BloodCode Red Team Starter Checklist

Legalni početak za ethical hacking, pentesting i red-team učenje

Autor: Stefan Spasov BloodCode

Kontakt: bloodcodehack@gmail.com | +381 63 146 0616 | elmconstruct.com

Pravilo broj 1

Red team bez dozvole nije red team. To je incident.

Ovaj checklist je za legalno učenje, sopstveni lab, CTF, TryHackMe, Hack The Box, PortSwigger Academy, akademiju ili ugovoreni test sa jasnim scope-om.

Ne koristi ga za tuđe sisteme bez pisanog ovlašćenja.

1. Mentalni model

- ☐ Razumem razliku između hakovanja, pentestinga i red-team simulacije.
- ☐ Znam da je cilj profesionalnog testiranja odbrana, ne šteta.
- ☐ Znam da svaki nalaz mora imati dokaz, uticaj i preporuku.
- ☐ Znam da dobar izveštaj vredi više od haotičnog korišćenja alata.
- ☐ Znam da se svaka vežba radi u labu ili ovlašćenom scope-u.

2. Legalni okvir

Pre bilo kakvog realnog testiranja mora postojati:

- ☐ Pisano ovlašćenje.
- ☐ Scope: domeni, IP opsezi, aplikacije, nalozi, cloud, lokacije.
- ☐ Out-of-scope lista.
- ☐ Pravila angažovanja.
- ☐ Vremenski prozor testiranja.
- ☐ Kontakt za hitne slučajeve.
- ☐ Stop conditions.
- ☐ Data handling pravila.
- ☐ NDA ako se radi sa firmom.

Ako nešto od ovoga ne postoji, ne testira se.

3. Lab okruženje

Minimalni lab:

- ☐ Jedna Linux mašina za učenje i beleške.
- ☐ Jedna namerno ranjiva web aplikacija.
- ☐ Jedan Windows test sistem ili AD lab ako učiš enterprise security.

- ☐ Odvojena mreža ili lokalno okruženje.
- ☐ Beleške za svaki test.
- ☐ Folder za dokaze, screenshotove i izveštaje.

Preporučene platforme:

- ☐ PortSwigger Web Security Academy.
- ☐ TryHackMe.
- ☐ Hack The Box Academy.
- ☐ OWASP Juice Shop lokalno.
- ☐ DVWA ili sličan lokalni lab.

4. Osnove koje moraš znati

Networking:

- ☐ IP, TCP, UDP.
- ☐ DNS.
- ☐ HTTP/HTTPS.
- ☐ TLS i sertifikati.
- ☐ Cookies i sessions.

Linux:

- ☐ Terminal.
- ☐ Permissions.
- ☐ Services.
- ☐ Logs.
- ☐ SSH.

Web security:

- ☐ Authentication.
- ☐ Authorization.
- ☐ IDOR/BOLA.
- ☐ XSS koncept i uticaj.
- ☐ SSRF koncept i bezbedno testiranje u labu.
- ☐ SQLi koncept u labu.
- ☐ File upload rizici.
- ☐ CORS.
- ☐ Security headers.

Reporting:

- ☐ Title.
- ☐ Summary.
- ☐ Impact.
- ☐ Preconditions.
- ☐ Steps to reproduce.
- ☐ Evidence.

- ☐ Severity.
- ☐ Remediation.

5. Prvi 30-dnevni plan

Dani 1-7: Temelj

- ☐ Nauči HTTP request/response.
- ☐ Nauči cookies, sessions i auth tokove.
- ☐ Prođi 10 PortSwigger lekcija.
- ☐ Napiši 3 mini izveštaja iz lab vežbi.

Dani 8-14: Web i API

- ☐ Vežbaj IDOR/BOLA u labu.
- ☐ Razumi role: admin, member, viewer, guest.
- ☐ Nauči šta znači tenant isolation.
- ☐ Napiši checklistu za jednu funkcionalnost.

Dani 15-21: Recon i scope

- ☐ Nauči pasivni recon.
- ☐ Nauči da čitaš program rules.
- ☐ Napravi asset map za sopstveni lab.
- ☐ Odvoji in-scope, maybe-scope i out-of-scope.

Dani 22-30: Izveštaji i odbrana

- ☐ Napiši jedan kompletan report.
- ☐ Dodaj executive summary.
- ☐ Dodaj remediation plan.
- ☐ Objasni koji log ili kontrola bi sprečila problem.

6. Greške početnika

- ☐ Jurenje alata pre razumevanja.
- ☐ Testiranje bez scope-a.
- ☐ Slanje nalaza bez uticaja.
- ☐ Preterivanje sa severity.
- ☐ Kopiranje payload-a bez razumevanja.
- ☐ Ignorisanje report writing-a.
- ☐ Mešanje realnih firmi sa lab vežbama.

7. Profesionalni standard

Pre nego što kažeš da je nešto ranjivost, proveri:

- ☐ Da li je asset u scope-u?

- ☐ Da li postoji realan security impact?
- ☐ Da li dokaz ne ugrožava tuđe podatke?
- ☐ Da li je reprodukcija bezbedna?
- ☐ Da li postoji remediation?
- ☐ Da li bi triager mogao da razume nalaz za 5 minuta?

8. BloodCode put dalje

Ako želiš strukturu bez lutanja, sledeći koraci su:

1. Red Team Master PDF.
2. BloodCode Red Team Academy syllabus.
3. Lab plan od 12 nedelja.
4. Report writing trening.
5. Mentorship ili community.

CTA:

Pošalji `RED TEAM` ili `PDF` na WhatsApp:

+381 63 146 0616

Email:

bloodcodehack@gmail.com