Soru	Amaç	Kullanılan Komut(lar) / Araç	Yöntem	Sonuç
To Identify the number of live machines in 192.168.10.0/24 subnet	Ağdaki canlı makineleri tespit etmek	nmap -sn 192.168.10.0/24	Ağ keşfi (Ping sweep)	5 canlı makine (gateway hariç)
Identify the IP address of a Linux-based machine with port 22 open	SSH portu açık Linux makineyi bulmak	nmap -p 22 --open 192.168.10.0/24, nmap -sV -p 22 192.168.10.111	Servis versiyon tespiti	OpenSSH 8.9p1 Ubuntu
Find the IP address of the Domain Controller machine in 192.168.0.0/24.	DC IP'sini bulmak	sudo nmap -p 53,88,135,389,445,636,3268,3269 192.168.0.0/24	Active Directory servis taraması	192.168.0.222
Perform a host discovery and identify the NetBIOS_Domain_Name of 192.168.0.222	NetBIOS domain adını bulmak	nslookup -A 192.168.0.222, nbtstat -A 192.168.0.222, nmap --script nbstat.nse	NetBIOS Enum	SKILL.CEH
Perform an intense scan and find out DNS_Tree_Name	DNS ağacı adını bulmak	nmap -A -p 3389 192.168.0.222	DNS & OS keşfi	SKILL.CEH.com
Identify	Zafiyetli SSH	sudo nmap -sV -p 22	Servis	OpenSS

version of OpenSSH running in 192.168.10.0/24	sürümünü bulmak	192.168.10.0/24	versiyon analizi	H 8.9p1 Ubuntu 3ubuntu0.10
Determine OS of machine hosting MySQL in 172.30.10.0/24	MySQL host'un OS'unu belirlemek	nmap -p 3306 172.30.10.0/24, nmap -A 172.30.10.99	DB servis analizi	Ubuntu
Determine IP of MSSQL server in 192.168.10.0/24	MSSQL barındıranı bulmak	nmap -p 1433 --open -sS -sV -T4 -n -Pn 192.168.10.0/24	Veritabanı servis tespiti	192.168.10.144
Perform DNS enumeration on www.certifiedhacker.com	NS sunucularını belirlemek	dig NS certifiedhacker.com, nslookup -type=NS certifiedhacker.com	DNS bilgi toplama	ns1.bluehost.com, ns2.bluehost.com
Find IP running SMTP service on 172.30.10.0/24	SMTP barındıranı bulmak	nmap -p 25 --open -sS -sV 172.30.10.0/24	Mail servis tespiti	172.30.10.200
Perform SMB Enumeration and check if Message signing required	SMB güvenliğini kontrol etmek	nmap -p 445 172.30.10.200 -sC -T5	SMB güvenlik analizi	Message signing not required
Perform vulnerability assessment on 2023 CWE Top 25 list	25. zafiyetin kimliğini bulmak	web: https://cwe.mitre.org/top25/archive/2023/	Zafiyet istihbaratı	CWE-276 Incorrect Default

				Permissi
Perform OpenVAS scan and find QoD% of medium severity	QoD oranını belirlemek	OpenVAS GUI (docker)	Otomatik zafiyet taraması	70
Identify FTP-related vulnerability on 192.168.10.144 using OpenVAS	FTP güvenlik açığını bulmak	OpenVAS Dashboard	Servis zafiyet analizi	FTP Unencrypted Cleartext Login
Perform brute-force on Linux FTP user nick	nick kullanıcısını kırmak	hydra -l nick -P rockyou.txt ftp://192.168.10.45	Parola brute-force	nick/summer2024 → https://www.crushftp.com/
Analyze Mscredremote.pcapng to get credentials for moviescope.com	HTTP POST verisini incelemek	Wireshark → http.request.method == POST	Trafik analizi	ketty/elma
Analyze ServerDoS.pcapng to identify UDP protocol	UDP uygulama protokolünü tespit etmek	Wireshark UDP port analizi	Protokol analizi	Quake
Analyze DD_attack.pc	DDoS saldırganını	Wireshark UDP filtre	Ağ saldırı analizi	192.168.10.144

apng and find attacker IP	bulmak			
Analyze PyD_attack.pcapng to find attacker targeting RPC	RPC saldırganını bulmak	Wireshark (tcp.port==135)	RPC flood analizi	172.30.10.99
Analyze Anti-DDoS reports and find attacker IP	Rapor dosyasında saldırgan IP'yi bulmak	grep / manuel inceleme	Log analizi	192.168.10.222
Perform AS-REP attack and crack vulnerable user	Joshua hesabını kırmak	GetNPUsers.py + john	Kerberos AS-REP Roasting	c3ll0@123
Exploit MSSQL misconfiguration to find MSS.txt size	Dosya boyutunu öğrenmek	mssqlclient.py + xp_cmdshell	SQL kod yürütme	7 bayt
Capture Maurice RDP credentials via brute-force	RDP parolasını bulmak	cme rdp ... -u Maurice -p rockyou.txt	Şifre püskürtme	Pumpkin@1234
Analyze Tools.rar to find last 4 SHA-256 characters	SHA256 hesaplamak	sha256sum Tools.rar	Hash analizi	0282
Find parent PID of H3ll0.exe	Process tree'yi incelemek	ProcMon (Process Monitor)	Dinamik malware analizi	6952

from				
Find entropy of Tornado.elf	Entropi ölçmek	binwalk --entropy Tornado.elf	Statik malware analizi	7.94
Find machine with rpcap remote capture enabled	rpcap hizmetini bulmak	nmap -p 2002 --open -sV 192.168.10.0/24	Servis tespiti	192.168.10.144
Extract hidden data from stealth.jpeg using steghide	Gizli mesajı bulmak	steghide extract -sf stealth.jpeg -p azerty@123	Steganografi analizi	3965222
Searchsploit AirDrop 2.0 vulnerability path	Exploit dosya yolunu bulmak	searchsploit airdrop	Exploit DB araması	android/dos/46445.c
Analyze $_Jack.pcapng to find victim IP	TCP hijack kurban IP’si	Wireshark TCP RST analizi	Oturum ele geçirme analizi	172.30.10.200
Analyze Intercep_$niffer.pcapng to find captured creds	HTTP şifreleri bulmak	Wireshark POST string arama	HTTP sniffing	lee/test
Analyze honeypot cowrie.log to find attacker IP	Saldırganı tespit etmek	tail cowrie.log	Honeypot log analizi	172.30.10.99

Find web server technology for www.certifiedhacker.com	Web sunucusunu tespit etmek	curl -I, nmap --script http-server-header	Web fingerprinting	Apache
Crack Martin's SSH and retrieve $ollers.txt	SSH girişini kırmak	hydra -l martin -P rockyou.txt ssh://192.168.10.101	SSH brute-force	i2tr&^72546HJ*
Crack FTP nick and find domain ID in w_domain.txt	FTP içeriğini incelemek	hydra -l nick -P rockyou.txt ftp://192.168.10.111	FTP brute-force + dosya analizi	moviescope.com ID: 7867721010
Exploit web app on port 8080 and read RootFlag.txt	Log4j zafiyetini istismar etmek	python3 poc.py, nc -lvp 9001	RCE istismarı	Ch@mp2022
Find Meta-Author of highlighted site in webpent.txt	Webpent.txt dosyasını bulup meta author çıkarmak	hydra smb, `curl -s site	grep author`	SMB erişimi + web meta analizi
Identify attack category of oldest CVE on www.goodshopping.com	CVE saldırı tipini bulmak	CVE arşivi	CVE analizi	Cross-Site Scripting
Identify missing security policy mitigating XSS/SQLi	Eksik politikayı bulmak	HTTP başlık analizi	Web güvenlik denetimi	Content Security Policy

Find number of Directory Listings in w_report.pdf	Dizin listeleme sayısını bulmak	pdftotext w_report.pdf	PDF analizi	12
Brute-force www.cehorg.com for user adam	Web parolasını bulmak	Web login brute-force	Web brute-force	orange1234
Find number of risk categories in moviescope.com HTML	HTML güvenlik raporu incelemek	strings veya grep	Web risk analizi	3
SQLi on moviescope.com – find user count	DB kullanıcı sayısı bulmak	sqlmap	SQL Injection analizi	5
Find WASC ID for SQL Injection	WASC kimliği belirlemek	web / OWASP	Zafiyet sınıflandırma	WASC-19
Decrypt BCtetx.txt using password from pawned.txt	Şifreli dosyayı çözmek	BCTextEncoder	Kriptografi analizi	(ryptD3(0d3
Find CRC ending with 614c inside APK	CRC değerini tespit etmek	`unzip -v *.apk	grep 614c`	APK statik analiz
Find image with MD5 ending	İlgili imzayı bulmak	`md5sum *	grep 24ccb`	Adli analiz / hash

24CCB in signature.zip				karşılaştırma
Identify phishing number from call_log_dump.log	Şüpheli çağrı numarasını bulmak	grep Outgoing	Mobil adli analiz	+1 (555) 678-9012
Analyze And_Dos.pcapng and determine severity	Saldırı şiddetini bulmak	Wireshark Expert Info	Ağ saldırı analizi	Warning
Analyze MQTT.pcapng (High_humidity)	Uyarı yüzdesini bulmak	Wireshark MQTT filtre	IoT protokol analizi	50
Decrypt cryt-128-06encr.hex and identify algorithm	Şifreleme türünü bulmak	CrypTool	Kriptografi analizi	Twofish/@!ph@
Decrypt MyVeracrypt volume (password: veratest)	Volume içeriğini incelemek	VeraCrypt GUI	Adli analiz	4 dosya
Dump contacts and find Maddy's country code	Kişi kaydındaki ülke kodunu bulmak	PhoneSploit → Dump Contacts	Mobil analiz	61
Analyze MQTT.pcapng (High_temperature)	Topic uzunluğunu bulmak	Wireshark MQTT filtre	IoT analiz	16

Attain KEYCODE-5 used in mobile phone	Tuş kodunu bulmak	PhoneSploit → Use Keycodes	Mobil cihaz etkileşimi	Power Button
Access and read confidential.txt on Android	Gizli dosyayı bulmak	PhoneSploit → Download File	Mobil dosya analizi	80099889
Retrieve LOIC attack screenshot and packets/sec	LOIC ekranındaki PPS'yi bulmak	PhoneSploit – Görsel Analiz	Görsel adli analiz	23 pkt/s
Compare hashes in FileHashes.txt and find tampered file	Değişen dosyayı tespit etmek	md5sum *, diff	Hash bütünlük kontrolü	Quotes
Decrypt secret VeraCrypt volume (password: test)	Volume dosyalarını saymak	VeraCrypt	Disk şifre çözme analizi	6 dosya