EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SKENIRANJE IN KIBERNETSKO IZVIDOVANJE

VSEBINA

Kaj je kibernetsko izvidovanje.

Vrste in podatki ki se zbirajo tekom izvidovanja.

Tehnike izvidovanja.

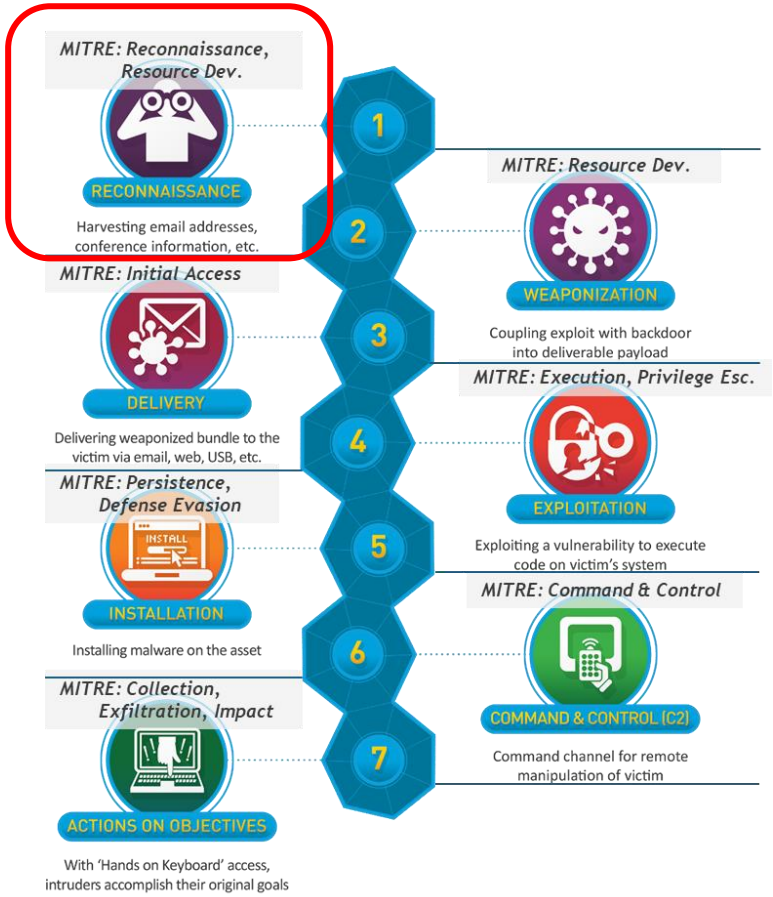
Zaznavanje in preprečevanje izvidovanja.

IZVIDOVANJE KOT PRIPRAVA NA NAPAD

Izvidovanje (Reconnaissance) je prva faza v modelu Cyber Kill Chain in predstavlja proces, v katerem napadalec zbira informacije o tarči, preden izvede dejanski napad.

Cilj te faze je razumeti okolje žrtve, prepoznati ranljivosti ter izbrati najučinkovitejši način napada, pri čemer se napadalec praviloma poskuša izogniti zaznavi.

Izvidovanje se izvaja v celotnem toku napada (enumeracija), ne nujno samo na začetku.



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

VRSTE IZVIDOVANJA

Pasivno izvidovanje

Zbiranje informacij brez neposrednega stika s sistemi tarče, npr.:

- javno dostopni viri, spletne strani, družbena omrežja, javni registri,
- podatki iz preteklih kompromitacij (data breaches),
- DNS zapisi, WHOIS podatki, javni IP naslovi.

Aktivno izvidovanje

Neposredna interakcija s tarčo, ki lahko pusti sledi v dnevnikih:

- skeniranje omrežij in vrat (port scanning),
- identifikacija storitev in verzij (service fingerprinting),
- testiranje osnovnih ranljivosti.

PODATKI KI SE ZBIRAJO Z IZVIDOVANJEM

Organizacijski podatki

Organizacija, povezane entitete.

Organizacijska struktura in ključne funkcije.

Partnerji in dobavitelji, IT ponudniki.

Fizične lokacije in varnost.

Podatki o zaposlenih

Osebni podatki, imena, emaili, telefonske številke.

Vloge in odgovornosti (CxO, vodje, IT, finance, operations,..)

Profili na družbenih omrežjih, navade in javno deljene informacije.

Ranljivosti

Znane ranljivosti (CVE).

Napačne konfiguracije.

Odprti administrativni dostopi.

Javno dostopni dnevniki, repozitoriji.

Podatki o IT infrastrukturi

Javni IP naslovi, geografske lokacije, oblaki.

Spletne domene in poddomene.

DNS zapisi (A, MX, TXT, SFP, DKIM)

Izpostavljene storitve in TCP/UDP vrata.

Vzorci vedenja

Delovni časi.

Odzivni časi služb in storitev.

Reakcije na skeniranja in testne poizvedbe.

Sistemski in tehnični podatki

Operacijski sistemi in verzije, verzije spletnih strežnikov in API.

Strežniška in aplikativna programska oprema.

Uporabljeni varnostni sistemi (NGFW, IPS, NDR, EDR, WAF)

Podatki iz preteklih incidentov

Podatki iz javno znanih vdorov.

Uhajanje gesel in email naslovov.

Podatki na tržnicah temnega spleta.

Dokumenti in vsebine

Javno dostopni dokumenti.

Metapodatki (uporabniška imena, verzije, poti,...).

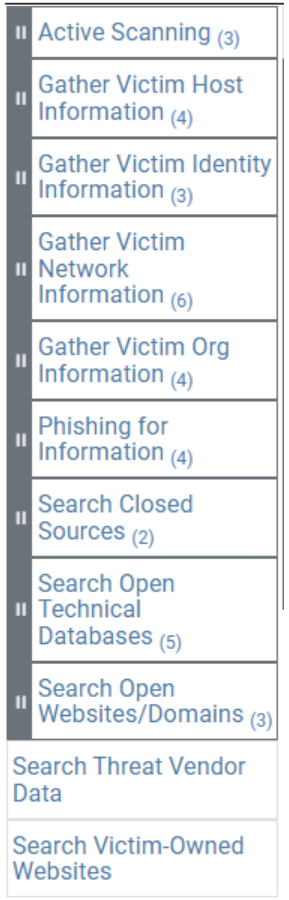
Konfiguracijske datoteke, koda, skripte.

TEHNIKE IN AKTIVNOSTI IZVIDOVANJA

Začetno pasivno in aktivno izvidovanje (Reconnaissaince)

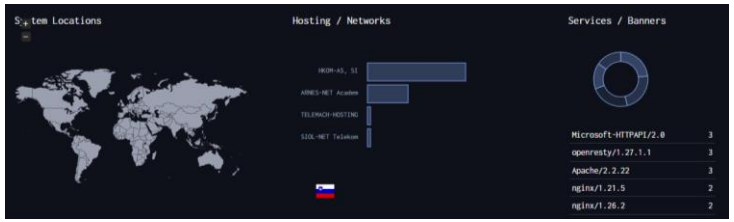
Pogosto prvi korak pred izvedbo ciljanega napada

- Odprta (OSINT) orodja in viri informacij (Maltego, theHarvester, Shodan, Censys), analiza javnih spletnih strani, družbenih omrežij, uporaba naprednih funkcij iskalnikov.
- Analiza DNS in WHOIS zapisov z Amass, Sublist3r, DNSDumpster
- Aktivno tehnično izvidovanje z Nmap, Masscan, WhatWeb, Nitko, BurpSuite
- Izvidovanje za socialni inženiring z Hunter.io, Recon-ng
- Pridobivanje podatkov iz temnega spleta

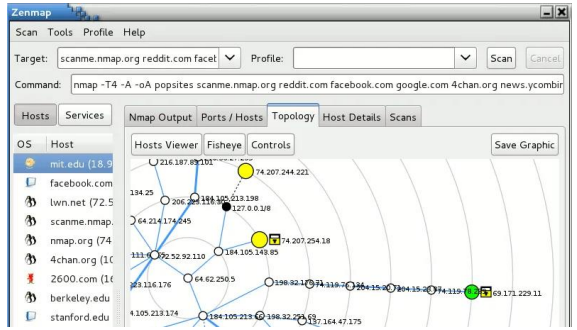


MITRE ATT&CK ima registriranih 11 tehnik izvidovanja v fazi Reconnaissance.
https://attack.mitre.org/tactics/TA0043/

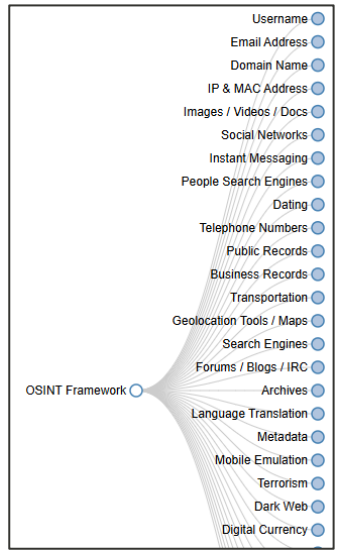
Shodan Internet skener.



DNS skener.



NMAP/ZENMAP omrežni skener.



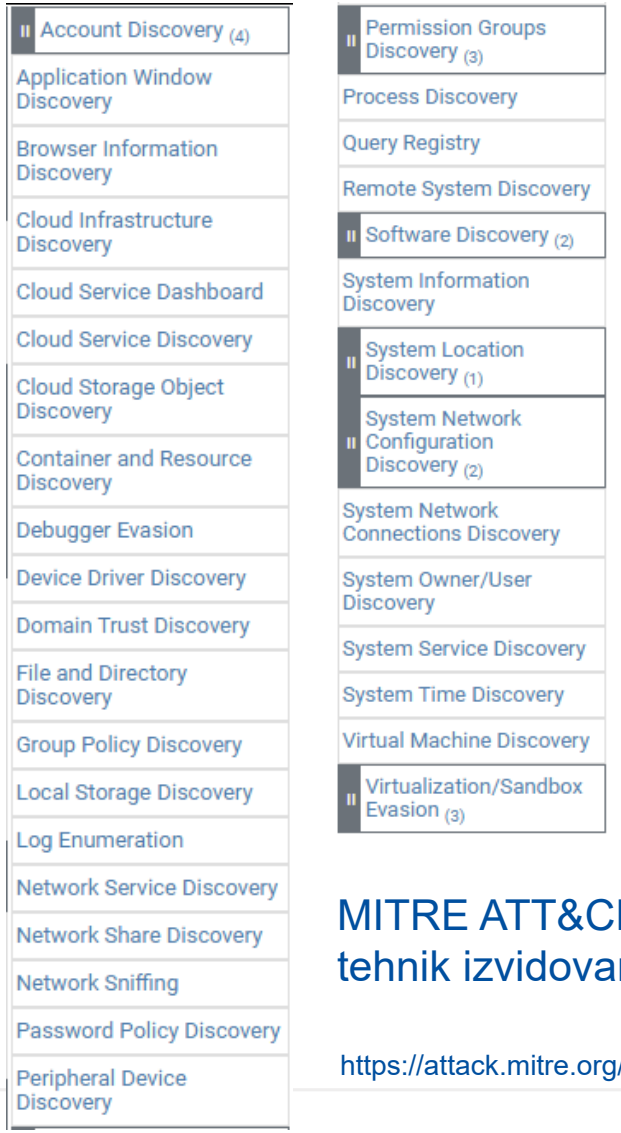
OSINT framework

TEHNIKE IN AKTIVNOSTI IZVIDOVANJA

Izvidovanje po začetni kompromitaciji (Discovery)

Predvideva se, da je napadalec že pridobil začetni dostop

- Začetni dostop pridobljen preko phishinga, ranljivosti ali ukradenih poverilnic.
- Izvidovanje znotraj omrežja, zbiranje tehničnih informacij, uporablja se večinoma legitimna orodja in se tako izogibajo zaznavam.
- Zbiranje informacij o identitetah in pravicah še posebej privilegiranih uporabnikih.
- Iskanje podatkov in sistemskih ciljev za izvedbo končnih akcij.



Pogosta hekerska orodja

BLOODHOUND
PowerShell + LOLBins
Seatbelt
SharpUp
SharpView
WinPEAS
ADRecon
PingCastle
SharpAppLocker
SharpShares
AzureHound

MITRE ATT&CK ima registriranih 34 tehnik izvidovanja v fazi Discovery

https://attack.mitre.org/tactics/TA0007/

ZAZNAVANJE IN PREPREČEVANJE IZVIDOVANJA

Zaznavanje in preprečevanje izvidovanja je učinkovita obrambna strategija, s katero zaznamo namero napada in se nanj lahko pripravimo, če do začetne kompromitacije že pride, pa to hitro zaznamo in zaustavimo.

Preprečevanje in omejevanje izvidovanja

Zmanjševanje napadne površine

- Zapiranje nepotrebnih storitev, vrat, administrativnih dostopov.
- Odstranitev starih domen in DNS zapisov.
- Skrivanje nepotrebnih informacij, verzije OS, aplikacij.

Upravljanje identitet in pravic

- Načelo najmanjših pravic, ločevanje administrativnih računov
- Omejitev LDAP poizvedb
- MFA za vse dostope, PAM za privilegirane račune.

Omrežna segmentacija

- Ločevanje, uporabniških, strežniških in administrativnih con v omrežju
- Preprečevanje nepotrebne komunikacije med segmenti in sistemi

Vabe in zavajanje napadalcev

- Uporaba vab (Deception) za zaznavanje aktivnosti napadalcev.

Uporaba kibernetske obveščevalne dejavnosti (CTI)

- Preverjanje obstoja ukradenih poverilnic, dokumentov in drugih podatkov na temnem spletu.
- Preverjanje aktivnosti ki vključujejo podatke naše organizacije in lahko kažejo na pripravo napada.
- Preverjanje dejavnosti hekerskih skupin, ki napadajo organizacije našega tipa in kakšne tehnike in orodja uporabljajo.

HVALA

+111 123 456 789

info@enisa.europa.eu