* **Question 1**

1 out of 1 points

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

* **Question 2**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following would be a valid CVE-ID? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | CVE-2004-0012 | | Answers: | exploit/adobe\_utilprintf | |  | CVE-2004-0012 | |  | exploit/windows/fileformat/adobe\_utilprintf | |  | CVE-04-000012 | |  |  |  |

* **Question 3**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | What does the following command do?:  searchsploit windows |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Searches a local copy of The Exploit DB | | Answers: | Launches an attack against a Windows system | |  | Searches for Metasploit exploits that target Microsoft Windows | |  | Searches a number of online vulnerability/exploit databases | |  | Searches a local copy of The Exploit DB | |  |  |  |

* **Question 4**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | 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 5**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | CVE is run by which of the following?: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | The MITRE Corporation | | Answers: | Cybersecurity and Communications | |  | The MITRE Corporation | |  | GCHQ | |  | The U.S. Department of Homeland Security | |  |  |  |

* **Question 6**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Metasploit exploit modules are written in which programming language? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Ruby | | Answers: | Ruby | |  | Java | |  | C | |  | C# | |  |  |  |

* **Question 7**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | What is a disadvantage of using Armitage's "Find Attacks" feature? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | May cause the remote system to crash: it launches attacks, including dangerous ones | | Answers: | Not as thorough as a vulnerability scan: false positives and false negatives | |  | All of these | |  | Causes lots of network traffic, including log entries that would raise suspicions | |  | May cause the remote system to crash: it launches attacks, including dangerous ones | |  |  |  |

* **Question 8**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | What port does CVE-2003-0352 affect? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | 135 | | Answers: | 8080 | |  | 21 | |  | 80 | |  | 135 | |  |  |  |

* **Question 9**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | 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 | |  | There are no fixes available for Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (CVE-2003-0352) | |  | Windows 2000 contains many security vulnerabilities such as buffer overflows, which will never be fixed since it has reached end of lifecycle | |  |  |  |

* **Question 10**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Stand-alone exploits were traditionally written in which programming language? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | C | | Answers: | C# | |  | Java | |  | C | |  | Ruby | |  |  |  |

* **Question 11**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Vulnerability analysis typically results in more false positives compared to a full penetration test |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | True | | Answers: | True | |  | False | |  |  |  |

* **Question 12**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following is NOT a Vulnerability scanner? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | MSF | | Answers: | MSF | |  | Nessus | |  | OpenVAS | |  | None of these | |  | Nexpose | |  |  |  |

* **Question 13**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A vulnerability scan will never crash the system being scanned |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | False | | Answers: | True | |  | False | |  |  |  |

* **Question 14**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following would NOT be conducted during a typical vulnerability scan? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Exploit vulnerabilities | | Answers: | Probe the system(s), to determine status and configuration of services | |  | Port scans | |  | Exploit vulnerabilities | |  | Service identification on each open port | |  |  |  |

* **Question 15**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following tools includes scripts for performing vulnerability analysis scans? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Nmap | | Answers: | Nmap | |  | Amap | |  | Msfconsole | |  | Dig | |  |  |  |

* **Question 16**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | If a Nessus scan reports that a system is vulnerable to a remote exploit with arbitrary code execution, this means: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | An attacker MAY be able to run commands on this service | | Answers: | An attacker MAY be able to run commands on this service | |  | An attacker WILL be able to run commands on this service | |  | An attacker WILL NOT be able to run commands on this service | |  | An attacker WILL be able to get a shell | |  |  |  |

* **Question 17**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | OpenVAS is a fork of which project? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Nessus | | Answers: | MSF | |  | Nessus | |  | Nexpose | |  | Nmap | |  |  |  |

* **Question 18**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | If a vulnerability scan reports that a system is vulnerable to the RPC DCOM buffer overflow vulnerability, then this system could be attacked/exploited using: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Stand-alone exploit code | | Answers: | Stand-alone exploit code | |  | Nexpose | |  | Nmap | |  | SNMP | |  |  |  |

* **Question 19**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | The steps of an attack typically involve this sequence of events: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Information gathering, exploitation, and post-exploitation | | Answers: | Scanning, footprinting, and hacking | |  | Exploitation, information gathering, covering tracks | |  | Maintaining access, information gathering, and hacking | |  | Information gathering, exploitation, and post-exploitation | |  |  |  |

* **Question 20**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Starting with a single IP address, how could an attacker determine the range of IP addresses used by the company? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Whois | | Answers: | Whois | |  | DNS | |  | Domain bruteforcing | |  | The dig command | |  |  |  |

* **Question 21**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | dig +short google.co.uk  The above command will return what? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Mail server(s) | | Answers: | Mail server(s) | |  | Domain name(s) | |  | The name server(s) used to provide authoritative information about the DNS zone | |  | A listing of various types of DNS records | |  | The results of a DNS zone transfer | |  | IPv6 address(es) | |  | IP address(es) that the domain name resolves to | |  |  |  |

* **Question 22**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | RIPE and ARIN are examples of: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Regional internet registries | | Answers: | Regional internet registries | |  | Registrars | |  | Protocols | |  | Exploits | |  |  |  |

* **Question 23**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | 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 24**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | Passive information gathering is likely to be detected by: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | All of these | | Answers: | Firewalls | |  | None of these | |  | Intrusion prevention systems (IPS) | |  | Intrusion detection systems (IDS) | |  | All of these | |  | Anti-malware | |  |  |  |

* **Question 25**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | Starting with a domain such as google.com, what technique could be used to find domains such as mail.google.com? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | dig +short google.com | | Answers: | Whois | |  | Subdomain brute-forcing | |  | Scanning | |  | dig +short google.com | |  | Enumeration | |  |  |  |

* **Question 26**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | dig +short -x 130.57.5.70  The above command will return what? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Mail server(s) | | Answers: | The name server(s) used to provide authoritative information about the DNS zone | |  | IP address(es) that the domain name resolves to | |  | Mail server(s) | |  | A listing of various types of DNS records | |  | IPv6 address(es) | |  | Domain name(s) | |  | The results of a DNS zone transfer | |  |  |  |

* **Question 27**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | An attacker usually starts the first stages of an attack knowing: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | A domain name or IP address | | Answers: | A domain name or IP address | |  | The vulnerabilities on the target system | |  | The passwords for the target system | |  | The software installed on the target system | |  |  |  |

* **Question 28**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following statements is TRUE? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | An EXE wrapper can join a Trojan horse and a normal program into one program, so that it appears less malicious to a user | | Answers: | An EXE wrapper is used to bind a program to another network | |  | An EXE wrapper program is a type of Trojan horse | |  | An EXE wrapper can join a Trojan horse and a normal program into one program, so that it appears less malicious to a user | |  | An EXE wrapper uses an exisiting program as a template for binding payloads into a malware executable | |  |  |  |

* **Question 29**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Signature-based antimalware often fails because of: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | False negatives: new malware | | Answers: | False positives: new malware | |  | False positives: well known malware | |  | False negatives: new malware | |  | False negatives: well known malware | |  |  |  |

* **Question 30**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | An infected computer that is under the control of an attacker is known as a: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Rootkit | | Answers: | Buffer overflow | |  | Software vulnerability | |  | Worm | |  | Virus | |  | Zombie | |  | Logic bomb | |  | Rootkit | |  | Trojan horse | |  |  |  |

* **Question 31**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | 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 website that the program was obtained from was secured using SSL | |  | Proves who authored the software, assuming you check and trust the certificate authority (CA) and no one else has the author's private key | |  | Proves that the software is safe to run | |  | Proves nothing | |  |  |  |

* **Question 32**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Malware which poses as legitimate software is a: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Trojan Horse | | Answers: | Worm | |  | Logic bomb | |  | Virus | |  | Trojan Horse | |  |  |  |

* **Question 33**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Black-lists provide more security than white-lists but are harder to maintain |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | False | | Answers: | True | |  | False | |  |  |  |

* **Question 34**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Malware is software which: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Is designed to do malicious things | | Answers: | Contains mistakes in logic | |  | Contains design flaws | |  | Contains implementation mistakes | |  | Is designed to do malicious things | |  |  |  |

* **Question 35**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Android runs the Linux kernel: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | True | | Answers: | True | |  | False | |  |  |  |

* **Question 36**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Linus Torvalds is: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Creator, chief architect, and coordinator of the Linux kernel | | Answers: | Creator, chief architect, and coordinator of the Linux kernel | |  | The founder of the Free Software Foundation | |  | The CEO of and creator of Linux | |  | The CEO of Linux | |  |  |  |

* **Question 37**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | /bin/bash is an example of: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | An absolute filename | | Answers: | An absolute filename | |  | A configuration file | |  | This is not a file | |  | A relative filename | |  |  |  |

* **Question 38**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | Linux is certified Unix: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | True | | Answers: | True | |  | False | |  |  |  |

* **Question 39**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | UNIX is now a: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Trademark, and standard | | Answers: | Trademark, and standard | |  | Trademark, and a particular operating system | |  | Standard, and a particular operating system | |  | Standard, and a Linux system | |  |  |  |

* **Question 40**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | An example of a *Unix-like* system (not officially Unix) is: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Linux | | Answers: | DOS | |  | Windows | |  | Linux | |  | Mac OS X | |  |  |  |

* **Question 41**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | On Unix each process has its own address space, which means: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Processes cannot communicate with each other | | Answers: | The kernel cannot access the memory of processes | |  | Programs maintain their own variable name-space | |  | Processes cannot modify each others allocated memory | |  | Processes cannot communicate with each other | |  |  |  |

* **Question 42**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | If you try to connect to a remote system on port 80 using Telnet or Netcat, and you cannot connect, then you can deduce that: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | There is no webserver on the host, or it is blocked by a firewall | | Answers: | There is no FTP server on the host, or it is blocked by a firewall | |  | There is no FTP server on the host | |  | There is no webserver on the host | |  | There is no webserver on the host, or it is blocked by a firewall | |  |  |  |

* **Question 43**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | What will the following command do?  sudo nmap -p 23 10.72.35.207 |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | None of these services | | Answers: | All of these services | |  | Scan for a ftp server | |  | Scan for an email server | |  | Scan for a web server | |  | None of these services | |  | Scan for an SSH server | |  |  |  |

* **Question 44**

1 out of 1 points

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

* **Question 45**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Given the below invocation and output of Nmap, what can you conclude?  nmap localhost -p 22 Starting Nmap 5.61TEST2 ( http://nmap.org ) at 2013-10-15 16:09 BST Nmap scan report for localhost (127.0.0.1) Host is up (0.000028s latency). PORT   STATE SERVICE 22/tcp open  ssh |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | The local system has an ssh server running | | Answers: | The remote system is listening to port 22 | |  | The remote system is not available | |  | The local system has an ssh server running | |  | The local system has a firewall rule that denies access to port 22 | |  |  |  |

* **Question 46**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | What will the following command do?  sudo nmap -p 20-1000 10.72.35.207 |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | All of these services | | Answers: | Scan for a ftp server | |  | None of these services | |  | Scan for a web server | |  | Scan for an email server | |  | Scan for an SSH server | |  | All of these services | |  |  |  |

* **Question 47**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A SYN scan works by: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Not answering the SYN/ACK with an ACK | | Answers: | Not answering the SYN with a SYN/ACK | |  | Completing the full three-way handshake | |  | Not answering the SYN/ACK with an ACK | |  | Sending a RST packet | |  |  |  |

* **Question 48**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | How many possible TCP ports exist? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | 65535 | | Answers: | 65535 | |  | 2048 | |  | 65355 | |  | 1024 | |  |  |  |

* **Question 49**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | What will the following command do?  sudo nmap -p 22 10.72.35.207 |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Scan for an SSH server | | Answers: | Scan for an SSH server | |  | None of these services | |  | Scan for a web server | |  | All of these services | |  | Scan for a ftp server | |  | Scan for an email server | |  |  |  |

* **Question 50**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | The term "attack surface" refers to: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | The various ways an attacker can interact with a system or software | | Answers: | All software installed on a system | |  | The various ways an attacker can interact with a system or software | |  | Services that are behind a firewall | |  | The amount of damage an attacker can cause after taking control of a system | |  |  |  |

* **Question 51**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which command will show the options for configuring the windows/shell\_bind\_tcp payload?: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | msfpayload windows/shell\_bind\_tcp O | | Answers: | msfpayload windows/shell\_bind\_tcp O | |  | msfpayload windows/shell\_bind\_tcp S | |  | msfpayload windows/shell\_bind\_tcp P | |  | msfpayload windows/shell\_bind\_tcp C | |  |  |  |

* **Question 52**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following commands will generate an executable that adds a user to a Windows system: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | msfvenom -p windows/adduser USER=tux PASS=lives -f exe > t.exe | | Answers: | msfvenom -p windows/adduser USER=tux PASS=lives -f exe > t.exe | |  | msfvenom -p windows/adduser USER=tux PASS=lives | |  | msfvenom -p windows/adduser -f > t.exe | |  | msfvenom -p windows/adduser USER=tux PASS=lives -f C | |  |  |  |

* **Question 53**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A small program that takes advantage of a security problem is known as a(n): |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Exploit | | Answers: | Exploit | |  | Malware | |  | Exploitation | |  | Payload | |  | Shell code | |  | Buffer overflow | |  | Software vulnerability | |  |  |  |

* **Question 54**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A reverse shell is more likely to evade firewalls than a bind shell? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | True | | Answers: | True | |  | False | |  |  |  |

* **Question 55**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following is NOT a type of module available in Metasploit Framework (MSF)? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Malware | | Answers: | Payload | |  | Exploit | |  | Post-Exploitation | |  | Malware | |  |  |  |

* **Question 56**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | The code that takes affect after compromising a system is known as a(n): |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Payload | | Answers: | Malware | |  | Exploitation | |  | Buffer overflow | |  | Shell code | |  | Exploit | |  | Software vulnerability | |  | Payload | |  |  |  |

* **Question 57**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Posting details of a new software vulnerability to the Internet, without first contacting the software authors or vendors, is known as: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Full disclosure | | Answers: | Full disclosure | |  | Grey hat hacking | |  | White hat hacking | |  | Responsible disclosure | |  |  |  |

* **Question 58**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A mistake by a software developer can result in enabling attackers to take control of the program |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | True | | Answers: | True | |  | False | |  |  |  |

* **Question 59**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of the following would be most likely to help you to identify any software installed on a machine that was vulnerable to attack via a buffer overflow? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Vulnerability analysis | | Answers: | Software updates | |  | Antimalware | |  | Vulnerability analysis | |  | Software patching | |  |  |  |

* **Question 60**

1 out of 1 points

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

* **Question 61**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Which of these interfaces for MSF are designed for one-line use from a command prompt/shell? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | msfcli | | Answers: | msfconsole | |  | Metasploit community | |  | Armitage | |  | msfcli | |  |  |  |

* **Question 62**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | linux:~> id -u  1000  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 63**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | A sandbox can typically be used to: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Restrict what an attacker can do after taking control of a process | | Answers: | Modify timestamps | |  | Restrict what an attacker can do after taking control of a process | |  | Maintain access after an attack | |  | Restrict what each user on a system can do | |  |  |  |

* **Question 64**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | msf > use post/linux/gather/hashdump  msf post(checkvm) > set SESSION 1  msf post(checkvm) > exploit  Given the above commands, what could an attacker do with the output? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | The output is the pain-text passwords! They could try using these credentials to get access to other services | | Answers: | They could use the core dump to determine the exact state of the kernel, such as a list of all the current processes on the system | |  | The output is the pain-text passwords! They could try using these credentials to get access to other services | |  | They could try to crack the hashes | |  | This attack won't work, because they forgot to set IP addresses | |  |  |  |

* **Question 65**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | An exploit that is run as a normal user and is used to obtain superuser access, is known as: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | a local privilege escalation exploit | | Answers: | an arbitrary code execution expliot | |  | a local privilege escalation exploit | |  | a horizontal escalation attack | |  | Meterpreter | |  |  |  |

* **Question 66**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | 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 | |  | Information gathering | |  | Attacks to obtain privileges not normally afforded to the attacker | |  | Make modifications to protected files | |  |  |  |

* **Question 67**

0 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | 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: | Deleting log files | | Answers: | Deleting log files | |  | Disabling logging from the attacked system | |  | Modifying log files | |  | All of these | |  |  |  |

* **Question 68**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | meterpreter > getuid  What would the above command be used to do? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Determine the security context | | Answers: | Attack a local system | |  | Attack a remote system | |  | Conduct a privilege escalation attack, in an attempt to get root | |  | Determine the security context | |  |  |  |

* **Question 69**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | If an attacker gets a shell with the security context of a normal user: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | It is sometimes possible to use a local privilege escalation attack to get a superuser shell, if there is a vulnerability present | | Answers: | It is always possible to use a remote escalation attack to get a superuser shell | |  | It is sometimes possible to use a local privilege escalation attack to get a superuser shell, if there is a vulnerability present | |  | It is never possible to use a local privilege escalation attack to get a superuser shell | |  | It is always possible to use a local privilege escalation attack to get a superuser shell | |  |  |  |

* **Question 70**

1 out of 1 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Port forwarding would be used by an attacker: |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | For pivoting attacks through a compromised system | | Answers: | For pivoting attacks through a compromised system | |  | To use up all of a local system's resources, resulting in a DoS | |  | For post-exploitation examination of the remote system's hard disk | |  | As an advanced method of scanning for open ports | |  |  |  |