# Cyber Security-Edge Program

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

|  |
| --- |
| **12. 26 October, 2024** Self study: Netcat reverse shell  **Exploitation tool:** metasploit framework  Target : 192.168.10.92    Penetration testing  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXd0CbWhzGGnbWB9BDkJN2k4RNVKII_eq6VRJuQxhdGvOYCei-u4JxRQSa60TFQaGg0uP2fFc7g8RkD01iEKqPdW4vXB2Yw7aTFpm9OV-64JWqM31mUxGBw_WTSV3JoA4C9Jsnet6PUn_v1XlmlKLt4I4Yo?key=Vk71agtBjgu2Ts9zXFwT4Q**  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfzRWtdQPjM5TeXxuzgPMLPm6eu38TSvgfsuCXRUYo3MjZDB40FSg72NVE33Nl_kkAvQLkt0c-VfnBeujNtMN3dH8wSJGIhkdoyNi1Zp1t9nFlpOVI9Wrg2CL45JefBZMs8ZdlDhIWcRHy-GXgcaTtu6913?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXctVX_Jm765tQyVYqHBYsOBp9LsiI6SKRKEnncNgtmkblYCPuB8BBSj_ab7JunJ80DPgyLTFiwe_aTFD9LLj4vQQtVkCGf6XduYd1zatT-_H4HpMOjDtiwP7tChIESVsfeyhzMMtoARAGbf6bNkmvv4kbb6?key=Vk71agtBjgu2Ts9zXFwT4Q  MS17-010 is a critical security update for Microsoft Windows that addresses multiple vulnerabilities in Microsoft Server Message Block 1.0 (SMBv1). The most severe of these vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to an SMBv1 server.  Here's a breakdown of the key information about MS17-010:  Vulnerabilities:   * Remote Code Execution: This is the most serious vulnerability, allowing an attacker to remotely execute code on a vulnerable system. This could lead to complete system compromise. * Information Disclosure: This vulnerability could allow an attacker to gain access to sensitive information from a vulnerable system.   Impact:  If a system is vulnerable to MS17-010, it could be exploited by attackers to gain unauthorized access, steal data, or deploy malware. This could have serious consequences for individuals and organizations.  Mitigation:  The best way to protect against MS17-010 is to install the security update provided by Microsoft. This update patches the vulnerabilities and prevents exploitation.  Additional Considerations:   * SMBv1: It is recommended to disable SMBv1 if it is not necessary, as this protocol is older and less secure. * Network Security: Implementing strong network security practices, such as firewalls and intrusion detection systems, can help protect against attacks. * User Education: Educating users about the risks of phishing attacks and other social engineering techniques can help prevent successful attacks.   Resources:   * Microsoft Security Bulletin MS17-010:<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> * MS17-010: Description of the security update for Windows SMB Server:<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> * MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption - Rapid7:<https://www.rapid7.com/blog/post/2017/05/20/metasploit-the-power-of-the-community-and-eternalblue/>   I hope this information is helpful. Please let me know if you have any other questions.  **METASPLOITABLE:**  HELP  Search ms17-010  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfSBM21HIV4b5QI--i8INbEKuopAvuu67t4G8qAEZYrIEjZ0-DwBZbHW8OoDfhzqwkXRxIIZCAxtIV-BNh4muGjMNg2yTEY3hPl7tR2wcNLAAcKZcSqoMUl5QyCtudceBq_jndNWMbu4Gn1J_o1YKVejws?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfSdf_8u4LzOz8i7lPP2J6N7wxMsEvh-SbPWPXMdTfrj34xSa3P6LaAfjhvS3WNWmK1DOfeZZi-pPd1nl0dd039AmzwOiH2lSrrutKCO9AyoMx5MM6ke-HRZ3RTFT0pszdl7UAJQI0yKhAoiBOg4iFARfbc?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdQuOMS6k3ZcDnQCDywpa6aZUhgeVUkixtobl5I4vv4fQI1iqM5bLpXYCizsVVkafCQs1ZzaHox0aKOz0OAwk4lvJii75YpIKHPyGFJZil1YGRYPwqkNSl1dsMkRxPGSlXz7hy7LVD9wlzh-sNknmyeFixH?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfKshXjVFFsGXa5vjkzOpwsrTyF45Jqv3GMv70oUDEneEGSIlqo-SC0HPUEqTxCp6uBJGQSkJtSrREA9sN1dO1HM34IuHQOeJ8ruUhKwYNx8-qdfPXURH2ezv7jneRXJCwMDBbGCRnf6YG5C0YwJV_ocg0?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfYy-4fCtSpJ_hMAq1hj4ZtF0mdAxbxelDIfamu2pg1YBJmHNXq6_OuT_7UDyWCCLZksagiUT2Rl1WMMZSs6nyZd5XtCUu6tTDD10Py7-6Ji5sZv5K0vZFPdLUZ4N6s1rVNxmND8rYz9aZHwWja0MKvlw_m?key=Vk71agtBjgu2Ts9zXFwT4Q  LHOST- lishtener host  **Run**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXd2n-yDKtTxOEjQ4gd5Dm3-Jn-HfxyG2ixHf18u6HvTa-OwFMOlAnJ1XASTawuYP2mdt-O0nquGuwmm6DhTZVNOzr60XihN7Kg-Pn86r3snl9pngBnrt41BoZPk4hx_2WpFU0v_Q7BQW8I3_HXh2Qr7awX8?key=Vk71agtBjgu2Ts9zXFwT4Q**  **SAM DB: as a hash**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXdMz3O4ZRf7agY2R0SRrLdJOBeoLp6wp5z53pTKKN4NdjCf17YGlBAZKbTOC7W8YbBhlPMJ4AJB-GpMJWQ1fO4jU2dTx_ZK73E7cG847FtQCz6jWFpMfKXbTSL6u6nJryoT3ODbU9SiS8vb2VynEvdoLT-d?key=Vk71agtBjgu2Ts9zXFwT4Q**  **Password cracking:**  **hashcat\*\***  **John the ripper**  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdW2X1VayKg2_3xiA9-5fZsaqxGYzcKZCAU5dFit_5sIsfzSnGNdXvrz5Ln1LESwjbzmQu9bLIOFar1kGv8pgiXp0gCugQ6OdZQXpicj5FcWgFQ_4gVbaFuvdViOkRoV_sv834d59m3jTblWWutnRErkHnv?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfZGxbpbsMnEmCU4Qieo_rE8zDk6B5Nhui89UqN2WujG03FE4QImNIOZXSKq6xThAoVtGKsJU5vxsJ-L-LFNPELKAROAx58lt4-j7lbvUxACieibiDl-1-38l4qUfev236P8P1cQtIOLBP9bfCPaBXoFwFy?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfysIn--TxPa_AK4rUJ9IneXI11xWZa4B1TmjZLLk86WsyGPiNh5PI_hEdcZDEzGcG4Kkf9Nj1t7obWzoZnf1EyuW9eoqykV1aENogyymdUDUkt-RBjyZmvQDU2KX0eEHFZK9oU1CSGEXpoFFsQ0v96ZDRA?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdIcgi2Vobc80NG_fzKHTVo0M5tJRST4MTETBr9oql8L79DsJR8iogB5QUvfjwvRrSeuc24534nvvVhARjdaRZ6YNkFGvnixjKmWpdt_P9ArnBi15HuavOxQhVnLcMQ31bAmmVSx3rP5ZJqbP5X_Vcmvkl9?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXeVcESiXauki-JdPpCxRiD3GToFf3Acrthgee8RNaHfX3IBbKaZk0h6c0b8JJi36XUYugZl5-4HwQX9uN2nT7M_xe2vSfqP1fP0V0A5bELULzwqzTSEc4_SAtJa5SdJQ8NDInl-0mO3Eez-7vSJ1gfW-xVs?key=Vk71agtBjgu2Ts9zXFwT4Q  **Pico ctf kali**  **192.168.10.104**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXfTOhAd8BORIfGrOGzG-3vBriT0vp2go7OiCdIAaGf3ODnlW1fC9m7ecKPo8B_3juz0kjcg0ipnVU4-7RjENMUTfoS6QUqC0GoFijpRjNQQp2b1-BB3sQBVyPp89ezFlfRnkCdaBuw6pchEmeMnXTN4iZxh?key=Vk71agtBjgu2Ts9zXFwT4Q**  ProFTPD 1.3.5 is an older version of the ProFTPD FTP server software that contains a critical vulnerability in its mod\_copy module. This vulnerability allows remote attackers to execute arbitrary commands on the server, potentially leading to complete system compromise.  Vulnerability Details:   * CVE-2015-3306: This vulnerability allows attackers to read and write arbitrary files using the SITE CPFR and SITE CPTO commands. * Remote Code Execution: By exploiting this vulnerability, attackers can execute malicious code on the server, gaining unauthorized access and control.   Mitigation:  To protect your system from this vulnerability, it is crucial to update ProFTPD to a more recent and secure version. The latest version of ProFTPD addresses this and other security issues.  Additional Security Best Practices:   * Keep Software Updated: Regularly update all software, including ProFTPD, to the latest versions to address security vulnerabilities. * Strong Passwords: Use strong, unique passwords for all user accounts, including the FTP server administrator account. * Secure Configuration: Configure ProFTPD securely, limiting access to authorized users and directories. * Network Security: Implement strong network security measures, such as firewalls and intrusion detection systems. * User Awareness: Educate users about the risks of phishing attacks and other social engineering techniques.   If you are unable to update ProFTPD immediately, consider implementing additional security measures, such as disabling the mod\_copy module or restricting access to the FTP server.  By following these guidelines, you can significantly reduce the risk of exploitation and protect your system from attacks targeting ProFTPD 1.3.5.  192.168.10.104/backdoor.php?cmd=whoami  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfwD1u0dLXcHlTt9rvh3rRVrNwliL9B5SCC7Q20I0wUhX8p508JapsT7e4C4JFkMC-84EUcAmgyj6su65mhMu-FsrXYET7eI3x6fZAiCRkoEVrl0ECyAPqmv9fnzuoGESxyS8WSogmB35WsPv43URzJQow?key=Vk71agtBjgu2Ts9zXFwT4Q  https://github.com/t0kx/exploit-CVE-2015-3306  Reverse shell cheat sheet → pentest monkey https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet  cmd=which nc  nc=netcat  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdELdONg8-7bFbP2NtpPamiEM4v1iqrur-X0VY1EItEfTuDBjBvDGtTr0d_4wYesgpEiU2o6IWmx8WrNDk1097oBllHn4NN5EO4vtcXtQ2Jlw4wVn6Ad3SaoJ1hFNf03ZtqlTvfVVuRrUQbivfw6NOk4Td4?key=Vk71agtBjgu2Ts9zXFwT4Q  Tty shell upgrade  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfmQZsJn8Kq1mZdag47XcifDfEPBNoU61raBmW-TTVjcRyWzF7CzqGgFhyDpnkVS6tpQ3w9IbMFu7Qm3tTSmv2P2MCEW2WyzQJxYCbd4IisIAmCo1K0Ix9t9GxyBxeLcxwk6CSbx9hrTOPcPBAQwwRhNVBQ?key=Vk71agtBjgu2Ts9zXFwT4Q |