Ofenzivna sigurnost

Kibernetički teren

Danijel Živković, 14. siječanj, 2026.

Pregled predavanja

- Motivacija
- Pitanja za ispit
- Uvod
- Ravnine kibernetičkog prostora
- OCOKA analiza
- Okvir za korištenje kibernetičkog terena
- Ograničenja

Motivacija

- Kibernetičke operacije postaju ravnopravan oblik sukoba uz kinetičko ratovanje
- Kibernetički teren nije statičan i intuitivan kao fizičko bojište
- Puno teže odrediti ključni teren

Pitanja za ispit

- Zašto je teže odrediti ključni teren unutar kibernetičkog ratovanja u odnosu na kinetičko?
- Navedite ravnine kibernetičkog prostora.
- Objasnite *Obstacles* dio OCOKA analize kibernetičkog terena.
- Koji je zadnji korak unutar okvira za korištenje kibernetičkog terena? Ukratko opišite koji mu je cilj.
- Koje su poteškoće s kojima se napadač susreće prilikom analize kibernetičkog terena?

Uvod – kinetičko ratovanje

- Prostor
  - cjelokupno fizičko operativno okruženje
- Teren
  - struktura i obilježja fizičkog prostora
- Ključni teren
  - područje čije zauzimanje ili zadržavanje daje prednost

Različite definicije kibernetičkog terena

- Različiti autori daju različite definicije
  - Neki autori navode da se kibernetički teren sastoji samo od fizičkih objekata
  - Većina drugih se slaže da je kombinacija fizičkih i virtualnih obilježja
- Autori također daju i različite reprezentacije
  - Neki ga predstavljaju pomoću 3 sloja/ravnine, neki pomoću 5
- Sposobnost analize terena je važnija od same terminologije

Uvod – kibernetičko ratovanje

- Kibernetički prostor
  - cjelokupna digitalna domena djelovanja
- Kibernetički teren
  - sustavi, uređaji, protokoli, podatci, softver, procesi i kibernetički identiteti koji čine, nadziru i upravljaju kibernetičkim prostorom
- Kibernetički ključni teren
  - elementi kibernetičkog terena čija kontrola daje prednost

Razlike između terena

- Kinetičko ratovanje
  - Promjene spore i lako uočljive
  - Fizički vezan uz geografiju samog prostora
  - Lako vidljivo tko ima kontrolu nad terenom

- Kibernetičko ratovanje
  - Izrazito dinamičan – moguće promjene u roku milisekundi
  - Često nije vezan uz fizički prostor
  - Nije lako znati tko ima kontrolu nad terenom

Dinamičnost kibernetičkog terena

- Software Defined Networking
  - Logička topologija se mijenja bez promjene hardvera
  - Pristupni pravci se mogu trenutno preusmjeriti
- Virtualizacija, oblak
- Automatizacija
- Honeypot, honeynet
  - Umjetno stvoreni dijelovi terena, brzo se postavlja, uklanja ili premješta

Ravnine kibernetičkog prostora

- Analitički slojevi kroz koje promatramo prostor

- Geografska ravnina
  - Fizička lokacija infrastrukture
  - Najmanje dinamičan dio kibernetičkog terena
  - Podatkovni centri, energetske stanice, podmorski kabeli

- Fizička ravnina
  - Hardverske komponente
  - Usmjerivači, preklopnici, serveri, USB uređaji

Ravnine kibernetičkog prostora

- Logička ravnina
  - Programska podrška i logičke veze
  - Aplikacije, protokoli, operacijski sustavi, DNS
- Ravnina kibernetičkih identiteta
  - Digitalni identiteti
  - Korisnički i administratorski računi, digitalni certifikati
- Nadzorna ravnina
  - Nadzor, upravljanje i kontrola kibernetičkim operacijama
  - C2 serveri, SOC, SIEM

OCOKA analiza

- Standardni okvir za procjenu fizičkog prostora u borbenim operacijama

- O – Observation and Fields of Fire
- C – Cover and Concealment
- O – Obstacles
- K – Key Terrain
- A – Avenues of Approach

OCOKA analiza kibernetičkog terena

- Observation and Fields of Fire
  - Izviđanje – IP lookup, skeniranje mreža i portova
  - Analiza dolaznog i odlaznog prometa – IP adrese, TTL
  - Izviđanje daje uvid u polja vatre

- Cover and Concealment
  - Cover – vatrozid, sustavi za sprječavanje upada (IPS)
  - Concealment – obfuskacija, rootkit

OCOKA analiza kibernetičkog terena

- Obstacles
  - Tehnologije i politike koje ograničavaju slobodu kretanja unutar mreže
  - Kontrole pristupa, vatrozid, ograničenja propusnosti
  - Razlika između zaklona i prepreka nije uvijek jasna

- Avenues of Approach
  - Vektori pristupa
  - Logičke veze relevantnije od fizičkih
  - HTTP pristup web serveru, phishing

Okvir za korištenje kibernetičkog terena

- Ključni teren je subjektivan
  - Ovisi o iskustvu, kontekstu, pristupu i o onome što osoba smatra uspješnom obranom/napadom

- Koraci:
  1. Identifikacija potencijalno ciljanih resursa
  2. Enumeracija vektora pristupa
  3. Analiza polja vatre
  4. Postavljanje prepreka i zaklona te osiguranje prikrivenosti

Okvir za korištenje kibernetičkog terena

1. Identifikacija potencijalno ciljanih resursa
   - Utvrditi koje sustave, podatke i procese napadač može smatrati vrijednima
   - Jako bitno razlikovati što je važno organizaciji, a što napadaču
   - Podatci, korisnički računi, pomoćni sustavi

2. Enumeracija vektora pristupa
   - Razmotriti sve izravne i neizravne vektore prema identificiranim resursima
   - Važno u obzir uzeti sva vanjska sučelja i sve ravnine
   - Mrežna sučelja, neizravna sučelja (npr. USB mediji), ljudski resursi

Okvir za korištenje kibernetičkog terena

3. Analiza polja vatre

- Odrediti s kojih pozicija napadač može promatrati sustav ili izvesti napad (vantage points)
- Proces postaje iterativan: takve pozicije je također potrebno zaštititi
- Kroz ovaj proces ključni teren postaje jasniji: sve one pozicije (dijelovi kibernetičkog terena) koje napadaču daju polje vatre
- Analizu potrebno proširiti i na sustave treće strane kako bi se umanjio rizik napada neizravnim vektorom pristupa

Okvir za korištenje kibernetičkog terena

4. Postavljanje prepreka i zaklona te osiguranje prikrivenosti

- Ograničiti vektore pristupa i površinu napada – vatrozidi, IPS, zatvaranje nepotrebnih portova
- Napadači s dovoljno znanja i resursa će uvijek pronaći način, stoga je korisno uložiti resurse i u obmanu (honeypot, honeynet)

Perspektiva napadača

- Napadač koristi sličan analitički proces kao i branitelj
- Cilj mu je rekonstruirati obrambenu analizu i time identificirati sustave s najvećim operativnim učinkom
- Poteškoće napadača:
  - Djeluje s nepotpunim informacijama
  - Potreba za prikrivanjem aktivnosti i izbjegavanjem detekcije
  - Stalni rizik upada u honeynet i honeypot

Ograničenja

- Ne postoji univerzalna ili “objektivna” mapa kibernetičkog terena
  - Ovisi o kontekstu, izrazito je dinamičan
- Nemogućnost potpune analize svih mogućih scenarija
- Visoki zahtjevi u pogledu stručnosti, iskustva i specijaliziranih vještina

Zaključak

- Analiza kibernetičkog terena daleko je zahtjevnija od analize fizičkog terena
- Cilj nije doći do doslovne analogije terena, već do efikasnog i univerzalnog načina analize
- Sposobnost analize kibernetičkog terena važnija je od same definicije

Literatura

[1] David Raymond, *Key Terrain in Cyberspace: Seeking the High Ground.* NATO Cooperative Cyber Defence Centre of Excellence, 2014. https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

[2] Alexander Grandin, *Cyberspace Geography and Cyber Terrain: Challenges Producing a Universal map of Cyberspace.* 22nd European Conference on Cyber Warfare and Security, ECCWS 2023, https://www.researchgate.net/publication/371704343_Cyberspace_Geography_and_Cyber_Terrain_Challenges_Producing_a_Universal_map_of_Cyberspace

Hvala!