CERTIFIED ETHICAL HACKER

1)An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

Aircrack-ng

2) Which of the following is a passive wireless packet analyser that works on Linux-based Systems?

Kismet

3) Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

ESP transport mode

4) The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's common Vulnerabilities and exposures(CVE) as CVE-204-0160. 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?

Private

5) 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?

Attempts by attackers to access web sites that trust the web browser user by stealing the user's authentication credentials.

6) When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

Modifying and replaying captured network traffic

7) Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did chandler use in this context?

Heuristic Analysis

8) You have successfully comprised a server having an IP address of 10.10.10.5 you would like to enumerate all machines in the same network quickly. What is the best nmap command you will use?

Nmap -T4 -F 10.10.10.1/24

9) How can rainbow tables be defeated?

Password salting

10) An internet service provider(ISP) has a need to authenticate users connecting via analog modems, Digital subscriber Lines(DSL), wireless data services, and Virtual Private Networks(VPN) over a Frame Relay Network which AAA protocol is the mose likely able to handle this requirement?

RADIUS

11) 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 defences and gain access to the prometric Online Testing-Reports https://ibt1.prometric.com/users/custom/report-queue/rq-str... Corporate network. What tool shoud the analyst use to perform a Blackjacking attack?

BBProxy

12) while using your bank's online servicing you notice the following string in the URL bar:

http://www.MypersonalBank.com/account?id=3689409110283 89&Damount=10980&Camout=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

Web Parameter Tampering

13) Which of the following antennas is commonly used in communications for a frequency band of 10MHz to VHF an UHF?

Yagi antenna

14) What is the process for allowing or blocking a specific port in the windows firewall?(For example, TCP port 22 inbound)

The firewall rule must be added from within the application that is using that port.

15) Websites and web portals that provide web services commonly use the Simple Object Access Protocol(SOAP), Which of the following is an incorrect definition or characteristics of the protocol?

Only compatible with the application protocol HTTP

16) what is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?s

Through web servers utilizing CGI(Common Gateway Interface)to send a malformed environment variable to a vulnerable web server

17) Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results? TCP port 21 no response TCP port 22 no response TCP port 23 Time-to live exceeded

The scan on port 23 passed through the filetering device. This indicates that port 23 was not blocked at the firewall.

18) Which method of password cracking takes the mose time and effort?

Brute force

19) You have compromised a server on a network and successfully opened a shell. You aimed to identify all operatinf systems running on the network. However, as you attempt to fingerprint all machiens in the network using the nmap syntax below, it is not going through. invictus@victim_server:~$ nmap -T4 -O 10.10.10.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxx xxxxxxxxxx. QUITTING! What seems to be wrong?

OS Scan requires root privileges

20) 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, 192.168.1.124. An attacker is trying to find those servers but her cannot see them in his scanning. The command he is using is namp 192.168.1.64/28 why he cannot see the servers?

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.

21) During the process of encryption and decryption, what keys are shared?

Public Keys

22) You have gained physical access to a windows 2008 R2 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 toolkit, you have an ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user’s password or activate disabled Windows accounts?

CHNTPW

23) 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 organziation's interest and your liabilities as a tester?

Rules of Engagement

24) 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?

An authentication system that creates one-time passwords that are encrypted with secret keys.

25) 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?

Metasploit

26) Id executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

Civil

27) 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?

C:\compmgmt.msc

28) From the following table, identify the wrong answer in terms of Range(ft). Standart Range(ft) 802.11a 150-150 802.22b 150-150 802.16(WiMax) 30 miles

802.11a

29) Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

Logic tier

30) Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

UDP 514

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

TCP SYN

32) What is a "Collision attack" in cyptography?

Collision attacks try to find two inputs producing the same hash

33) which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature based IDS?

Can identify unknown attacks

34) If you want to only scan fewer ports that the default scna using Nmap tool, which option would you use?

-F

35) You need a tool that can do network intrusion prevention and intrusion Detection function as a network sniffer and record network activity. What tool would you most likely select?

Snort

36) Your company performs penetration test and security assessments for small and medium-sized business in the lcal area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking. What should you do?

Immediately stop work and contact proper legal authorities

37) CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office New York, you craft a specially formatted email message and send it across the internet to an employee of Company XYZ. The employee of Company XYZ is

aware your test. Your email message looks like this : From: jim_miller@companyxyz.com TO:michelle_saunders@companyxyz.com Subject: Test message Date:4/3/2017 14:37 The employee of companyXYZ receives your email message. This Proves that CompanyXYZs email gateway doesn't prevent what?

Email Spoofing

38) What is not a PCI compliance recommendation?

Use encryption to protect all transmission of card holder data over any public network

39) What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

Cross-site request forgery

40) In IPv6 what is the major differenct concerning application layer vulnerabilities compared to IPv4?

Vulnerabilities in the application layer are independent of the network layer, Attacks and mitigation techniques are almost identical.

41) Which of the following provides a security professional with most information about the system's security posture?

Port scanning, banner grabbing, service identification

42) What would you enter if you wanted to perform a stealth scan using Nmap?

Nmap -sS

43) When you are getting information about a web server, it is very important to know the HTTP Methods(GET,POST,HEAD,PUT,DELETE, TRACE) that are available because there are two critical methods(PUT AND DELETE)

PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods(GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What nmap script will help you with this task?

http-methods

44) Which results will be returned with the following google search query? Site:target.com-site:Marketing.target.com accounting

Resutls for matches on target.com and Marketing.target.com that include the word accounting

45) Which of the following describes the characteristics of a Boot Sector Virus?

Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

46) You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

Nmap -sT -O -T0

47) Which of the following is the best countermeasure to encrypting ransomwares?

Keep some generation of off-line backup

48) #!/usr/bin/python import socket buffer=(“”A””) counter=50 while len(buffer) <= 100; buffer.append(“”A””*counter) counter=counter+50 commands=(“”HELP””,STATS ,””,””RTIME ,””,””LTIME,’’’’,’’’’srun ,’’’’,’’’’TRUN , ‘’’’,’’’’GMON ,’’’’,’’’’GDOG ,’’’’,’’’’KSTET ,’’’’,’’’’GTER ,’’’’,’’’’HTER’’’’ ,’’’’,’’’’LTER ,’’’’,’’’’KSTAN, ‘’’’) for command in commands;
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect((‘127.0.0.1’,9999)) s.recv(50) s.send(command+buffstring)
s.close() what is the code written for?

Buffer Overflow

49) A company's web development team has become aware of a certain type of security vulnerability in their web software. To mitigate the possibility of this vulnerabilitiy being exploited, the team wants to modify the software requiremetns to disallow users from entering HTML as input into their web application. What kind of web application vulnerability likely exists in their software?

Cross-site scripting vulnerability

50) What is the lest important information when you analyse a public IP address in a security alert?

ARP

51) Rebecca commonly sees an error on her windows system that sates that a Data execution prevention (DEP) error has taken place. Which of the following is most likely taking place?

Mallicious code is attempting to execute instruction in a non-executable memory region.

52) 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 complemented, the student decides to write a script that pulls password from a list of commonly used passwords attack is the student attempting?

Dictionary attack

53) Which tool can be used to silently copy files form USB devices?

USB Dumper

54) A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data centre is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

Network elements must be hardened with user ids and strong passwords, Regular security tests and audits should be performed

55) On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service. What is the name of the process by which you can determine those critical business?

Business Impact Analysis(BIA)

56) Cross-site request forgery involves:

Modification of a request by a proxy between client and server

57) While performing online banking using a web browser, a use receives an email that contains a link to an interesting web site. When the user clicks on the link, another web browser sessin starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What web browser-based security vulnerability was exploited to compromise the user?

Cross-site Request Forgery

58) What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

Encrypt the data on the hard drive

59) What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyses the received response?

Active

60) Which access control mechanism allows for multiple systems to use a central authentication server(CAS) that permits users to authenticate once and gain access to multiple systems?

Single sign-on

61) Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect SQL injection attacks?

Web application firewall

62) Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

Internet Key Exchange (IKE)

63) You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible intrusion Detection System. What is the best approach?

Install Cryptcat and encrypt outgoing packets from this server.

64) A company's policy requires employees to perform the transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic form the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic which command can be used as a display filter to find unencrypted file transfers?

Tcp.port = = 21 ||tcp.port ==22

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. He also 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 the ftp, and the permitted hosts cannot access 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

The ACL 104 needs to be first because is UDP

The ACL for FTP must be before the ACL 110

The ACL 110 needs to be changed to port 80

The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23. Which of the following IP addresses could be leased as a result of the new configuration?

10.1.4.156

10.1.4.254

10.1.5.200

10.1.255.200

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

PPP

SET

IPSEC

PEM

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

DMS-specific SQLi

Classic SQLi

Compound SQLi

Blind SQLi

From the following table, identify the wrong answer in terms of Range (ft).

Standard	Range (ft)
802.11a	**150-150**
802.11b	**150-150**
802.11g	**150-150**
802.16 (WiMax)	**30 miles**

802.16 (WiMax)

802.11a

802.11b

802.11g

Answer

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?

c:\ncpa.cpl

c:\services.msc

c:\compmgmt.msc

c:\gpedit

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

Integrity

Authentication

Non-Repudiation

Confidentiality

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

Bluejacking

Bluesnarfing

Bluesmacking

BlueSniffing

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

IDS log

Internet Firewall/Proxy log

Event logs on the PC

Event logs on domain controller

Scenario: 1. Victim opens the attacker's web site. 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'. 3. Victim clicks to the interesting and attractive content url. 4. 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?

Session Fixation

HTML Injection

HTTP Parameter Pollution

ClickJacking Attack

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service. What is the name of the process by which you can determine those critical businesses?

Emergency Plan Response (EPR)

Business Impact Analysis (BIA)

Disaster Recovery Planning (DRP)

Risk Mitigation

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 firewall IPTable

An Intrusion Detection System

A Router IPTable

FTP Server rule

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

Backdoor

False-negative

Brute force attack

False-positive

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

Botnet Trojan

Ransomware Trojans

Banking Trojans

Turtle Trojans

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?

Double quote

Exclamation mark

Semicolon

Single quote

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

msfd

msfencode

msfpayload

msfcli

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

HIDS

WISS

NIDS

WIPS

What is the least important information when you analyze a public IP address in a security alert?

DNS

ARP

Whois

Geolocation

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?

Permissive policy

Remote-access policy

Acceptable-use policy

Firewall-management policy

Based on the below log, which of the following sentences are true? Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.

SSH communications are encrypted itâ€™s impossible to know who is the client or the server.

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

Capturing a network traffic for further analysis

Identifying operating systems, services, protocols and devices

Modifying and replaying captured network traffic

Collecting unencrypted information about usernames and passwords

Why containers are less secure than virtual machines ?

Host OS on containers has a larger surface attack.

A compromise container may cause a CPU starvation of the host.

Containers are attached to the same virtual network.

Containers may fullfill disk space of the host.

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?

Double quote

Exclamation mark

Semicolon

Single quote

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.

As long as the physical access to the network elements is restricted, there is no need for additional measures

The operator knows that attacks and down time are inevitable and should have a backup site

Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through. invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING! What seems to be wrong?

OS Scan requires root privileges.

This is a common behavior for a corrupted nmap application.

The outgoing TCP/IP fingerprinting is blocked by the host firewall.

The nmap syntax is wrong.

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine. What nmap script will help you with this task?

http-git

http enum

http-methods

http-headers

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

Web form input validation

Cross-Site Scripting

Cross-Site Request Forgery

Clickjacking

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

Announced

Reverse Social Engineering

Piggybacking

Tailgating

Based on the below log, which of the following sentences are true? Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.

SSH communications are encrypted itâ€™s impossible to know who is the client or the server.

What is the process for allowing or blocking a specific port in the Windows firewall? (For example, TCP port 22 inbound)

This is not possible without installing third-party software since Windows only allows changing firewall settings for individual applications.

A rule matching these requirements can be created in "Windows Firewall with Advanced Security", located in the Control Panel.

The firewall rule must be added from within the application that is using that port.

The only way to implement a specific rule like this is to use the "netsh" program on the command-line.

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?

The network must be down and the nmap command and IP address are ok

He needs to add the command ""ip address"" just before the IP address

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

He needs to change the address to 192.168.1.0 with the same mask

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

hping2 -1 host.domain.com

hping2 host.domain.com

hping2 -i host.domain.com

hping2 --set-ICMP host.domain.com

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

tcp.port == 21

tcp.port == 21 || tcp.port == 22

tcp.port != 21

tcp.port = 23

Answer

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

SSL

Ipsec

SFTP

FTPS

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

nmap -A - Pn

nmap -sP -p-65535 -T5

nmap -A --host-timeout 99 -T1

nmap -sT -O -T0

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

AH Tunnel mode

ESP tranport mode

AH permiscuous

ESP confidential

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?

Malicious code is attempting to execute instruction in a non-executable memory region.

A page fault is occurring, which forces the operating system to write data from the hard drive

Malware is executing in either ROM or a cache memory area.

A race condition is being exploited, and the operating system is containing the malicious process

You have gained physical access to a Windows 2008 R2 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 toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

John the Ripper

Cain & Abel

CHNTPW

SET

Which type of security feature stops vehicles from crashing through the doors of a building?

Bollards

Receptionist

Turnstile

Mantrap

Which method of password cracking takes the most time and effort?

Shoulder surfing

Brute force

Dictionary attack

Rainbow tables

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?

Hacking Active Directory

Shoulder-Surfing

Privilege Escalation

Port Scanning

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 organization's interest and your liabilities as a tester?

Rules of Engagement

Service Level Agreement

Non-Disclosure Agreement

Project Scope

What is a "Collision attack" in cryptography?

Collision attacks try to break the hash into three parts to get the plaintext value.

Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.

Collision attacks try to get the public key

Collision attacks try to find two inputs producing the same hash

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?

Dictionary attack

Brute-force attack

Session hijacking

Man-in-the-middle attack

What is the least important information when you analyze a public IP address in a security alert?

DNS

ARP

Whois

Geolocation

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?

Permissive policy

Remote-access policy

Acceptable-use policy

Firewall-management policy

An attacker scans a host with the below command. Which three flags are set? # nmap -sX host.domain.com

This is ACK scan. ACK flag is set.

This is Xmas scan. URG, PUSH and FIN are set.

This is SYN scan. SYN flag is set.

This is Xmas scan. SYN and ACK flags are set.

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?

Root

Shared

Public

Private

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

Transport

Application

Session

Presentation

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

Session hijacking

Cross-site scripting

Cross-site request forgery

Server side request forgery

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?

Proxychains

Burpsuite

Maskgen

Dimitry

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

ACK flag probe scanning

ICMP Echo scanning

SYN/FIN scanning using IP fragments

IPID scanning

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristics of the protocol?

Provides a structured model for messaging

Based on XML

Only compatible with the application protocol HTTP

Exchanges data between web services

What would you enter if you wanted to perform a stealth scan using Nmap?

nmap -sM

nmap -sU

nmap -sS

nmap -sT

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?

The client cannot see the SSID of the wireless network

The WAP does not recognize the client's MAC address

Client is configured for the wrong channel

The wireless client is not configured to use DHCP

During the process of encryption and decryption, what keys are shared?

Public keys

Public and private keys

Private keys

User passwords

Which of the following program infects the system boot sector and the executable files at the same time?

Stealth virus

Polymorphic virus

Macro virus

Multipartite Virus

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

Passive

Active

Distributive

Reflective

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication "open" but sets the SSID to a 32-character string of random letters and numbers. What is an accurate assessment of this scenario from a security perspective?

Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.

Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".

It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.

Which of the following provides a security professional with most information about the system's security posture?

Social engineering, company site browsing, tailgating

Wardriving, warchalking, social engineering

Phishing, spamming, sending trojans

Port scanning, banner grabbing, service identification

ping -* 6 192.168.0.101 output Pinging 192.168.0.101 with 32 bytes of data: Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.0.101: Packets: Sent = 6, Received = 6, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms What does the option * indicate?

t

n

s

a

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

Omnidirectional antenna

Yagi antenna

Parabolic grid antenna

Dipole antenna

In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name

Both pharming and phishing attacks are identical

Both pharming and phishing attacks are purely technical and are not considered forms of social engineering

In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name

Answer | Mark for review and Next

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

TCP SYN

TCP Connect scan

Spoof Scan

Idle Scan

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

False positive

True positive

True negative

False negative

An IT employee got a call from one our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

Disregarding the call, the employee should hang up.

Since the company's policy is all about Customer Service, he/she will provide information.

The employee can not provide any information; but, anyway, he/she will provide the name of the person in charge.

The employee should not provide any information without previous management authorization.

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 by 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?

Cross-site scripting

Banner grabbing

Whois database query

SQL injection

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

Install and use Telnet to encrypt all outgoing traffic from this server.

Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Use Alternate Data Streams to hide the outgoing packets from this server.

Install Cryptcat and encrypt outgoing packets from this server.

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

Single sign-on

Windows authentication

Discretionary Access Control (DAC)

Role Based Access Control (RBAC)

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

dns --snoop update.antivirus.com

dnsnooping -rt update.antivirus.com

nslookup -norecursive update.antivirus.com

nslookup -fullrecursive update.antivirus.com

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

Allocate funds for staffing of audit log review

Perform a vulnerability scan of the system

Determine the impact of enabling the audit feature

Perform a cost/benefit analysis of the audit feature

"..... 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 users 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 the appropriate choice.

Evil Twin Attack

Signal Jamming Attack

Sinkhole Attack

Collision Attack

Answer

Which system consists of a publicly available set of databases that contain domain name registration contact information?

IANA

WHOIS

IETF

CAPTCHA

Which tool can be used to silently copy files from USB devices?

USB Dumper

USB Sniffer

USB Snoopy

USB Grabber

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?

An authentication system that uses passphrases that are converted into virtual passwords

An authentication system that creates one-time passwords that are encrypted with secret keys

A biometric system that bases authentication decisions on physical attributes.

A biometric system that bases authentication decisions on behavioral attributes

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

Wireshark with Airpcap

Ethereal with Winpcap

Airsnort with Airpcap

Wireshark with Winpcap

Answer

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

if (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit

Emil uses nmap to scan two hosts using this command: nmap -sS -T4 -O 192.168.99.1 192.168.99.7 He receives this output: Nmap scan report for 192.168.99.1 Host is up (0.00082s latency). Not shown: 994 filtered ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 53/tcp open domain 80/tcp open http 161/tcp closed snmp MAC Address: B0:75:D5:33:57:74 (ZTE) Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33 Network Distance: 1 hop Nmap scan report for 192.168.99.7 Host is up (0.000047s latency). All 1000 scanned ports on 192.168.99.7 are closed Too many fingerprints match this host to give specific OS details Network Distance: 0 hops What is his conclusion?

He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7

Host 192.168.99.7 is down (Marked for Review)

Host 192.168.99.1 is the host that he launched the scan from

Host 192.168.99.7 is a an iPad.

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

Ettercap

Aircrack-ng

Wireshark

Tcpdump

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users

LDAP Injection attack

Cross-Site Request Forgery (CSRF)

SQL injection attack

Cross-Site Scripting (XSS)

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access. A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

Biological motion cannot be used to identify people

The solution will have a high level of false positives

Although the approach has two phases, it actually implements just one authentication factor

The solution implements the two authentication factors: physical object and physical characteristic

Answer | Mark for review and Next

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause?

- **The attacker altered or erased events from the logs.**
- The security breach was a false positive.
- The network devices are not all synchronized.
- Proper chain of custody was not observed while collecting the logs.

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned. Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

- **"GET /restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"**
- "GET /restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
- "GET /restricted/ HTTP/1.1 Host: westbank.com"
- "GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

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 the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball 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 must be present to make this remote attack possible?

Brute force login

Directory traversal

File system permissions

Privilege escalation

When tuning security alerts, what is the best approach?

Tune to avoid False positives and False Negatives

Decrease False negatives

Rise False positives Rise False Negatives

Decrease the false positives

Which of the following statements is TRUE?

Packet Sniffers operate on the Layer 1 of the OSI model.

Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.

Packet Sniffers operate on Layer 2 of the OSI model.

Packet Sniffers operate on Layer 3 of the OSI model.

An attacker changes the profile 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?

SQL Injection

Browser Hacking

Cross-Site Request Forgery

Cross-Site Scripting

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

Can identify unknown attacks

Produces less false positives

Requires vendor updates for new threats

Cannot deal with encrypted network traffic

When tuning security alerts, what is the best approach?

Tune to avoid False positives and False Negatives

Decrease False negatives

Rise False positives Rise False Negatives

Decrease the false positives

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23. Which of the following IP addresses could be leased as a result of the new configuration?

10.1.4.156

10.1.4.254

10.1.5.200

10.1.255.200

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. He also 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 the ftp, and the permitted hosts cannot access 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

The ACL 104 needs to be first because is UDP

The ACL for FTP must be before the ACL 110

The ACL 110 needs to be changed to port 80

The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

Answer | Mark for review and Next

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

Vulnerabilities in the application layer are greatly different from IPv4

Implementing IPv4 security in a dual-stack network offers protection from IPv6 atttacks too.

Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addressed

Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised. What kind of attack does the above scenario depict?

Spear Phishing Attack

Rootkit Attack

Advanced Persistent Threats

Botnet Attack

What is correct about digital signatures?

A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

Digital signatures are issued once for each user and can be used everywhere until they expire.

Digital signatures may be used in different documents of the same type.

A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

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?

c:\ncpa.cpl

c:\services.msc

c:\compmgmt.msc

c:\gpedit

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

Bluejacking

Bluesnarfing

Bluesmacking

BlueSniffing

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

Manipulate format strings in text fields

SYN Flood

Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

SSH

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service. What is the name of the process by which you can determine those critical businesses?

Emergency Plan Response (EPR)

Business Impact Analysis (BIA) (Marked for review)

Disaster Recovery Planning (DRP)

Risk Mitigation