Ofenzivna sigurnost

Mapiranje i analiza površine napada

Leon Sattvik Kolenc, 26. 1. 2025.

Pregled predavanja

- Definicija mapiranja i analize površine napada
- Automatizacija procesa
- Perspektiva i pristupi crvenog i plavog tima
- Česte greške
- Primjer

Motivacija

- Moderni sustavi su kompleksni, raspodijeljeni te se konstantno mijenjaju, potreban je sistematičan pristup identifikaciji elemenata koji mogu biti napadnuti, te sprječavanju štete.
- Kontinuirana analiza sustava i sučelja u kombinaciji s pravilnom prioritizacijom dovodi do uspješne zaštite kritičnih točaka sustava

Pitanja za ispite

- Opišite glavni cilj analize površine napada.
- Navedite barem tri primjera točke ulaza napada.
- Navedite i objasnite pipeline za mapiranje i analizu površine napada.
- Što radi Attack Surface Management (ASM) platforma?
- Opišite razlike u pristupu analizi površine napada crvenog tima i plavog tima.

Površina napada

- Skup svih mjesta u sustavu gdje informacije i komande ulaze ili izlaze
- U praktičnom smislu:
  - UI forme i polja za unos
  - HTTP Headeri i cookies
  - API, datoteke, baze podataka
  - E-mail
  - Fizički pristup i sami ljudi….

Analiza površine napada

- U kompleksnim sustavima imamo na tisuće točaka napada, potrebno ih je klasificirati, mapirati na potencijalne napade i prioritizirati
- Glavni cilj analize je prijelaz s reagiranja na sigurnosne incidente na njihovo sprječavanje
  - Kontinuirani i iterativni proces

Identifikacija

- Razumijevanje sustava se dobiva korištenjem samog servisa
- Identificiramo i pratimo životni ciklus vrijednih podataka
  - Sigurnost backup sustava
- Razmotriti trenutačnu funkcionalnost sigurnosnih mehanizama
- Društveno inženjerstvo i fizička sigurnost

Korigiranje i mitigacija

- Sakupljena lista točaka napada se mapiraju na napade te sukladno ozbiljnosti prioritiziraju
  - Risk management
- Smanjuje se površina napada gdje je to moguće
  - Eliminacija zastarjelih funkcionalnosti, izolacija koda koji je prethodno bio otvoren prema internetu etc.
- TODO Lista: čišćenje koda, primjena zakrpi

ASM Pipeline i automatizacija

- Pasivno izviđanje: OSINT & DNS/WHOIS
  - Javno dostupne informacije koje nam mogu poslužiti za izvlačenje daljnjih informacija o sustavu i društveni inženjering
- Aktivno skeniranje: Nmap, OWASP Amass
  - Detekcija poslužitelja, otvorenih portova, servisa, OS verzija
- Unutarnja analiza sustava: Microsoft Attack Surface Analyzer, Lynis
  - *“Snapshotta”* sustav i detektira izmjene u konfiguraciji nakon instalacije novih funkcionalnosti

ASM Pipeline i automatizacija (2)

- Threat framework: MITRE ATT&CK
  - Mapiranje detektiranih točaka na napade za bolje prioritiziranje
- Attack Surface Management (ASM) platforma
  - Automatizira i auto-ažurira pipeline detekcije, enumeracije i klasifikacije ranjivosti dobivenih analizom površine napada

Česti propusti

- Statične analize
  - Sustavi se mijenjaju kroz vrijeme, te je potrebna kontinuirana analiza
  - Oslanjanje na zastarjelim listama
- Preveliko oslanjanje na automatizirane alate
  - Slijepo praćenje rezultata scannera može dovesti do slijepih točaka u sustavu zbog manjka konteksta
- Neispravno prioritiziranje
  - Jednaki tretman svih pronađenih propusta može dovesti do zatrpavanja kritičnih propusta manje opasnima

Različite perspektive plavog i crvenog tima

Crveni tim

- Gdje možemo i koliko daleko?
- Traže jednu rupu
- Otkriće → Učinak
- Eksploatabilnost

Plavi tim

- Gdje mogu i kako ih zaustaviti ili detektirati?
- Traže sve rupe
- Otkriće ↔ Mitigacija
- Minimizacija rizika i otpornost

Prednosti sistematičnog pristupa

- Temeljit pregled sustava daje povećanu vidljivost rizika
- Poboljšana reakcija i mitigacija incidenata
  - Poznavanje površine napada ubrzava detekciju i odgovor
- Kontinuirano poboljšava sigurnosnu arhitekturu
- Visoki stupanj automatizacije

Mane sistematičnog pristupa

- Velik utrošak resursa
  - Veliki i dinamički sustavi zahtijevaju često i kompleksno ažuriranje definicija površina napada sustava
- Lažne pozitivne detekcije
  - Nmap ponekad netočno prepozna zatvorene portove kao otvorene
- Veliki trošak implementacije sustava
- Automatizirani sustav može imati slijepe točke

Primjer: FERbanka.hr

Fer je odlučio otvorit malu banku za studente te je odlučio provesti mapiranje površine napada.

- FAZA 1: Enumeracija sustava Amass
  - Amass nam je otkrio četiri javno dostupne poddomene:
    - *Online.ferbanka.hr* → Glavni korisnički portal
    - *api.ferbanka.hr* → API server
    - *dev.ferbanka.hr* → Razvojno okruženje
    - *legacy-api.ferbanka.hr* → (!)Zaboravljen/Zastarjeli API

Primjer: FERbanka.hr (2)

- FAZA 2: Aktivno skeniranje – Nmap
  - Aktivno skeniramo sve dobivene poslužitelje:
    - *Online.ferbanka.hr* →443:*Apache HTTP Server 2.4.59* (!) Kritično ranjiva verzija
    - *legacy-api.ferbanka.hr* → 8080: *Node.JS Server* koji javlja greške, pritom cureći unutarnje putanje (Path Traversal CVE-2025-27210)
- FAZA 3: Unutarnja analiza: Microsoft ASA:
  - Odradimo unutarnji sken poslužitelja razvojnog okruženja:
    - *Dev.ferbanka.hr* → SMB Server je konfiguriran sa *Everyone: Full Control* dozvolama

Primjer: FERbanka.hr (3)

- FAZA 4: Analiza i mapiranje: MITRE ATT&CK

Resurs	ATT&CK Taktika	ATT&CK Tehnika	Opis
Online.ferbanka.hr	INICIJALNI PRISTUP IZVRŠAVANJE	**Exploit Public-Facing Application**	Ranjivi Apache server
legacy-api.ferbanka.hr	IZVIĐANJE	**Gather Victim Org Information**	Curenje unutarnjih informacija
Dev.ferbanka.hr	ESKALACIJA PRIVILEGIJA LATERALNO KRETANJE	**Network Share Discovery**	Ranjiva konfiguracija SMB Servera

Zaključak

- Mapiranje površine napada je ključan dio kontinuiranog održavanja sigurnosti sustava
- Proces je vrlo jednostavno automatizirati, no potrebno je dobro razmotriti sustav i mimo pipeline rješenja kako bi se eliminirale potencijalne slijepe točke

Literatura

- [1] Y. Jiang, “MITRE ATT&CK Applications in Cybersecurity and the Way Forward,” *National University of Singapore & NCS Cyber Special Ops R&D*, 2025. [Online]. Dostupno: https://arxiv.org/html/2502.10825v1. Pristupljeno: 11. 1. 2026.
- [2] CyCognito, “Attack Surface Mapping: Top 7 Techniques, Challenges and Best Practices.” [Online]. Dostupno: https://www.cycognito.com/learn/attack-surface/attack-surface-mapping/. Pristupljeno: 11. 1. 2026.
- [3] Darktrace, “Understanding Your Organization’s Attack Surface and Why It Poses a Risk.” [Online]. Dostupno: https://www.darktrace.com/blog/understanding-your-organizations-attack-surface-and-why-it-poses-a-risk. Pristupljeno: 11. 1. 2026.
- [4] M. Husák, “Attack Surface Management: State of the Art and Operational Challenges,” *2025 IEEE 11th International Conference on Network Softwarization (NetSoft)*, 2024. [Online]. Dostupno:https://www.researchgate.net/publication/393897467_Attack_Surface_Management_State_of_the_Art_and_Operational_Challenges. Pristupljeno: 11. 1. 2026.

Literatura

- [5] J. Foley, “Attack Surface Mapping with OWASP Amass,” *YouTube*, OWASP. [Online]. Dostupno: https://www.youtube.com/watch?v=Ui35-YEbBiA. Pristupljeno: 11. 1. 2026.
- [6] OWASP, “Attack Surface Analysis Cheat Sheet.” [Online]. Dostupno: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html. Pristupljeno: 11. 1. 2026.
- [7] MITRE, “ATT&CK Data & Tools.” [Online]. Dostupno: https://attack.mitre.org/resources/attack-data-and-tools/. Pristupljeno: 11. 1. 2026.
- [8] MITRE, “ATT&CK Techniques.” [Online]. Dostupno: https://attack.mitre.org/techniques/. Pristupljeno: 11. 1. 2026.

Dodatna literatura

- [9] M. Howard, “Measuring Relative Attack Surfaces,” *Carnegie Mellon University*, 2003. [Online]. Dostupno: https://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf. Pristupljeno: 11. 1. 2026.
- [10] J. Guo, “Attack surface analysis and mitigation for near-field communication networks and devices in smart grids,” *State Grid Jiangsu Electric Power Co., Ltd. Research Institute*, 2025. [Online]. Dostupno: https://www.sciencedirect.com/science/article/pii/S2590005625000748. Pristupljeno: 11. 1. 2026.
- [11] JUMPSEC, “SPRING Industry Briefing – Attack Surface Mapping in Action,” *YouTube*. [Online]. Dostupno: https://www.youtube.com/watch?v=3eHZE6b_WAw. Pristupljeno: 11. 1. 2026.

Hvala!