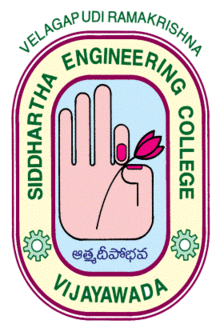
****   

**20IT4607: ETHICAL HACKING HOME ASSIGNMENT-II QUESTIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Question | CO | BTL |
| 1. | Network attacks often begin by gathering information from a company’s Web site because Web pages are an easy way for attackers to discover critical information about an organization. Many tools are available for this type of information gathering. For example, Paros is a powerful tool for UNIX and Windows OSs that can be downloaded free (www.parosproxy.org). Explain in detail the process a security tester uses when beginning a security test. | CO1 | Analyze |
| 2. | Security testers need to know how to use tools for gathering information about networks. With the Whois utility, you can discover which network configuration factors might be used in attacking a network. Explain the step wise procedure of how to use footprinting tools, such as the SamSpade Whois utility | CO1 | Evaluate |
| 3. | Knowing the e-mail addresses of employees can help you discover security vulnerabilities and gather competitive intelligence data. For example, you might discover that an employee has joined a newsgroup using his or her corporate e-mail account and shared proprietary information about the company. IT employees, when posting technical questions to a newsgroup, might reveal detailed information about the company’s firewall or IDS, or a marketing director might mention a new ad campaign strategy the company is considering. Determine e-mail addresses for corporate employees. | CO1 | Analyze |
| 4. | Many companies include cookies in their Web pages to gather information about visitors to their Web sites. This information might be used for competitive intelligence or, for example, to determine visitors’ buying habits. Security testers should know how to verify whether a Web page contains cookies. Determine whether cookies are present in Web pages. | CO1 | Analyze |
| 5. | Web bugs are considered more invasive than cookies. As a security professional, you should understand how companies use them to gather information on users who visit Web sites. Gain an understanding of data collection with Web bugs. | CO1 | Analyze |
| 6. | When foot printing a network, finding the IP addresses and hostnames of all servers, computers and other nodes connected to the network is important. With commands such as Dig, you can perform zone transfers of DNS records. You can then use this information to create network diagrams and establish good picture of how the network is organized. For example, you can see how many hosts are on the network and how many subnets have been created. Perform a zone transfer on a DNS server. | CO1 | Evaluate |
| 7. | In this activity, you learn the piggybacking skills used to gain access to areas restricted to authorized personnel. Assume you’re conducting a security test and need access to a company’s server room. To enter the room, you must scan an access card over a card reader, and then push open a door within several seconds, during which time a bell rings softly. If the door isn’t opened in the allotted time, the card must be swiped again. Form teams of two and demonstrate to the class how you would use piggybacking to get into the classroom if it was secured. One student should pretend to be an authorized user while the other student uses piggybacking techniques to gain entry. Have a class discussion about these attempts, and note which one was the most successful. Learn how piggybacking can be used to gain access to restricted areas. | CO1 | Apply |
| 8. | a. In this activity, you’re introduced to using Nmap for quick scans of a network. You send a SYN packet to a host on the attack network your instructor has supplied. In this example, the attack network IP addresses are 193.145.85.201 to 193.145.85.211, but your attack range might be different. Make sure to follow the rules of engagement, and don’t perform port scanning on any systems not included in the IP range your instructor gives you. Learn the basic commands and syntax of Nmap.  b. In this activity, you continue to use Nmap for port scanning on your attack network. You add to the parameters used in Activity 5-1 and send FIN, XMAS, and ACK packets to selected ports. You should practice these commands until they are second nature, but Fyodor developed a well-written help page (called a “man page” in UNIX/Linux circles) that you can use as a resource. You begin this activity by looking at this help page. Perform more complex port-scanning attacks with Nmap. | CO1  CO1 | Analyze  Apply |
| 9. | In this activity, you see how security testers can craft IP packets to find out what services are running on a network. The more ways you know how to send a packet to an unsuspecting port on a computer and get a response, the better. If a computer doesn’t respond to an ICMP packet sent to a particular port, it doesn’t mean any packet sent to the same port will get the same response. You might need to send different packets to get the results you need for a thorough security test. Learn to craft IP packets with Fping and Hping | CO1 | Apply |
| 10. | Learn to create, save and run an executable script. Many hacking tools are written in scripting languages, such as VBScript or JavaScript. In this activity you can create a script that populates a file with a range of IP addresses. This type of file can be used as an input file for Nmap or Fping. | CO1 | Apply |
| 11. | Gathering Information on a Network’s Active ServicesAfter conducting a zone transfer and running security tools on the Alexander Rocco network, you’re asked to write a memo to the IT manager, Bob Jones, explaining which tools you used to determine the services running on his network. Mr. Jones is curious about how you gathered this information. You consult the OSSTMM and read Section C on port scanning and the “Internet Technology Security” section, particularly the material on identifying services, so that you can address his concerns. Based on this information, write a one-page memo to Mr. Jones explaining the steps you took to find this information. Your memo should mention any information you found in the OSSTMM that relates to this stage of your testing | CO1 | Apply |
| 12. | **Finding Port-Scanning Tools**  Security Consulting Company, which has employed you as a security tester, has asked you to research any new tools that might help you perform your duties. It has been noted that some open-source tools your company is using lack simplicity and clarity or don’t meet the company’s expectations. Your manager, Gloria Petrelli, has asked you to research new or improved products on the market. Based on this information, write a one-page report for Ms. Petrelli describing some port-scanning tools that might be useful to your company. The report should include available commercial tools, such as Retina or Languard, and their costs. | CO1 | Apply |
| 13. | **Using an E-mail Address to Determine a Network’s Operating System**  Alexander Rocco Corporation has multiple OSs running in its many offices. Before conducting a security test to determine the vulnerabilities you need to correct, you want to determine whether any OSs are running that you’re not aware of. Mike Constantine, the network administrator/security officer, is resistant to giving you information after he learns you’re there to discover network security vulnerabilities. He sees you as a threat to his position. After several hours of interviews, you can ascertain only that Mike’s personal e-mail address is mtscon@gmail.com, and Oracle 8i is running on one of the company’s systems. Based on this information, answer the following questions: 1. What tools might you use after learning Mike’s e-mail address? 2. What did you determine after entering Mike’s e-mail address in the http:// groups.google.com Web site? 3. Could the information you learned from http://groups.google.com be used to conduct vulnerability testing or exploits? Write a memo to the IT manager, Bob Jones, about the possibility of a NetWare server being part of the company’s network. Make sure your memo explains how you gathered this information and offers constructive feedback. Your memo shouldn’t point a finger at any company employees; it should discuss problems on a general level. | CO1 | Apply |
| 14. | **Using Dumpster-Diving Skills**  You have observed that Alexander Rocco Corporation uses Alika’s Cleaning Company for its janitorial services. The company’s floors are vacuumed and 106 Chapter 4 mopped each night, and the trash is collected in large bins placed outside for pickup on Tuesdays and Fridays. You decide to visit the dumpster Thursday evening after the cleaning crew leaves. Wearing surgical gloves and carrying a large plastic sheet, you place as much of the trash on the sheet as possible. Sorting through the material, you find the following items: a company phone directory; a Windows NT training kit; 23 outdated Oracle magazines; notes that appear to be programs written in HTML, containing links to a SQL Server database; 15 company memos from key employees; food wrappers; an empty bottle of expensive vodka; torn copies of several resumes; an unopened box of new business cards; and an old pair of women’s running shoes. Based on this information, write a two-page report explaining the relevance these items have. What recommendations, if any, might you give to Alexander Rocco management? | CO1 | Apply |

Write according to your batch number (Your batch number is your question number)

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **ROLL NO** | **NAME OF THE STUDENTS** | **BATCH** |
| 1 | 208W1A1266 | ALAPATI RENUKA | **1** |
| 2 | 208W1A1267 | ALAVALA LAKSHMI SANKEERTHANA |
| 3 | 208W1A1268 | ALURI CHARAN |
| 4 | 208W1A1269 | AMPALAM YAMUNA |
| 5 | 208W1A1270 | ANJU PRIYA MANAM |
| 6 | 208W1A1271 | ANNAM JITIN CHAND | **2** |
| 7 | 208W1A1272 | ANNAM SIRI VARSHINI |
| 8 | 208W1A1273 | BANAVATHU MOUNICA KAUMUDHI |
| 9 | 208W1A1274 | BATCHU ANUSH GUPTA |
| 10 | 208W1A1275 | BHAGAVATULA APARNA |
| 11 | 208W1A1276 | CH VAMSI SATYANARAYANA | **3** |
| 12 | 208W1A1277 | CHAGARLAMUDI HEMAN SAI |
| 13 | 208W1A1278 | CHATRASI AMAR LOKESH VENKATA SIVA SAI |
| 14 | 208W1A1279 | CHEEDELLA KUSHMITHA |
| 15 | 208W1A1280 | CHENNAREDDY LAKSHMI NARASIMHAM |
| 16 | 208W1A1281 | CHINAMUTTEVI DEEPIKA | **4** |
| 17 | 208W1A1282 | DHARMAPURI MAHITH PAUL |
| 18 | 208W1A1283 | GANDABATHULA SAI VAMSI |
| 19 | 208W1A1284 | JAGANNADHAM PAVANI |
| 20 | 208W1A1285 | JAGANNADHAM TEJA |
| 21 | 208W1A1286 | JASTHI VIVEK VARDHAN | **5** |
| 22 | 208W1A1287 | KAKUMANU CHRISTT VICTOR |
| 23 | 208W1A1288 | KANCHARLA PRABHU RAM |
| 24 | 208W1A1289 | KANTAMNENI MAHITA |
| 25 | 208W1A1290 | KESIREDDY LAKSHMIKA |
| 26 | 208W1A1291 | KOLLURI MOUNAV | **6** |
| 27 | 208W1A1292 | KOMMAREDDY LEELA SATYA |
| 28 | 208W1A1293 | KOMMINENI UDAY KIRAN |
| 29 | 208W1A1294 | KOWTHAVARAPU DHATRI PHANI PRIYA |
| 30 | 208W1A1295 | MANOHAR RAJ KOKKILIGADDA |
| 31 | 208W1A1296 | MAREEDU GEETHIKA | **7** |
| 32 | 208W1A1297 | MEDISETTY LIKHITHA |
| 33 | 208W1A1298 | MOHAMMAD NEELOFAR JAHA |
| 34 | 208W1A1299 | MOHAMMAD RIZWANULLAH |
| 35 | 208W1A12A0 | MOTAMARRI JAYA NAGA VENAKTA SAI |
| 36 | 208W1A12A1 | NAGARAJU AJAY KUMAR VARMA | **8** |
| 37 | 208W1A12A2 | NEELAM B V D SOUJITHA |
| 38 | 208W1A12A3 | PALLETI DIVYA SREE |
| 39 | 208W1A12A4 | PANCHUMARTHI YOGESWARA SAI SRINIVAS |
| 40 | 208W1A12A5 | PANITINI MONICA |
| 41 | 208W1A12A6 | PARASA NIRUPAMA | **9** |
| 42 | 208W1A12A8 | PAVAN KUMAR MEKA |
| 43 | 208W1A12A9 | PERNI DEVI DIVYA SRI |
| 44 | 208W1A12B0 | POLAVARAPU VENKATA NAGA RISHITHA CHOWDARY |
| 45 | 208W1A12B1 | POLUKONDA GUNA SRI MANJUNADH |
| 46 | 208W1A12B2 | PORITIGADDA LIKHITHA | **10** |
| 47 | 208W1A12B3 | POTLURU SRI SASHANK |
| 48 | 208W1A12B4 | POTNURU RAJU DEEPAK |
| 49 | 208W1A12B5 | PRATHIPATI VASAVI |
| 50 | 208W1A12B6 | PULAPAKA VARUN KUMAR |
| 51 | 208W1A12B7 | RANGISETTI LAKSHMI SRAVANTHI | **11** |
| 52 | 208W1A12B8 | RAYIDI SAI SREE SRESTA |
| 53 | 208W1A12B9 | REVALAMADUGU RAGHU VARMA |
| 54 | 208W1A12C0 | SAINI ROSHINI |
| 55 | 208W1A12C1 | SAMBANA HARSHITHA |
| 56 | 208W1A12C2 | SAMSANI ABHI VENKATA SAI | **12** |
| 57 | 208W1A12C3 | SHETTY VENU |
| 58 | 208W1A12C4 | TEKI BHARGAV TIRUPATHI KAMARAJU |
| 59 | 208W1A12C5 | TULLURI NAGA VENNELA |
| 60 | 208W1A12C6 | TUMMALA VENKATA NAGA NYMISHA |
| 61 | 208W1A12C7 | VEMULAPALLI SAIESH | **13** |
| 62 | 208W1A12C8 | YESU RAJU PARUSU |
| 63 | 218W5A1207 | ANGADALA DIVYA SAI |
| 64 | 218W5A1208 | MAHALI TIRUMALA RAJU |
| 65 | 218W5A1209 | PALLAPATI LATHASRI |
| 66 | 218W5A1210 | TATA TEJASWINI | **14** |
| 67 | 218W5A1211 | THOKALA JOY JEEVAN |
| 68 | 218W5A1212 | BURADA PAVAN |