were truncated.
This made it easy to crack.

QUESTION 13
You are doing a pentest against an organization that has just recovered from a major cyber attack. The CISO and CIO want to completely and totally eliminate risk. What is one of the first things you should explain to these individuals?

A. Explain to them that they need to buy more services.
B. Start the wireshark application to sniff traffic
C. Explain that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Tell him everything is going to A ok and collect that check!

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
IT Security is about mitigating risks
There is always residual risk unless an asset is removed completely.

QUESTION 14
What is the best way to defend against network sniffing?

A. Using encryption protocols to secure network communications.
B. Use Static IP's
C. Register all machines MAC address in a Centralized Database
D. Restrict physical access to server rooms host critical servers.

Correct Answer: A
Section: Sniffers
Explanation

Explanation/Reference:
Although securing radio emissions is also important, using encryption means that captured traffic is less likely to be compromised.

QUESTION 15
An organization has just experienced a breach. The investigator/incident handler attempts to correlate the information in all of the logs, the sequence of many of the logged events don't match up or line up properly. What is likely the cause?

A. The attacker altered or erased events from the logs.
B. Proper chain of custody was not observed while collecting the logs
C. The breach didn't really happened. The dreamed it.
D. The network devices are not all synchronized

Correct Answer: A
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Since an attack was mentioned,
The attacker altered or erased events from the logs.
Is the best answer.
However, D is also a decent answer, as if NTP isn't used, you would find it difficult to line up/correlate the time stamps.

QUESTION 16
You send a receptionist an email that has pdf attached. The pdf has a malicious link in it. When the receptionist opens the email, he clicks on the link and is infected with malware that gives you access to his network. What type of testing method did you use for this attack?

A. Tailgating
B. Eavesdropping
C. Piggybacking
D. Social engineering

Correct Answer: D
Section: Social Engineering
Explanation

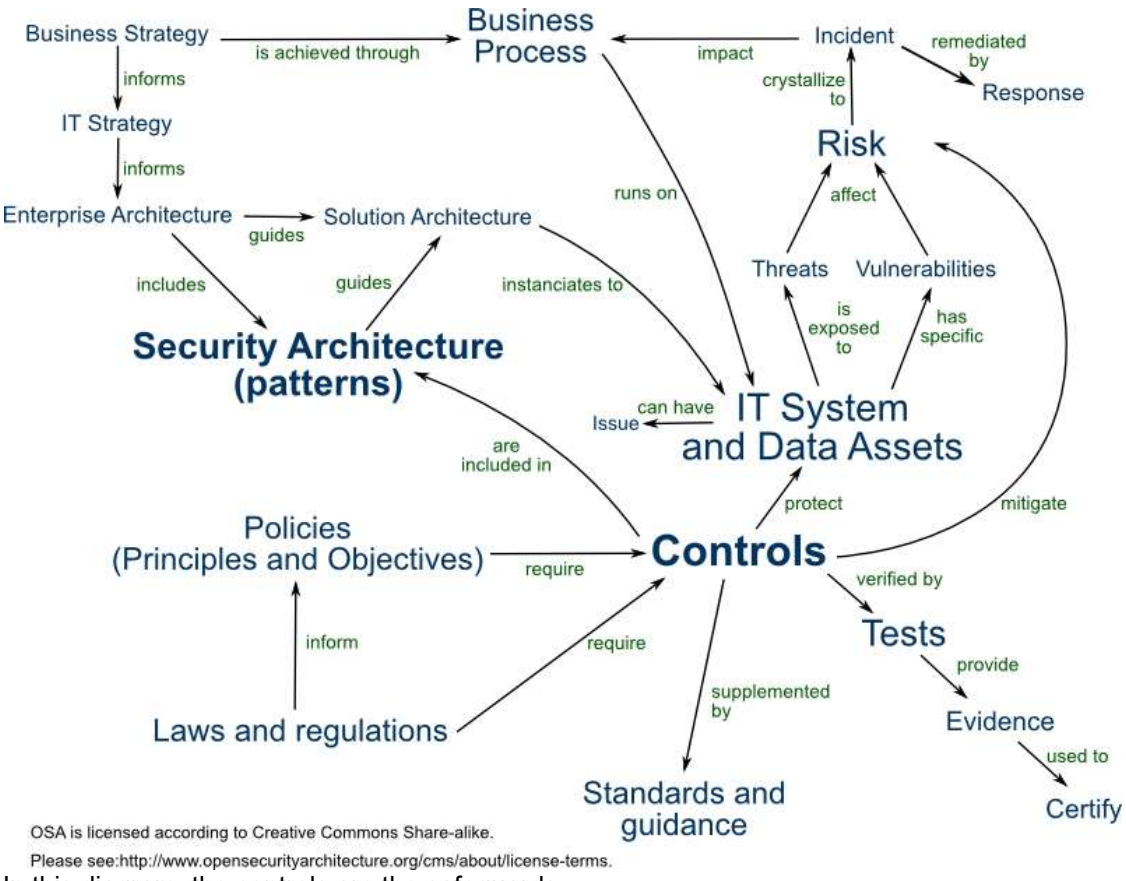
Explanation/Reference:
Social Engineering involves many techniques.
This is an example of Phishing.

QUESTION 17
Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Logical interfaces and controls
C. Physical security
D. DMZ

Correct Answer: A
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:



In this diagram, the controls are the safeguards.
By Open Security Architecture - http://www.opensecurityarchitecture.org/cms/foundations/osa-taxonomy, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=11796253

QUESTION 18
What is the best description of SQL Injection?

A. It is a MiTM attack
B. It is an attack used to modify the code in an application
C. It is an attack used to gain unauthorized access to a database
D. It is a Denial of Service Attack (DoS)

Correct Answer: C
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
SQL- Structured Query Language
By inserting commands that will be interpreted by the SQL server, you can manipulate that system to gain access to the data, or even manipulate the underlying system.

QUESTION 19
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris
B. Voice
C. Fingerprints

D. Height and Weight

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Although tools like Iris identification have limitations, Height and Weight are the least likely to be used.

QUESTION 20
Heartbleed bug leaves which type of key exposed?

A. Shared
B. Public
C. Florida
D. Private

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.[65]

An attack may also reveal private keys of compromised parties,[25][27][66] which would enable attackers to decrypt communications (future or past stored traffic captured via passive eavesdropping, unless perfect forward secrecy is used, in which case only future traffic can be decrypted if intercepted via man-in-the-middle attacks).

https://en.wikipedia.org/wiki/Heartbleed

Generally, it is difficult to get the certificate private key, although it is possible. It is much more likely to get session keys. However, you can get clear text of just about anything that was sent by the vulnerable server (or client). This means that you don't need the keys in any case.

QUESTION 21
You have compromised a server. You want to communicate and pivot traffic from one place to the next over the network securely and evade detection by IDS, etc. What is the best approach?

A. Install and use telnet which is by default encrypted.
B. Use ADS
C. Install cryptcat and encrypt all outgoing packets from this server.
D. Use Http

Correct Answer: C
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Pivoting is redirecting the output sent to one machine to another.
redir and FPipe are examples
we can also use netcat or ncat to do the same
Tools like cryptcat add the ability to encrypt the data to avoid an IDS/IPS

nc -l -p 1521 -e “nc internal.db.srv 1521

There are similar commands for cryptcat

QUESTION 22
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Inherent Risk
B. Residual Risk
C. Impact Risk
D. Deferred Risk

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Inherent Risk: The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)

Residual Risk: The risk that remains after controls are taken into account (the net risk or risk after controls).

http://ishandbook.bsewall.com/risk/Assess/Risk/inherent_risk.html

QUESTION 23
A penetration tester just scanned a device and found that ports 21, 23, 80, 139, 515, 631, and 9100 open. What is likely to be installed based on these ports being open?

A. The host is likely a Windows machine
B. The host is likely a printer.
C. The host is likely a router
D. The host is likely a Linux machine

Correct Answer: B
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
21- FTP
23- Telent
80- HTTP
139- Netbios
515- Line PRinter Daemon (LPD)
631- CUPS
9100- LPR RAW Printing

QUESTION 24
Your IDS admin gets an alert for the IDS. The associated packets are saved as a pcap file. What type of network tool can be used to determine if these packets are generally malicious or simply a false positive?

A. Intrusion Prevention System
B. Network Sniffer
C. Vulnerability Scanner
D. Protocol Analyzer

Correct Answer: D
Section: Sniffers
Explanation

Explanation/Reference:
A protocol analyzer, like wireshark, or tcptrace, can read capture files.

QUESTION 25
A hacker has successfully infected an internet facing server which he will then use to send junk mail, take part in the coordinated attacks, or host junk email content. Which sort of trojan infects this server?

A. Ransomware Trojans
B. Botnet Trojan
C. Banking Trojans
D. Turtle Trojans

Correct Answer: B
Section: Malware
Explanation

Explanation/Reference:
The idea is that a Botnet Trojan has a payload that makes the computer part of the botnet.
Botnet is the key term, as it related to the tasks a remotely controlled PC might be set to.

QUESTION 26
While doing some online banking Keatron receives an email that contains a link to an interesting web site. When he clicks on the link another browser session opens and shows a video of dogs playing a bass guitar. The next day Keatron's bank contacts him indicating that his bank account has been accessed from a foreign country. What browser based security vulnerability was exploited?

A. Cross Site Scripting
B. Web Form input validation
C. Cross Site Request forgery
D. Clickjacking

Correct Answer: C
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
Cross-Site Request Forgery, or CSRF for short is a common and regular online attack. CSRF also goes by the acronym XSRF and the phrase “Sea-Surf”. CSRF attacks include a malicious exploit of a website in which a user will transmit malicious requests that the target website trusts without the user’s consent. In Cross-Site Scripting (XSS), the attacker exploits the trust a user has for a website, with CSRF on the other hand, the attacker exploits the trust a website has against a user’s browser.

The idea is that Keatron was already on the banking site, or was authenticated to it when he clicked the link. The bank site trusted Keatron, and the malicious code made his already authenticated system send the money.

https://www.acunetix.com/websitesecurity/csrf-attacks/

QUESTION 27
Which of the following is most secure for storing backup tapes?

A. Inside the data center for faster retrieval in a fireproof safe.

B. On a different floor in the same building
C. In a climate controlled facility offsite
D. In a cool dry environment

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Offsite is key.

QUESTION 28
The white box testing methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the internal operation of a system is known to the tester
D. The internal operation of a system is only partly accessible to the tester.

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Black box testing

takes an external perspective of the test object to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid input and determines the correct output. There is no knowledge of the test object's internal structure.

White box testing

uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. In electrical hardware testing, every node in a circuit may be probed and measured; an example is in-circuit testing (ICT).

QUESTION 29
Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG
B. SMS
C. ICMP
D. SNMP

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
In addition to the syslog protocol, we usually need to have NTP to make sure syslog messages are synchronized to allow correlation.

QUESTION 30
Which of the following is a low tech way of gaining unauthorized access to systems?

A. Sniffing
B. Scanning
C. Social engineering
D. Eavesdropping

Correct Answer: C
Section: Social Engineering
Explanation

Explanation/Reference:

QUESTION 31
Which of the following is most effective ways to prevent Cross Site Scripting flaws in software applications?

A. Verify access right before allowing access to protected information and UI controls.
B. Use security policies and procedures to define and implement proper security settings.
C. Use digital certificates to authenticate a server prior to sending data.
D. Validate and escape all information sent to a server

Correct Answer: D
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

The idea is that the user trusts the site, and they run the code.

Usually XSS is performed by entering code into an input field on a form in such away that other users will execute the code when they access the same site.

QUESTION 32
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Application layer port numbers and transport layer headers.
B. Transport layer port numbers and application layer headers
C. Presentation layer headers and session layer port numbers
D. Network layer headers and the session layer port numbers.

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Application layer has headers and codes, but no real addressing
Transport layer has port numbers (TCP/UDP)
Network layer has IP addresses
Data Link (ethernet) has MAC addresses

QUESTION 33

During a routine assessment you discover information that suggests the customer is involved in human trafficking.

A. Confront the client in a respectful manner and ask about the data
B. Ignore the data, complete the job, collect a check. Keep it moving!
C. Immediately stop work and contact the proper legal authorities
D. Copy the data to a thumb drive and keep it as leverage.

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

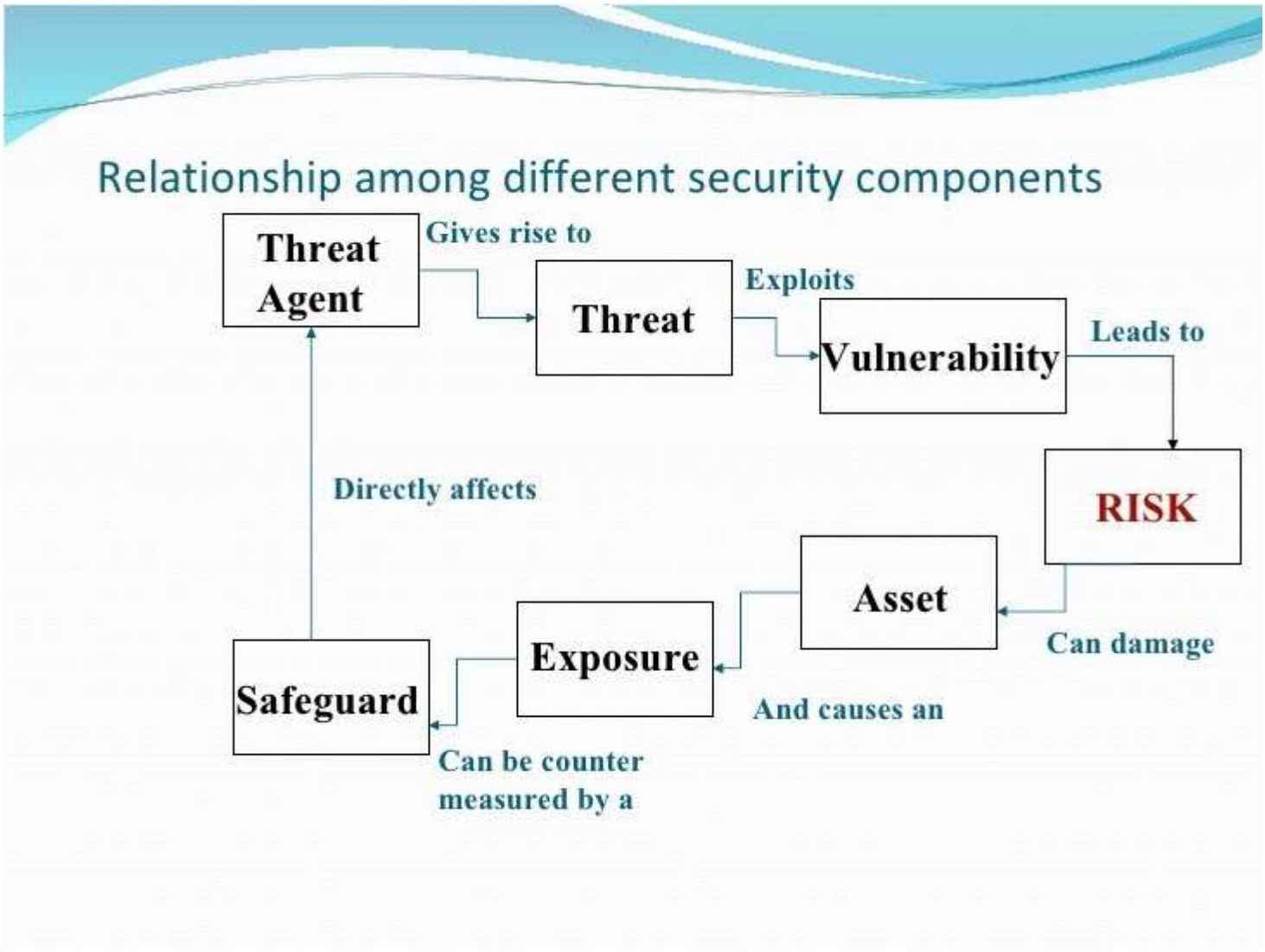
Explanation/Reference:
An NDA doesn't mean you cannot prevent crimes.

QUESTION 34
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosures, denial of service or modification of data. Which term best matches this definition?

A. Risk
B. Threat
C. Attack
D. Vulnerability

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:



QUESTION 35
While using your banks online services you notice the following string in the URL bar; http:// www.mypersonalmoney.com/account?id=8949339&Damount=10980&Camount=21" You notice that if you modify the Damount and Camount values and submit the request, the data on the web page reflect the changes. Which type of vulnerability is present on this site?

A. Web Parameter Tampering
B. Cookie Tampering
C. XSS Reflection
D. SQL Injection

Correct Answer: A
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
owasp: The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

QUESTION 36
Nmap -sn 192.168.153.200-215.

The above nmap command performs which of the following?

A. A port scan
B. A trace sweep
C. A ping scan
D. An operating system detect scan

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

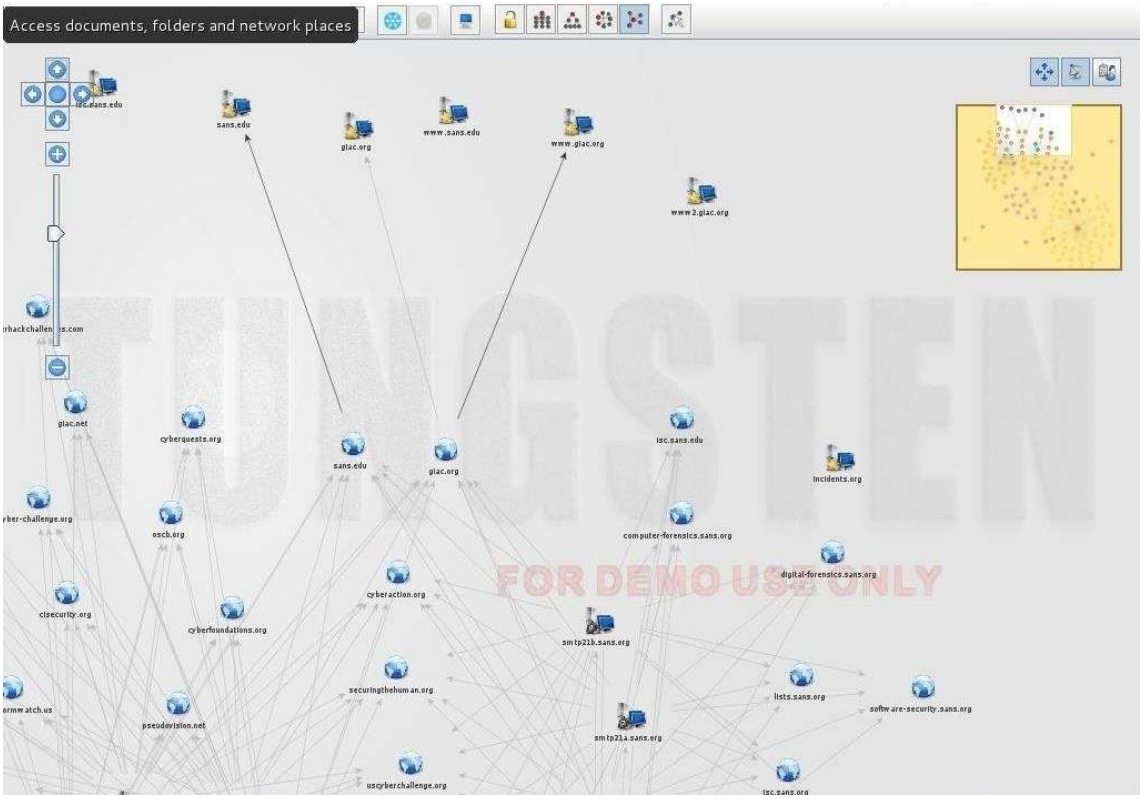
Explanation/Reference:
-sn is a network scan or ping scan
-sP is a probe scan, which will ping on remote networks and use arp on local networks.

QUESTION 37
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Wireshark
B. Metasploit
C. Cain & Abel
D. Maltego

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:
http://null-byte.wonderhowto.com/how-to/hack-like-pro-use-maltego-do-network-reconnaissance-0158464/



QUESTION 38
Which Google command will help you search files using Google as a search engine?

A. domain: target.com archive:xls username password email
B. site: target.com filetype:xls username password email
C. site: target.com file:xls username password email
D. inurl: target.com filename:xls username password email

Correct Answer: B
Section: Tools
Explanation

Explanation/Reference:
The filetype:xls specifies to only return results of type .xls

site: target.com filetype:xls username password email looks for excel spreadsheets found at target.com with username, password or email in the contents.

QUESTION 39
You have several firewall and router logs that are in plain-text. You must review these to evaluate traffic. You know that in order to do this fast and efficiently, you must user regular expressions. Which command-line utility are you most likely to use?

A. Relational Database
B. Grep
C. MS Excel
D. Notepad

Correct Answer: B
Section: Tools

Explanation

Explanation/Reference:
Global regular expression print

Prints found regular expressions to screen.

QUESTION 40
What is the most important phase in ethical hacking in which you need to spend a considerable amount of time?

A. Gaining access
B. Footprinting
C. Escalating privileges.
D. Network mapping

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Wiki: Footprinting is the technique of gathering information about computer systems and the entities they belong to.

basically the reconnaissance step

QUESTION 41
Which of the following is a command line packet analyzer similar to the GUI-based Wireshark

A. Jack the ripper
B. Nessus
C. ethereal
D. tcpdump

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:
tcpdump can be used when you don't have access to a GUI

QUESTION 42
Which of the following is an extremely common IDS evasion technique in the web world?

A. Using Unicode characters
B. subnetting
C. port knocking
D. spyware

Correct Answer: A
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Unicode can present multiple ways for a character to be represented, even though it isn't supposed to.

If an IDS has rules to look for certain text in a packet, it may miss packets that have unicode, but they may get processed by their targets:

http://vulneapplication/../../appusers.txt will be blocked

http://vulneapplication/%C0AE%C0AE%C0AF%C0AE%C0AE%C0AFappusers.txt will get through.

Other site-
http://www.iss.net/threats/advise95.html

QUESTION 43
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files and one is a binary file named nc (netcat). The logs show the user logged in anonymously, uploaded the files, extracted the contents and ran the script using a function provided by the ftp server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port. What kind of vulnerability had to have existed to make this remote attack possible?

A. Privilege Escalation
B. Directory Traversal
C. File system permissions
D. Brute Force Login

Correct Answer: A
Section: Exploits
Explanation

Explanation/Reference:
The key item here is the "ran the script using a function provided by the ftp server's software"
assuming the FTP has higher privileges, this can be considered privilege escalation.

QUESTION 44
The Open Web Application Security Project is the worldwide non-profit organization focused on improving the security of software. What item is the primary concern on OWASP's Top 10 Project list of most critical web application security risks?

A. Path Disclosure
B. Cross Site Request Forgery
C. Injection
D. Cross Site Scripting

Correct Answer: C
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
https://www.owasp.org/index.php/Main_Page

QUESTION 45
Which tool performs comprehensive tests against web servers, including dangerous files and CGI's?

A. Nikto
B. Snort
C. John the Ripper

D. Dsniff

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
Cirt: Niktois an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items
Snort is an IDS/IPS
John the Ripper is for password cracking
Dsniff is credential sniffing and MiTM, among others

QUESTION 46
Which of the following types of firewalls ensures that the packets are part of an established session?

A. Stateful Inspection firewall
B. Switch-level firewall
C. Application-level firewall
D. Circuit-level firewall

Correct Answer: A
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Stateful firewalls block traffic by default.
They will allow the return of traffic that is a response to internally generated traffic.

In action
Step 1- Host 1 sends request to Server 1 Host 1 >>>>>>>>>>FIREWALL >>>>>>>>>>>>Server1
Step 2- Server 1 responds. The stateful firewall allows it Host 1 <<<<<<<<<<FIREWALL <<<<<<<<<<<<Server1

Preventing Access
Malicious user tries to get to Host 1- Host 1 FIREWALL <<<<<<<<<<<<Server1
Firewall stops the traffic as it isn't part of a communication session.

QUESTION 47
It is important to enumerate which HTTP methods (GET POST HEAD PUT DELETE TRACE) a web server has available. Which nmap script will help you discover the methods?

A. http enum
B. http-git
C. http-methods
D. http-headers

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
http-methods- obvious answer
nmap --script http-methods <target>

Script Output

```
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

nmap -sV --script=http-enum <target>
Script Output

```
Interesting ports on test.skullsecurity.org (208.81.2.52):
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-enum:
|   /icons/: Icons and images
|   /images/: Icons and images
|   /robots.txt: Robots file
|   /sw/auth/login.aspx: Citrix WebTop
|   /images/outlook.jpg: Outlook Web Access
|   /nfservlets/servlet/SPSRouterServlet/: netForensics
|_  /nfservlets/servlet/SPSRouterServlet/: netForensics
```

nmap -sV --script=http-headers <target>
Script Output

```
PORT   STATE SERVICE
80/tcp open  http
| http-headers:
|   Date: Fri, 25 Jan 2013 17:39:08 GMT
|   Server: Apache/2.2.14 (Ubuntu)
|   Accept-Ranges: bytes
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
```

QUESTION 48
You are using nmap to resolve domain names to ip addresses for a ping sweep later. Which of the following commands (Linux command) looks for host IP addresses?

A. host -t AXFR hackedme.com
B. host -t soa hackedme.com
C. host -t a hackedme.com
D. host -t ns hackedme.com

Correct Answer: C
Section: Tools
Explanation

Explanation/Reference:
host is another command like dig or nslookup for making manual name resolution.

The key item here is the request for the -a, which will return all record types.

host manpage: The -a(all) option is equivalent to setting the -voption and asking hostto make a query of type ANY.

QUESTION 49
An attacker has installed a RAT trojan on a host. The attacker now has control of the machine through the RAT (remote access trojan). The attacker wants to now ensure that if the user attempts to go to www.mybank.com that the user is directed to a phishing site. Which file does the attacker need to modify to make this happen?

A. Sudoers
B. Boot.ini
C. Hosts
D. Networks

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:
The hosts file is the first place that a system checks first, before checking with DNS.

/etc/hosts

/windows/system32/drivers/etc

QUESTION 50
This attack is based on attackers running exploits on well-known and likely visited trusted sites. They exploit the sites and plant malware on the site, knowing that eventually their targets will visit the site and become infected. What type of attack is this?

A. Spear Phishing
B. Watering Hole Attack
C. Heartbleed
D. Shellshock

Correct Answer: B
Section: Exploits
Explanation

Explanation/Reference:
Like an APT.

QUESTION 51
In 2014 there was a vulnerability in GNU's bash shell. It gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch a denial of service attack, or disrupt websites. What is this vulnerability known as?

A. Rootshock
B. Rootshell
C. Shellbash
D. Shellshock

Correct Answer: D
Section: Exploits
Explanation

Explanation/Reference:
bash shell- shellshock

QUESTION 52
Which wireless hacking tool attacks WEP and WPA-PSK?

A. Airguard
B. WLAN-crack
C. wificracker
D. Aircrack-ng

Correct Answer: D
Section: Wireless
Explanation

Explanation/Reference:

QUESTION 53
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. NIST-800-53
B. EU Safe Harbor
C. HIPAA
D. PCI-DSS

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 54
You need to monitor all traffic on your local network for suspicious activity and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host based IDS
B. Network based IDS
C. Firewall
D. Proxy

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Network based tracks for all traffic on the network....
IDS for looking at suspicious activity

QUESTION 55
This asymmetric cipher is based on factoring the product of two large prime numbers. What cipher is being described?

A. RSA

B. MD5
C. SHA
D. RC5

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
RSA- Asymmetric for Public/Private Keys
MD5- Hash
SHA - Hash
RC5- Symmetric key Encryption

QUESTION 56
What is a collision attack in cryptography?

A. Collision attacks try to get the public key
B. Collision attacks try to find two inputs that produce the same hash
C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
D. Collision attacks try to break the hash into three parts.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:

QUESTION 57
Which IPSEC mode should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. ESP confidential
C. AH permiscuous mode
D. AH Tunnel Mode

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
ESP mode provides for encryption
AH only provides authentication
Transport mode will encrypt payload
Tunnel mode encrypts the payload and original IP addresses

QUESTION 58
Which command will allow you to enumerate all machines on the network quickly?

A. nmap -T4 -O 10.10.1.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -q 10.10.1.0/24
D. nmap -T4 -F 10.10.1.0/24

Correct Answer: D
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
-T4 is fast
-F: Fast mode - Scan fewer ports than the default scan

QUESTION 59
An ISP needs to authenticate users connecting using analog modems, DSL, wireless data services, and Virtual Private Networks (VPN) over frame relay networks. Which AAA protocol is most likely able to handle this requirement?

A. RADIUS
B. TACACS+
C. Kerberos
D. DIAMETER

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
Both RADIUS and TACACS+ support all these requirements. Most ISPs use RADIUS even though TACACS+ is a bit more secure.
DIAMETER is a remote access protocol, but isn't as widely supported yet. It has wide adoption in IMS (IP multimedia services)

QUESTION 60
You are doing a penetration test and gathering information. You have found pdfs, docs, and images. You decide to extract metadata from these files and analyze it. What tool will help you with the task?

A. cdpsnarf
B. Dimitry
C. Metagoofil
D. Armitage

Correct Answer: C
Section: Tools
Explanation

Explanation/Reference:
Metagoofilis an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

QUESTION 61
You have gained access to a Windows 2008 Server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux Live CD. Which Linux based tool has the ability to change any user's password or activate disabled Windows accounts?

A. John the Ripper
B. SET
C. CHNTPW
D. Cain & Abel

Correct Answer: C
Section: Password Cracking
Explanation

Explanation/Reference:
Wiki: chntpwis a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes Booting from the Linux CD/USB and accessing the drive without the windows protections on the SAM file.

QUESTION 62
You have two machines. The first machine (192.168.153.99) has snort installed, and the second machine (192.168.153.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice the kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check and see if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to the kiwi syslog machine?

A. ipaddress=192.168.153.150 -- port=514
B. Summon "The Force" and make it happen with your mind.
C. tcp.srcport==514 && ip.src==192.168.153.99
D. tcp.dstport==514 && ip.dst==192.168.153.150

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:
Looking for traffic TO Kiwi
syslog uses port 514 (this is where kiwi will listed)
Kiwi is running on 192.168.153.150
Note= Syslog uses UDP, so watch out on the test.

QUESTION 63
Which of the following tools can be used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. OpenVAS
C. Nessus
D. tcptraceroute

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
Tcptrace.org: Analyzes the dump file format generated by tcpdumpand other applications. Tracks host sessions and graphs rate of traffic

QUESTION 64
Which of the of the following security operations is used for determining the attack surface of an organization?

A. Training employees on the security policy regarding social engineering.
B. Using configuration management to determine when and where to apply security patches.
C. Running a network scan to detect network services in the corporate DMZ.
D. Reviewing the need for a security clearance for each employee.

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Identification of assets

QUESTION 65
env x='(){::};echo exploit' bash -c 'cat /etc/passwd'

What is the Shellshock bash vulnerability attempting to do on this vulnerable Linux host?

A. Removes the passwd file.
B. Add new user to the passwd file
C. Display passwd contents to prompt
D. Changes all password in passwd

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:
env x='(){::};echo exploit' bash -c 'cat /etc/passwd'

The idea of shellshock is that whatever you enter in the second part- -c 'cat /etc/passwd' will be executed, even if it is supposed to be blocked.

QUESTION 66
During a security audit of IT processes the auditor finds that there were no documented security procedures. What should the IS auditor do?

Choose all of the correct answers (multiple possibilities).

A. Terminate the audit.
B. Identify and evaluate existing practices.
C. Conduct compliance testing
D. Create a procedures document

Correct Answer: BC
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
If there are no official documented procedures, you audit the "standard" practices in use, as even informal ones would be discoverable through discussion.

If there are compliance related issues, they can still be tested.

QUESTION 67
You try to run the command nmap -T4 -O 10.10.10.0/24 from your command shell in Linux. You are not root (your prompt is a $ instead of #). You get an error message that says "Quitting".
What is mostly like the cause?

A. This is common behavior for a corrupted application.
B. The nmap syntax is wrong.

C. An OS scan requires root privileges.
D. Blocked.

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
stu@ubuntu:~$ nmap -O 192.168.132.0/24
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

QUESTION 68
What is the most common method to exploit the shellshock vulnerability?

A. SSH
B. String manipulation
C. Syn flood
D. CGI

Correct Answer: D
Section: Exploits
Explanation

Explanation/Reference:
Symantec: The most likely route of attack is through Web servers utilizing CGI (Common Gateway Interface)
curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/

This will sent an HTTP request to http://example.com that will make the CD eject....
https://blog.cloudflare.com/inside-shellshock/

() { :; }; is the key to shellshock

QUESTION 69
During a blackbox pentest you attempt to pass IRC traffic over port 80/tcp from a compromised web enabled host. The traffic gets blocked; however outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

A. Stateful
B. Circuit
C. Packet Filtering
D. Application

Correct Answer: D
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
An Application firewall recognizes the syntax and protocol of the application that should be using certain ports. It can then block traffic that is trying to using those ports for other reasons.

An application layer firewall is a kind Proxy Server

QUESTION 70
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a

sophisticated attack. Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?

A. zero-sum
B. zero-hour
C. zero-day
D. no-day

Correct Answer: C
Section: Malware
Explanation

Explanation/Reference:

QUESTION 71
TJ Max breach happened in part because this type of weak wireless security was implemented.

A. WPA2
B. TKIP
C. Wired Equivalent Privacy (WEP)
D. WiFi protected access (WPA)

Correct Answer: C
Section: Wireless
Explanation

Explanation/Reference:

QUESTION 72
What is the process of logging, recording and resolving events that take place in an organization?

A. Internal Procedure
B. Security Policy
C. Incident Management Process
D. Metrics

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 73
PGP, SSL, IKE are all examples of which type of cryptography?

A. Hash Algorithm
B. Secret Key
C. Private Key
D. Public Key

Correct Answer: D
Section: Cryptography

Explanation

Explanation/Reference:
I wish they had asymmetric as an option.....
NOTE: Digest and hash are the same thing

QUESTION 74
This configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described.

A. Promiscuous Mode
B. WEM
C. Port forwarding
D. Multicast

Correct Answer: A
Section: Wireless
Explanation

Explanation/Reference:
Promiscuous modeis a type of computer networking operational modein which all network data packets can be accessed and viewed by all network adapters operating in this mode.

QUESTION 75
How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
B. It sends a request packet to all the network elements, asking for the domain name from a specific IP.
C. It sends a reply packet for a specfic IP, asking for the MAC address.
D. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
The Address Resolution Protocol is a request and reply protocol that runs encapsulated by the line protocol. ARP is only for LOCAL traffic, it doesn't go past the router.

QUESTION 76
Which of the following is the greatest threat passed by backup?

A. A backup is unavailable during disaster recovery
B. A backup is the source of Malware or illicit information
C. A backup is incomplete because no verification was performed
D. An un-encrypted backup can be misplaced or stolen

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Although "A backup is unavailable during disaster recovery" and "A backup is incomplete because no verification was performed" are good answers, either one could be selected. They are both issues related to using the backup.

The asnwer "An un-encrypted backup can be misplaced or stolen" is something about the backup, regardless of its usefulness in recovery. The idea here is that some mitigations of risk (doing backups to prevent data loss), lead to additional risks.

QUESTION 77
The "black box testing" methodology enforces which kind of restriction?

A. Only the internal operation of a system is known to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Attack used to simulate an outsider

Black box testing

takes an external perspective of the test object to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid input and determines the correct output. There is no knowledge of the test object's internal structure.

White box testing

uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. In electrical hardware testing, every node in a circuit may be probed and measured; an example is in-circuit testing (ICT).

QUESTION 78
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

A. Maskgen
B. Burpsuite
C. Proxychains
D. Dimitry

Correct Answer: B
Section: Tools
Explanation

Explanation/Reference:
Burp Suite and Paros are both proxy tools

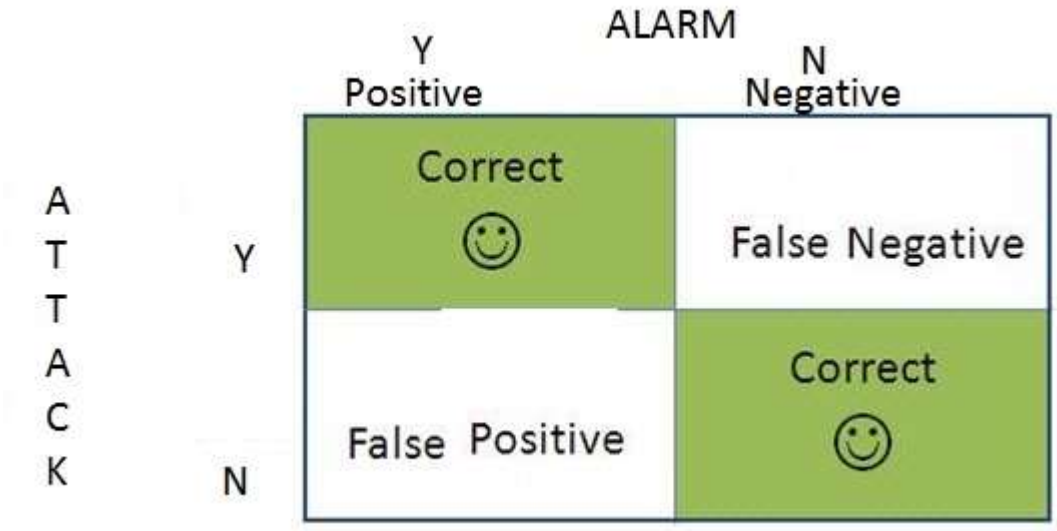
QUESTION 79
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. True Positive

B. False Negative
C. False Positive
D. True Negative

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:



QUESTION 80
The security concept of "separation of duties" is most similar to the operation of which type of security device?

A. Firewall
B. Bastion host
C. Honeypot
D. Intrusion Detection System

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
A Bastion hostis a special purpose computer on a network specifically designed and configured to withstand attacks.
The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

QUESTION 81
The "gray box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is completely known to the tester.
B. Only the internal operation of a system is known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Correct Answer: D

Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Secureideas: Grey box –This type of assessment has many definitions to many people.It is in between black box and white box testing.In this scenario, the tester may receive architectural diagrams, credentials, demonstrations of the application, communication with the target, and much more.

QUESTION 82
Which of the following is assured by the use of a hash?

A. Authentication
B. Confidentially
C. Availability
D. Integrity

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
Nothing is assured but a hash algorithm does provide the illusion of integrity and that is good enough to answer this question.
A keyed hash can provide a little more assurance.

QUESTION 83
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

A. HIPAA
B. ISO/IEC 27002
C. FISMA
D. COBIT

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 84
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
B. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
C. Attempts by attacks to access the user and password information stores in the company's SQL database.
D. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

Correct Answer: D

Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
Wikipedia:
In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft).

QUESTION 85
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

alert tcp any any -> 192.168.100.0/24 21 (msg: "'FTP on the network!"";)

A. An Intrusion Detection System
B. A Router IPTable
C. A firewall IPTable
D. FTP Server rule

Correct Answer: A
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Snort.org: http://manual.snort.org/node28.html

Rule will alert in the case of any tcp traffic going to 192.168.100.0/24 network for ports 21

QUESTION 86
This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

A. Institute of Electrical and Electronics Engineers (IEEE)
B. Center for Disease Control (CDC)
C. International Security Industry Organization (ISIO)
D. Payment Card Industry (PCI)

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 87
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Netstumbler
B. Kismet

C. Nessus
D. Abel

Correct Answer: B
Section: Wireless
Explanation

Explanation/Reference:
NetStumbler(also known as Network Stumbler) is a tool for **Windows** that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN

NetStumbler sends out 802.11 "Probe Request" frames for the SSID "ANY". Normally, any AP will answer with a "Probe Response" frame containing it's SSID and capability information (does the AP support WEP, what speeds does it support, etc..).

Kismet simply listens to the "Beacon Frame" that each AP sends out constantly, usually 5-10 per second or so. The SSID is embedded within the frame.

QUESTION 88
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A. Client is configured for the wrong channel
B. The wireless client is not configured to use DHCP
C. The client cannot see the SSID of the wireless network
D. The WAP does not recognize the client's MAC address

Correct Answer: D
Section: Wireless
Explanation

Explanation/Reference:
MAC Address Filtering can be put in place on WAPs

QUESTION 89
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

A. Download and Install Netcat
B. Disable Key Services
C. Disable IPTables
D. Create User Account

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
You want to maintain access.
Stetting up netcat as a listener on a port will give you a backdoor.
It can also help you ex filtrate data, like the password file.

Create User account is a good second option.

QUESTION 90

Jimmy is standing outside a secure entrance to a facility. He is pretending to be having a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close. What just happened?

A. Phishing
B. Masquerading
C. Piggybacking
D. Whaling

Correct Answer: C
Section: Social Engineering
Explanation

Explanation/Reference:
Piggybacking, Tailgating.

Wiki: Piggybacking(security), when an authorized person allows (intentionally or unintentionally) others to pass through a secure door.

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.

To describe the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person, the term tailgating is also used. "Tailgating" implies without consent (similar to a car tailgating another vehicle on the freeway), while "piggybacking" usually implies consent of the authorized person.

https://en.wikipedia.org/wiki/Piggybacking_(security)

QUESTION 91
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Intrusion Prevention System (IPS)
B. Protocol analyzer
C. Vulnerability scanner
D. Network sniffer

Correct Answer: B
Section: Tools
Explanation

Explanation/Reference:
A tool like Wireshark.

QUESTION 92
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $100
B. $146
C. $1320
D. $440

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
AV*EF=SLE; Asset Value * Exposure Factor= Single Loss Expectancy (exposure factor of 1 means it WILL happen)
SLE*ARO=ALE do the math Single Loss Expectancy * Annual Rate of Occurance= Annual Loss Expectancy

: If you do not include the labor cost the $300*1*.33=$99 (too exact)

If you include labor then:
AV=$300 + 14 hours*$10 = $440
SLE = $440*1 = $440
ARO = 1/3 or .33 (once very 3 years)
$440*.33= $146.6666666666667 AL

QUESTION 93
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

A. SYN Flood
B. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
C. SSH
D. Manipulate format strings in text fields

Correct Answer: B
Section: Exploits
Explanation

Explanation/Reference:
Symantec: The most likely route of attack is through Web servers utilizing CGI (Common Gateway Interface)
curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/

This will sent an HTTP request to http://example.com that will make the CD eject....
https://blog.cloudflare.com/inside-shellshock/

() { :; }; is the key to shellshock

QUESTION 94
Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A. Agile Process
B. Lean Coding
C. Object Oriented Architecture
D. Service Oriented Architecture

Correct Answer: D
Section: Web andapp Vulnerabilities

Explanation

Explanation/Reference:
Wiki: A service-oriented architecture(SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

QUESTION 95
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, The technique provides 'security through obscurity'. What technique is Ricardo using?

A. Steganography
B. Public-key cryptography
C. Encryption
D. RSA algorithm

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Is the practice of concealing a file, message, image, or video within another file, message, image, or video.

QUESTION 96
Which of the following is the successor of SSL?

A. TLS
B. GRE
C. RSA
D. IPSec

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2246: The differencesbetween this protocol and SSL3.0 are not dramatic, but they are significant enough that TLS1.0 and SSL3.0 do not interoperate (although TLS1.0 does incorporate a mechanism by which a TLSimplementation can back down to SSL3.0).

QUESTION 97
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Port scanner
B. Intrusion Detection System
C. Protocol analyzer
D. Vulnerability scanner

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:

Webopedia: The automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened

QUESTION 98
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Access Point
B. Wireless Analyzer
C. Wireless Access Control List
D. Wireless Intrusion Prevention System

Correct Answer: D
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities.

QUESTION 99
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

A. Use encrypted communications protocols to transmit PII
B. Use full disk encryption on all hard drives to protect PII
C. Use a security token to log into all Web applications that use PII
D. Use cryptographic storage to store all PII

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Not sure I like this answer.....
Many Web App vulnerabilities relate to gaining access to the data directly...I think token might be better.

QUESTION 100
Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is the middle step called?

A. String validating the code
B. Sandboxing the code
C. Third party running the code
D. Fuzzy-testing the code

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Sandboxing is a technique to limit access to other parts of a system.
Often seen in security in relationship to what a program can access on a particular machine.

QUESTION 101
In order to have an anonymous Internet surf, which of the following is best choice?

A. Use Tor network with multi-node
B. Use shared WiFi
C. Use SSL sites when entering personal information
D. Use public VPN

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".[8][9] Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays[10] to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

QUESTION 102
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. BBCrack
B. Blooover
C. BBProxy
D. Paros Proxy

Correct Answer: C
Section: Tools
Explanation

Explanation/Reference:

QUESTION 103
An attacker tries to do banner grabbing on a remote web server and executes the following command.
$nmap -sV host.domain.com -p 80
He gets the following output.
Starting Nmap 6.47 (http://nmap.org) at 2014-12-08 19:10 EST Nmap scan report for host.domain.com (108.61.158.211) Host is up (0.032s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
Service detection performed. Please report any incorrect results at http://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds What did the hacker accomplish?

A. The hacker should've used nmap -O host.domain.com
B. nmap can't retrieve the version number of any running remote service.
C. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server
D. The hacker successfully completed the banner grabbing.

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Wrong command for banner grabbing...
nmap -sV --script=banner <target>
Script Output

21/tcp open ftp
|_ banner: 220 FTP version 1.0\x0D\x0A

But it is the best answer

QUESTION 104
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACK
   Connection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACK
   Connection Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: SYN, SYN-ACK, ACK
   Connection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: ACK, ACK-SYN, SYN
   Connection Termination: FIN, ACK-FIN, ACK

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
SYN- SYN/ACK- SYN

QUESTION 105
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28. Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok
B. He needs to change the address to 192.168.1.0 with the same mask
C. He needs to add the command ""ip address"" just before the IP address
D. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range

Correct Answer: D
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

SUBNETTING TABLE

	128	64	32	16	8	4	2	1
Bits borrowed	1	2	3	4	5	6	7	8
Subnet Mask	128	192	224	240	248	252	n/a	n/a
/Mask	/25	/26	/27	/28	/29	/30	n/a	n/a
Wildcard Masks	.127	.63	.31	.15	.7	.3	n/a	n/a
Networks*	2	4	8	16	32	64	n/a	n/a
Hosts	126	62	30	14	6	2	n/a	n/a

* It is assumed that ip subnet zero is permitted on the cisco device.

This table is for the 4th octet.

QUESTION 106
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/password How can he use it?

A. The password file does not contain the passwords themselves.
B. The file reveals the passwords to the root user only.
C. He cannot read it because it is encrypted
D. He can open it and read the user ids and corresponding passwords.

Correct Answer: A
Section: Password Cracking
Explanation

Explanation/Reference:
It does have the usernames

QUESTION 107
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Exclamation mark
B. Single quote
C. Semicolon
D. Double quote

Correct Answer: B
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 108
Scenario:
Victim opens the attacker's web site.

Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?"
Victim clicks to the interesting and attractive content url. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?

A. ClickJacking Attack
B. HTTP Parameter Pollution
C. HTML Injection
D. Session Fixation

Correct Answer: A
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
OWASP
Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

QUESTION 109
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Basic example to understand how cryptography works is given below:
SECURE (plain text)
+1 (+1 next letter. for example, the letter ""T"" is used for ""S"" to encrypt.) TFDVSF (encrypted text)
+ = logic => Algorithm
1= Factor => Key

Which of the following choices are true about cryptography?

A. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.
B. Algorithm is not the secret, key is the secret.
C. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
D. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:

QUESTION 110
You want to analyze packets on your wireless network. Which program would you use?

A. Airsnort with Airpcap
B. Ethereal with Winpcap
C. Wireshark with Airpcap
D. Wireshark with Winpcap

Correct Answer: D
Section: Wireless
Explanation

Explanation/Reference:
You can capture and analyze wireless with Wireshark and WinpCap

Airsnort is for cracking WEP keys
AirpCap is required to inject for windows.

QUESTION 111
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system. If a scanned port is open, what happens?

A. The port will ignore the packets
B. The port will send a SYN
C. The port will send an ACK
D. The port will send an RST

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Closed ports send a reset for a TCP SYN
Open Ports send a syn/ack for a TCP SYN

Open ports ignore packets that aren't part of an existing connection (except for SYN)
Closed ports send a RST

QUESTION 112
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what is meant by processing?

A. The amount of time and resources that are necessary to maintain a biometric system
B. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information.
C. The amount of time it takes to convert biometric data into a template on a smart card
D. How long it takes to setup individual user accounts

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 113

How can rainbow tables be defeated?

A. Passwords salting
B. All uppercase character passwords
C. Lockout accounts under brute force password cracking attempts
D. Use of non-dictionary words

Correct Answer: A
Section: Password Cracking
Explanation

Explanation/Reference:

QUESTION 114
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Acceptable-use policy
B. Remote- access policy
C. Firewall-management policy
D. Permissive policy

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Modems, even for dial out, would be covered under remote access.

QUESTION 115
You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

A. Physically go to each server
B. Scan servers with Nmap
C. Scan servers with MBSA
D. Telnet to every port on each server

Correct Answer: B
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

QUESTION 116
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. OS X
B. Unix
C. Linux

D. Windows

Correct Answer: D
Section: Exploits
Explanation

Explanation/Reference:
shellshock was about the bash shell
No bash shell in windows

QUESTION 117
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Information protection policy
B. Remote access policy
C. Network security policy
D. Access control policy

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 118
A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

A. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.
B. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
C. Try to sell the information to a well-paying party on the dark web.
D. Ignore it.

Correct Answer: B
Section: Exploits
Explanation

Explanation/Reference:
Full Disclosure vs.....

QUESTION 119
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfencode
B. msfcli
C. msfd
D. msfpayload

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference:
Note: msfencode was removed on 2015-06-08

msfencode is another great little tool in the framework's arsenal when it comes to exploit development. Most of the time, one cannot simply use shellcode generated straight out of msfpayload. It needs to be encoded to suit the target in order to function properly. This can mean transforming your shellcode into pure alphanumeric, getting rid of bad characters or encoding it for 64 bit target.

Msfvenom is the combination of payload generation and encoding. It replaced msfpayload and msfencode on June 8th 2015.

QUESTION 120
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Time-to-check to time-to-use flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Input validation flaw

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:

QUESTION 121
Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA/local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?

A. Macro Virus
B. Worm
C. Trojan
D. Key-Logger

Correct Answer: C
Section: Malware
Explanation

Explanation/Reference:

QUESTION 122
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

A. Dictionary attack
B. Session hijacking
C. Brute-force attack
D. Man-in-the-middle attack

Correct Answer: A
Section: Password Cracking

Explanation

Explanation/Reference:

QUESTION 123
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
B. Vulnerabilities in the application layer are greatly different from IPv4
C. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addressed
D. Implementing IPv4 security in a dual-stack network offers protection form IPv6 attacks too.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 124
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Make sure that legitimate network routers are configured to run routing protocols with authentication.
B. Disable all routing protocols and only use static routes
C. Redirection of the traffic cannot happen unless the admin allow it explicitly
D. Only using OSPFv3 will mitigate this risk.

Correct Answer: A
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
If the rogue device can't convince the other routers to route through him, he wont be successful.
Router protocol authentication will limit the ability of a rogue router to affect performance and routing decisions in official equipment.

QUESTION 125
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.
Example: allintitle: root passwd

A. Gaining Access
B. Maintaining Access
C. Reconnaissance
D. Scanning and Enumeration

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Really, any phase. We all forget stuff.
But use your Google-Fu for research at the start.

QUESTION 126
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account. What should you do?

A. Do not transfer the money but steal the bitcoins.
B. Transfer money from the administrator's account to another account
C. Do not report it and continue the penetration test
D. Report immediately to the administrator

Correct Answer: D
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:
Assuming it isn't the administrators computer.

QUESTION 127
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Use a firewall between the public network and the payment card data
D. Rotate employees handling credit card transactions on a yearly basis to different departments.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 128
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the account was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

A. The CFO can use a hash algorithm in the document once he approved the financial statements
B. The CFO can use an excel file with a password
C. The document can be sent to the accountant using an exclusive USB for that document
D. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Comparing the hash to the one the CFO creates will validate that no changes have been made to the statements since the approval.

QUESTION 129

Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
C. Results for matches on target.com and Marketing.target.com that include the word "accounting"
D. Results matching "accounting" in domain target.com but not on the site Marketing.target.com

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:

QUESTION 130
Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Compound SQLi
B. Blind SQLi
C. DMS-specific SQLi
D. Classic SQLi

Correct Answer: B
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
OWASP
Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible. .

https://www.owasp.org/index.php/Blind_SQL_Injection

QUESTION 131
Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

A. Nothing, but suggest to him to change the network's SSID and password
B. Log onto his network, after all it is his fault that you can get it.
C. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
D. Only use his network when you have large downloads so you don't tax your own network

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 132
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation
B. Port Scanning
C. Shoulder-Surfing
D. Hacking Active Directory

Correct Answer: A
Section: Exploits
Explanation

Explanation/Reference:

QUESTION 133
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network?
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any access-list 108 permit tcp any eq ftp any
access-list 102 deny tcp any any

A. The ACL 104 needs to be first because is UDP
B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
C. The ACL 110 needs to be changed to port 80
D. The ACL for FTP must be before the ACL 110

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
There is so much wrong with this question and the asnwers, it is hard to start.
However, having a deny tcp any any at the start will mean that all TCP traffic will be blocked. Once a packet matches a statement, it doesn't get evaluated against any other statements.

A more legitimate questions would have something as follows:
access-list 102 deny tcp any any
access-list 102 permit udp host 10.0.0.3 any
access-list 102 permit tcp host 10.0.0.2 eq www any access-list 108 permit tcp any eq ftp any
access-list 102 deny tcp any any

Which would mean all the statements are in the same access list that we are assuming was applied to the interface.

QUESTION 134
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data through a technique known as wardriving. Which Algorithm is this referring to?

A. Wi-Fi Protected Access (WPA)

B. Wired Equivalent Privacy (WEP)
C. Wi-Fi Protected Access 2 (WPA2)
D. Temporal Key Integrity Protocol (TKIP)

Correct Answer: B
Section: Wireless
Explanation

Explanation/Reference:

QUESTION 135
There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

A. Polymorphism
B. Escrow
C. Collision
D. Collusion

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
In cryptography, a collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision. In contrast to a preimage attack the hash value is not specified.
https://en.wikipedia.org/wiki/Collision_attack

QUESTION 136
..... is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting user by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there. Fill in the blank with appropriate choice.

A. Evil Twin Attack
B. Collision Attack
C. Sinkhole Attack
D. Signal Jamming Attack

Correct Answer: A
Section: Wireless
Explanation

Explanation/Reference:

QUESTION 137
An attacker changes the profile picture information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
<iframe > src=http://www.vulnweb.com/updateif.php style="display:none" > </iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. SQL Injection
B. Browser Hacking
C. Cross-Site Scripting
D. Cross-Site Request Forgery

Correct Answer: C
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:
The question isn't great, but the idea is that the code will be executed when the victim logs back in. The code will execute on the client's machine.
It doesn't take advantage of the victim being authenticated elsewhere, so it is an example of cross site scripting.

Fundamental difference is that CSRF (Cross-site Request forgery) happens in authenticated sessions when the server trusts the user/browser, while XSS (Cross-Site scripting) doesn't need an authenticated session and can be exploited when the vulnerable website doesn't do the basics of validating or escaping input.

In case of XSS, when the server doesn't validate or escapes input as a primary control, an attacker can send inputs via request parameters or any kind of client side input fields (which can be cookies, form fields or url params). These can be written back to screen , persisted in database or executed remotely. For CSRF, consider an example when you are logged in into your banking site and at the same time logged into Facebook in another tab in same browser. An attacker can place a malicious link embedded in another link or zero byte image which can be like yourbanksite.com/transfer.do?
fromaccnt=youraccnt&toaccnt=attackersAccount&amt=2500. Now, if you accidentally click on this link , in the background transfer can happen though you clicked from the Facebook tab.

This is because your session is still active in browser and browser has your session id. This is the reason the most popular CSRF protection is having another server supplied unique token generated and appended in the request. This unique token is not something which is known to browser like session id. This additional validation at server (i.e whether the transfer request also contains the correct CSRF

QUESTION 138
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Security
B. Scalability
C. Key distribution
D. Speed

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
Symmetric encryption is much faster to process large amounts of data.
Key management is the issue.
That is why most systems use asymmetric protocols for key exchange of a shared key that will be used to actually encrypt and decrypt data.

QUESTION 139
An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

A. Use an IDS in the entrance doors and install some of them near the corners

B. Use lights in all the entrance doors and along the company's perimeter
C. Install a CCTV with cameras pointing to the entrance doors and the street
D. Use fences in the entrance doors

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 140
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Rainbow Table Attack
B. Brute Force Attack
C. Dictionary Attack
D. Hybrid Attack

Correct Answer: A
Section: Password Cracking
Explanation

Explanation/Reference:

QUESTION 141
Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. Not informing the employees that they are going to be monitored could be an invasion of privacy.
B. All of the employees would stop normal work activities
C. The network could still experience traffic slow down.
D. IT department would be telling employees who the boss is

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
This is fairly standard behavior for most companies.
If it is on the company network, the company has a right to it.

QUESTION 142
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass though the packet-filtering of the firewall.

A. Session hijacking
B. Network sniffing
C. Firewalking
D. Man-in-the-middle attack

Correct Answer: C
Section: Recon, Scanning, Enumeration

Explanation

Explanation/Reference:
To determine a rule on a given gateway, the scanner sends a probe to a metric located behind the gateway, with a TTL one higher than the gateway. If the probe is forwarded by the gateway, then we can expect to receive an ICMP_TIME_EXCEEDED reply from the gateway next hop router, or eventually the metric itself if it is directly connected to the gateway. Otherwise, the probe will timeout.
https://nmap.org/nsedoc/scripts/firewalk.html

QUESTION 143
Which of the following programming languages is less susceptible to buffer overflow attacks, due to built-in bounds checking mechanism?
Code:
#include
int main () {
char buffer[8];
strcpy(buffer,""11111111111111111111111111111"");
}
Output:
Segmentation fault

A. Python
B. C++
C. Java
D. C#

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:
Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows.

OWASP

Platforms Affected
Almost every platform, with the following notable exceptions:

Java/J2EE – as long as native methods or system calls are not invoked.
.NET – as long as unsafe or unmanaged code is not invoked (such as the use of P/Invoke or COM Interop).
PHP, Python, Perl – as long as external programs or vulnerable extensions are not used.

QUESTION 144
Which of the following programs is usually targeted at Microsoft Office products?

A. Stealth virus
B. Multipart virus
C. Macro virus
D. Polymorphic virus

Correct Answer: C
Section: Malware
Explanation

Explanation/Reference:

QUESTION 145
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

A. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
B. First the ping sweep to identify live hosts and then the port scan on the live hosts. The way he saves time.
C. The port scan alone is adequate, This way he saves time.
D. The sequence does not matter. Both steps have to be performed against all hosts.

Correct Answer: B
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
nmap -sn for a ping sweep to get a list of hosts.

QUESTION 146
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal, Whitebox
B. Internal, Blackbox
C. External, Whitebox
D. External,Blackbox

Correct Answer: B
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 147
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Polymorphic virus

Correct Answer: A
Section: Malware
Explanation

Explanation/Reference:
polymorphics try to hide as well, but do it by changing their code as they move amongst systems.

QUESTION 148

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of his Windows system you find two static routes:
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1
What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted
C. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to external gateway
D. Both static routes indicate that the traffic is internal with different gateway

Correct Answer: C
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:
Answer based on the fact that 10.0.0.0 is a reserved address used for internal traffic.
0.0.0.0 is a default- all non-recognized IP addresses, which would usually be external, get routed this way.

QUESTION 149
What is the role of test automation in security testing?

A. Test automation is not usable in security die to the complexity of the tests
B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies
C. It is an option but it tends to be very expensive
D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 150
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start using netcat to port 80. The engineer receives this output:

HTTP/1.1 200 OK Server: Microsoft-IIS/6 Expires: Tue, 17 Jan 2011 01:41:33 GMT Date: Mon, 16 Jan 2011 01:41:33 GMT Content-Type:text/html Accept-Ranges: bytes Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT ETag: "b0aac0542e25c31:89d" Content-Length: 7369

Which of the following is an example of what the engineer performed?

A. Banner grabbing
B. Whois database query
C. Cross-site scripting
D. SQL injection

Correct Answer: A

Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

QUESTION 151
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address
B. The computer is using an invalid IP address
C. The gateway and the computer are not on the same network
D. The computer is not using a private IP address

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reserved addresses don't route through the "public" internet, but can be used across a provide WAN.
10.0.0.0- 10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0 - 192.168.255.255

QUESTION 152
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. BIOS password
B. Password protected files
C. Hidden folders
D. Full disk encryption

Correct Answer: D
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:

QUESTION 153
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A page fault is occurring, which forces the operating system to write data from the hard drive
B. A race condition is being exploited, and the operating system is containing the malicious process
C. Malicious code is attempting to execute instruction in a non-executable memory region
D. Malware is executing in either ROM or a cache memory area

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:
This behavior occurs because Microsoft Windows XP SP2 uses the Data Execution Prevention (DEP) feature to help prevent damage from viruses and from other security threats.

DEP works alone or with compatible microprocessors to mark some memory locations as "non-executable." If a program tries to run code from a protected location, DEP closes the program and notifies you, whether the code is malicious or not.

QUESTION 154
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520. What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Root
B. Shared
C. Private
D. Public

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:

QUESTION 155
Which of these is capable of searching for and locating rogue access points?

A. NIDS
B. HIDS
C. WISS
D. WIPS

Correct Answer: D
Section: Wireless
Explanation

Explanation/Reference:
NIDS- Network intrusion detection system
HIDS- Host Intrusion detection System
WISS-???
WIPS- Wireless Intrusion Prevention System

QUESTION 156
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark
B. Metasploit
C. Nessus
D. Maltego

Correct Answer: B
Section: Tools

Explanation

Explanation/Reference:

QUESTION 157
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. TCP ping
B. Hping
C. Traceroute
D. Broadcast ping

Correct Answer: B
Section: Tools
Explanation

Explanation/Reference:
Hping allows you to select the port and flags you set and may sneak through a firewall.

QUESTION 158
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. smtp port
B. request smtp 25
C. tcp.contains port 25
D. tcp.port eq 25

Correct Answer: D
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
This is an example of a capture filter
a display filter would be smtp

QUESTION 159
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 -i host.domain.com
B. hping2 -1 host.domain.com
C. hping2 --set-ICMP host.domain.com
D. hping2 host.domain.com

Correct Answer: B
Section: Tools
Explanation

Explanation/Reference:
http://www.hping.org/manpage.html
Protocol Selection

Default protocol is TCP, by default hping2 will send tcp headers to target host's port 0 with a winsize of 64 without any tcp flag on. Often this is the best way to do an 'hide ping', useful when target is behind a firewall that drop ICMP. Moreover a tcp null-flag to port 0 has a good probability of not being logged.
-0 --rawip
RAW IP mode, in this mode hping2 will send IP header with data appended with --signature and/or --file, see also --ipproto that allows you to set the ip protocol field.

-1 --icmp
ICMP mode, by default hping2 will send ICMP echo-request, you can set other ICMP type/code using --icmptype --icmpcode options.

-2 --udp
UDP mode, by default hping2 will send udp to target host's port 0. UDP header tunable options are the following: --baseport, --destport, --keep.

-9 --listen signature
HPING2 listen mode, using this option hping2 waits for packet that contain signature and dump from signature end to packet's end. For example if hping2 --listen TEST reads a packet that contain 234-09sdflkjs45-TESThello_world it will display hello_world.

QUESTION 160
Which service in a PKI will vouch for the identity of an individual or company?

A. CR
B. KDC
C. CBC
D. CA

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
Certificate Authority

QUESTION 161
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan
B. TCP Connect scan
C. TCP SYN
D. Idle Scan

Correct Answer: B
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Most IDS will detect a regular port scan

QUESTION 162
What two conditions must a digital signature meet?

A. Must be unique and have special characters.
B. Has to be the same number of characters as a physical signature and must be unique.
C. Has to be unforgeable, and has to be authentic.

D. Has to be legit and neat.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:

QUESTION 163
Which of the following is a series vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. SSL/TLS Renegotiation Vulnerability
B. POODLE
C. Heartbleed Bug
D. Shellshock

Correct Answer: C
Section: Exploits
Explanation

Explanation/Reference:
Heartbleed was specifically related to the heartbeat feature, which wasn't always enabled.

QUESTION 164
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of emails?

A. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.
B. A blacklist of companies that have their mail server relays configured to be wide open.
C. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
D. Mail relaying, which is a technique of bouncing e-mail from internal to external mail servers continuously.

Correct Answer: D
Section: Exploits
Explanation

Explanation/Reference:

QUESTION 165
Which of the following Nmap commands will produce the following output?
Output:
Starting Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs

17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown

A. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
B. nmap -sN -Ps -T4 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

Correct Answer: D
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
-sS and -sU means do both TCP syn and UDP scans.

QUESTION 166
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on physical attributes.
B. An authentication system that creates one-time passwords that are encrypted with secret keys
C. A biometric system that bases authentication decisions on behavioral attributes
D. An authentication system that uses passphrases that are converted into virtual passwords

Correct Answer: B
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:

QUESTION 167
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Authenticate
B. Encrypt
C. Protect the payload and the headers
D. Work at the Data Link Layer

Correct Answer: D
Section: Defense- IDS, Firewalls & Honeypots
Explanation

Explanation/Reference:

QUESTION 168
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case. Metasploit Framework has a module for the technique; psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump,pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'

A. NT:LM
B. NTLM:LM
C. LM:NTLM
D. LM:NT

Correct Answer: C
Section: Password Cracking
Explanation

Explanation/Reference:

QUESTION 169
What is the difference between the AES and RSA algorithms?

A. Both are symmetric algorithms, but AES uses 256-bit keys.
B. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.
C. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
D. Both are asymmetric algorithms, but RSA uses 1024-bit keys.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:

QUESTION 170
The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:
Time:Mar 12 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination 192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 12 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
What type of activity has been logged?

A. Port scan targeting 192.168.1.106
B. Teardrop attack targeting 192.168.1.106
C. Denial of service attack targeting 192.168.1.103

D. Port scan targeting 192.168.1.103

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
same source and destination IP with a range of common ports.

QUESTION 171
A security team is doing a network scan. While doing reconnaissance on a host, they found several ports opened that were confusing in concluding the Operating System (OS) version installed.
Based on the NMAP result below, which OS is likely to be installed on the target machine?

Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
80/tcp open http
139/tcp open netbios-ssn
515/tcp open
631/tcp open ipp
9100/tcp open
MAC Address: 00:00:48:0D:EE:8

A. The host is likely a Windows machine
B. The host is likely a Linux machine
C. The host is likely a printer
D. The host is likely a router

Correct Answer: C
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

QUESTION 172
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

A. ICMP could be disabled on the target server
B. ARP is disabled on the target server
C. You need to run ping with root privelege
D. TCP/IP doesn't support ICMP

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
ICMP being disabled is the best answer.

Specific ICMP message types could be blocked as well (ICMP Echo reply, ICMP TTL Exceeded, etc).

ARP is necessary for local network communication.
You don't usually need root access to ping
ICMP is a protocol in the TCP/IP stack

QUESTION 173
Which of the following Nmap commands will produce an X-mas tree scan?

A. nmap -sX 192.168.1.1
B. nmap -sN -Ps -T4 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

Correct Answer: A
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:

QUESTION 174
Which flags are used in an Nmap X-mas scan?

A. FIN
B. PUSH, URG, FIN
C. SYN, FIN
D. SYN, ACK

Correct Answer: B
Section: Recon, Scanning, Enumeration
Explanation

Explanation/Reference:
Null scan (-sN)
Does not set any bits (TCP flag header is 0)

FIN scan (-sF)
Sets just the TCP FIN bit.

Xmas scan (-sX)
Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

QUESTION 175
Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Eradication phase
B. Recovery phase
C. Containment phase
D. Preparation phase
E. Identification phase

Correct Answer: D
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 176
XOR is a common cryptographic tool.
10110001 XOR 00111010 is?

A. 10111100
B. 11011000
C. 10011101
D. 10001011

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
XOR-
10110001
00111010

Result
10001011

XOR truth table

Input		Output
A	B	
0	0	0
0	1	1
1	0	1
1	1	0

QUESTION 177
First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?

A. Delete the email and pretend nothing happened.
B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.
C. Forward the message to your company's security response team and permanently delete the message from your computer.
D. Reply to the sender and ask them for more information about the message contents.

Correct Answer: C
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 178
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

A. Social Engineering
B. Piggybacking

C. Tailgating
D. Eavesdropping

Correct Answer: A
Section: Social Engineering
Explanation

Explanation/Reference:

QUESTION 179
The following are types of Bluetooth attack EXCEPT_____?

A. Bluejacking
B. Bluesmaking
C. Bluesnarfing
D. Bluedriving

Correct Answer: D
Section: Tools
Explanation

Explanation/Reference:
Although Bluedriving can refer to driving around trying to identify bluetooth devices, each of the others are specific types of attacks.

QUESTION 180
A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

A. Insufficient security management
B. Insufficient database hardening
C. Insufficient input validation
D. Insufficient exception handling

Correct Answer: A
Section: Web andapp Vulnerabilities
Explanation

Explanation/Reference:

QUESTION 181
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:

QUESTION 182
Perspective clients want to see sample reports from previous penetration tests.
What should you do next?

A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.

Correct Answer: A
Section: Intro to Ethical Hacking
Explanation

Explanation/Reference:

QUESTION 183
Which of the following is a tool that will copy details from a USB drive without user knowing it?

A. USBDumper
B. USBShuffle
C. USBCrash
D. dd

Correct Answer: A
Section: Tools
Explanation

Explanation/Reference: