# Cyber Security-Edge Program

|  |
| --- |
| Name: Afrin Faria  ID: 2111270  Batch: B11 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **10. 19 October 2024** **Vulnerability Analysis and Penetration Testing**  [**www.tinyurl.com/vaAnalysis**](http://www.tinyurl.com/vaAnalysis) **download 3 files**  Create a report Vulnerability found in 2024 of any product using CVE Details  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcjnCp6HM-s-lOt9vjk_Qs5MJ2g9aRKaUg0ig34znKaFRh-LTLW5qcMFytGDHRETKY8v5gKpMs_-R8vYi5oRseYf5Z8U9FyZdABNRyYAy7aJBQ8zIigOC5o4r8tIm5oWl3jvE1-D_tO6NpuRLDWx4xgW0c-?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdWArjWxRvbRNEeI-6P_c6hV4GGNz6v0W6YBe_3rsrNjaIB966YGLMT4GtSr_ci-sYUGwpjBbODxxo6FHL-N2hVNnxHY4o_SBKPEkmXICX-KviskQ8kk9hyXPs7-0FWTfloWx7nEc-7Bx9I9is_B4fRW2c?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXeBjqocNV6_VC0gRAbMvc_U5X3lGwLydKAFxd9yqUvg22gDhpWNaTKIAnpQzq83V9Uzka2fY_IesjEVFqCdoZXd8Aa7pxwFj3Api516Ud0a9zYgFMNAAaoq3Fad86_f7aDzDQksUyMyNAeazMnxbVDdu0Gp?key=Vk71agtBjgu2Ts9zXFwT4Q  Cvss score:  <https://en.wikipedia.org/wiki/Zero-day_vulnerability>  Trend analysis  Check point threat map  Live cyber threat map : to use the protocols used in various attacks throughout the world https://threatmap.checkpoint.com/  **Advance Search Engine For RECON:**   1. <https://leakix.net/graph> 2. Then search juniv.edu 3. Then export to png   https://lh7-rt.googleusercontent.com/docsz/AD_4nXeDZQKsNhPRJbyK5xAAKTToYrTEkDDsNkqQ8NkRDVZ_-x90e4f4dmveS2clDB807AAikEghekv7UDC71uAHVWazpL2rdvAUtbqZDNb4CHC1fTd7wmfZ18J1ZpBY8x6-FD_NYDm2xo-wePizO0G1D-xxHoaD?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXelSe8nQwezMyn6f5uKgvGEwG148_ENTNcSQu-h5b1JnLazHC9QACXGMzXDsnPNGrXBS1RG5FBManvxunXnXTxAck7SqIclOHUzAQfr5vnZQ0KF-ruyZwXkcfRsH1OhCsrIdlwrFZnGnOhOqg3kFkl9-5hw?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXd90C2lxwUSl1p0DBlFAH04a8qkEjGbxNrvNuxODy3XrW--vzKSl0ThaxiDw_f0Sl5lI-PjvGRsiLU4Y8Cj9FV_UoVnEvQXPrhJTjY9cYTsykooclPIpD-WLdKl-JucxTLgjL6QfLSZTSq370kQpPkcgG_E?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfAU27t4T4e1awWxTH8wpBr_a6JecLRf5ry645bWk4Rl4uwV9lnRput6p3TVVOovkKVvnrzDHnEctiO5qPQdTarh_Shvhqr93xph4T1psRn--9vGk9XD1GvrQJVozgQvf8ilQyK0C4Cns0X0P_H5WkeHBgt?key=Vk71agtBjgu2Ts9zXFwT4Q  <https://www.ipvoid.com/whois/>  A: ipV4  MX:mailbox  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdobA3WpIJ0jM1sHe91jSzyZDsBJwOU0uWMnaNZ6ZwnRd_0AS3eD13Fx1KhdsdOEV2_mQfPT2h8etSuwdmLSdH7XAqjVc_zu5GutAGAv_Ggdsba2M3IvyyTIGb29Usct-UnSiD5GkZXfdN7OEGKqYVJI1S0?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXeCOvi21vfXlJFoEDTJ1A9neKBMnvFj6CEwqZP1Vs063cNEN2hZNEvzVHmD-eUYenh3DU3ireQA-DoldyCuHe5hFuEF_2Qhzu8rNvCd4xpUFu0q33Uni5Q6iGcT6GTwY1SeHo0YgpcrxnrEg1Bqh_Myxno?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcuwaYYRohY4E5-T8vapEAzRaxlSnQ6GM_5l7rgrtPunOMmL3iXmaAbF-rxKvbB_20Dac9DOPH4mJas7VIHCu1vNq30Bi6vyPZszq6Nt07hYzV2jr4gTA68f_qfv96PzCyRScnhq_8s9k2ONy8IbXfjBPka?key=Vk71agtBjgu2Ts9zXFwT4Q  Search tools: Ip blacklist tools  https://lh7-rt.googleusercontent.com/docsz/AD_4nXe-D3ONsumW-m-uhXJ-yTfQlIkMgVd5-IAzF4dzTErNpYKcfyPI85Kw-b86Tq_gRX2NmUVlikHYyN-uvqztTRFGAXAtdYEDhAe792DOoQPoFOLffriLIwtcYuWDwgO3nxgulNEZ1qhAq6a3hDg1RIspFBM?key=Vk71agtBjgu2Ts9zXFwT4Q   |  | | --- | | Vulnerability Analysis and Research using Online database | | Vulnerability Scanning using Manual Tools | |  | | Automated Vulnerability Assessment | | Reporting |   Information gathering: Vulnerability Analysis and Research using Online Database **Understanding the Vulnerability Landscape:**   * **Online Databases:** Leveraging platforms like CVEdetails, NVD, and Exploit-DB to access a vast repository of known vulnerabilities and their associated exploits. * **Research Methodology:**   + **Keyword Searches:** Identifying vulnerabilities based on specific keywords, software versions, or attack vectors.   + **Advanced Filtering:** Utilizing filters to narrow down results based on vulnerability severity, CVSS scores, and publication dates.   + **Trend Analysis:** Analyzing vulnerability trends to understand emerging threats and prioritize mitigation efforts. * **Data Extraction and Analysis:**   + **Exporting Data:** Downloading vulnerability information in CSV or XML formats for further analysis.   + **Data Visualization:** Using tools like Excel or data visualization software to create charts and graphs for better understanding. * **Knowledge Base Creation:** Building a comprehensive knowledge base of vulnerabilities relevant to the organization's systems and applications.  Vulnerability Scanning using Manual Tools **Hands-on Assessment:**   * **Manual Tools:** Employing tools like Nmap**, Nessus, (vulnerability scanner                                                                                                           ) install it o**r OpenVAS to conduct vulnerability scans. * Zenmap download * SLA: Service level agreement * **Scanning Process:**   + **Network Discovery:** Identifying network devices and their services.   + **Vulnerability Identification:** Scanning for known vulnerabilities in operating systems, applications, and network components.   + **Exploit Testing:** (Optional) Attempting to exploit identified vulnerabilities to assess their impact. * **Manual Analysis:**   + **Interpreting Results:** Analyzing scan reports to identify potential vulnerabilities and their severity.   + **Prioritizing Vulnerabilities:** Determining which vulnerabilities pose the greatest risk to the organization.   + Critical→ med→  low→  info   + We can't discard any vulnerability in spite of having lower priority   + **TOOLS:**   + Brup suite : live vul finding , training is in there portswigger community edition   + To know specific vulnerability   https://lh7-rt.googleusercontent.com/docsz/AD_4nXfu0uwdrz1ShGAPTCUSWtWeJ7sMBZsRtJWSvl2slxkBX2W9-TAEu0z3SM7c-XW3uIBYDoSFPKRDRA-53FID43qUavvDLZPBi2KfOOJ2mejQ5zT21DoHGiY02tXw_nBTES6OOUhctCr_N65C7GnCD87Yld1K?key=Vk71agtBjgu2Ts9zXFwT4Q   * **Verification and Validation:**   + **Cross-referencing with Online Databases:** Comparing scan results with known vulnerabilities to confirm accuracy.   + **Manual Testing:** Performing additional tests to verify the existence and exploitability of vulnerabilities.  Automated Vulnerability Assessment **Leveraging Technology for Efficiency:**   * **Automated Tools:** Utilizing automated vulnerability scanners like Qualys, Rapid7 Nessus, or Tenable.sc. * **Scanning Configurations:**   + **Customizing Scans:** Configuring scan parameters to target specific systems, applications, or vulnerabilities.   + **Scheduling Scans:** Automating regular scans to ensure ongoing monitoring. * **Reporting and Analysis:**   + **Automated Reporting:** Generating detailed reports on identified vulnerabilities.   + **Integration with Other Tools:** Integrating with asset management, configuration management, and incident response systems. * **Continuous Monitoring:**   + **Real-time Updates:** Staying informed about new vulnerabilities through automated updates.   + **Proactive Response:** Implementing timely patches and mitigations to address identified vulnerabilities.  Reporting **Communicating Findings and Recommendations:**   * **Report Structure:**   + **Executive Summary:** Providing a concise overview of the vulnerability assessment.   + **Detailed Findings:** Describing identified vulnerabilities, their severity, and potential impact.   + **Recommendations:** Suggesting remediation strategies and best practices for addressing vulnerabilities. * **Stakeholder Communication:**   + **Target Audience:** Identifying the appropriate stakeholders to receive the report (e.g., IT management, security team, executive leadership).   + **Effective Delivery:** Choosing a suitable format (e.g., email, presentation) and tailoring the communication to the audience's needs. * **Follow-up and Tracking:\*\*\***   + **Monitoring Remediation Efforts:** Ensuring that recommended actions are implemented.   + **Tracking Progress:** Measuring the effectiveness of mitigation strategies and identifying areas for improvement.   https://lh7-rt.googleusercontent.com/docsz/AD_4nXdDGEDtYXUXzjChCrWzOG3X4p4xycG0j0QC4jdOJOA52XxBdvd8jxGNIcAz91E8u_bnK7sUc7_W8bIIcCCKE6oxKy-2vqQ4tF_q7ZQEDeJEREj4q9y9Ial0DQsUIL8Odz4QpIPlcLYQCn0P5Ch6bTy2jWoJ?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXf2d8fkenNU-lOFMpXFthTifdcLNwWcH3Zw9nmk54mlG5O_65c2ipnY6vfc68vpMeKHT1ZdCHUHVber5L-SrSnupLuJajuHeE1wprVrTiiCVcE-BO8cZxV6eyV-wpR-WLXzYrjSQwoLHkIgLtTu8cPHMYw?key=Vk71agtBjgu2Ts9zXFwT4Q  **SOC Analyst: siem**   * Log analysis and reporting * Event viewer → windows log → security * https://app.any.run/tasks/c62ec182-df4f-4725-8fd7-c34ff6796ba5   ZENMAP:  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfv2gcyl1oB_EdWyKV_7JPBwA_NkssWrKd3VCb75Cln3lE0JhNu3kbL572Pp_2-Yw9FwO4jXaeQjbvY4-EPCwuCtSo1gGHuc3rEn_AxDh3YopghgMrlTO-RgtdbRpp1LX9hnoNMA-XUNT749vmbpAOaXAQ?key=Vk71agtBjgu2Ts9zXFwT4Q  **Nessus:installing** |