# Cyber Security-Edge Program

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

|  |
| --- |
| **7. 28th September,2024** Nmap -sn -192.168.10.0/24 to check available ip  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcZH1R9wxxRQQlxhcq_eMkvXxkalLkMrIwjnsUByaQo7DYoSFBBYna5Tw8RIydwbui_LJej5JPAo9AwlMUqkmZWm9dqn1kpjdVgVnwCROvqM74K5T6-3IcjAnARm5Yfc2QzJxOpFOg30dBtZqcVw1MX9AXB?key=Vk71agtBjgu2Ts9zXFwT4Q  Target 192.168.10.100 – metasploitable-2  Sscanning techniques: **TCP scan**  https://lh7-rt.googleusercontent.com/docsz/AD_4nXflE-NwK3RMpgdv34GYR_3fMe5TvmGHX2lLg6oB4vImzlOfqsK5rRg8aqziYmfHdoM-PPv3bE2Fd4tAi0uZQnU9y0r8hGccPfB99JgDj6y8fHpu3AC-FkitlrxM6bgSczW7aFVKQ5Z1Vga46zRJUUyLuUC6?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXdcu234Lk-C8fNo7JQiIBOoSVN5jqLF4rf6IYark5rlmNCNf5VoKJJ5KdU5zWNgPEk2CNGN2Glmhdnp-5P7imFDXmesrQWjncSHGadqpIec_q8xYa1dcwWYzTTyRjQCsQYC7k4VKxxyITw2pCi8OX45_VED?key=Vk71agtBjgu2Ts9zXFwT4Q  **All: nmap -sT 192.168.10.100 -p-**  **nmap -sT 192.168.10.10 0-65535**  **UDP:**  nmap -sU 192.168.10.100  **Sync Scan:**  nmap -sS 192.168.10.100  Syn → ack←  RST→  https://lh7-rt.googleusercontent.com/docsz/AD_4nXel9ipueys4lyoLoyQi0tUPfMkOXj8KM5XyYRsmhv0K-ynbxHduGCFk7Ajg0kTseWVcHuBZrsHzru9Hz-DR9fcs1WmCR3rLCVkxyyPOG-mdKHmyv7i3-bjFfDFyjusT2Ns_Bq1Dg3zRODzz1xnVdvKA6Sf3?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXeeR4bM3YsqZ4-cLp77FLXMd122A8IWtY-55M-Flj40tgzuzPF53ZiqQhWTvcFzjl7lV3630vBLMWjF7akMYQzvXNqG5gs8GgSAC-fLrkjeT6s4gINNcFdd9QgEKwLser5uh_TzEkHmSvJ25Ovs3F5nlzx2?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXf6rs4V8vbZ5YG47-QaHS-FlxOagahqHHmolJAOxfSb7XXjteCOD5ghBxn3u0FtAa61iN-h1uWcdD-aN-ufyv96ylyGx0ST6wxLC3QgssGeSExK7rUqOZjl-tFPV7DDD612RWltO65mnHj06Xbh2ASfHaM?key=Vk71agtBjgu2Ts9zXFwT4Q  Difference in backend: using wireshark  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfYk1cqkweY1tRObwWr2BtKU9gz8gq0RgVtGV7OqitvlWtSceY2k9JLzwZkd6FT8eOufJ82cQYx5zO-6V7arIkla_Kvooge2SXcGRjJ0BQUp5uEwmiHDqyaa8oWU0VOaiMz_asfaMrwvfW_HRh5OTjhBX1K?key=Vk71agtBjgu2Ts9zXFwT4Q    https://lh7-rt.googleusercontent.com/docsz/AD_4nXcO29nL5YLJIFuOKUAjT90wi8irGZ57VOmIuUmQ2L7VgzLFLuhsMdcqbLCoYTzaXzFOra1B9uTqAV5N-YQlagS-zTFAs4q6wAxqj9NETbmtk7y0HJda6Vi3Sc8yikrtruErbOXz0QVTZcjceCK_X66RWaA9?key=Vk71agtBjgu2Ts9zXFwT4Q  Sync scan:  https://lh7-rt.googleusercontent.com/docsz/AD_4nXf1pQNIDqnmBxvuvmq6M-AO85eRJdKV_x5USnJpHbe9-zHQnENEOBu-RrkDh9ZxvpnwK7NFHhtxArPEQypv5LbGFiML2uxkTm2uQbgSGU1OXFsyHD9G512Un3l4TKrfMCw16_RHIGdwaAp9Zw8xVlbnVpJa?key=Vk71agtBjgu2Ts9zXFwT4Q  Service version: nmap -sS 192.168.10.100 -p 80 -sV  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcFJLcJzPENtr4qw_2kZpVl2U5YqYWJhh7omu0lHNT0DqUi_ybO0-VWb1qK9j9Ie6JVpnrw6Ad0-xsk4k2z7VUtDVSodlyPkFrNYbL51s--l-fF7LIcCxKnKMZ6jjLgkNxAP80vr7O55MIFt45vJDxqOUQL?key=Vk71agtBjgu2Ts9zXFwT4Q  Version theke security gap ber kora  https://lh7-rt.googleusercontent.com/docsz/AD_4nXe2P3EQmtucpdQc3lun9HDOarLdlH6anE7pl7rPI2Fhv-ojPzqFy8zw9pG1nX_agc4v8xDh0eBzFQmeoDQtLSPSpEPoZpcKiTjoRrUFoaQX9ZAxjARy1slACG2or7LvhVKWyIhvjh70ij04EPxAtOUnidEe?key=Vk71agtBjgu2Ts9zXFwT4Q  **Nmap scan speed:**  Reducing scan speed to prevent get blocked  Min T0 MAX T5  nmap -T0 default T4  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcsI3kHlXwTmldFVQdjFRaubujHoG8je7q6vF7Omd2P-zyqSv_D9EVBDemDZ5bubM7CP_K9wtoLPyttlDjmwZsiTFegw4b41D2AkGzz6Ab3o6b8UiP1se8-GNcdwNOpaU_7-kCfrxR3j998WP238x4WqK4?key=Vk71agtBjgu2Ts9zXFwT4Q  **Inverse Scan to bypass Firewall:**  If there no ping there's no reachability  If open no ack , if close get ack from RST  GIT: updating commands  New target 192.168.10.198  Ping 192.168.10.198  ttl=128/126 → windows  ttl=64 → linux  -sX -xmacs  -sM -maimon  nmap.org  **Scan behind Firewall:**  Packet fragmentation scan  **Decoy scan** : block kore dile scan korte parbo na , tai random ip diye scan kora jate net admin bujhte na pare.  Nmap 192.162.10.198  -D RND:10  **Network Enumeration:**  Information gathering  Network scanning  Enumeration  Target er sathe connected hoye more info gather kora, actively query korar process  Hostname, username. Group, ip and routing table, etc  SMTP Enumeration:  Ki ki user oi server e exist kore  Apt-get install netcat-traditional  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfn5xMI010C_WS0wA6UWP-OXfeok86NXG3igOmzx_qCLClhVyrgn9DF_eLJObGVKPtKbnAEbnemn3cNumT13x8hwvOkUR19omeuCR6k2tH-1HyAdieRbukJRmqj7LHfY77g1dO7DOnl8BkLEOo5bvdu7z6F?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXeq63wzT0CN4_6fd6oBpcuwoaAUVfRIKrAkHCyqU75xqy8EfaOCYo3sxmyXBPF_aTUjllEkEWvsOFZBlsG9XpuKxPXFTFG_pEcaY_km6Tkt4KcR9prXorqq8mufOZDYaXf4UakhMBoeGQIkk2rQzhHfik70?key=Vk71agtBjgu2Ts9zXFwT4Q  Smtp cmds: vrfy root  Vrfy test  test.com  hunter.io =  email search vrfy  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcsquaGP4DHEqx2UDdsOjQNxLycdjWzDBAVOo6n7CcTc8K-BAJbp3DrA4uyIKqCWFqLPjCMy91bW4zzkWbSXpvkM6PlF5vAYScXheoXrK_Ei45of0k7xchkYmKvpvjwDWSwFYPL8boUMvSeS8nK5vs6Cqw?key=Vk71agtBjgu2Ts9zXFwT4Q  To save= ctrl+x  Then press y  Then press ENTER  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfGLoaX03kjbSpiTGdZ_PNqXyjx_8JX42c5LpHP1iWUpFAF4UWej25kd4gJ0Ha5Kc53DjMsV0VXZvv8b3fZVZWGkCtm_uNSINx2Lj3w-i7JjnBD0nSNg_Bs1y4brawIID8yx-6cdjtdrVRpVZ9MqeJ5msQ?key=Vk71agtBjgu2Ts9zXFwT4Q  Nfs for linux file sharing protocol.  https://lh7-rt.googleusercontent.com/docsz/AD_4nXe2lSZ1-S-MslXilujBaQB5NJD67blBix_RUy_JxWGQKB6QDbvsFE2xJ0QzHPbNNGaK92KUykNDPot9EIt6vNlydVN8Fc7KC1Ry4JcDmCBzMwZ4vNMBLylCG06Vi-TCyQl4bEyiTyGR7VYBdi_StPLK5Zbf?key=Vk71agtBjgu2Ts9zXFwT4Q  https://lh7-rt.googleusercontent.com/docsz/AD_4nXfrGf9Rt-vqco1PIxW2jzF9GaDPx65Wn3-iTz_EsbYIxn6kQyOG070X6er5oMbcPgUnnF6h4b9NvnCTb53QpzPiQeuQj3eEYefZBL_QbLHWRUGGkOQ7NssdvlNyADWohlcidcPDa_oK0xTldWmbXDNBpRLx?key=Vk71agtBjgu2Ts9zXFwT4Q  Apt-get update  Apt install nfs-common  Showmount -e 192.168.10.100  https://lh7-rt.googleusercontent.com/docsz/AD_4nXcnlV-_sNcNcNGDZXtG7sVFiJmPi6Cnl8UB1mTXuqV-af76xDRwNfYsA0g3RcZK0BfFolZJ-2fdo_5xqB8ors7OdfLyoQRN6HrbnVq6EmTX-ztBI2JBQgrH7GR_vGu-USXXiJTV8dSedJCk3669f-GEvBhh?key=Vk71agtBjgu2Ts9zXFwT4Q  <https://book.hacktricks.xyz/network-services-pentesting/7-tcp-udp-pentesting-echo> |