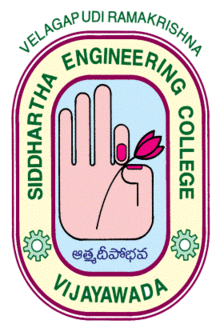
****   

**20IT4607 : ETHICAL HACKING HOME ASSIGNMENT-1 QUESTIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Question | CO | BTL |
| 1. | Some of the most common types of penetration tests are external, which is usually done off-site against an external network, internal where the assessment is conducted from within the target network, web application tests which objective is to find security vulnerabilities in web-based applications through both manual and automated tests, social engineering which tries to exploit to weak link in most organisation i.e. its employees, through phishing, vishing, tailgating, phyisical testing, media drops etc. What types of penetration testing assessments are there and explain how each of the penetration test can be applied for various applications.  b. Companies typically rely on one of the five standardized penetration testing methods: **OWASP, OSSTMM, ISSAF, PTES**, and **NIST**. Explain in detail about the 5 types of standardized penetration testing methodologies. | CO1  CO1 | Apply  Evaluate |
| 2. | a. Discuss in detail about the different steps involved in the penetration testing with the help of a neat diagram?  b. (i) Explain in detail about penetration testing scope (ii) How Often Should You Run Penetration Tests?(iii) What Is the End Result of a Penetration Test? | CO1  CO1 | Evaluate  Evaluate |
| 3. | a. Rules of Engagement (RoE) is a document that deals with the manner in which the penetration test is to be conducted. What are the directives that should be clearly spelled out in RoE before you start the penetration test.  b. Hackers start to learn about the system and look for potential entry points during the intelligence gathering stage. This phase requires the team to primarily gather information about the target, but testers can also discover surface-level weak points. Explain The reconnaissance step which includes the scan of different sites and networks. | CO1  CO1 | Remember  Evaluate |
| 4. | a. What types of penetration testing teams are there and what are their responsibilities? b. Briefly discuss about Penetration Testing Approaches (Areas of Testing). Write a short notes on each approach of Network Penetration Testing & Exploitation, Web Application Security Tests, Client-Side or Website & Wireless Network, Social Engineering Attacks, Physical Testing, Cloud Pen Testing | CO1  CO1 | Remember  Evaluate |
| 5. | a. Methodologies are not rigid and should not be applied to a penetration test in a rigid manner. It is often necessary to expand on any process beyond documented best practices; penetration testing is no exception. Explain in detail among **the OSSTMM and the NIST, which methodology is the best?**  **b.** You can filter ports on the firewall to block specific malware and protect the network from unnecessary traffic. For instance, some companies block port 21, the FTP port, when the company does not host or allow FTP communications. Explain in detail about what do you mean by port and analyze the reason of why you need to block the port no 21. | CO1  CO1 | Analyze  Analyze |
| 6. | a. Discuss in detail about OWASP and justify how we use OWASP for all “application penetration tests” we do here at the RHA InfoSEC.  b. You can use PGP to encrypt email messages or some other form of a public private key pair system where only the sender and the recipient can read the messages. Explain in detail about how can you encrypt email messages using Pretty Good Privacy (PGP). | CO1  CO1 | Evaluate  Analyze |
| 7. | a. When the scope of the penetration test is defined, the category/type of the penetration test engagement is also defined along with it. The entire penetration test can be Black Box, White Box, or Gray Box depending upon what the organization wants to test and how it wants the security paradigm to be tested. Explain in detail about the categories of penetration tests and where these type of penetration testings can be applied.  b. A hacker can use the man in the middle attack with the Diffie Hellman exchange since neither side of the exchange is authenticated. Users can use SSL or encryption between messages to add some kind of security and authentication. Explain in detail about man in the middle attack | CO1  CO1 | Apply  Analyze |
| 8. | a. Explain in detail about NIST and the steps involved in the methodology with the help of a neat diagram.  b. The HTTP protocol allows for security behind authenticated pages and directories. If the user does not enter the right username and password, the server returns a 403 authentication HTTP error. This protects from unauthorized users. Evaluate **how do you add security to a Website?** | CO1  CO1 | Remember  Evaluate |
| 9. | **a. Write short notes on how will you protect the data during and after Penetration Testing?**  **b. What is Packet Sniffing? Explain in detail about What type of tools are there for Packet Sniffing?** | CO1  CO1 | Evaluate  Analyze |
| 10. | a. There are several types of penetration tests performed, Explain in detail about the types of penetration tests and which type of penetration test can be used for testing a network environment for potential security vulnerabilities and threats.  b. Penetration tests may include social engineering techniques. These techniques are not without controversy though. More detailed information about the problems occuring with social engineering and penetration tests is available under exploitation. One safety measure against social engineering attacks can be trainings for your employees. **Does Redteam Pentesting Do Social Engineering?** | CO1  CO1 | Evaluate  Evaluate |
| 11. | a. How to Detect an ARP Cache Poisoning Attack? A variety of commercial and open-source software exists to detect ARP cache poisoning, but you can easily check the ARP tables on your own computer without installing anything. On most Windows, Mac, and Linux systems, issuing the “arp -a” command from a terminal or command line will display the current IP-to-MAC address mappings of the machine. Explain in detail about the above scenario.b. How to Prevent ARP Poisoning Attacks? Explain in detail about the following prevention tips: static ARP tables, switch security, Physical security, Network isolation, Encryption. | CO1  CO1 | Analyze  Evaluate |
| 12. | a. Explain in detail about three types of DDoS attacks: 1. Application layer attacks 2. Protocol attacks 3. Volumetric attacks and also some of the common DDoS attacks like SYN flood attack, HTTP flood attack, DNS amplification, DDoS mitigation with neat diagrams.  b. **What is the operating system that is commonly used for hacking? List all the types of operating systems and explain their functionalities when hacking is done.** | CO1  CO1 | Evaluate  Analyze |
| 13. | **a. What is Ethical Hacking? What are the steps performed by Hackers to hack a System or Network.**  **Take a simple application and check with any of your scanning tool to identify what type of data is present and can be affected in your target system. Explain the scenario in detail.**  **b. What are the various sniffing tools available? Explain in detail about the following sniffing tools:**Wireshark, WinDump, Ettercap, Diff, EtherApe, MSN Sniffer | CO1  CO1 | Apply  Analyze |
| 14. | a. What is Spoofing? Explain in detail about the following types of Spoofing attacks: IP Spoofing Attack., DNS Spoofing Attack, Media Access Control (MAC), ARP Spoofing Attack.  b. What is dsniff? Installation is to be done and find where can I find dsniff packages for Solaris and write a brief note on how can I detect dsniff on my network? | CO1  CO1 | Understand  Implement |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **ROLL NO** | **NAME OF THE STUDENTS** | **BATCH** |
| 1 | 208W1A1201 | B DINAKAR LAXMI VISWANATH | **1** |
| 2 | 208W1A1202 | BAJI SOTSAVA SKANDHA |
| 3 | 208W1A1203 | BALLA RAJA SAI PRANEETH |
| 4 | 208W1A1204 | BANAVATHU NAVYA |
| 5 | 208W1A1205 | BOGGULA RAJESWARI |
| 6 | 208W1A1206 | BONDALAPATI MAHESH | **2** |
| 7 | 208W1A1207 | BURRA SHREE SHARVANI |
| 8 | 208W1A1208 | CHANDAKA SANDHYARANI |
| 9 | 208W1A1209 | CHENNU DEEPTHI |
| 10 | 208W1A1210 | CHODAVARAPU DEVI KANAKA SAI SRI LIKHITHA |
| 11 | 208W1A1211 | DEVULAPALLI PRANEETHA | **3** |
| 12 | 208W1A1212 | ESA VINAY |
| 13 | 208W1A1213 | GANDIKOTA PRASANTH SATYA SAI KIRAN |
| 14 | 208W1A1214 | GOPU NITHIN SAI |
| 15 | 208W1A1215 | GORIPARTHI AASHRITHA |
| 16 | 208W1A1216 | GUDAVALLI HRUTHI SRI | **4** |
| 17 | 208W1A1217 | GUDAVALLI VISHNU VARDHAN |
| 18 | 208W1A1218 | JULURU HASWITHA |
| 19 | 208W1A1219 | KANUGULA BHARGAVI |
| 20 | 208W1A1220 | KANURI DILIP KUMAR |
| 21 | 208W1A1221 | KASIREDDI SUVARNA | **5** |
| 22 | 208W1A1222 | KASULA PAVAN SAI |
| 23 | 208W1A1223 | KESARI GOPI KISHORE REDDY |
| 24 | 208W1A1224 | KOLUPURI ROHITH |
| 25 | 208W1A1225 | KONDA AJAY |
| 26 | 208W1A1226 | KONUMURI KALYAN SUHAS | **6** |
| 27 | 208W1A1227 | MADDINENI SYAM PRAKASH |
| 28 | 208W1A1228 | MANDAVA VENKATA SRI SAI SURYA |
| 29 | 208W1A1229 | MARRI TANUJA |
| 30 | 208W1A1230 | MEESALA VEERA VENKATA AJAY KUMAR |
| 31 | 208W1A1231 | MIRIYALA SAI MANIKANTA | **7** |
| 32 | 208W1A1232 | MOHAMMED SAMEENA SULTANA |
| 33 | 208W1A1233 | MOHAMMED ZUBAIR |
| 34 | 208W1A1234 | MUNDRU SATHVIK BABU |
| 35 | 208W1A1235 | NANDIGAMA SUSHMA |
| 36 | 208W1A1236 | NIKITHA TRIPURANENI | **8** |
| 37 | 208W1A1237 | NAGA VENKATA LAKSHMI THANUJA DEVATHU |
| 38 | 208W1A1238 | NUKELLA MANASA DEVI |
| 39 | 208W1A1239 | NUTI VENKAT KIRAN |
| 40 | 208W1A1240 | PALADUGU BHAVYA SRI |
| 41 | 208W1A1241 | PALLI UDAYMANIKANTA | **9** |
| 42 | 208W1A1242 | PANUGANTI THARUN SAI |
| 43 | 208W1A1243 | PARVATANENI CHAITANYA SWAROOP |
| 44 | 208W1A1244 | PARVATANENI PRAVALI |
| 45 | 208W1A1245 | PERIKALA CHANDANA |
| 46 | 208W1A1246 | POLEPALLI S R NITHIN KALYAN | **10** |
| 47 | 208W1A1247 | POTHURAJU YASASWINI |
| 48 | 208W1A1248 | SALA ANIL KUMAR |
| 49 | 208W1A1249 | SHAIK AFFROZ |
| 50 | 208W1A1250 | SHAIK NISSAR HUSSAIN NOORANI |
| 51 | 208W1A1251 | SOMULA GEETHANJALI | **11** |
| 52 | 208W1A1252 | SRI HARA VENKATESH YARLAGADDA |
| 53 | 208W1A1253 | SYAM PRATAP POTLURI |
| 54 | 208W1A1254 | TALLURI PRANOOM KEERTHI RATHNA |
| 55 | 208W1A1255 | TIRUNAGARI LAHARI SUVARCHALA |
| 56 | 208W1A1256 | TRISHA SAI PALADUGU | **12** |
| 57 | 208W1A1257 | TUMMALA YASWANTH SAI |
| 58 | 208W1A1258 | VADAPALLI TEJA |
| 59 | 208W1A1259 | VALLURI DEEKSHITHA |
| 60 | 208W1A1260 | VAMSI SONTHINENI |
| 61 | 208W1A1261 | VASAMSETTI DEEPTHI SASIDHAR | **13** |
| 62 | 208W1A1262 | VATTIPALLI SPANDANA |
| 63 | 208W1A1263 | VELISALA JAHNAVI |
| 64 | 208W1A1264 | VUDATHA VENKATA PAVAN SAI HARI VAMSI |
| 65 | 208W1A1265 | YANALA GOPI KRISHNA |
| 66 | 218W5A1201 | DODDAPANENI SADHRUSYA | **14** |
| 67 | 218W5A1202 | GAMGOLU PRASANNA KUMAR |
| 68 | 218W5A1203 | MARADANI SUVARNA JYOTHI |
| 69 | 218W5A1204 | PADAMATI SATYA KIRAN |
| 70 | 218W5A1205 | PENTAPATI SRI VIJAYA |
| 71 | 218W5A1206 | SHAIK SHAHIN |