|  |
| --- |
| **STUDENT ANSWER SHEET** |
| |  | | --- | | 1. **Which of the following terms are used to indicate types of hackers? Select all correct options.***[1 Mark(s)]* | | A. White Hats  B. Black Hats  C. Blue Hats  D. Green Hats | |
| |  | | --- | | 2. **Which is the alternate term used for ?information gathering??***[1 Mark(s)]* | | A. Whois  B. e-mailTrackerPro  C. Footprinting  D. Scanning | |
| |  | | --- | | 3. **Which security techniques are employed for Footprinting?***[1 Mark(s)]* | | A. DNS queries  B. Network enumeration  C. e-mail access  D. Password display | |
| |  | | --- | | 4. **Which are the three important tools to perform competitive intelligence and information gathering?***[1 Mark(s)]* | | A. Split-DNS  B. SpyFu  C. EDGAR  D. KeywordSpy | |
| |  | | --- | | 5. **Which is the correct countermeasure of footprinting?***[1 Mark(s)]* | | A. Perform the shutdown activity  B. Take a backup of only working files  C. Configure the routers that deny the footprinting requests  D. Remove the network cables | |
| |  | | --- | | 6. **Which is the phase where the attacker collaborates maximum information regarding a target that would be attacked?***[1 Mark(s)]* | | A. Scanning  B. Maintaining access  C. Reconnaissance  D. Gaining access | |
| |  | | --- | | 7. **Which type of scanning detects open TCP/IP ports and services on a system?***[1 Mark(s)]* | | A. Port scanning  B. Vulnerability scanning  C. Network scanning  D. Stealth scanning | |
| |  | | --- | | 8. **Which of the following are stages of scanning methodology?***[1 Mark(s)]* | | A. Covering tracks  B. Banner grabbing  C. Service identification  D. Vulnerability scanning | |
| |  | | --- | | 9. **In which type of scan does a hacker send a TCP frame with no flags to the target port?***[1.5 Mark(s)]* | | A. FIN scan  B. Null scan  C. Xmas scan  D. Stealth scan | |
| |  | | --- | | 10. **Which of the following tools carry out network inventory mapping tasks?***[1.5 Mark(s)]* | | A. Netscan  B. Nmap  C. Netifera  D. Net tools suite pack | |
| |  | | --- | | 11. **Which enumeration synchronises clocks of computers that have been networked?***[1.5 Mark(s)]* | | A. LDAP enumeration  B. NTP enumeration  C. HTTP enumeration  D. UNIX/LINUX enumeration | |  | |
| |  | | --- | | 12. **Generally, a malicious hacker passes through 5 phases when progressing through an attack. Which of the following are the first three phases of the attack, arranged in the correct order?***[1.5 Mark(s)]* | | A. Scanning, Reconnaissance, Gaining Access  B. Reconnaissance, Scanning, Gaining Access  C. Gaining Access, Scanning, Reconnaissance  D. Reconnaissance, Gaining Access, Scanning | |
| |  | | --- | | 13. **Which are the four existing Regional Internet Registry (RIR's)?***[2 Mark(s)]* | | A. APNIC, LICNIC, ARIN, LACNIC  B. RIPE NCC, LACNIC, ARIN, APNIC  C. RIPE NCC, NANIC, ARIN, APNIC  D. RIPE NCC, ARIN, APNIC, LATNIC | |
| |  | | --- | | 14. **Why the HTTrack tool is used?***[2 Mark(s)]* | | A. Gathering the financial information of the target  B. Performing offline Whois lookup  C. Mirroring a Website  D. All of the above | |
| |  | | --- | | 15. **DNS records provide important information about location and types of servers. What does MX record indicates?***[2 Mark(s)]* | | A. A pointer to another part of the domain name  B. A host address  C. A mail exchange for the domain  D. The canonical name of an alias | |

|  |
| --- |
| **STUDENT ANSWER SHEET** |
| |  | | --- | | 1. **Which port number is associated with HTTP?***[1 Mark(s)]* | | A. 25  B. 21  C. 110  D. 80 | |
| |  | | --- | | 2. **Name the process in which active connections to systems and directed queries are involved?***[1 Mark(s)]* | | A. Scanning  B. Enumeration  C. Footprinting  D. Sniffing | |
| |  | | --- | | 3. **Which of the following steps are involved in enumeration?***[1 Mark(s)]* | | A. Collect information about the host through null sessions  B. Gather the details of user accounts using the tool GetAcct  C. Scan SNMP port  D. DNS Zone Transfer | |
| |  | | --- | | 4. **What are the three broad categories of cybercrime? Select all correct options.***[1 Mark(s)]* | | A. Where the computer is a target  B. Where the computer is a weapon  C. Where the computer is an accessory  D. Where the computer an alibi | |
| |  | | --- | | 5. **Which of the following are cyber-crimes according to the Australian Institute of Criminology? Select all correct options.***[1 Mark(s)]* | | A. Communications in furtherance of criminal conspiracies  B. Scanning of Website data  C. Telecommunication piracy  D. Dissemination of offensive material | |
| |  | | --- | | 6. **What are the main attributes of the domain of information security? Select all correct options.***[1 Mark(s)]* | | A. Scanning of Website data  B. Information technology security  C. Information insurance  D. Information assurance | |
| |  | | --- | | 7. **Which of the following statements are true about ethical hacking? Select all correct options.***[1 Mark(s)]* | | A. It involves breaking into computers  B. It is legal  C. It is illegal  D. It helps to identify weaknesses in a computer system | |
| |  | | --- | | 8. **Which of the following terms are used to indicate types of hackers? Select all correct options.***[1 Mark(s)]* | | A. White Hats  B. Black Hats  C. Blue Hats  D. Green Hats | |
| |  | | --- | | 9. **For which reason people generally search the domain names in the WHOIS database?***[1.5 Mark(s)]* | | A. For expiration dates by the individuals  B. For transferring ownership by the registrars  C. For removing virus and malware  D. For investigating criminal activity by authorities | |
| |  | | --- | | 10. **What information will be included in the Public WHOIS Database Listing?***[1.5 Mark(s)]* | | A. Password details  B. Correspondence Address  C. Domain registration Fee details  D. Website Hosting IP address | |
| |  | | --- | | 11. **ARIN provides services related to the technical coordination and management of Internet number resources and it distributes Internet number resources including IPv4 and IPv6 address space and AS numbers.***[1.5 Mark(s)]* | | A. Domain name lookup  B. Whois  C. American Registry for Internet Numbers (ARIN)  D. Nslookup | |
| |  | | --- | | 12. **In which type of scan does a hacker send a TCP frame with no flags to the target port?***[1.5 Mark(s)]* | | A. FIN scan  B. Null scan  C. Xmas scan  D. Stealth scan | |
| |  | | --- | | 13. **Which of the following should an ethical hacking report contain? Select all correct options.***[2 Mark(s)]* | | A. Firewall configuration information  B. Vulnerabilities identified  C. Type of Testing  D. Proposed countermeasures | |
| |  | | --- | | 14. **Which of the following best describes a piece of software or technology that takes advantage of a bug, glitch or vulnerability, leading to unauthorised access on a computer system?***[2 Mark(s)]* | | A. Threat  B. Vulnerability  C. Exploit  D. Attack | |
| |  | | --- | | 15. **Which of the following are the three main principles of security?***[2 Mark(s)]* | | A. Confidentiality  B. Integrity  C. Availability  D. Authentication | |

|  |
| --- |
| **STUDENT ANSWER SHEET** |
| |  | | --- | | 1. **What are the main attributes of the domain of information security? Select all correct options.***[1 Mark(s)]* | | A. Scanning of Website data  B. Information technology security  C. Information insurance  D. Information assurance | |
| |  | | --- | | 2. **Which of the following statements are true about ethical hacking? Select all correct options.***[1 Mark(s)]* | | A. It involves breaking into computers  B. It is legal  C. It is illegal  D. It helps to identify weaknesses in a computer system | |
| |  | | --- | | 3. **Which of the following terms are used to indicate types of hackers? Select all correct options.***[1 Mark(s)]* | | A. White Hats  B. Black Hats  C. Blue Hats  D. Green Hats | |
| |  | | --- | | 4. **Which is the alternate term used for ?information gathering??***[1 Mark(s)]* | | A. Whois  B. e-mailTrackerPro  C. Footprinting  D. Scanning | |
| |  | | --- | | 5. **Which security techniques are employed for Footprinting?***[1 Mark(s)]* | | A. DNS queries  B. Network enumeration  C. e-mail access  D. Password display | |
| |  | | --- | | 6. **Which are the three important tools to perform competitive intelligence and information gathering?***[1 Mark(s)]* | | A. Split-DNS  B. SpyFu  C. EDGAR  D. KeywordSpy | |
| |  | | --- | | 7. **Which is the correct countermeasure of footprinting?***[1 Mark(s)]* | | A. Perform the shutdown activity  B. Take a backup of only working files  C. Configure the routers that deny the footprinting requests  D. Remove the network cables | |
| |  | | --- | | 8. **Which is the phase where the attacker collaborates maximum information regarding a target that would be attacked?***[1 Mark(s)]* | | A. Scanning  B. Maintaining access  C. Reconnaissance  D. Gaining access | |
| |  | | --- | | 9. **Which information sources are looked out by the hacker while gathering the initial information?***[1.5 Mark(s)]* | | A. Open source  B. Domain  C. Whois  D. Nslookup | |
| |  | | --- | | 10. **For which reason people generally search the domain names in the WHOIS database?***[1.5 Mark(s)]* | | A. For expiration dates by the individuals  B. For transferring ownership by the registrars  C. For removing virus and malware  D. For investigating criminal activity by authorities | |
| |  | | --- | | 11. **What information will be included in the Public WHOIS Database Listing?***[1.5 Mark(s)]* | | A. Password details  B. Correspondence Address  C. Domain registration Fee details  D. Website Hosting IP address | |
| |  | | --- | | 12. **ARIN provides services related to the technical coordination and management of Internet number resources and it distributes Internet number resources including IPv4 and IPv6 address space and AS numbers.***[1.5 Mark(s)]* | | A. Domain name lookup  B. Whois  C. American Registry for Internet Numbers (ARIN)  D. Nslookup | |

|  |
| --- |
| **STUDENT ANSWER SHEET** |
| |  | | --- | | 1. **Which are the three important tools to perform competitive intelligence and information gathering?***[1 Mark(s)]* | | A. Split-DNS  B. SpyFu  C. EDGAR  D. KeywordSpy | |
| |  | | --- | | 2. **Which is the correct countermeasure of footprinting?***[1 Mark(s)]* | | A. Perform the shutdown activity  B. Take a backup of only working files  C. Configure the routers that deny the footprinting requests  D. Remove the network cables | |
| |  | | --- | | 3. **Which is the phase where the attacker collaborates maximum information regarding a target that would be attacked?***[1 Mark(s)]* | | A. Scanning  B. Maintaining access  C. Reconnaissance  D. Gaining access | |
| |  | | --- | | 4. **Which type of scanning detects open TCP/IP ports and services on a system?***[1 Mark(s)]* | | A. Port scanning  B. Vulnerability scanning  C. Network scanning  D. Stealth scanning | |
| |  | | --- | | 5. **Which of the following are stages of scanning methodology?***[1 Mark(s)]* | | A. Covering tracks  B. Banner grabbing  C. Service identification  D. Vulnerability scanning | |
| |  | | --- | | 6. **Which port number is associated with HTTP?***[1 Mark(s)]* | | A. 25  B. 21  C. 110  D. 80 | |
| |  | | --- | | 7. **Name the process in which active connections to systems and directed queries are involved?***[1 Mark(s)]* | | A. Scanning  B. Enumeration  C. Footprinting  D. Sniffing | |
| |  | | --- | | 8. **Which of the following steps are involved in enumeration?***[1 Mark(s)]* | | A. Collect information about the host through null sessions  B. Gather the details of user accounts using the tool GetAcct  C. Scan SNMP port  D. DNS Zone Transfer | |
| |  | | --- | | 9. **Which information sources are looked out by the hacker while gathering the initial information?***[1.5 Mark(s)]* | | A. Open source  B. Domain  C. Whois  D. Nslookup | |
| |  | | --- | | 10. **For which reason people generally search the domain names in the WHOIS database?***[1.5 Mark(s)]* | | A. For expiration dates by the individuals  B. For transferring ownership by the registrars  C. For removing virus and malware  D. For investigating criminal activity by authorities | |
| |  | | --- | | 11. **What information will be included in the Public WHOIS Database Listing?***[1.5 Mark(s)]* | | A. Password details  B. Correspondence Address  C. Domain registration Fee details  D. Website Hosting IP address | |
| |  | | --- | | 12. **ARIN provides services related to the technical coordination and management of Internet number resources and it distributes Internet number resources including IPv4 and IPv6 address space and AS numbers.***[1.5 Mark(s)]* | | A. Domain name lookup  B. Whois  C. American Registry for Internet Numbers (ARIN)  D. Nslookup | |
| |  | | --- | | 13. **John, the network administrator of a company, is performing a security audit of the internal network of the organisation. Which of the following correctly describes the John?s activity?***[2 Mark(s)]* | | A. Black-box testing  B. White-box testing  C. Active testing  D. Passive testing | |
| |  | | --- | | 14. **Which of the following should an ethical hacking report contain? Select all correct options.***[2 Mark(s)]* | | A. Firewall configuration information  B. Vulnerabilities identified  C. Type of Testing  D. Proposed countermeasures | |
| |  | | --- | | 15. **Which of the following best describes a piece of software or technology that takes advantage of a bug, glitch or vulnerability, leading to unauthorised access on a computer system?***[2 Mark(s)]* | | A. Threat  B. Vulnerability  C. Exploit  D. Attack | |