Ofenzivna sigurnost

Lateralno kretanje

Dino Dervišević, 03.11.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Otkrivanje (Discovery)
- Lateralno kretanje i eskalacija privilegija
- Tehnike i primjeri lateralnog kretanja
- Prevencija lateralnog kretanja
- Zaključak

Motivacija

- Početni upad u mrežu daje ograničen pristup
  - Stvarni ciljevi (podaci, kritični sustavi) su drugdje u mreži
- Lateralno kretanje stvara put kroz mrežu
  - Širi opseg napada i kompromitira mrežu
  - Povećava kontrolu nad mrežom
- Napadač mora znati kuda se kreće → mrežu je potrebno analizirati

Pitanja za ispite

- Objasnite kako eskalacija privilegija pomaže pri lateralnom kretanju.
- Nabrojite barem 3 tehnike otkrivanja (*discovery*).
- Objasnite kako udaljene usluge (SSH, RDP) mogu omogućiti lateralno kretanje i zašto je to teško otkriti?
- Opišite kako radi *Overpass the hash* napad.
- Što je *Zero Trust* pristup i kako on pomaže u spriječavanju lateralnog kretanja?

Otkrivanje (Discovery) [8]

- Faza u kojoj napadač prikuplja informacije o mreži kako bi planirao lateralno kretanje
- Ciljevi:
  - Pronaći put do kritičnih sustava
  - Shvatiti hijerarhiju profila i sustava
  - Identificirati korisnike s administratorskim pravima
  - Otkriti mrežnu topologiju i odnose između uređaja
  - Pronaći ranjivosti u konfiguraciji mreže

Tehnike Otkrivanja (1/2) [9]

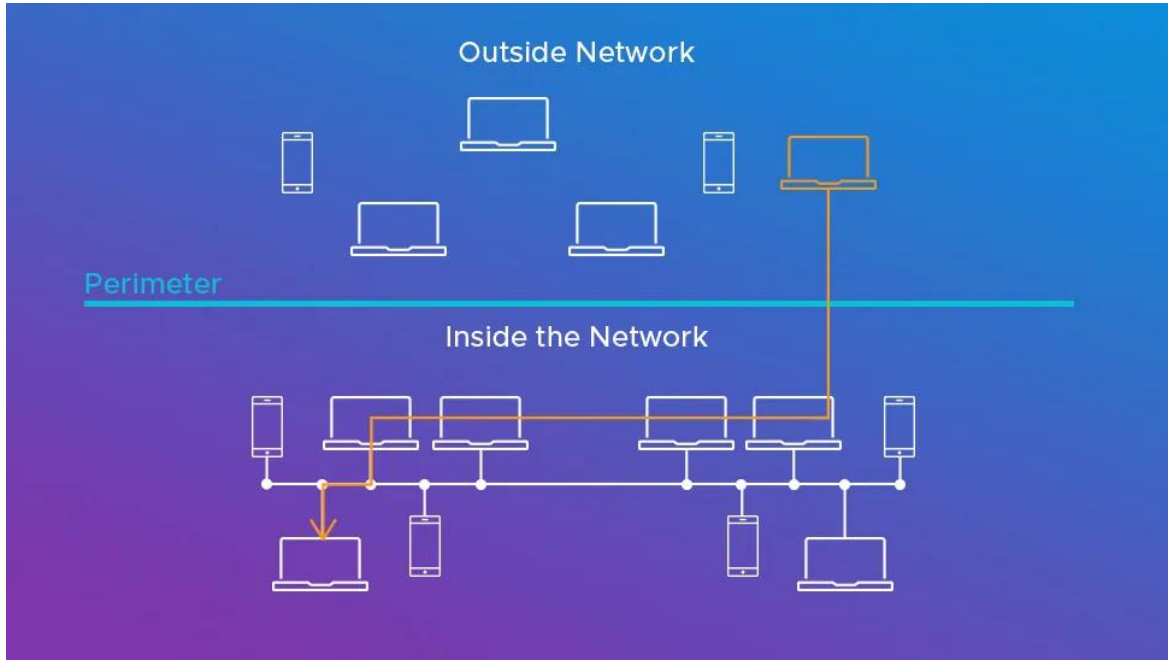
- Otkrivanje računa
  - Cilj je dobiti listu svih valjanih računa ili email adresa na mreži
  - Uvelike olakšava *Spearphishing* i napade koji koriste valjane račune
  - Ako je već u mreži, napadač može koristiti `PowerShell`, `Bloodhound` ili slične alate
- Otkrivanje mrežnih veza sustava
  - Izviđaju se sve veze prema sustavu ili s njega
  - `netstat` – alat za skeniranje mrežnih veza

Tehnike Otkrivanja (2/2) [9]

- Otkrivanje informacija o sustavu
  - Informacije o OS-u i hardveru (točna verzija, arhitektura…)
  - `Systeminfo`
- Otkrivanje mrežnih usluga
  - Otkrivaju se svi servisi koji se izvode na mreži
  - Skeniranje portova za otkrivanje servisa
  - Najčešće korišten alat: `nmap`

Što je lateralno kretanje? [1]

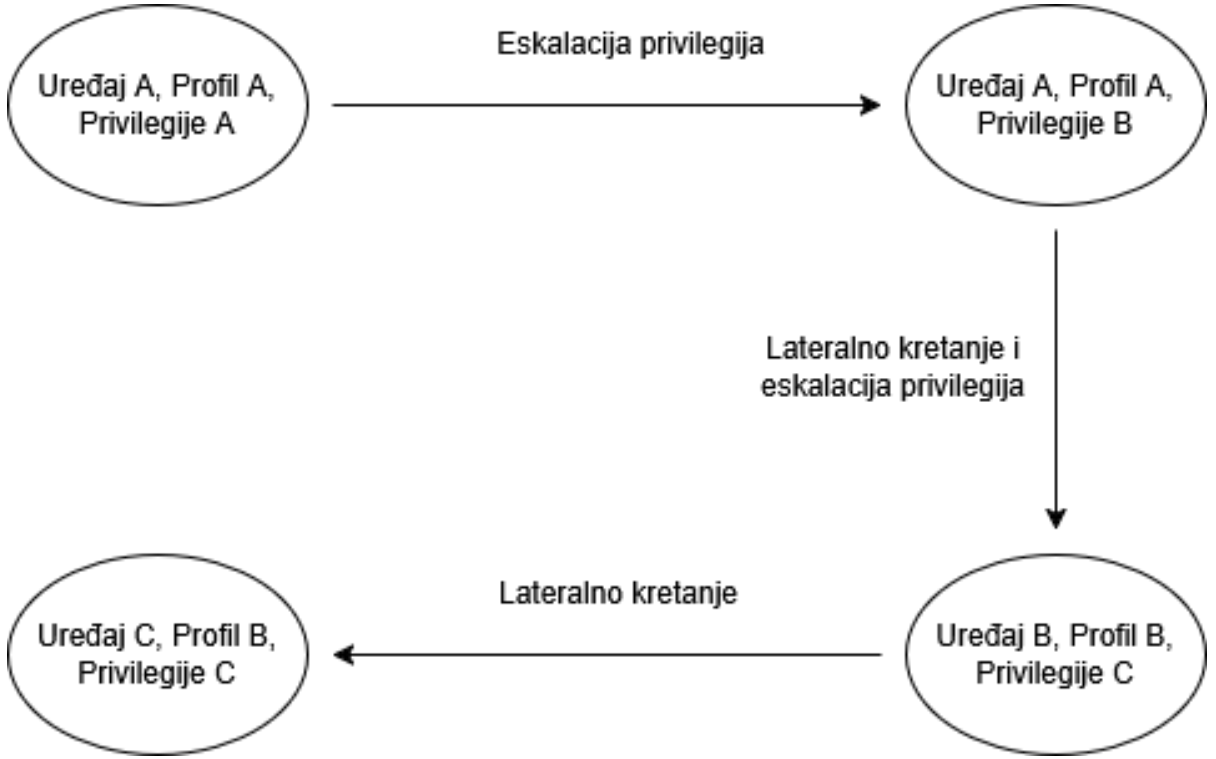
- Skup tehnika kretanja s jednog uređaja na druge uređaje unutar mreže
- *Living off the land*
- Dvije vrste:
  - Autentificirani napadi
  - Neautentificirani napadi



Izvor: [7]

Eskalacija privilegija [10]

- Tehnike za dobivanje viših privilegija na mreži
- Vertikalno kretanje u mreži
- Često je preduvjet za učinkovito lateralno kretanje



Tehnike lateralnog kretanja (1/2) [2]

- Pass the hash
  - Korištenje ukradenog NTLM hash-a lozinke za autentifikaciju
  - Hash se krade izravno iz memorije ili alatom (npr. Mimikatz)
- Pass the ticket
  - Krađa Kerberos TGT (*Ticket Granting Ticket*) ticketa (tokena) sesije
  - *Golden ticket* - KRBTGT hash kojim možemo sami stvarati tickete
    - Ukraden od Domain kontrolera
- Overpass the hash
  - *Pass the hash* koji pretvara NTLM hash lozinke u Kerberos tickete

Tehnike lateralnog kretanja (2/2) [2]

- Iskorištavanje udaljenih usluga
  - Napadač pristupi udaljenim uslugama poput RDP, SSH, VNC…
  - Koriste već postojeće sesije
  - Alternativno, prijave se istim vjerodajnicama kao i za profil
- Lateralni prijenos
  - Napadač prenosi maliciozne dokumente ili alate na druge uređaje

Ostale tehnike lateralnog kretanja [2]

- Unutarnji *Spearphishing*
- Manipulacija dijeljenog sadržaja
- Iskorištavanje ranjivosti udaljenih usluga

Primjeri napada

- Hive napad na Microsoftov Exchange Server 2022. [6]
  - *Pass the hash* pomoću Mimikatz-a
- BlackCat/ALPHV napad na Change Healthcare 2024. [5]
  - Ukradenim vjerodajnicama napadači su se širili po mreži te ukrali i kriptirali podatke
  - Ucijenili za Change Healthcare 22 milijuna dolara

Obrana – *Zero trust* principi [11]

- Nema implicitnog povjerenja – svakog se kontinuirano provjerava
- Princip najmanjih privilegija
- Mrežna segmentacija
- Višefaktorska autentifikacija
- Eksplicitna verifikacija svih resursa

Zaključak

- Lateralno kretanje omogućuje napadaču pristup kritičnim resursima i njegovom cilju napada
- Ključno je prvo analizirati mrežu tehnikama otkrivanja
- Tehnike lateralnog kretanja se većinski temelje na autentifikaciji
- Najbolja obrana je pratiti *Zero trust* principe

Literatura

- [1] Anas Mabrouk, ”Lateral Movement Attacks Datasets: Benchmarking, Challenges, and Solutions”, 2024., https://www.proquest.com/docview/3161607098?%20Theses&fromopenview=true&pq-origsite=gscholar&sourcetype=Dissertations%20
- [2] MITRE ATT&CK, https://attack.cloudfall.cn/tactics/TA0008/
- [3] s0cm0nkey’s Security reference guide, https://s0cm0nkey.gitbook.io/s0cm0nkeys-security-reference-guide/red-offensive/lateral-movement#http-tunnel
- [4] paloalto networks, What is Lateral Movement?, https://www.paloaltonetworks.com/cyberpedia/what-is-lateral-movement#technicques
- [5] William Toll, Elisity Blog, ”The Top 11 Cyberattacks Using Lateral Movement: A 2023-2024 Analysis for Enterprise Security Leaders”, https://www.elisity.com/blog/the-top-11-cyberattacks-using-lateral-movement-a-2023-2024-analysis-for-enterprise-security-leaders

Literatura

- [6] Kurt Baker, Crowdstrike, ”Pass-the-Hash Attack”, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/pass-the-hash-attack/
- [7] Chad Skipper, VMware Security Blog, ”Lateral Movement: What It Is and How to Block It”, https://blogs.vmware.com/security/2022/05/what-is-lateral-movement.html
- [8] Kurt Baker, Crowdstrike, Lateral Movement Explained, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/
- [9] MITRE ATT&CK, https://attack.cloudfall.cn/tactics/TA0007/
- [10] MITRE ATT&CK, https://attack.cloudfall.cn/tactics/TA0004/
- [11] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, ” Zero Trust Architecture”, 2020. ,https://doi.org/10.6028/NIST.SP.800-207

Hvala!