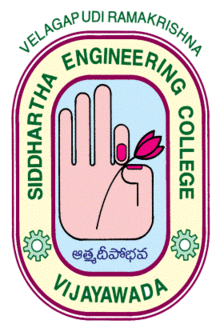
****   

**20IT4607: ETHICAL HACKING PROJECT QUESTIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Question | CO | BTL |
| 1. | **Downloading and Installing MBSA**  Download and install Microsoft Baseline Security Analyzer.  Description: In this activity, you download and install MBSA, a helpful tool for discovering vulnerabilities in Windows systems, Explain in detail the steps involved for MBSA installation. | CO3 | Implement |
| 2. | Using MBSA to Scan the Local Computer Use MBSA to scan the local computer for weak or missing passwords. Description: In this activity, you scan your computer with MBSA to discover vulnerabilities, including weak or missing passwords. At the end of the activity, submit a summary of your findings to your instructor, along with brief recommendations for correcting the problems you found | CO3 | Implement |
| 3. | **Using OpenVAS to Discover Vulnerabilities on a Linux Computer**  Use OpenVAS to discover vulnerabilities on a Linux computer.  Description: OpenVAS is a helpful tool for enumerating an OS. Not only does it warn testers of possible vulnerabilities, but it also makes recommendations to help correct any problems that are discovered. In this activity, you configure OpenVAS to scan your partner’s Linux computer and discover any vulnerabilities an attacker might use to gain access. | CO3 | Implement |
| 4. | Discovering Exploits for Linux SystemsResearch the Internet to discover Linux exploits. Figure 8-14 The OpenVAS report window Courtesy Course Technology/Cengage Learning Linux OS Vulnerabilities 229Description: In this activity, you visit a Web site listing exploits you can use to attack different OSs. As a security tester, you should be aware of the resources available to both security testers and attackers. | CO3 | Implement |
| 5. | **Using Tools to Find Linux Rootkits**  Learn how to find Linux rootkits on the Internet and use a rootkitchecking program.  Description: Attackers can locate rootkits for many Linux platforms easily. In this activity, you visit the www.packetstormsecurity.org Web site, which has thousands of tools and exploits that attackers or security professionals can use. You also run a rootkit detection program included with BackTrack to find rootkits running on your system | CO3 | Implement |
| 6. | **Securing an Older Linux OS**  After conducting footprinting and using social-engineering techniques on the Alexander Rocco network, you have determined that the company is running several applications on Linux computers. You also discover that the payroll system runs on several Red Hat Enterprise Linux 3 (RHEL 3) servers. You need to ensure that this version will be supported with patches from the vendor until the new payroll system is installed in 2011. Based on this information, write a brief report stating whether the systems can be secured until they’re replaced in 2011, and include recommendations for securing these systems. | CO3 | Implement |
| 7. | **Detecting Unauthorized Applications**  In conducting a review of the OSs running on the Alexander Rocco network, you detect a program that appears to be unauthorized. No one in the department knows how this program got on the Linux computer. The department manager thinks the program was installed before his start date three years ago. When you review the program’s source code, you discover that it contains a buffer overflow exploit. Based on this information, write a report to the IT manager stating what course of action should be taken and listing recommendations for management | CO3 | Implement |
| 8. | **Validating Password Strength for Alexander Rocco Corporation**  After discovering that most computers and servers at Alexander Rocco run many different versions of Windows, your supervisor has asked you to write a report on the issue of password vulnerabilities. Write a one-page memo to your supervisor describing the password-cracking areas you will test. Your memo should be based on the information you find in Section 11,“Password Cracking,” of the OSSTMM | CO3 | Implement |
| 9. | **Installing Internet Information Services**  Install IIS on your Windows computer.  Description: To create a Web site, you need to install IIS on your Windows computer. Although IIS is deployed on a server in a production environment, preproduction Web development and testing are typically done on workstations. IIS 5.1 is available in Windows XP Professional, IIS 7 is available in Vista (Business, Ultimate, and Enterprise editions), and IIS 7.5 is available in Windows 7 (Professional, Ultimate, and Enterprise). Because IIS isn’t installed by default, in this activity, you install it and use your Web browser to check that it was installed correctly | CO3 | Implement |
| 10. | **Creating a Virtual Directory**  Learn how to create a virtual directory on an IIS Web server. Description: After IIS is installed and physical directories are created, a Web administrator should create virtual directories that prevent site visitors from seeing the physical directory structure. In this activity, you create a virtual directory, using the directory you created in the above question (9) | CO3 | Implement |
| 11. | Creating an ASP Web PageUse ASP to create dynamic Web pages and be able to recognize ASP Web pages. Description: ASP Web pages are created on the Web server and enable a developer to create dynamic Web pages. In this activity, you create an ASP Web page and use a Web browser to view the page. | CO3 | Implement |
| 12. | **Working with Apache Web Server**  Explore basic settings and tasks in Apache Web Server. Description: Without a doubt, you’ll run across Apache Web Server systems when conducting a security test. Because Apache is a sophisticated, modular Web server, mastering its features and options can take considerable time. Apache’s layout varies, depending on the OS. For example, Apache in Fedora Linux is different from Apache in Ubuntu Linux. In this activity, you explore basic Apache Web Server commands and learn how to find and modify some configuration options (called “Apache directives”). | CO3 | Implement |
| 13. | **Identifying SQL Injection Vulnerabilities**  Recognize the many platforms that have SQL injection vulnerabilities. Description: After determining that a Web application is using a back-end database server to store data, a security tester should attempt to test the Web application for SQL injection vulnerabilities. In this activity, you visit the Common Vulnerabilities and Exposures (CVE) Web site to identify some known vulnerabilities | CO3 | Implement |
| 14. | **Determining Vulnerabilities of Web Servers**  After conducting preliminary security testing on the Alexander Rocco Corporation network, you have identified that the company has seven Web servers. One is a Windows 2000 Server system running IIS 5.0. Curt Cavanaugh, the Webmaster and network administrator, says the Web server is used only by sales personnel as a front-end to update inventory data on an Oracle database server. He says this procedure needs to be done remotely, and it’s convenient for sales personnel to use a Web browser when out of the office. Based on this information, write a one-page report on any possible vulnerabilities in the current configuration of the company’s Web server. Use the tools you have learned to search for possible vulnerabilities of IIS 5.0. Your report should include any recommendations that might increase Web security | CO3 | Implement |
| 15 | 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 | CO2 | Implement |
| 16 | **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. | CO2 | Implement |
| 17 | **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. | CO2 | Implement |
| 18 | **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? | CO2 | Implement |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | **2** |
| 6 | 208W1A1271 | ANNAM JITIN CHAND |
| 7 | 208W1A1272 | ANNAM SIRI VARSHINI |
| 8 | 208W1A1273 | BANAVATHU MOUNICA KAUMUDHI |
| 9 | 208W1A1274 | BATCHU ANUSH GUPTA | **3** |
| 10 | 208W1A1275 | BHAGAVATULA APARNA |
| 11 | 208W1A1276 | CH VAMSI SATYANARAYANA |
| 12 | 208W1A1277 | CHAGARLAMUDI HEMAN SAI |
| 13 | 208W1A1278 | CHATRASI AMAR LOKESH VENKATA SIVA SAI | **4** |
| 14 | 208W1A1279 | CHEEDELLA KUSHMITHA |
| 15 | 208W1A1280 | CHENNAREDDY LAKSHMI NARASIMHAM |
| 16 | 208W1A1281 | CHINAMUTTEVI DEEPIKA |
| 17 | 208W1A1282 | DHARMAPURI MAHITH PAUL | **5** |
| 18 | 208W1A1283 | GANDABATHULA SAI VAMSI |
| 19 | 208W1A1284 | JAGANNADHAM PAVANI |
| 20 | 208W1A1285 | JAGANNADHAM TEJA |
| 21 | 208W1A1286 | JASTHI VIVEK VARDHAN | **6** |
| 22 | 208W1A1287 | KAKUMANU CHRISTT VICTOR |
| 23 | 208W1A1288 | KANCHARLA PRABHU RAM |
| 24 | 208W1A1289 | KANTAMNENI MAHITA |
| 25 | 208W1A1290 | KESIREDDY LAKSHMIKA | **7** |
| 26 | 208W1A1291 | KOLLURI MOUNAV |
| 27 | 208W1A1292 | KOMMAREDDY LEELA SATYA |
| 28 | 208W1A1293 | KOMMINENI UDAY KIRAN |
| 29 | 208W1A1294 | KOWTHAVARAPU DHATRI PHANI PRIYA | **8** |
| 30 | 208W1A1295 | MANOHAR RAJ KOKKILIGADDA |
| 31 | 208W1A1296 | MAREEDU GEETHIKA |
| 32 | 208W1A1297 | MEDISETTY LIKHITHA |
| 33 | 208W1A1298 | MOHAMMAD NEELOFAR JAHA | **9** |
| 34 | 208W1A1299 | MOHAMMAD RIZWANULLAH |
| 35 | 208W1A12A0 | MOTAMARRI JAYA NAGA VENAKTA SAI |
| 36 | 208W1A12A1 | NAGARAJU AJAY KUMAR VARMA |
| 37 | 208W1A12A2 | NEELAM B V D SOUJITHA | **10** |
| 38 | 208W1A12A3 | PALLETI DIVYA SREE |
| 39 | 208W1A12A4 | PANCHUMARTHI YOGESWARA SAI SRINIVAS |
| 40 | 208W1A12A5 | PANITINI MONICA |
| 41 | 208W1A12A6 | PARASA NIRUPAMA | **11** |
| 42 | 208W1A12A8 | PAVAN KUMAR MEKA |
| 43 | 208W1A12A9 | PERNI DEVI DIVYA SRI |
| 44 | 208W1A12B0 | POLAVARAPU VENKATA NAGA RISHITHA CHOWDARY | **12** |
| 45 | 208W1A12B1 | POLUKONDA GUNA SRI MANJUNADH |
| 46 | 208W1A12B2 | PORITIGADDA LIKHITHA |
| 47 | 208W1A12B3 | POTLURU SRI SASHANK |
| 48 | 208W1A12B4 | POTNURU RAJU DEEPAK | **13** |
| 49 | 208W1A12B5 | PRATHIPATI VASAVI |
| 50 | 208W1A12B6 | PULAPAKA VARUN KUMAR |
| 51 | 208W1A12B7 | RANGISETTI LAKSHMI SRAVANTHI |
| 52 | 208W1A12B8 | RAYIDI SAI SREE SRESTA | **14** |
| 53 | 208W1A12B9 | REVALAMADUGU RAGHU VARMA |
| 54 | 208W1A12C0 | SAINI ROSHINI |
| 55 | 208W1A12C1 | SAMBANA HARSHITHA |
| 56 | 208W1A12C2 | SAMSANI ABHI VENKATA SAI | **15** |
| 57 | 208W1A12C3 | SHETTY VENU |
| 58 | 208W1A12C4 | TEKI BHARGAV TIRUPATHI KAMARAJU |
| 59 | 208W1A12C5 | TULLURI NAGA VENNELA | **16** |
| 60 | 208W1A12C6 | TUMMALA VENKATA NAGA NYMISHA |
| 61 | 208W1A12C7 | VEMULAPALLI SAIESH |
| 62 | 208W1A12C8 | YESU RAJU PARUSU | **17** |
| 63 | 218W5A1207 | ANGADALA DIVYA SAI |
| 64 | 218W5A1208 | MAHALI TIRUMALA RAJU |
| 65 | 218W5A1209 | PALLAPATI LATHASRI | **18** |
| 66 | 218W5A1210 | TATA TEJASWINI |
| 67 | 218W5A1211 | THOKALA JOY JEEVAN |
| 68 | 218W5A1212 | BURADA PAVAN |