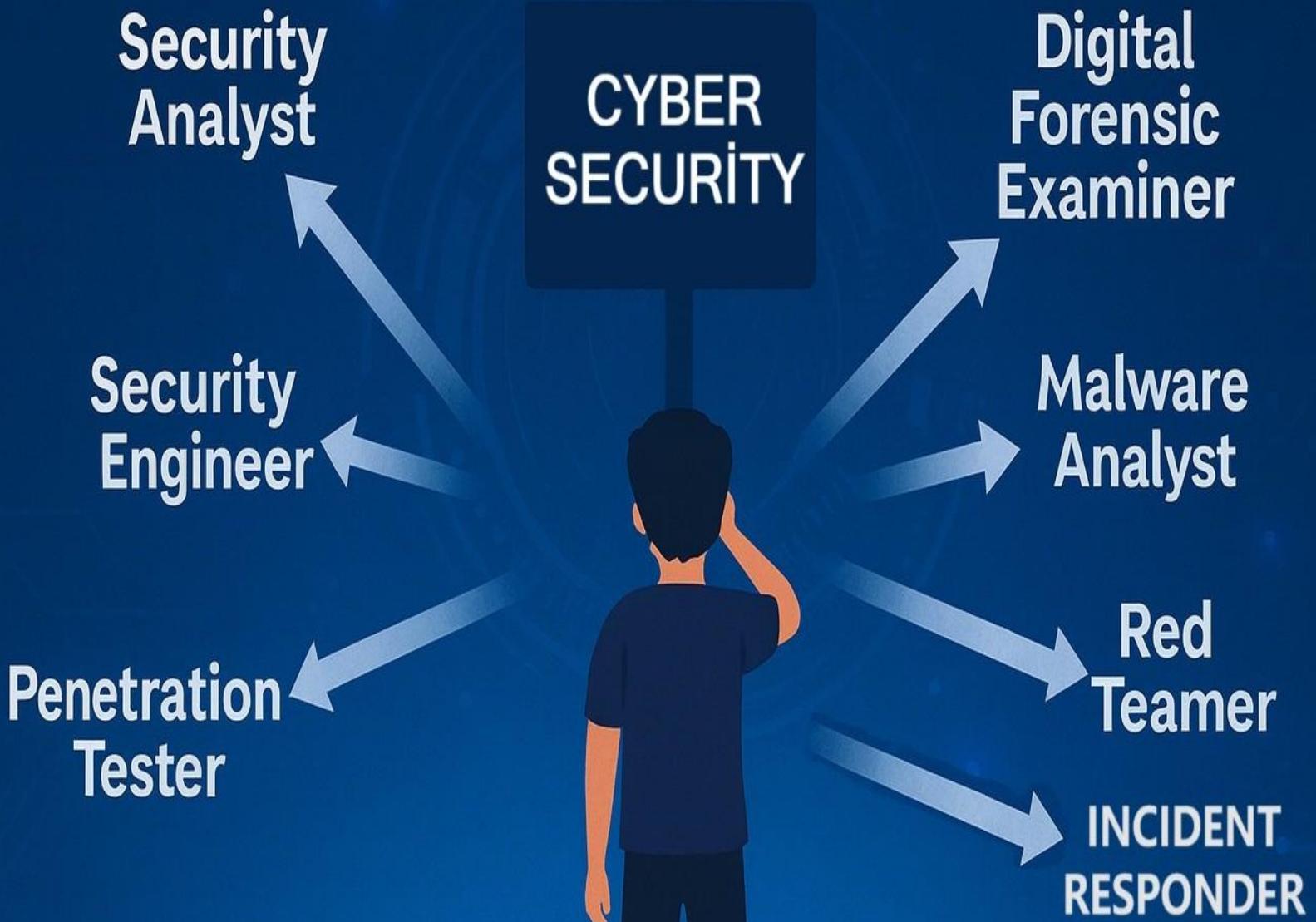


Siber Güvenlikte Kariyer Yolları





Siber Güvenliğin İki Yüzü: Red Team ve Blue Team

RED TEAM



Red team, sistemlere sizarak zayıf noktaları ortaya çıkarır. Saldırı simülasyonları ile savunma sistemlerini test eder.

BLUE TEAM



Blue Team, bu saldırılarla karşı koyar. İzleme, olay müdahalesi ve sistem güçlendirme ile kurumları korur.

Security Analyst

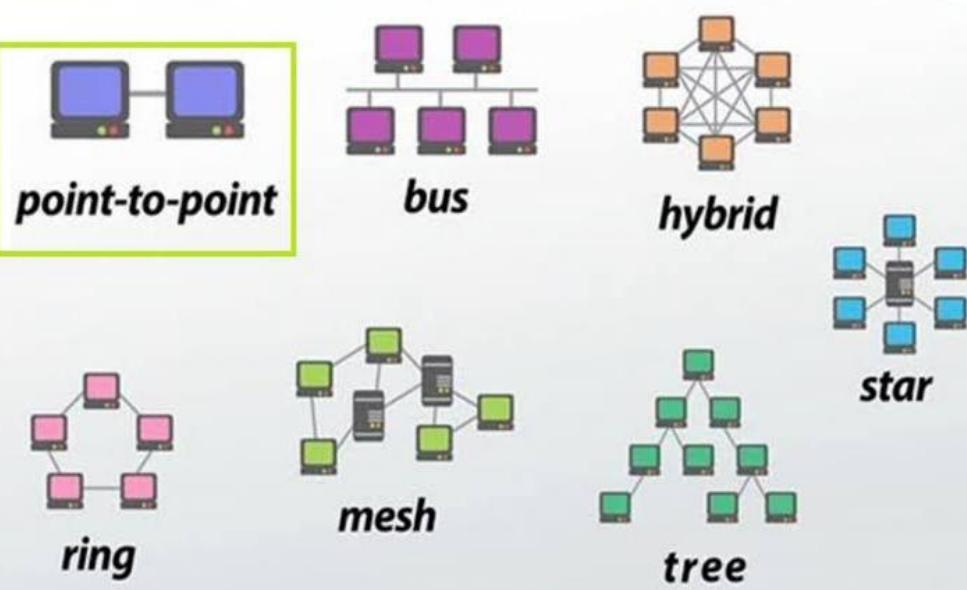


Sistem loglarını SIEM araçlarıyla analiz ederek şüpheli etkinlikleri tespit eder. SOC birimlerinde çalışır, veri sizıntısı gibi tehditleri erken fark edip raporlar.

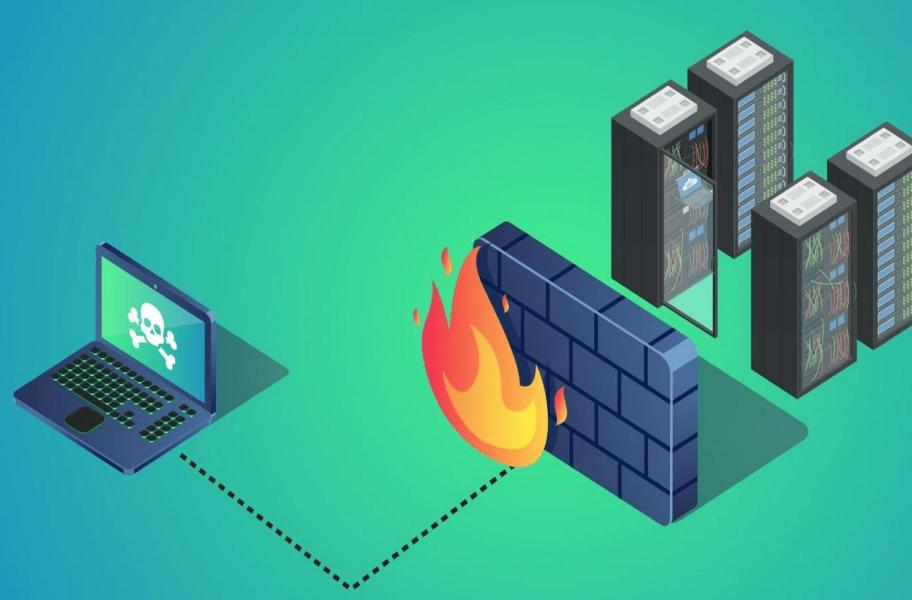
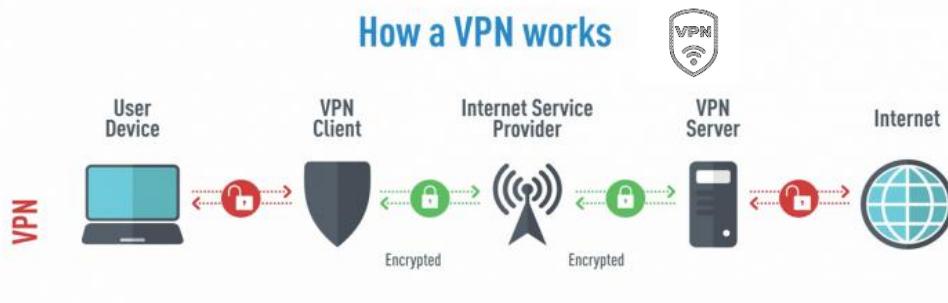
The screenshot shows a SIEM tool interface with the following sections:

- Hosts:** Shows 904 hosts, 10,633 successful user authentications, 33 failed user authentications, 1,165 unique source IPs, and 985 destination IPs.
- All Hosts:** A search bar with the query "host.name: \"finance-server\"". Below it are fields for "Fields", "Filter", and "event.action:config_change and event.dataset:file".
- Logs:** A log entry for "October 21, 2020 @ 19:40:15.160" with the message "audit-rule executed finance-server". The log details the session, host, and specific audit rule details.

Security Engineer



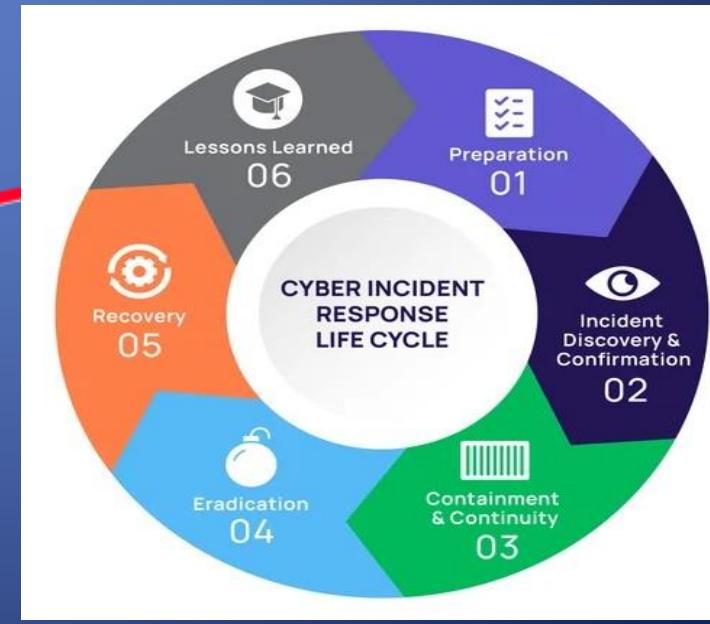
Ağ mimarisi kurar, firewall ve VPN sistemlerini yapılandırır. Zafiyetleri gidererek sistemleri daha dayanıklı hale getirir.



Incident Responder



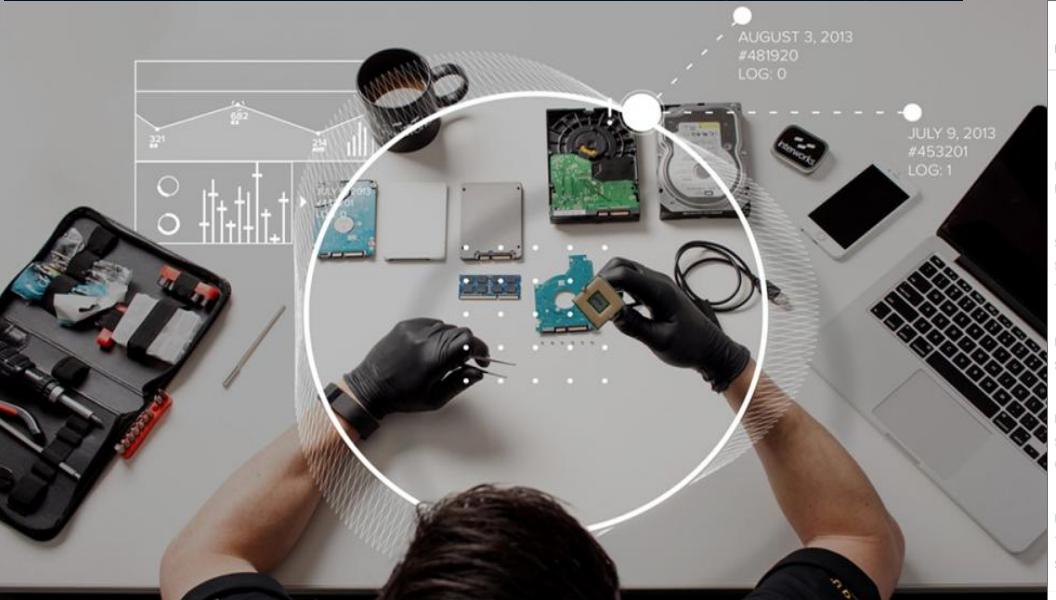
Saldırı anında müdahale eder, etkilenen sistemleri ağdan izole eder ve zararlı dosyaları temizler. Olayın kaynağını belirleyip rapor hazırlar.



Digital Forensics Examiner



Saldırı sonrası dijital delilleri inceler. Silinmiş dosyaları kurtarır, sistem geçmişini analiz eder ve hukuki süreçler için rapor hazırlar.

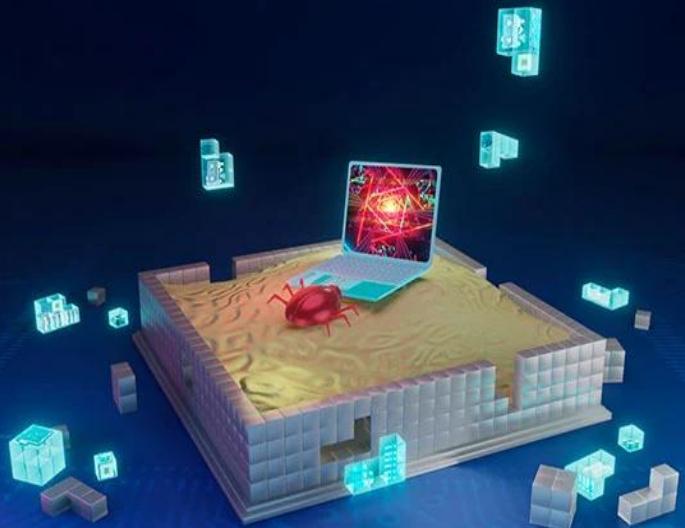


HEX-Editor

Encoding: ANSI (Windows)

	EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00	愤R@NTFS
Company (0:)	0000000010 00 00 00 00 F8 00 00 3F 00 FF 00 00 80 00 00ш.?..я..Т...
Local Disk	0000000020 00 00 00 80 00 80 00 FF D7 37 3A 00 00 00 00Р.Е.яУ7:....
	0000000030 00 00 0C 00 00 00 00 02 00 00 00 00 00 00 00 00#tсVИcVь
Name:	0000000040 F6 00 00 00 01 00 00 00 23 86 F1 56 C8 F1 56 FA	...в3ЛПРj. иhА...
File system:	0000000050 00 00 00 00 FA 33 C0 83 00 BC 00 7C FB 68 C0 07	..hf.JE..#fD..N
	0000000060 1F 1B 68 66 00 CB 8F 16 0E 00 66 81 5F 03 00 4B	TFSu.rKwСUH.r.ѓm
Space used:	0000000070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB	УсU.ЧВ..у.И5..fm
Space free:	0000000080 55 AA 75 06 F7 C7 01 00 75 03 E9 DD 00 1E 82 EC	.Л..гНз...яФ..Н.
Total size:	0000000090 18 68 1A 00 B4 48 8A 16 0E 00 8F B4 16 1F CD 13	цфД.Х.яб;..швј
	00000000A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3	..Е....Z3WР. +H
First sector:	00000000B0 0F 00 C1 2B 0F 01 04 1E 5A 33 DB B9 00 20 2B C8	фя.....#Ва...и
Sectors count:	32,768 00000000D0 4B 00 2B C8 77 EF B9 00 BB CD 1A 66 2A 75 2D	К.+Ишпё.»H.f#Au
	00000000E0 66 81 FB 54 43 50 41 75 24 81 F9 0E 01 00 16	fмTCРauѓm..rr...
Bytes per sector:	976,738,303 00000000F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 00	h..»hR..h..fsfsf
Sectors per cluster:	512 0000000100 55 16 16 68 B8 01 66 61 0E 07 CD 1A 33 CO 00	.н.хе.фа..Н.ЗА!
Cluster size:	4 KB 0000000110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1B	...у.ы.б.б.»....
	0000000120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00	.F...ш.и.ш.и.ш.и.
Physical Disk:	Samsung SSD 970 EVO 0000000130 00 66 50 00 53 68 01 00 60 10 00 B4 42 8A 16 0E	...F..ш.и.ш.и.ш.и.
Total size:	465.76 GB 0000000140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F	...<Ф.и.ш.и.ш.и.ш.и.
Sectors count:	976,773,168 0000000150 0B 82 16 00 66 FF 06 11 00 03 16 00 0E 00 8E C2 FF	...ш.и.ш.и.ш.и.ш.и.
	0000000160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00	...ш.и.ш.и.ш.и.ш.и.
...	0000000170 A1 FA 01 E8 03 00 F4 EB FD 8B FO AC 3C 00 74 09	...ш.и.ш.и.ш.и.ш.и.
	0000000180 B4 0E BB 07 00 CD 10 EB F2 C3 OD 04 20 64 69	...ш.и.ш.и.ш.и.ш.и.
...	0000000190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63	...ш.и.ш.и.ш.и.ш.и.
	00000001A0 62 75 20 72 65 61 00 00 0A 49 AF 54 AD 47 50	...ш.и.ш.и.ш.и.ш.и.

Malware Analyst



Sandbox ortamında zararlı yazılımları çalıştırarak davranışlarını analiz eder.
Hangi dosyalara eriştiğini ve hangi IP'lerle iletişim kurduğunu gözlemler.

```
152 } else {  
153     document.getElementById('bigImageDesc').innerHTML = descriptions[page * 9 + i - 1];  
154 }  
155 }  
156  
157 function updatePhotoDescription() {  
158     if (descriptions.length > (page * 9) + (currentImage - subImage) - 1) {  
159         document.getElementById('bigImageDesc').innerHTML = descriptions[page * 9 + i - 1];  
160     }  
161 }  
162  
163 function updateAllImages() {  
164     var i = 1;  
165     while (i < 10) {  
166         var elementId = 'foto' + i;  
167         var elementIdBig = 'bigImage' + i;  
168         if (page * 9 + i - 1 < photos.length) {  
169             document.getElementById(elementId).src = 'images/min/' + photojpeg[i - 1];  
170             document.getElementById(elementIdBig).src = 'images/big/' + photojpeg[i - 1];  
171         } else {  
172             document.getElementById(elementId).src = '';  
173         }  
174     }  
175 }
```

Penetration Tester

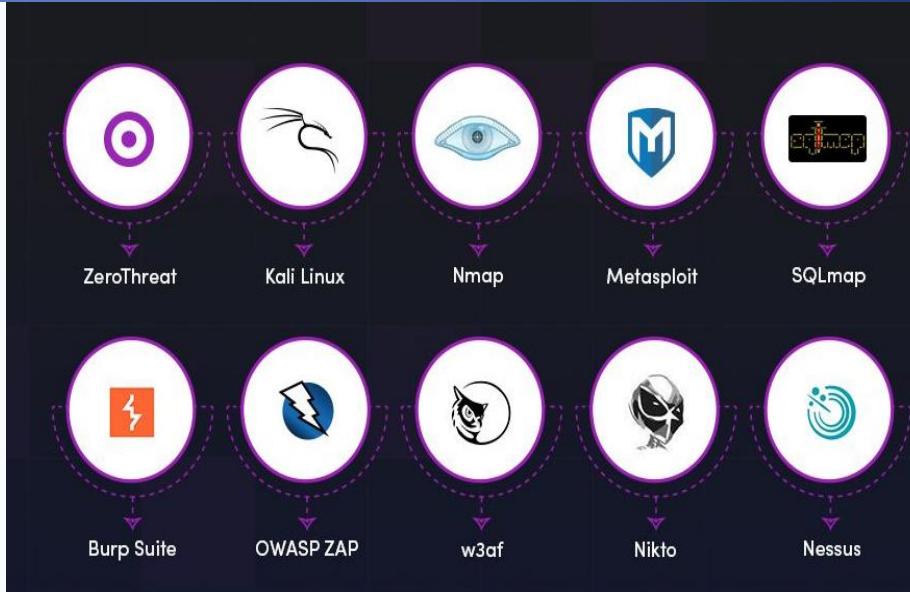
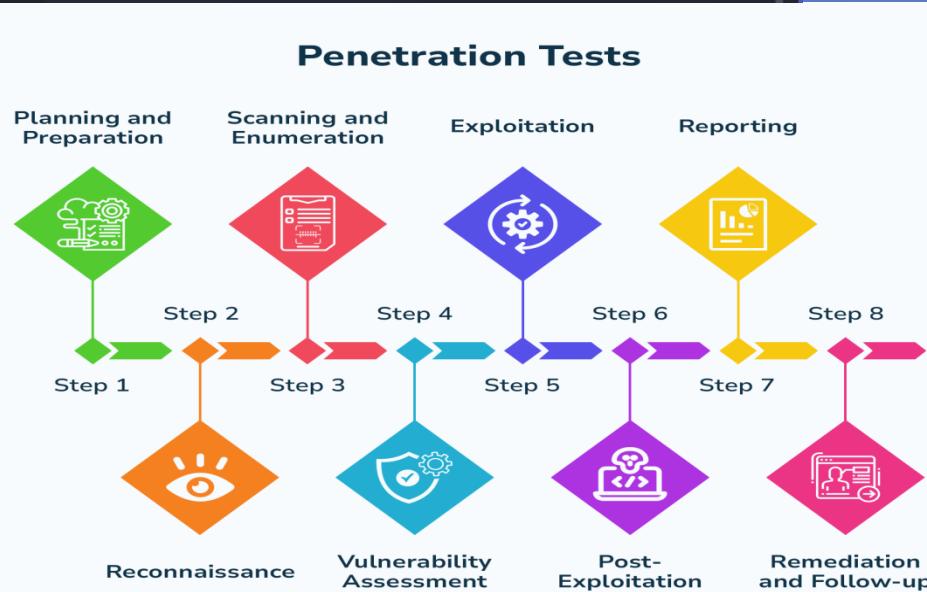
```
bobby2@kali: ~
File Actions Edit View Help

(bobby2@kali)-[~]
$ ssh bobby2@192.168.1.144
The authenticity of host '192.168.1.144 (192.168.1.144)' can't be established
.
ED25519 key fingerprint is SHA256:XPklf9+f+9ZvjTqNPnusNxz2DogfdS3cBG4rf00LIA
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.144' (ED25519) to the list of known hosts.
bobby2@192.168.1.144's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2022-06-25) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 24 03:19:53 2025 from 192.168.1.129
(bobby2@kali)-[~]
$
```

Etik hacker gibi sistemlere sizarak zafiyetleri tespit eder. SQL Injection, XSS, IDOR gibi açıkları bulur ve raporlar.



Red Teamer



Gerçek saldırı senaryoları uygular. Sosyal mühendislik, ağ saldıruları ve fiziksel güvenlik testleriyle kurumun savunma gücünü ölçer.



Kaynakça

- <https://cybersn.com/cybersecurity-career-center/>
- <https://tryhackme.com/room/careersincyber>
- [Top 10 Cybersecurity Jobs in 2025: High-Paying CS Roles | DxTalks](#)