- **Question 1**

0 out of 1 points

Local Web proxies such as Burp Suite or WebScarab are primarily used for:

Selected Answer:	Testing a website for security problems, by intercepting requests between a remote victim and a server
Answers:	Testing a website for security problems, by intercepting requests between a remote victim and a server
	Pivoting between compromised servers
	Testing a website for security problems, by intercepting requests between an attacker and a server
	Hiding the identity of the attacker

- **Question 2**

0 out of 1 points

Which of the following would NOT be conducted during a typical vulnerability scan?

Selected Answer:	Probe the system(s), to determine status and configuration of services
Answers:	Probe the system(s), to determine status and configuration of services
	Exploit vulnerabilities
	Port scans
	Service identification on each open port

- **Question 3**

0 out of 1 points

Which of the following is NOT an advantage of vulnerability scanning vs penetration testing

Selected Answer:	Systematic and consistent results
Answers:	Systematic and consistent results
	Automated and easy to conduct
	Less likely to cause accidental damage
	Thorough and complete

- **Question 4**

1 out of 1 points

OpenVAS is a fork of which project?

Selected Answer:	Nessus
Answers:	Nexpose
	Nessus
	MSF
	Nmap

- **Question 5**

1 out of 1 points

Which of the following tools includes scripts for performing vulnerability analysis scans?

Selected Answer: Nmap

Answers: Dig

Msfconsole

Amap

Nmap

- **Question 6**

1 out of 1 points

If a vulnerability scanner reports that port 80 is open on a Web server, what should you do:

Selected Answer: Nothing, this is normal

Answers: Nothing, this is normal

Investigate further, it looks like you have malware

Change to use a more up-to-date web server, this server is vulnerable to attack

Use a firewall to block the port

- **Question 7**

1 out of 1 points

A vulnerability scan will never crash the system being scanned

Selected Answer: False

Answers: True

False

- **Question 8**

1 out of 1 points

Which of the following is NOT a Vulnerability scanner?

Selected Answer: MSF

Answers: Nessus

None of these

OpenVAS

Nexpose

MSF

- **Question 9**

0 out of 1 points

If Nessus detects that a server has port 443 open, this most likely means:

Selected Answer: That it is probably a web server, and WILL be vulnerable to attack

Answers: That it is probably a web server

That the system is vulnerable to attack

That it is probably a web server, and WILL be vulnerable to attack

That the system is likely vulnerable to attack via the RPC DCOM vulnerability

- **Question 10**

1 out of 1 points

A current organisation should NOT use Windows Server 2000 as a webserver. Why not?

Selected Answer: Windows 2000 contains many security vulnerabilities such as buffer overflows, which will never be fixed since it has reached end of lifecycle

Answers: Windows 2000 was not designed to host websites

Windows should NEVER be used as a server

Windows 2000 contains many security vulnerabilities such as buffer overflows, which will never be fixed since it has reached end of lifecycle

There are no fixes available for Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (CVE-2003-0352)

- **Question 11**

1 out of 1 points

What port does CVE-2003-0352 affect?

Selected Answer: 135

Answers: 8080

21

80

135

- **Question 12**

0 out of 1 points

What is a disadvantage of using Armitage's "Find Attacks" feature?

Selected Answer: All of these

Answers: Causes lots of network traffic, including log entries that would raise suspicions

Not as thorough as a vulnerability scan: false positives and false negatives

May cause the remote system to crash: it launches attacks, including dangerous ones

All of these

- **Question 13**

1 out of 1 points

Metasploit exploit modules are written in which programming language?

Selected Answer: Ruby

Answers: C

Java

C#

Ruby

- **Question 14**

1 out of 1 points

Software vulnerabilities in operating systems, such as the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability, are becoming rarer, and many more attacks are now found in webservices and applications

Selected Answer: True

Answers: True

False

- **Question 15**

1 out of 1 points

Common Vulnerabilities and Exposures (CVE) is a database containing, which of the following:

Selected Answer: Brief details and links for public vulnerabilities

Answers: Exploit code

Brief details and links for public exploits

Brief details and links for public vulnerabilities

Detailed information about zero-day exploits

- **Question 16**

1 out of 1 points

Which of the following will NOT provide you with working exploit code?

Selected Answer: CVE database

Answers: Metasploit

The Exploit DB

SecurityFocus

CVE database

- **Question 17**

0 out of 1 points

Stand-alone exploits were traditionally written in which programming language?

Selected Answer: Java

Answers: C

Java

C#

Ruby

- **Question 18**

0 out of 1 points

What does the following command do?:

```
searchsploit windows
```

Selected Answer: Searches for Metasploit exploits that target Microsoft Windows

Answers: Launches an attack against a Windows system

Searches a local copy of The Exploit DB

Searches a number of online vulnerability/exploit databases

Searches for Metasploit exploits that target Microsoft Windows

- **Question 19**

0 out of 1 points

Which of the following is a **disadvantage** (for an attacker) of setting up a backdoor on a compromised system?

Selected Answer: A backdoor is an unreliable way of maintaining access

Answers: A backdoor always lets other attackers in

An extra user account will usually be detected by anti-malware software

It involves writing to disk, which leaves evidence

A backdoor is an unreliable way of maintaining access

- **Question 20**

0 out of 1 points

An **advantage** (for an attacker) of installing a rootkit, is that:

Selected Answer: Keeps a record of all of the attacker's actions, so that the attacker can easily attack the system in the future

Answers: It will typically automate the process of information gathering

It uses Metasploit to automate attacks

Keeps a record of all of the attacker's actions, so that the attacker can easily attack the system in the future

It persists on the victim system (possibly providing the attacker with a backdoor), and hides its presence to cover the attacker's tracks

- **Question 21**

0 out of 1 points

msf > use post/linux/gather/checkvm

msf post(checkvm) > show options

msf post(checkvm) > set SESSION 1

msf post(checkvm) > exploit

Given this sequence of commands, what has the attacker done?

Selected Answer: Run a program on the *attacker's* system to determine whether Kali Linux is running in a VM

Answers: Check whether the attacker has Meterpeter access

Run a program on the *attacker's* system to determine whether Kali Linux is running in a VM

Exploited a vulnerability on a remote system, to get a shell

Run a post-exploitation module to gather information from a compromised system

- **Question 22**

0 out of 1 points

If an attacked system is logging to a secure remote server, which of the following methods could be used to effectively cover the tracks of an attacker?

Selected Answer: All of these

Answers: All of these

Deleting log files

Disabling logging from the attacked system

Modifying log files

- **Question 23**

1 out of 1 points

After successful exploitation, the attack surface usually changes

Selected Answer: True

Answers: True

False

- **Question 24**

1 out of 1 points

On a Windows system, if an attacker has managed to compromise a system, and finds they have a security identifier (SID) of "S-1-5-21-1180699209-877415012-3182924384-500", which of the following will the attacker likely be able to modify?

Selected Answer: All of these

Answers: Files belonging to the corresponding user

Files owned by any user

Any programs or configuration files stored locally

All of these

- **Question 25**

0 out of 1 points

Which of the following statements about Meterpreter are true?

Selected Answer: All of these are true

Answers: Meterpeter always gives the attacker root access

Meterpreter can only be used to target vulnerabilities in Windows

All of these are true

Meterpreter makes life easier for the attacker, since it includes lots of features

- **Question 26**

1 out of 1 points

Which of the following would typically *only happen* during post-expliotation? (Not earlier in an attack)

Selected Answer: Make modifications to protected files

Answers: Launching an exploit

Attacks to obtain privileges not normally afforded to the attacker

Information gathering

Make modifications to protected files

- **Question 27**

0 out of 1 points

linux:~> id -u

0

Given the above output, which of the following will the attacker likely be able to modify?

Selected Answer: Files belonging to the corresponding user

Answers: Files belonging to the corresponding user

Files owned by any user

All of these

Any programs or configuration files stored locally

- **Question 28**

0 out of 1 points

Which of these interfaces for MSF are designed for one-line use from a command prompt/shell?

Selected Answer: msfconsole

Answers: Armitage

msfconsole

Metasploit community

msfcli

- **Question 29**

1 out of 1 points

Which of these interfaces for MSF can be used to exploit a vulnerability in a remote service?

Selected Answer: All of these options

Answers: msfcli

msfconsole

Metasploit community

Armitage

All of these options

- **Question 30**

1 out of 1 points

A payload that connects back to the attacker and grants them a command line access, is known as a:

Selected Answer: Reverse shell

Answers: Privilege escalation
Bind shell
Command shell
Reverse shell

- **Question 31**

0 out of 1 points

If an attacker starts with access to a user "bob", and ends up with access to user "fred". They have managed:

Selected Answer: Command injection

Answers: Vertical privilege escalation
Horizontal privilege escalation
Command injection
Buffer overflow

- **Question 32**

0 out of 1 points

Which of the following is NOT a type of module available in Metasploit Framework (MSF)?

Selected Answer: Post-Exploitation

Answers: Payload
Post-Exploitation
Malware
Exploit

- **Question 33**

0 out of 1 points

Malicious code inserted during an attack that connects back to the attacker to grant access to the computer is an example of a(n):

Selected Answer: Exploitation

Answers: Connection attack
Software vulnerability
Exploit
Exploitation
Malware
Payload
Buffer overflow

- **Question 34**

1 out of 1 points

A method of mitigating the effects of software vulnerabilities is to (best answer):

Selected Answer: Keep software up-to-date

Answers:
- Use an IDS
- Use encryption
- Keep software up-to-date
- Install antimalware

- **Question 35**

1 out of 1 points

A programmer makes a mistake that introduces a security problem. This is known as a(n):

Selected Answer: Software vulnerability

Answers:
- Shell code
- Exploitation
- Buffer overflow
- Software vulnerability
- Malware
- Exploit
- Payload

- **Question 36**

1 out of 1 points

A reverse shell is more likely to evade firewalls than a bind shell?

Selected Answer: True

Answers:
- True
- False

- **Question 37**

1 out of 1 points

Many penetration tests are conducted from Linux systems, this is primarily because:

Selected Answer: Many tools for testing security are available for Linux, and distributions are available that conveniently bundle testing tools

Answers:
- Linux is the software that runs on most servers
- Many tools for testing security are available for Linux, and distributions are available that conveniently bundle testing tools
- Linux is designed specifically for hacking activities
- Linux was created by Linus Torvalds

- **Question 38**

1 out of 1 points

A GNU/Linux distribution typically does NOT:

Selected Answer: Cost money to download

Answers: Cost money to download

Combine GNU with the Linux kernel

Include a package management system

Include system utilities and applications

- **Question 39**

1 out of 1 points

An example of a *Unix-like* system (not officially Unix) is:

Selected Answer: Linux

Answers: Windows

Mac OS X

Linux

DOS

- **Question 40**

0 out of 1 points

Unix security was originally designed to:

Selected Answer: Protect servers from attackers

Answers: Protect servers from attackers

Protect CPU time from leachers

Protect users from each other

Protect programs from tampering

- **Question 41**

1 out of 1 points

On Unix, filenames REQUIRE file extensions: for example, .JPG

Selected Answer: False

Answers: True
False

- **Question 42**

0 out of 1 points

Which of these statements about Richard Stallman is FALSE:

Selected Answer: He was the main author of the GPL license

Answers: He was the main author of the GPL license

He is a free software advocate

He founded the Free Software Foundation (FSF)

He pioneered copyleft

He created the Linux kernel

- **Question 43**

1 out of 1 points

Mac OS X is certified Unix:

Selected Answer: True

Answers: True
False

- **Question 44**

1 out of 1 points

Which of the following is TRUE of encode (-e) option of msfvenom?:

Selected Answer: It takes as input a payload and reencodes it to something else that has the same effect

Answers: It takes an executable and reencodes it by encrypting the instructions

It takes as input a payload and reencodes it to something else that has the same effect

It has a number of encoding methods which can be used to hide the presence of a rootkit within an operating system, by modifying system calls to avoid detection by anomaly-based antimalware

It generates a payload based on a set of parameters

- **Question 45**

1 out of 1 points

Why shouldn't the $PATH environment variable include "." (the current directory)?

Selected Answer: An attacker could place a script in a directory, which you may accidentally execute

Answers: This is not true, you should include "."

An attacker could place a script in a directory, which you may accidentally execute

Because it would be more like Windows

To provide an easy antimalware detection system

- **Question 46**

1 out of 1 points

Malware which poses as legitimate software is a:

Selected Answer: Trojan Horse

Answers: Virus

Logic bomb

Worm

Trojan Horse

- **Question 47**

0 out of 1 points

Anomaly-based antimalware works by:

Selected Answer: Detecting known malware

Answers: Prompting the user every time a program is run

Detecting suspicious activity

Detecting known malware

Comparing the program to the signatures of other malware

- **Question 48**

0 out of 1 points

Malware that is running as a normal Unix account can:

Selected Answer: All of these

Answers: All of these

Make changes to the kernel

Make changes to system programs (such as /bin/ls, cat, and man)

Read all of the user's personal files and Web history

- **Question 49**

0 out of 1 points

Malware which spreads directly to other computers is a:

Selected Answer: Virus

Answers: Virus

Logic bomb

Worm

Trojan Horse

- **Question 50**

1 out of 1 points

A program that has been digitally signed:

Selected Answer: Proves who authored the software, assuming you check and trust the certificate authority (CA) and no one else has the author's private key

Answers: Proves that the software is safe to run

Proves that the website that the program was obtained from was secured using SSL

Proves nothing

Proves who authored the software, assuming you check and trust the certificate authority (CA) and no one else has the author's private key

- **Question 51**

1 out of 1 points

Malware and software vulnerabilities are related because:

Selected Answer: Both have the potential to cause problems by misusing a user's authority

Answers: Both have the potential to cause problems by misusing a user's authority

Both are caused by programming mistakes

Both are malicious in design

Both are caused by innocent mistakes

- **Question 52**

0 out of 1 points

Digitally signed programs (executables with digital signatures) typically proves:

Selected Answer: That the program is safe to run

Answers: What the program does

Who the author was

That the program is safe to run

That the program is compiled

- **Question 53**

1 out of 1 points

nmap -sn 192.168.1.1

What does the above command do?

Selected Answer:	Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)
Answers:	Simply resolves the DNS name for the IP address
	A port scan
	A ping sweep (a simple ping echo request)
	Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)

- **Question 54**

0 out of 1 points

nmap -sL 192.168.1.1

What does the above command do?

Selected Answer:	Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)
Answers:	A port scan
	Simply resolves the DNS name for the IP address
	A ping sweep (a simple ping echo request)
	Attempts a series of actions to detect that the host is live (including an ICMP echo request and ICMP timestamp request)

- **Question 55**

0 out of 1 points

How many possible TCP ports exist?

Selected Answer:	65355
Answers:	1024
	65535
	2048

65355

- **Question 56**

1 out of 1 points

What will the following command do?

sudo nmap -p 21 10.72.35.207

Selected Answer:	Scan for a ftp server
Answers:	Scan for an email server
	Scan for a web server
	Scan for a ftp server
	All of these services
	Scan for an SSH server
	None of these services

- **Question 57**

1 out of 1 points

nmap -sn -PE 192.168.1.1

What does the above command do?

Selected Answer:	A ping sweep (a ping request) of a single system
Answers:	A port scan of a single system
	A ping sweep (a ping request) of a single system
	A ping sweep (a ping request) of a network range
	A port scan of a network range (multiple systems)

- **Question 58**

1 out of 1 points

Which of the following statements is true of a SYN scan?

Selected Answer:	It is faster for the scanner, since it does not need to establish a full TCP connection
Answers:	It is faster, since it does not require the scanner to send any packets to the target directly
	It is slower to perform the scan
	It is faster for the scanner, since it does not need to establish a full TCP connection
	It is faster, because it can connect to multiple ports at the same time

- **Question 59**

1 out of 1 points

What will the following command do?

sudo nmap -p 20-1000 10.72.35.207

Selected Answer: All of these services

Answers:
- Scan for an email server
- None of these services
- Scan for a web server
- Scan for an SSH server
- Scan for a ftp server
- All of these services

- **Question 60**

0 out of 1 points


A SYN scan works by:

Selected Answer: Sending a RST packet

Answers:
- Sending a RST packet
- Not answering the SYN with a SYN/ACK
- Not answering the SYN/ACK with an ACK
- Completing the full three-way handshake

- **Question 61**

1 out of 1 points


Scanning can be used:

Selected Answer: All of these

Answers:
- By a network admin to survey the network and check the hosts on the network are as expected
- All of these
- To get an idea of the IP addresses live on the network
- To check the services available on hosts on the network

- **Question 62**

1 out of 1 points


The Whois protocol uses which port?

Selected Answer: TCP port 43

Answers:
- TCP port 43
- UDP port 43
- UDP port 23
- TCP port 23

- **Question 63**

0 out of 1 points


A DNS zone transfer conducted by an attacker is an example of:

Selected Answer: A secure state

Answers: A secure method of configuring a server

A software vulnerability

A security misconfiguration

A secure state

- **Question 64**

1 out of 1 points

Given a single IP address, the attacker can likely use Whois and DNS to discover:

Selected Answer: All of these

Answers: IP address ranges used by the company

Email servers used by the company

Company contact details

All of these

- **Question 65**

1 out of 1 points

Information gathering does not usually involve

Selected Answer: Exploitation

Answers: Footprinting

Exploitation

Enumeration

Scanning

- **Question 66**

0 out of 1 points

information gathering is likely to be detected by:

Selected Answer: Intrusion prevention systems (IPS)

Answers: Anti-malware

Firewalls

Intrusion prevention systems (IPS)

None of these

Intrusion detection systems (IDS)

All of these

- **Question 67**

0 out of 1 points

An attacker usually starts the first stages of an attack knowing:

Selected Answer: The software installed on the target system

Answers: The vulnerabilities on the target system

A domain name or IP address

The software installed on the target system

The passwords for the target system

- **Question 68**

1 out of 1 points

Put the stages of attack into the correct order

Answers	Selected Answer
Post-exploitation	1. Footprinting
Exploitation	2. Scanning
Footprinting	3. Enumeration
Enumeration	4. Exploitation
Scanning	5. Post-exploitation

- **Question 69**

0 out of 1 points

dig @8.8.8.8 mydomain.co.uk AXFR

The above command does what?

Selected Answer: Attempts to use a reverse lookup on 8.8.8.8 to determine which domain name it points to, using mydomain.co.uk as the DNS server

Answers: Attempts to resolve the IP address for mydomain.co.uk using the DNS server 8.8.8.8

Attempts to use a reverse lookup on 8.8.8.8 to determine which domain name it points to, using mydomain.co.uk as the DNS server

Attempts to use a reverse lookup on 8.8.8.8 to determine which domain name it points to, and compares the answer to mydomain.co.uk

Attempts a zone transfer on mydomain.co.uk using the 8.8.8.8 server

- **Question 70**

0 out of 1 points

Starting with a domain such as google.com, what technique could be used to find domains such as mail.google.com?

Selected Answer: Scanning

Answers: Scanning

dig +short google.com

Whois

Subdomain brute-forcing

Enumeration

Sunday, 4 April 2021 11:51:01 o'clock BST