Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné testovanie a ofenzívne zručnosti

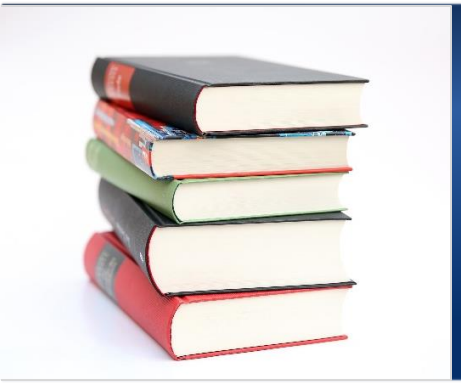
Zvyšovanie povedomia o KB a testovanie bezpečnosti (Blok VIII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Obsah

- Základné pojmy, ciele a význam penetračného testovania
- Prehľad najpoužívanejších metodík a rámcov
- Predstavenie nástrojov používaných pri ofenzívnych ativitách
- Úvod do ATT&CK taktík a techník
- Certfikácie a ďalšie vzdelávanie v oblasti ofenzívnej bezpečnosti

Úvod do témy a základné pojmy

Ofenzívna bezpečnosť

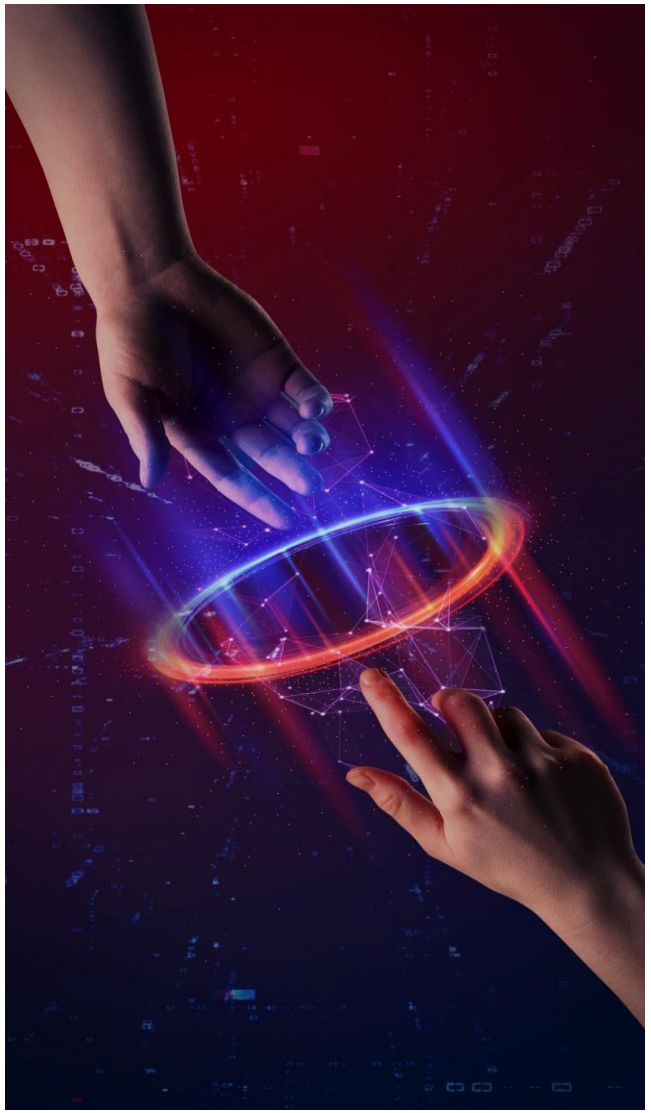
- **Ofenzívna bezpečnosť (offensive security)** je súbor aktivít, ktoré aktívne hľadajú slabé miesta v systémoch, aplikáciách a infraštruktúre skôr, než ich zneužije útočník.
- Nejde len o to **„hacknúť systém“** — cieľom je pochopiť, ako by to urobil skutočný útočník, a poskytnúť organizácii odporúčania, ako útokom predísť.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Čo všetko môže ofenzíva zahŕňať?

Nie je to len klasický pentest. Ofenzívne aktivity majú omnoho širší záber:

- **Penetration testing** (web, infra, mobil, cloud, VoIP…)
- **Red teaming** – simulácia reálnej kampane útočníka
- **Purple teaming** – spolupráca s obranným tímom na zlepšení detekcie
- **Výskum zraniteľností a exploit development**
- **Sociálne inžinierstvo a phishingové kampane**
- **Fyzické testovanie a bypass bezpečnostných kontrol**
- **OSINT, recon a profilovanie cieľa**
- **Adversary emulation** podľa konkrétnych APT skupín
- **Testovanie konfigurácií a hardeningu**
- **Vývoj nástrojov pre ofenzívu (C2, payloady, automatizácia)**



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Čo je bezpečnostné testovanie

- Systematické preverovanie odolnosti systémov
- Cieľ: nájsť a odhaliť zraniteľnosti
- Súčasť riadenia kybernetickej bezpečnosti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ciele testovania

- Overenie úrovne ochrany systémov
- Identifikácia rizík a slabých miest
- Overenie reakcie bezpečnostných tímov
- Zlepšenie bezpečnostných procesov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prečo je bezpečnostné testovanie dôležité

- Identifikácia zraniteľností
  - Odhaľuje zraniteľnosti skôr ako ich zneužijú útočníci
- Prevencia kybernetických útokov
  - Pomáha predchádzať napadnutiu systémov a služieb
- Zabezpečenie dát
  - Chráni dôvernosť, integritu a dostupnosť informácií
- Dodržiavanie noriem
  - Zabezpečuje súlad s požiadavkami ako GDPR či ISO 27001
- Zlepšenie opatrení
  - Prináša odporúčania na posilnenie bezpečnostných procesov
- Ochrana reputácie
  - Predchádza poškodeniu mena organizácie pri incidente

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

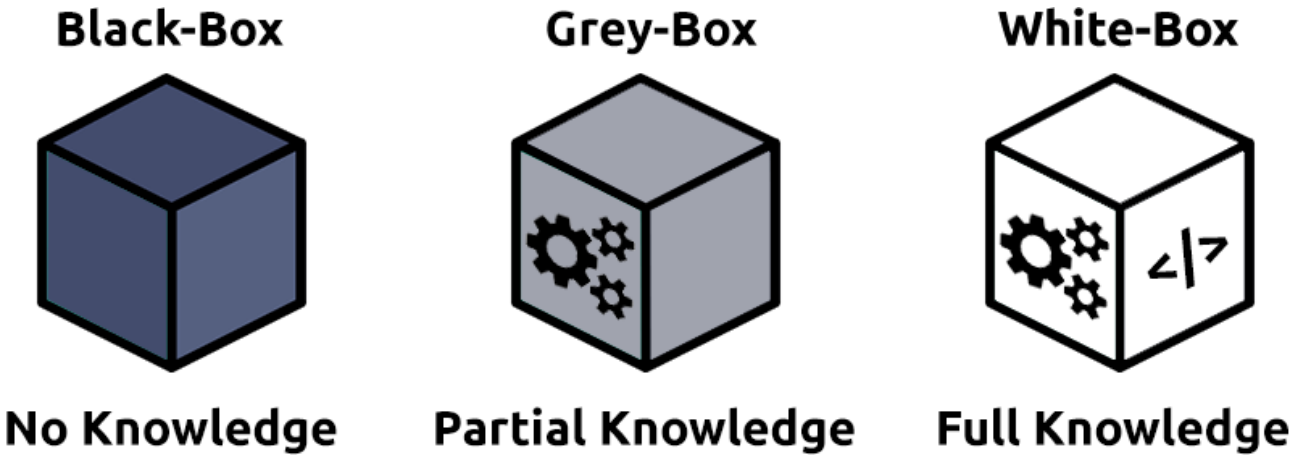
Etické a právne aspekty

- Etické zásady
  - Súhlas a zodpovednosť
    - Testovať len so súhlasom majiteľa
  - Dôvernosť
    - Zachovať mlčanlivosť
  - Zodpovedné zverejnenie
    - Hlásiť zraniteľnosti iba oprávneným osobám
  - Obmedzenie škôd
    - Cieľom je ochrana, nie útok
- Právne zásady
  - Písomná zmluva
    - Určuje rozsah a obmedzenia testu
  - Využívanie zraniteľností
    - Len podľa dohodnutého scenára
  - Dodržiavanie zákonov
    - Rešpektovanie legislatívy
  - Zodpovednosť
    - Prekročenie rozsahu = právne dôsledky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

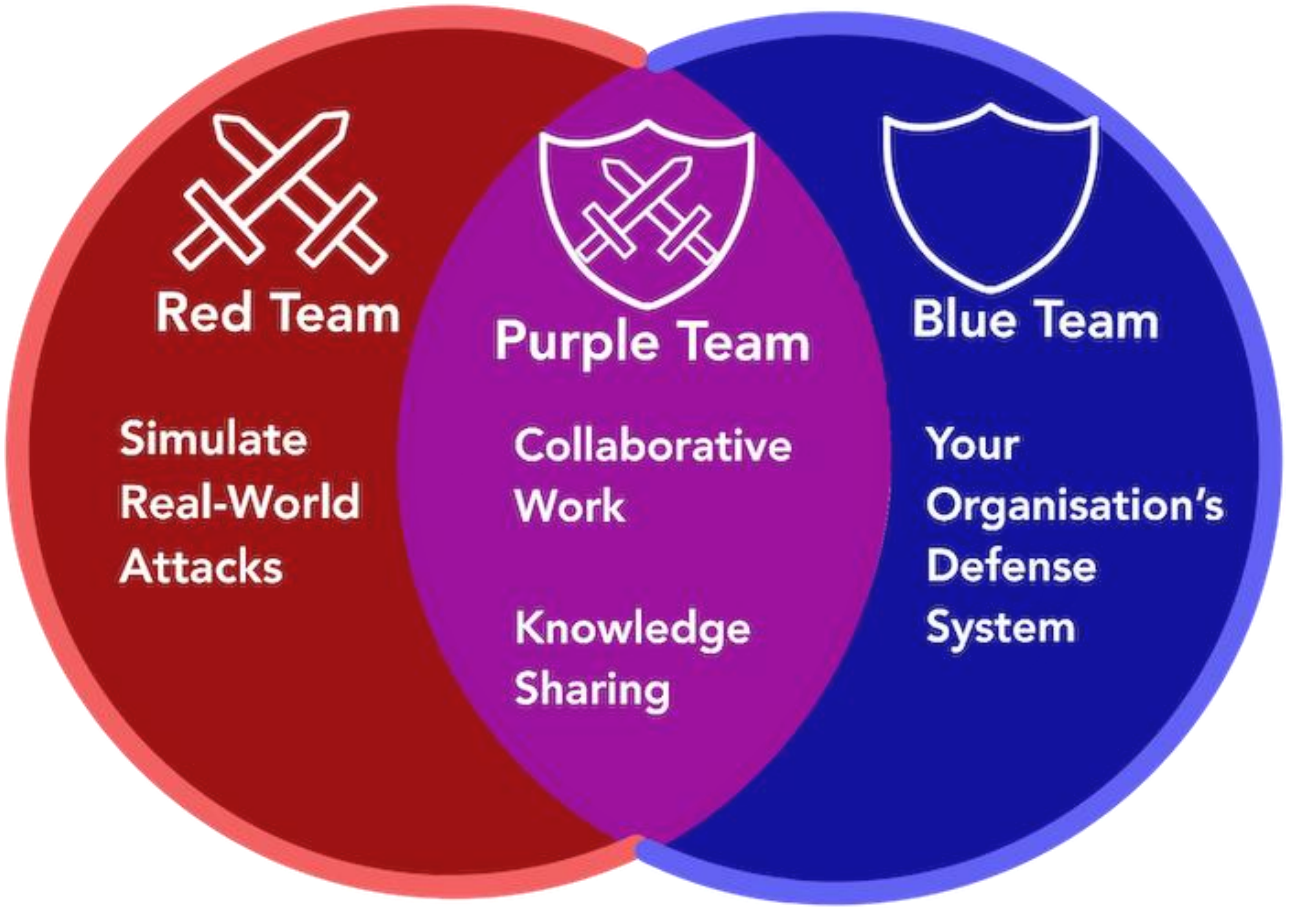
Typy testovania

- Podľa prístupu k informáciám
  - Black Box
    - Tester nemá informácie o systéme
  - White Box
    - Tester má prístup k dokumentácii a kódu
  - Grey Box
    - Tester má čiastočné informácie
- Podľa oblasti testovania
  - Externé testovanie
    - Simulácia útoku zvonku
  - Interné testovanie
    - Simulácia útoku zvnútra organizácie
  - Testovanie aplikácií
    - Hľadanie zraniteľností v aplikáciách
  - Fyzické testovanie
    - Kontrola fyzického zabezpečenia



Tímy v testovaní

- Red team
  - Útočníci (testujú)
- Blue team
  - Obrancovia (monitorujú)
- Purple team
  - Spolupráca oboch



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zhrnutie

- Testovanie = prevencia, nie útok
  - Cieľom je chrániť systémy, dáta a reputáciu
- Kľúčová oblasť bezpečnostného cyklu
  - Identifikácia zraniteľností, prevencia rizík, zlepšovanie opatrení
- Etické a právne zásady
  - Testovať so súhlasom, zachovať dôvernosť, dodržiavať zákony
- Typy testovania
  - Podľa prístupu k informáciám
    - Black Box / White Box / Grey Box
  - Podľa oblasti
    - Externé, interné, aplikácie, fyzické zabezpečenie
- Hlavné ciele
  - Overiť ochranu, identifikovať riziká, otestovať reakcie tímov, zlepšiť procesy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Proces penetračného testovania

Proces penetračného testovania

Fázy testu

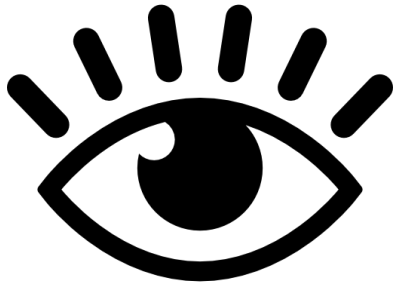
1. Príprava
2. Zber informácií
3. Skenovanie a enumerácia
4. Vyhodnotenie zraniteľností
5. Využitie zraniteľností (Exploitation)
6. Post-exploitation
7. Reporting
8. Náprava a následné opatrenia

Proces penetračného testovania

1. Príprava a dohoda

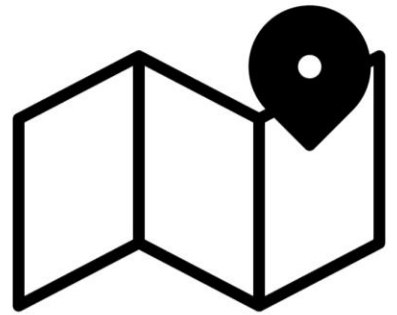
- Definovanie pravidiel testu
- Schválenie zo strany vedenia
- Stanovenie cieľov testovania
- Vybudovanie základov pre úspešný penetračný test
- Bez vykonávania konkrétnych testov

2. Prieskum (Reconnaissance)



- Zber základných informácií o organizácii a štruktúre
- Pasívny
  - Whois, Shodan, Google Dorking
- Aktívny
  - Nmap, ping sweep
- Cieľ: Pochopiť rozsah a povrch útoku
- Príklady: sociálne siete, webstránky, DNS

3. Enumerácia (Enumeration)



- Detailnejšie zisťovanie aktívnych systémov a účtov
- Cieľ: **detailný technický zoznam** dostupných služieb, účtov, portov, verzií, konfigurácií a ďalších komponentov.
- **Typické činnosti:**
  - enumerácia portov (Nmap)
  - enumerácia služieb a verzií (banner grabbing)
  - enumerácia používateľov (SMB, LDAP, SSH)
  - enumerácia zdieľaných priečinkov, domén, DNS zón
  - enumerácia webových endpointov (Dirbuster, FFUF)
  - zistenie OS, konfigurácií, protokolov, pluginov
- **Výsledok:**
  - **Zoznam aktív, služieb a technických detailov** → "čo všetko je dostupné?".

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

4. Hodnotenie zraniteľností (Vulnerability Assessment)

- fáza, v ktorej sa identifikujú, analyzujú a hodnotia zraniteľnosti nájdené počas zberu informácií a enumerácie.
- Cieľ: **zistiť, ktoré slabiny existujú**, aká je ich **kritickosť** a aký majú **dopad** na systém – a to ešte pred pokusom o ich zneužitie (exploitation).
- Zahŕňa:
  - **Identifikáciu zraniteľností**
    - využitie automatizovaných skenerov (Nessus, OpenVAS, Qualys)
    - manuálne overovanie slabín zistených počas enumerácie
  - **Koreláciu a overenie nálezov**
    - odstránenie false positives
    - konsolidácia nálezov z viacerých zdrojov
  - **Analýzu rizika** (Risk Rating)
    - CVSS score
    - exploitability (ako ľahko sa dá využiť)
    - dopad (confidentiality, integrity, availability)
  - **Prioritizáciu**
    - triedenie zraniteľností podľa rizika a pravdepodobnosti zneužitia

5. Využitie zraniteľností (Exploitation)

- Fáza, kde tester aktívne využíva identifikované zraniteľnosti
- Cieľ: preukázať reálne riziko a možný prístup útočníka k systémom
- Techniky: sociálne inžinierstvo, útoky na heslá, zneužitie známych softvérových chýb

6. Post-exploitation

- Fáza po úspešnom preniknutí do systému
- Tester skúma dopad zraniteľností
- Kľúčové aktivity:
  - Laterálny pohyb
  - Eskalácia oprávnení
  - Zber citlivých dát
  - Udržanie prístupu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

7. Reporting

- Dokumentovanie zraniteľností, rizík, ktoréprinášajú a odporúčania na nápravu
- Obsahuje:
  - Zhrnutie nájdených problémov
  - Popis zraniteľností a ich dopadu
  - Hodnotenie rizík a závažnosti
  - Konkrétne odporúčania na nápravu
- Použitie:
  - Podklad pre tím zodpovedný za nápravu
  - Udržiavanie informácií o bezpečnosti
  - Pomoc pri ďalšej analýze rizík

8. Náprava a následné opatrenia

- Implementácia opráv a odporúčaní z penetračného testu
- Zabezpečenie odstránenia zraniteľností
- Proces nápravy:
  - Implementácia opráv
  - Posilnenie bezpečnostných politík
  - Opätovné testovanie
- Prečo je to dôležité:
  - Znižuje riziko útokov
  - Chráni dôverné dáta
  - Pomáha splniť bezpečnostné regulácie
  - Posilňuje dôveru zákazníkov a partnerov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typické chyby pri testovaní

- Test bez súhlasu
- Zasahovanie do produkcie
- Nesprávne vyhodnotenie nálezov
- Slabý reporting

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Úloha penetračného testera

- Simuluje reálne kybernetické útoky, aby odhalil a otestoval zraniteľnosti IT systémov skôr, než ich zneužijú útočníci
- Kľúčové činnosti
  - Prieskum
  - Analýza
  - Exploitácia
  - Hodnotenie rizík
  - Odporúčanie a report
- Potrebné zručnosti
  - Znalosť sietí, OS, infraštruktúry
  - Programovanie
  - Aktuálne trendy v kybernetickej bezpečnosti
  - Etický a legálny prístup pri testovaní

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

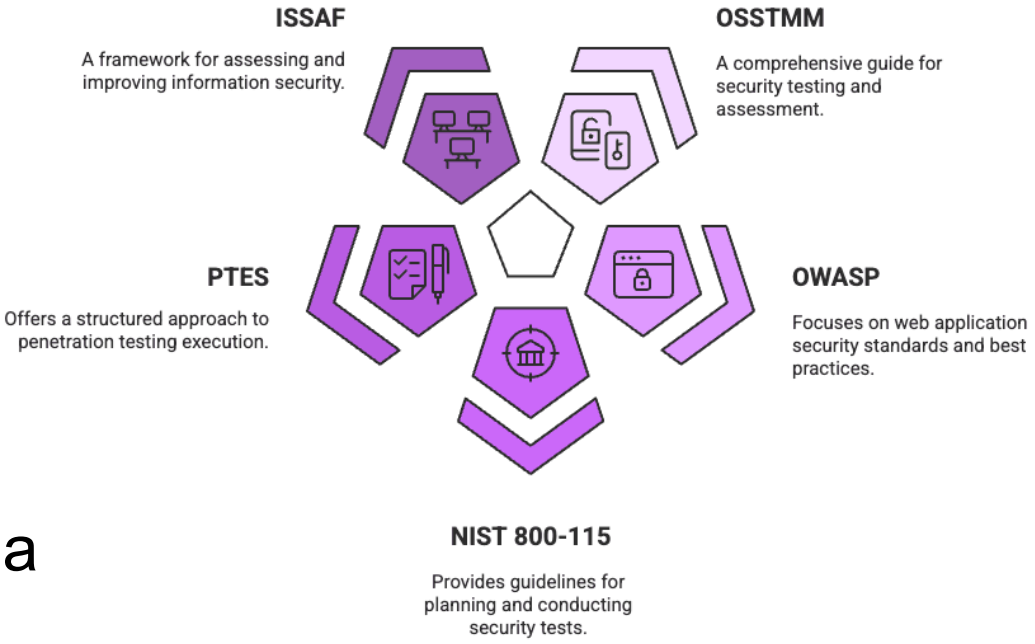
Metodiky a rámce penetračného testovania

Metodika

- Zabezpečuje konzistentnosť testov
- Umožňuje porovnateľné výsledky
- Zvyšuje dôveryhodnosť testovania
- Podklad pre reporting a audit

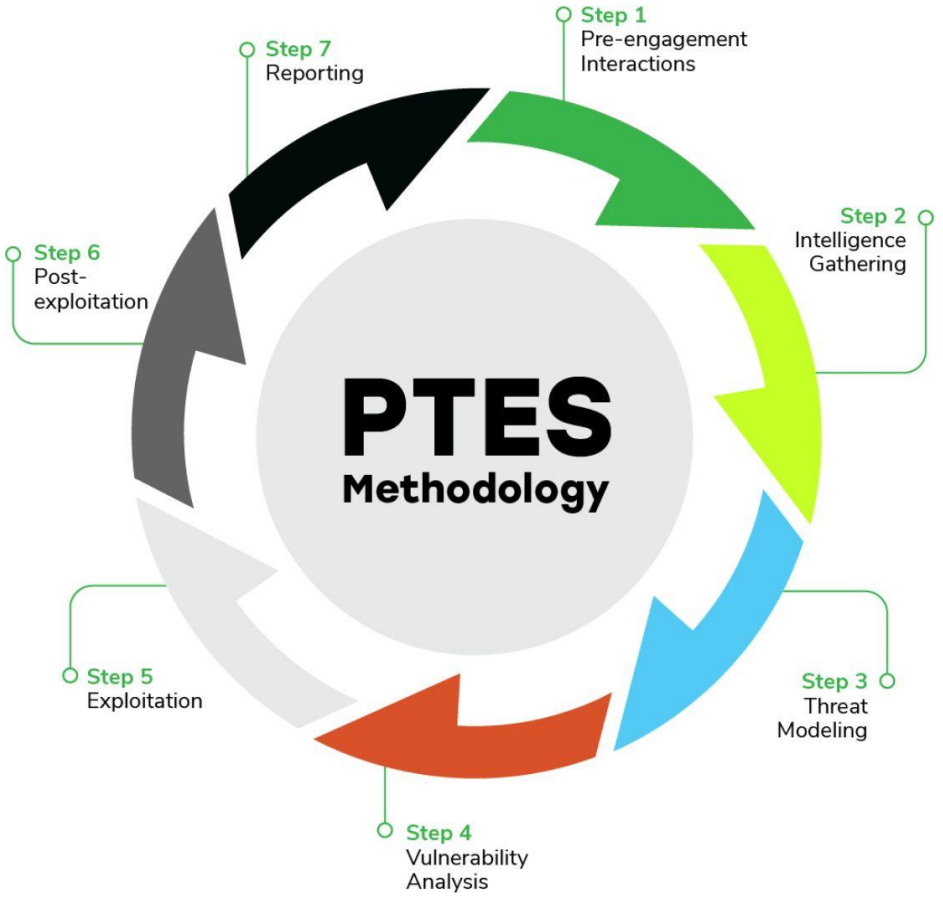
Bežné metodiky a štandardy penetračného testovania

- PTES - Štandard vykonávania penetračných testov
- PCI-DSS – Bezpečnosť v platobnom sektore (karty)
- OSSTMM – Metodika testovania (open-source)
- OWASP – Príručka testovania webovej bezpečnosti
- NIST SP 800-115 – Praktické usmernenia NIST pre testy
- ISSAF – Rámec hodnotenia bezpečnosti



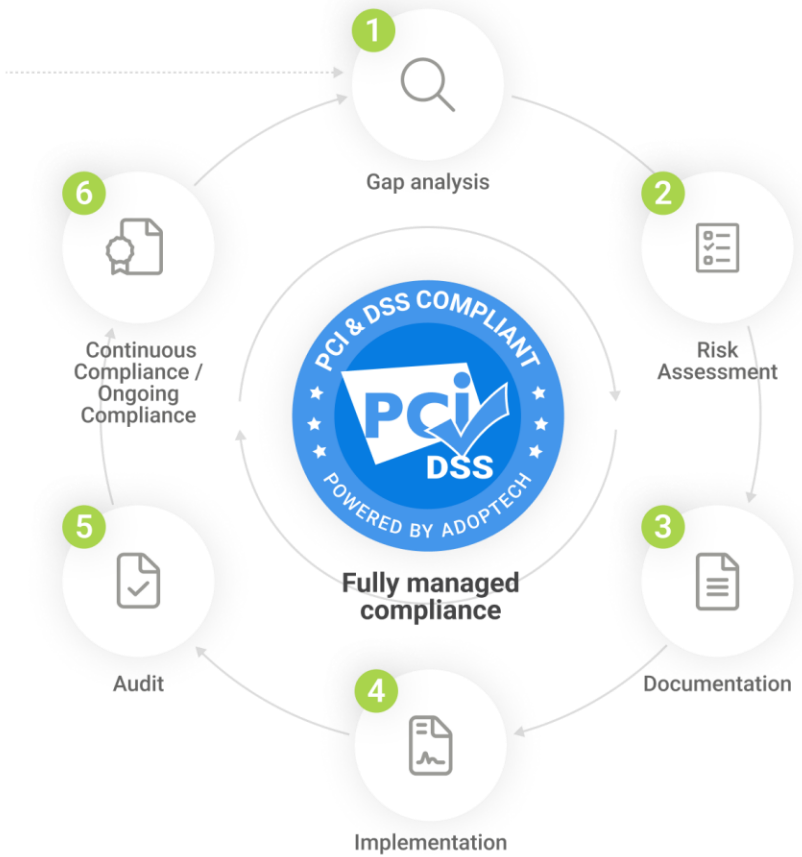
PTES

- Rámec pre celý proces penetračného testu – od dohody až po report
- 7 hlavných fáz:
  - Pred začatím
  - Zber informácií
  - Modelovanie hrozieb
  - Analýza zraniteľností
  - Vykonanie útoku
  - Post-exploitačná fáza
  - Reportovanie



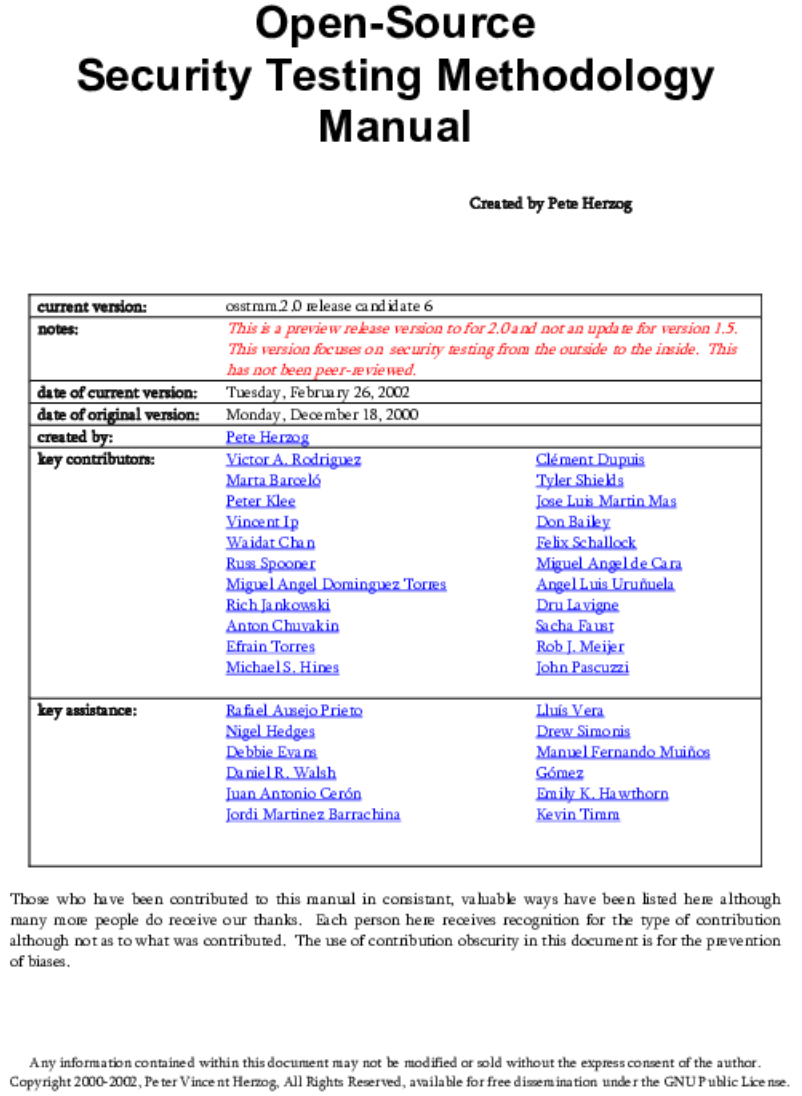
PCI-DSS

- Globálne fórum, ktoré vytvára a rozvíja bezpečnostné štandardy na ochranu platobných údajov
- Cieľom je zlepšiť bezpečnosť platobných dát po celom svete
- Ako zabezpečuje platby:
  - Správa globálnych bezpečnostných štandardov pre platby
  - Validácia a zverejňovanie produktov spĺňajúcich PCI štandardy
  - Školenie a certifikácia odborníkov a organizácií
  - Poskytovanie bezplatných odporúčaní a zdrojov pre bezpečné platby
  - Vyžaduje vykonávanie bezpečnostného testovania



OSSTMM

- Vyvíjané a spravované organizáciou ISECOM (Institute for Security and Open Methodologies)
- Rámec určený pre bezpečnostné audity podľa regulačných a priemyselných požiadaviek
- Slúži ako základ pre tvorbu vlastnej metodiky prispôsobenej konkrétnym normám a reguláciám
- Päť bezpečnostných oblastí:
  - Ľudská bezpečnosť
  - Fyzická bezpečnosť
  - Bezdrôtová bezpečnosť
  - Bezpečnosť telekomunikácií
  - Bezpečnosť dátových sietí



Open-Source
Security Testing Methodology
Manual

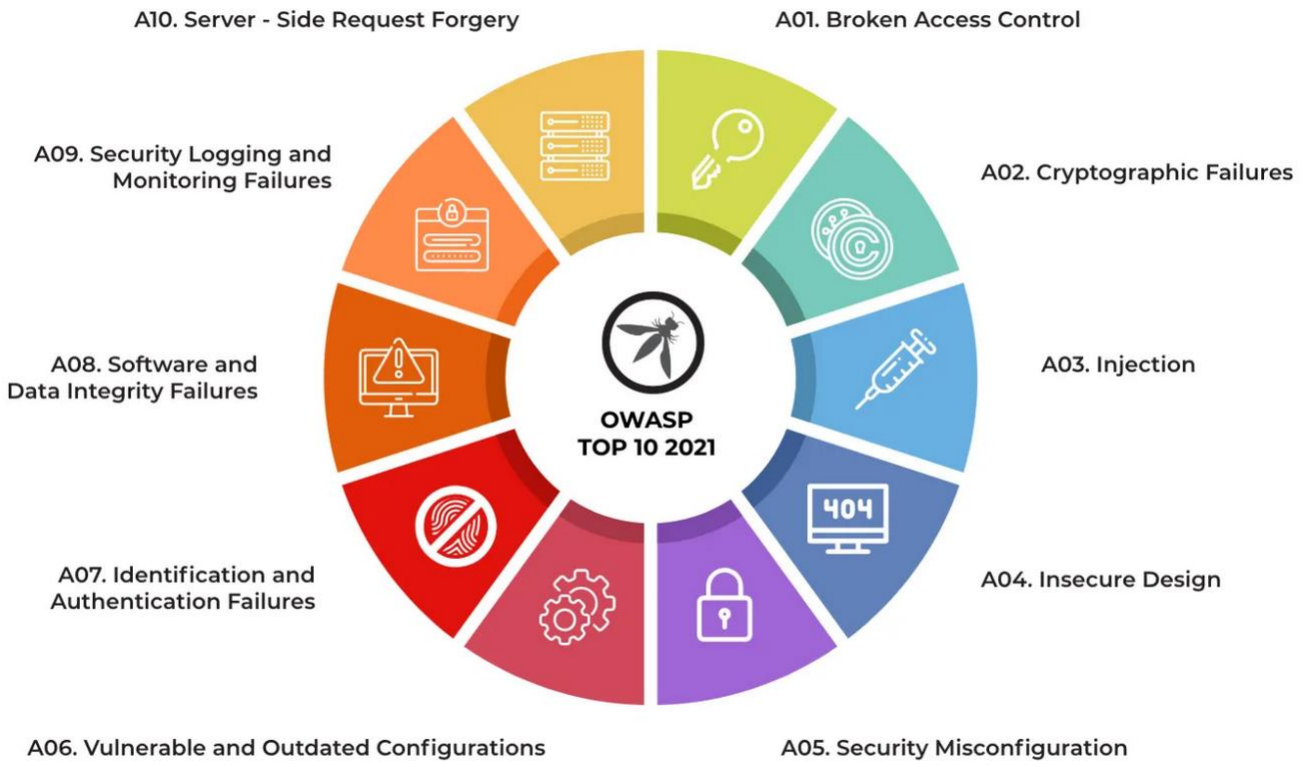
Created by Pete Herzog

current version:	osstmm.2.0 release candidate 6	
notes:	*This is a preview release version to for 2.0 and not an update for version 1.5. This version focuses on security testing from the outside to the inside. This has not been peer-reviewed.*	
date of current version:	Tuesday, February 26, 2002	
date of original version:	Monday, December 18, 2000	
created by:	Pete Herzog	
key contributors:	Victor A. Rodriguez Marta Barceló Peter Klee Vincent Ip Waidat Chan Russ Spooner Miguel Angel Dominguez Torres Rich Jankowski Anton Chuvakin Efrain Torres Michael S. Hines	Clément Dupuis Tyler Shields Jose Luis Martin Mas Don Bailey Felix Schallock Miguel Angel de Cara Angel Luis Uruñuela Dru Lavigne Sacha Faust Rob J. Meijer John Pascuzzi
key assistance:	Rafael Ausejo Prieto Nigel Hedges Debbie Evans Daniel R. Walsh Juan Antonio Cerón Jordi Martinez Barrachina	Lluís Vera Drew Simonis Manuel Fernando Muiños Gómez Emily K. Hawthorn Kevin Timm

Those who have been contributed to this manual in consistant, valuable ways have been listed here although many more people do receive our thanks. Each person here receives recognition for the type of contribution although not as to what was contributed. The use of contribution obscurity in this document is for the prevention of biases.

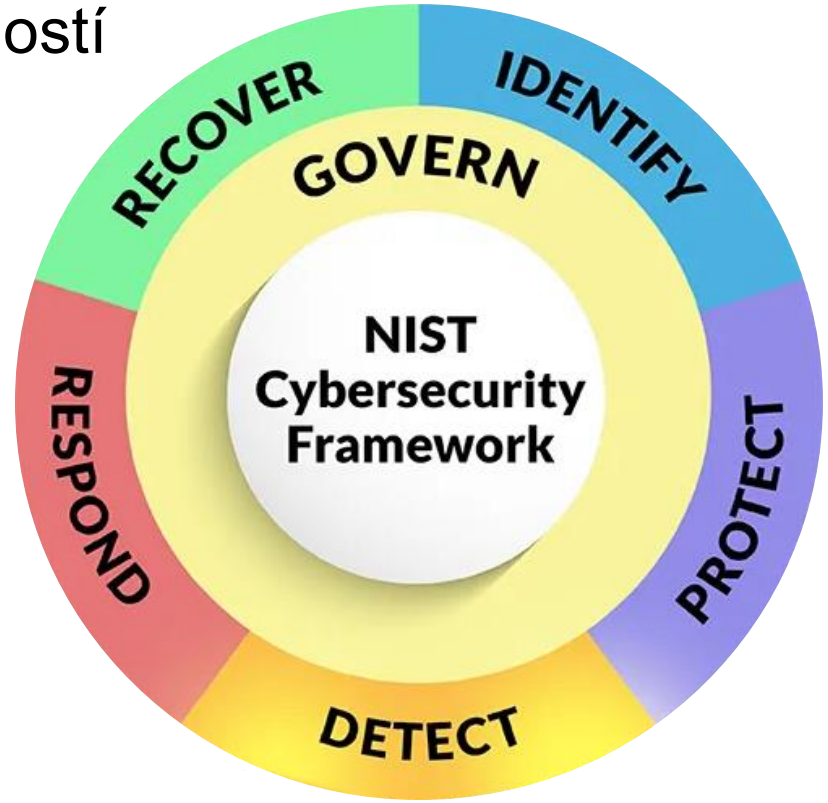
OWASP

- Nezisková organizácia zameraná na zlepšenie bezpečnosti softvéru prostredníctvom otvorenej komunity, vzdelávania a nástrojov
- Základné hodnoty:
  - Otvorenosť
  - Inovácie
  - Globálnosť
  - Integrita



NIST SP 800-115

- Príručka od NIST pre systematické testovanie a hodnotenie bezpečnosti IT systémov
- Cieľ: Odhaľovať a predchádzať zneužitiu zraniteľností
- Techniky:
  - Skenovanie zraniteľností
  - Penetračné testovanie
  - Hodnotenie bezpečnostných kontrol
- Fázy penetračného testovania podľa NIST:
  - Prieskum
  - Identifikácia zraniteľností
  - Využitie zraniteľností
  - Reportovanie nálezov

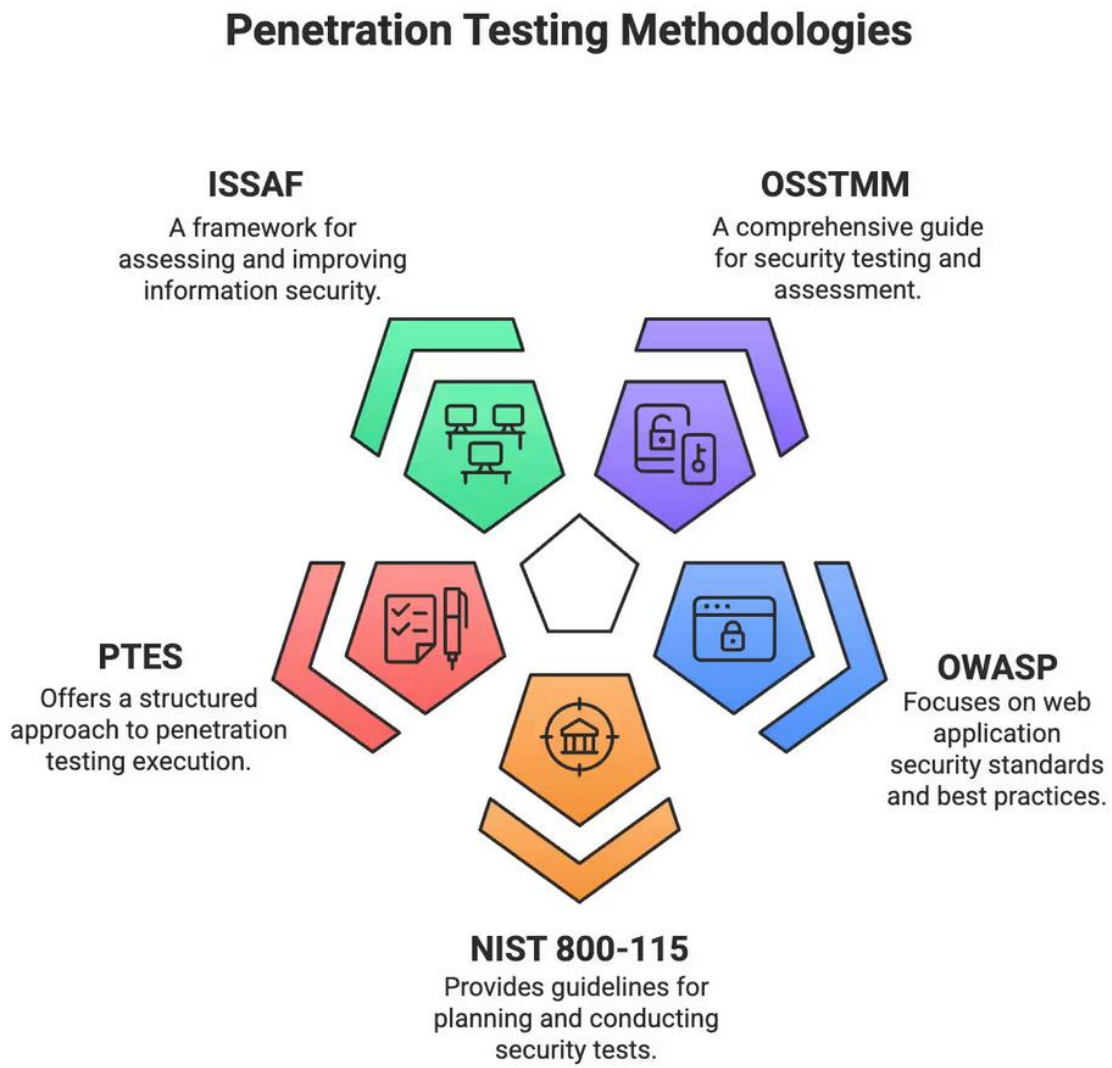


ISSAF

- Metodika a rámec pre penetračné testy a hodnotenie bezpečnosti informačných systémov
- Účel: Poskytnúť štruktúrovaný proces na identifikáciu rizík, zraniteľností a návrh nápravných opatrení
- Hlavné fázy:
  1. Plánovanie a príprava
  2. Hodnotenie
  3. Reportovanie a čistenie artefaktov

Výber vhodnej metodiky

- Neexistuje univerzálna metodika
- Metodika sa vyberá podľa prostredia a cieľa testovania
- Prehľad:
  - OSSTMM – komplexné a merateľné hodnotenie bezpečnosti
  - OWASP – webové aplikácie, API a mobilné aplikácie
  - NIST SP 800-115 verejná správa a regulované prostredie
  - PTES – technicky hlboké penetračné testy
  - ISSAF – holistické hodnotenie vrátane procesov a ľudí

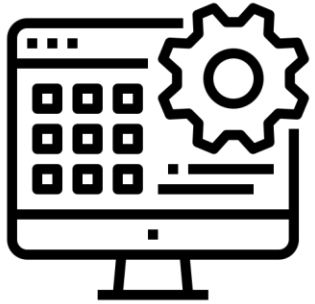


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroje pre ofenzívne bezpečnostné testovanie

Nástroje pre ofenzívne bezpečnostné testovanie

- nástroj = prostriedok
- Prehľad kategórií nástrojov podľa predmetu testu:
  A. aplikačné
  B. infraštruktúrne
  C. simulácia útočníka
- Open-source vs. komerčné
- Automatizácia vs. manuálne použitie



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

A. Aplikačné testovanie

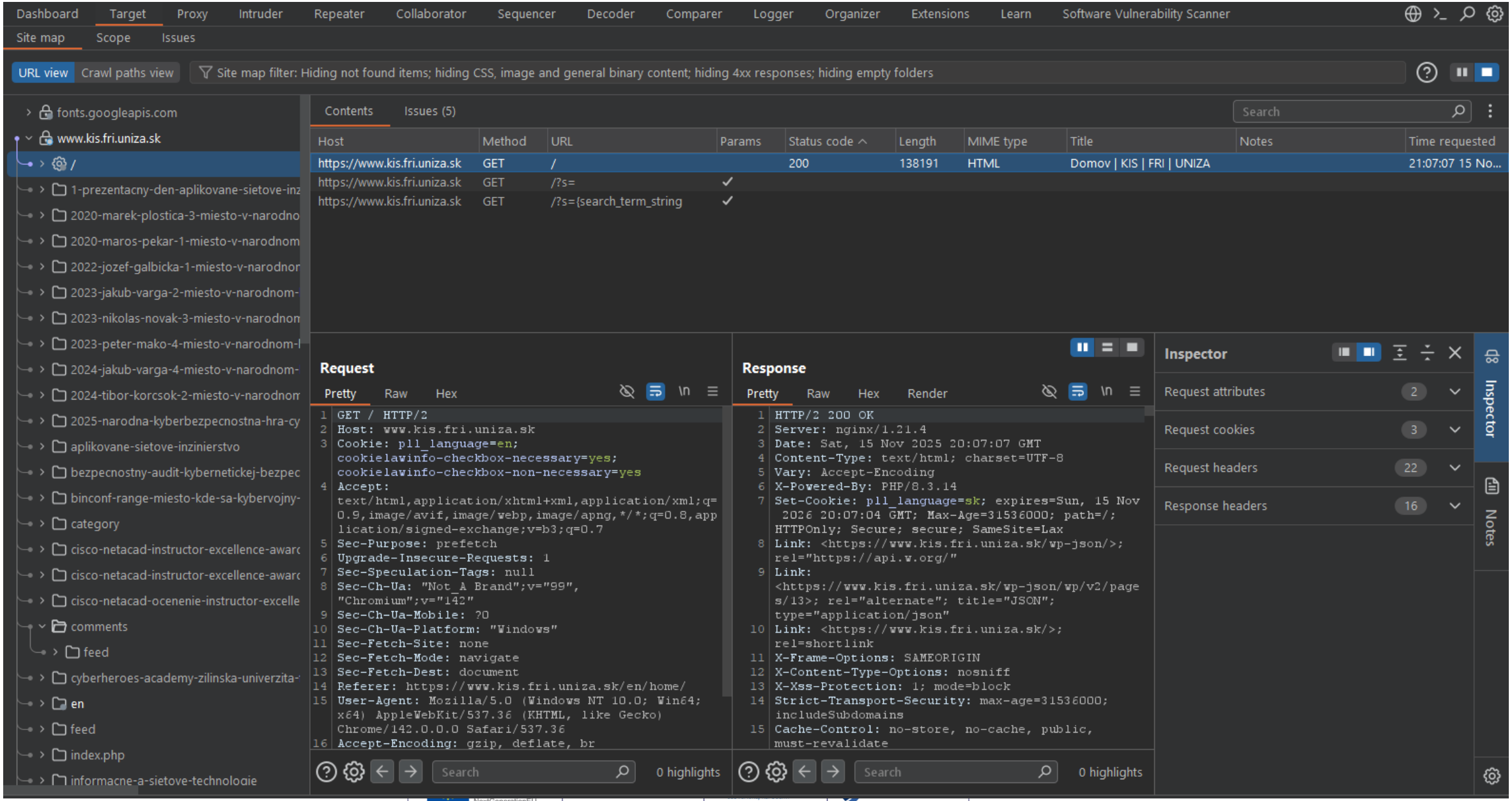
- **A1. Webové aplikácie + API**
  - Burp Suite, OWASP ZAP, Caido, Nuclei, Nikto
- **A2. Mobilné aplikácie**
  - MOBSF, Oversecured, Frida, Ostorlab

A1. Webové aplikácie

- **Burp Suite**
  - Slúži ako Proxy - narábanie s HTTP požiadavkami
  - Mimo základnej funkčnosti obsahuje užitočné moduly ako Repeater a Intruder
  - Rozšíriteľný o moduly (väčšina z nich je v platenej licencii)
  - Obsahuje automatizované skenovanie zraniteľností
  - Vysoko modulárny nástroj (napísaný v jazyku Java)
- **OWASP ZAP**
  - Open-source verzia Burp Suite
  - Má väčšiu funkcionalitu ako community verzia Burp Suite (bezplatná)
  - Menší počet rozšírení písaných komunitou

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Nástroj burp suite, od spoločnosti Portswigger. Zobrazenie hlavného menu s URL adresami



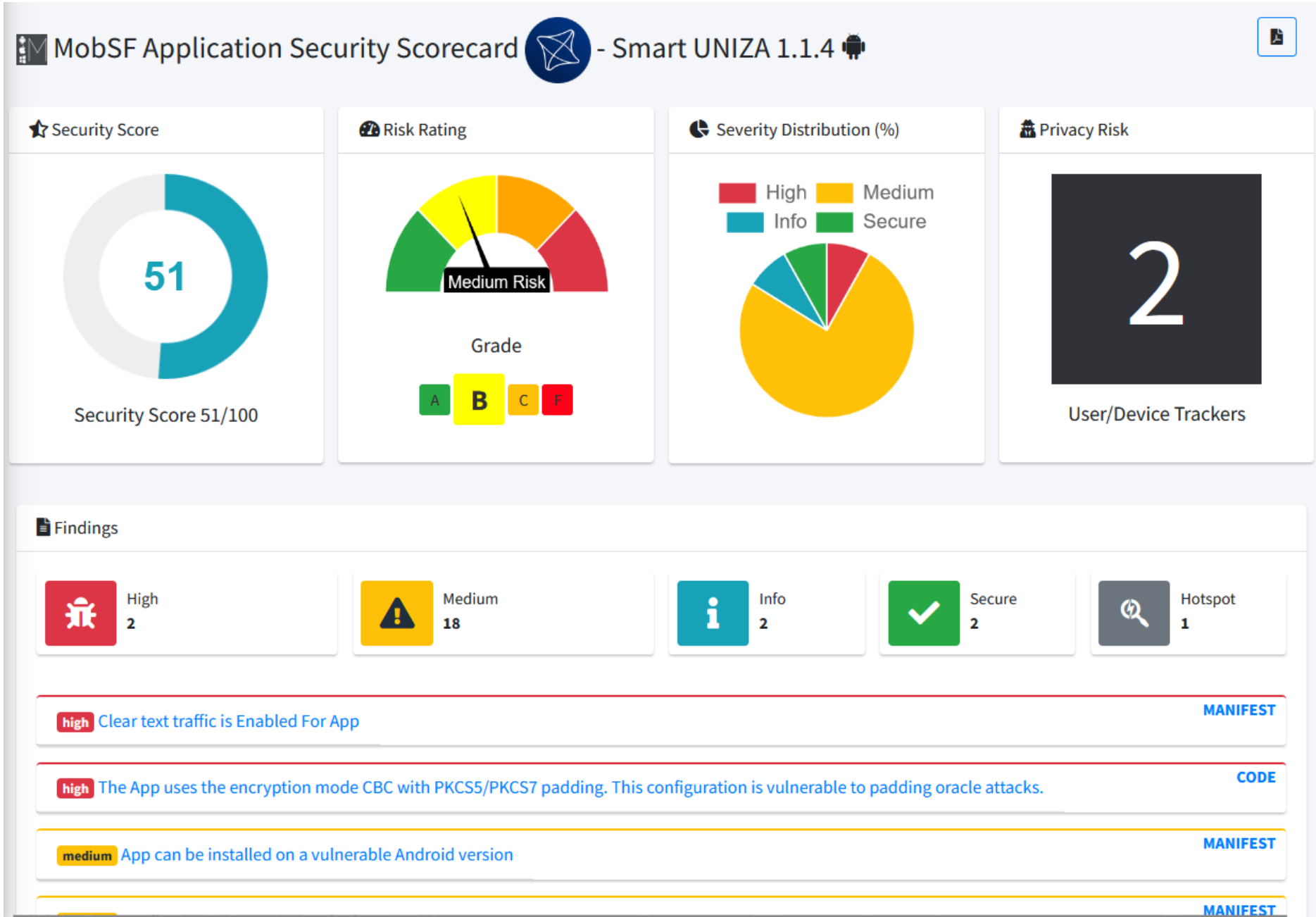
A2. Mobilné aplikácie

- **Mobile Security Framework (MobSF)**
  - Platforma umožnujúca analýzu aplikácií pre OS Android, iOS a Windows Mobile.
  - Statická analýza (SAST) podporuje binárne súbory ako APK, IPA, APPX či priamo zdrojový kód aplikácie.
  - Dynamická analýza (DAST) podporuje Android a iOS aplikácie (vrátane analýzy sieťovej prevádzky)
- **Oversecured**
  - Komerčná platforma ktorá kombinuje SAST a DAST skenovanie
  - Podpora pre iOS a Android
  - API integrácie pre Jira a Slack

Odkazy

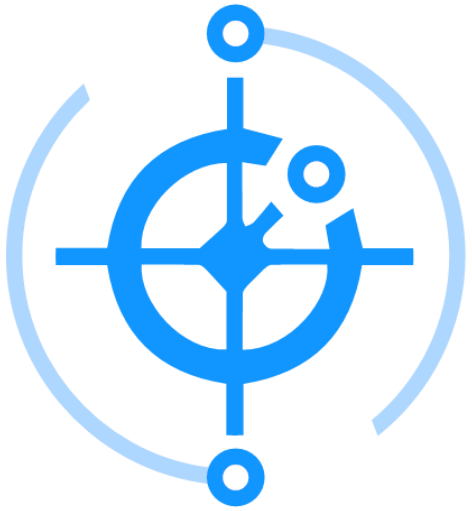
- **Mobile Security Framework (MobSF)**
  - https://mobsf.live/

Nástroj mobsf. Vyhodnotenie mobilnej aplikácie pre Android: Smart UNIZA.



B. Infraštruktúra

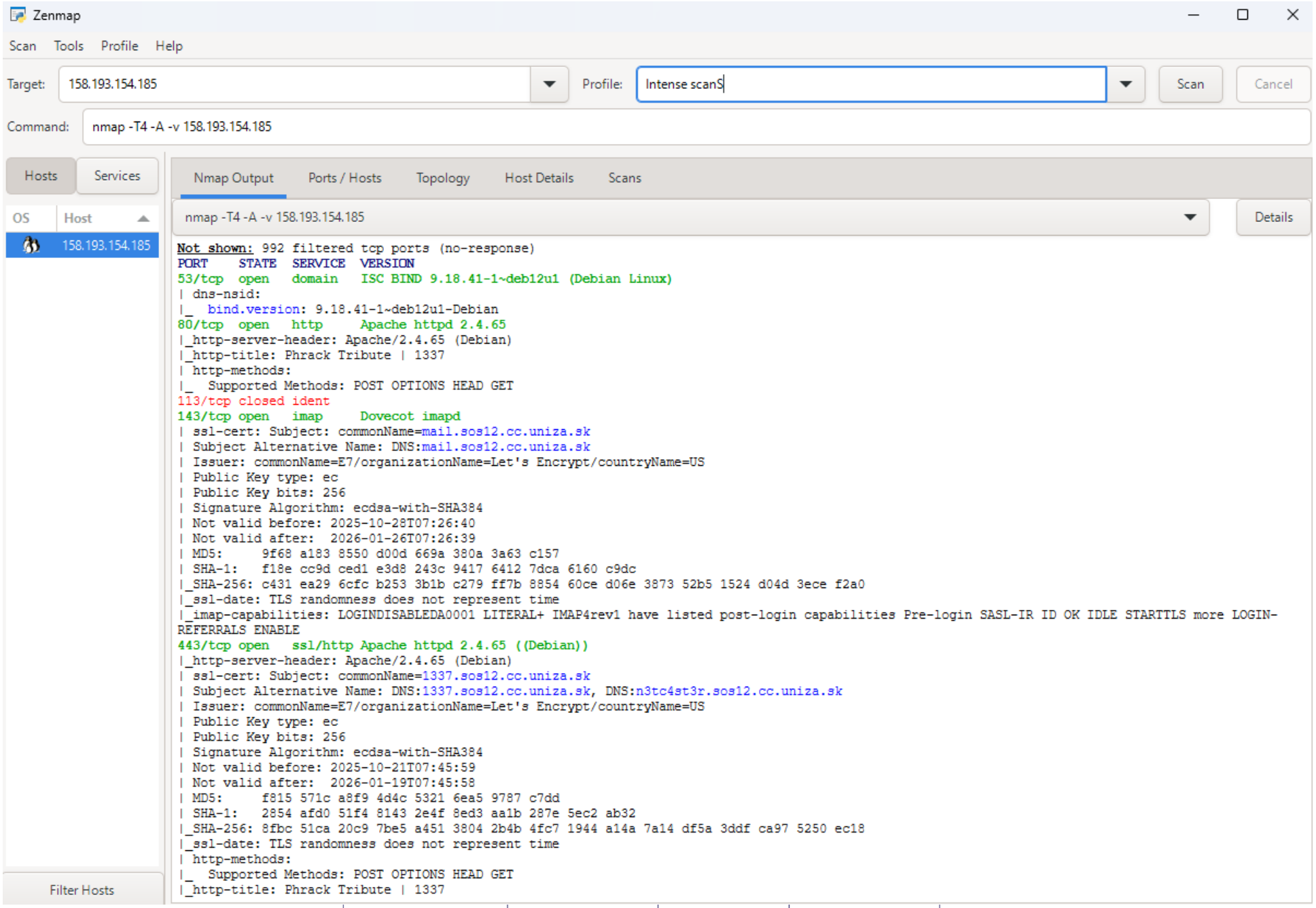
- **B1. Sieťové skenovanie, enumerácia a exploitácia**
  - Masscan, nmap, rustscan
  - Metasploit
- **B2. Active Directory**
  - Bloodhound, CrackMapExec, ADSearch
  - Responder, Rubeus
- **B3. Cloud**
  - ScoutSuite, CloudMapper, Prowler, Pacu



B1. Sieťové skenovanie a enumerácia

- **Masscan**
  - Rýchly skener TCP portov
- **Nmap (Zenmap)**
  - Open-source nástroj na skenovanie siete
  - Konfigurovateľný – obmedzenie rýchlosti skenu, nastavenie skenovacej techniky, obchádzanie firewallu
  - Vykonáva základnú enumeráciu zraniteľností – perl skripty
- **Metasploit**
  - Exploitačná a post-exploitačná platforma
  - Obsahuje verejne dostupné a komunitou vytvorené exploity

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

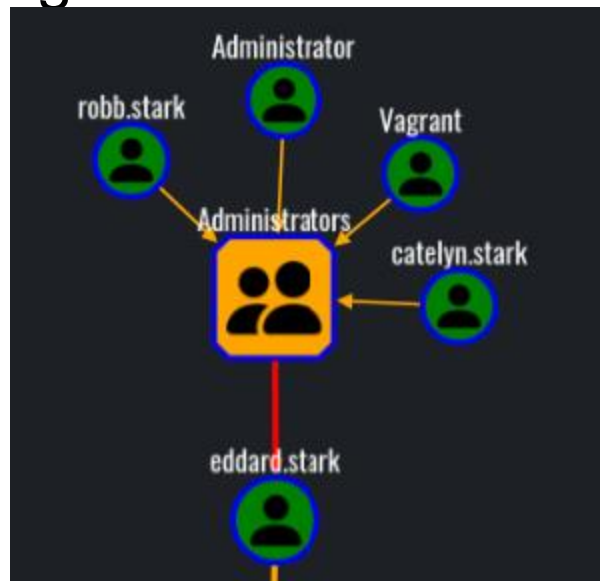

Zenmap
Scan Tools Profile Help
Target: 158.193.154.185
Profile: Intense scanS
Scan
Cancel
Command: nmap -T4 -A -v 158.193.154.185
Hosts
Services
OS
Host
158.193.154.185
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 158.193.154.185
Details
Not shown: 992 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain ISC BIND 9.18.41-1~deb12u1 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.18.41-1~deb12u1-Debian
80/tcp open http Apache httpd 2.4.65
|_http-server-header: Apache/2.4.65 (Debian)
|_http-title: Phrack Tribute | 1337
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
113/tcp closed ident
143/tcp open imap Dovecot imapd
| ssl-cert: Subject: commonName=mail.sos12.cc.uniza.sk
| Subject Alternative Name: DNS:mail.sos12.cc.uniza.sk
| Issuer: commonName=E7/organizationName=Let's Encrypt/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA384
| Not valid before: 2025-10-28T07:26:40
| Not valid after: 2026-01-26T07:26:39
| MD5: 9f68 a183 8550 d00d 669a 380a 3a63 c157
| SHA-1: f18e cc9d ced1 e3d8 243c 9417 6412 7dca 6160 c9dc
|_SHA-256: c431 ea29 6cfc b253 3b1b c279 ff7b 8854 60ce d06e 3873 52b5 1524 d04d 3ece f2a0
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: LOGINDISABLEDA0001 LITERAL+ IMAP4rev1 have listed post-login capabilities Pre-login SASL-IR ID OK IDLE STARTTLS more LOGIN-REFERRALS ENABLE
443/tcp open ssl/http Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
| ssl-cert: Subject: commonName=1337.sos12.cc.uniza.sk
| Subject Alternative Name: DNS:1337.sos12.cc.uniza.sk, DNS:n3tc4st3r.sos12.cc.uniza.sk
| Issuer: commonName=E7/organizationName=Let's Encrypt/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA384
| Not valid before: 2025-10-21T07:45:59
| Not valid after: 2026-01-19T07:45:58
| MD5: f815 571c a8f9 4d4c 5321 6ea5 9787 c7dd
| SHA-1: 2854 afd0 51f4 8143 2e4f 8ed3 aa1b 287e 5ec2 ab32
|_SHA-256: 8fbc 51ca 20c9 7be5 a451 3804 2b4b 4fc7 1944 a14a 7a14 df5a 3ddf ca97 5250 ec18
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-title: Phrack Tribute | 1337

B2. Active Directory

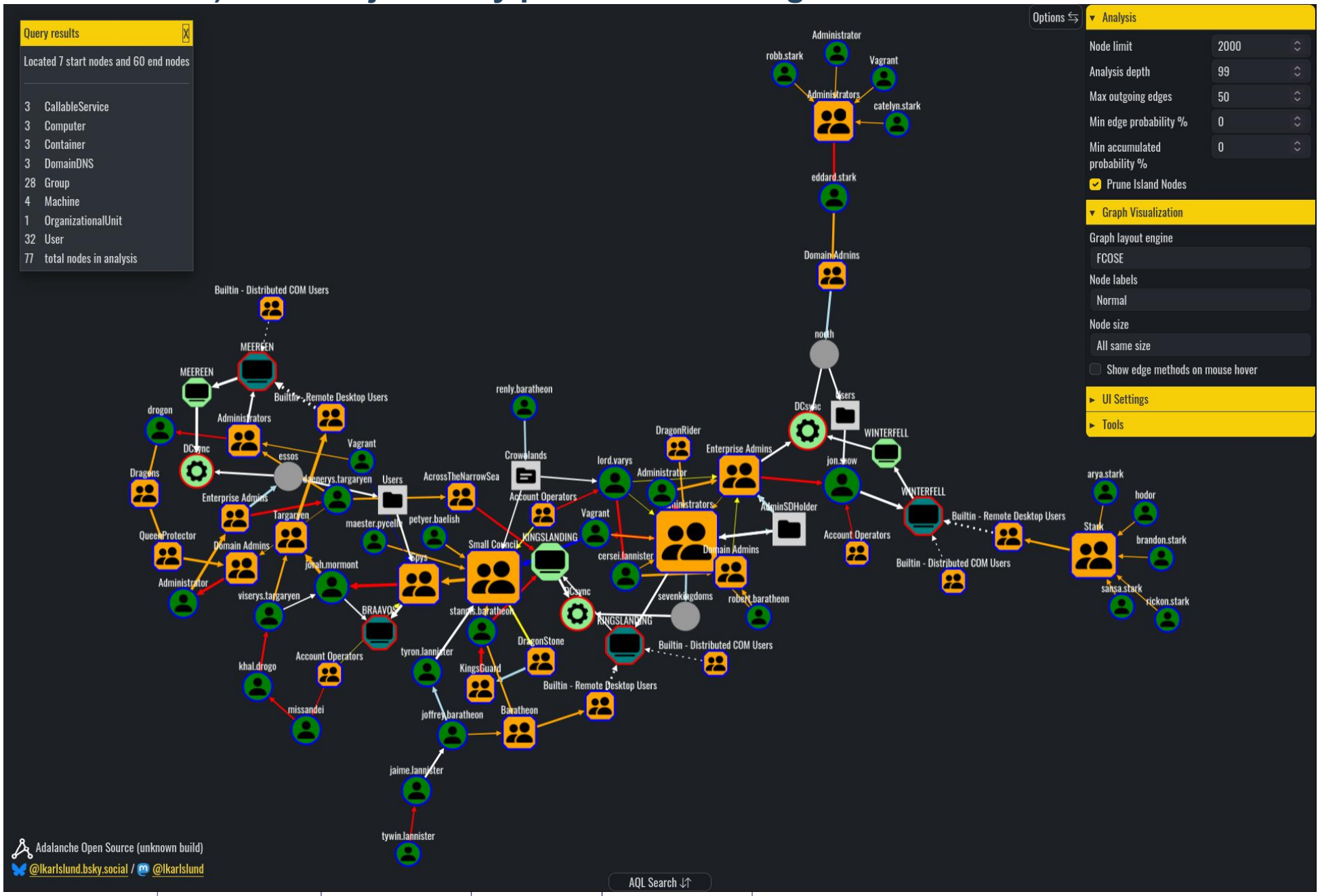
- Active Directory je stále najčastejší cieľ útočníkov a red team cvičení.

Nástroje:

- **Bloodhound & Sharphound**
  - Zber dát z domnénového prostredia
  - Vyhodnotenie útočných ciest a vektorov prostredníctvom grafov
- **Impacket**
  - Zbierka Python skriptov pre komunikáciu so sieťovými protokolmi ako SMB, LDAP, WMI, MSRPC a iné
- **Adalanche**
  - Zobrazenie vzťahov v doméne prostredníctvom grafov
  - Slúži na rýchlu identifikáciu miskonfigurácií



Ukážka z nástroja adalanche, zobrazená je infraštruktúra GOAD (Game of Active Directory – ide o lab pre testovanie zraniteľného AD). Zobrazuje vzťahy prostredníctvom grafov.



B3. Cloud infra

- **Prowler**
  - Auditný nástroj ktorý na základe štandarov dokáže identifikovať nezhody v konfigurácii
  - Podporované prostredia: AWS, Azure, Google Cloud, Kubernetes, M365, Github, Oracle Cloude a mnohé iné
- **ScoutSuite**
  - Open-source nástroj pre audit cloud prostredí
  - Primárna podpora: AWS, Azure a Google Cloud
- **Pacu**
  - Exploitačný nástroj pre prostredie AWS

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Exploitačný nástroj pre prostredie AWS

Pacu

Ukážka z nástroja PACU, identifikácia možností v prípade eskalácie privilégií v prostredí AWS

```
Pacu (pacu-test:None) > run iam__privesc_scan
  Running module iam__privesc_scan...
[iam__privesc_scan] Escalation methods for current user:
[iam__privesc_scan]   CONFIRMED: PutGroupPolicy
[iam__privesc_scan]   CONFIRMED: PutUserPolicy
[iam__privesc_scan] Attempting confirmed privilege escalation methods...

[iam__privesc_scan]   Starting method PutGroupPolicy...

[iam__privesc_scan]     Is there a specific group to target? Enter the nam
e now or just press enter to enumerate a list of possible groups to choose
 from:
[iam__privesc_scan] Found 0 groups that the current user belongs to. Choos
e one below.
[iam__privesc_scan] Choose an option:
[iam__privesc_scan] Uncaught error, counting this method as a fail: invali
d literal for int() with base 10: ''
[iam__privesc_scan]   Method failed. Trying next potential method...
[iam__privesc_scan]   Starting method PutUserPolicy...

[iam__privesc_scan] Trying to add an administrator policy to the current u
ser...

[iam__privesc_scan]   Successfully added an inline policy named 6q5152teut
! You should now have administrator permissions.


[iam__privesc_scan] iam__privesc_scan completed.

[iam__privesc_scan] MODULE SUMMARY:

  Privilege escalation was successful

Pacu (pacu-test:None) >
```


Financované Európskou úniou NextGenerationEU

C. Adversary Emulation

Simulácie reálnych útočníkov:

- Adversary emulation testuje nie to, či systém má chybu, ale to, či vieme útok odhaliť včas.
- Vychádzame z MITRE ATT&CK, kde sú popísané taktiky a techniky reálnych útočníkov.
- Používa sa to pri red teamoch, purple teamoch aj ako dlhodobý bezpečnostný program.

Kategórie:

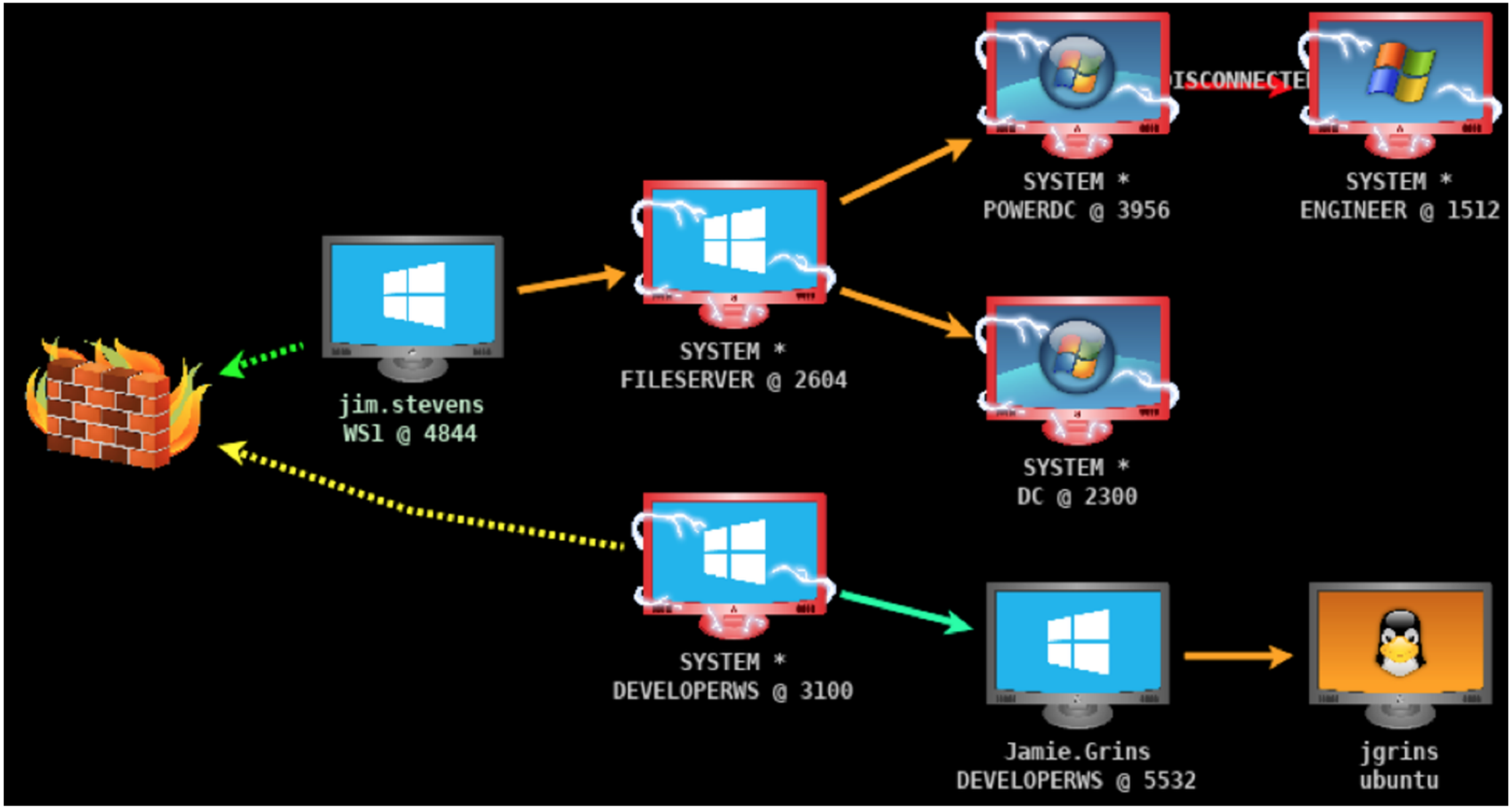
- **C1. Command and Control**
  - AdaptixC2, Mythic, Covenant, Cobalt Strike
- **C2. Breach and Attack Simulation**
  - Cymulate, AttackIQ, SafeBreach, XM Cyber, Caldera
- **C3. Emulácia TTP**
  - Atomic Red Team

C1. Command and Control

- **AdaptixC2**
  - Post-exploitačná platforma podporujúca OS ako MacOS, Linux, Windows
  - Podporuje Beacon Object Files (BOFs), ktoré umožňujú spúšťať vlastné malé programy napísané v jazyku C

- **Cobalt Strike**
  - Komerčný nástroj, ktorého predaj je veľmi obmedzený
  - Jeden z najstabilnejších, ktorý je používaný reálnymi útočnikmi
  - Umožňuje vlastné nastavenia pre beacon-y

Ukážka prostredia Cobalt Strike, čo vidí operátor. Kompromitované stanice s rôznymi verziami operačných systémov.



C2. Breach and Attack Simulation

- **Cymulate**
  - Komerčný produkt umožňujúci validáciu hrozieb, simuláciu útočných aktivít a validáciu bezpečnostných mechanizmov
  - Obsahuje zoznam hrozieb, ktorý je neustále aktualizovaný (oproti open-source riešeniam, ktoré sa spoliehajú na komunitu)

- **SafeBreach**
  - Podobný nástroj ako Cymulate, s menším počtom testovacích scenárov
  - Lacnejšie riešenie ako jeho konkurencia

- **AttackIQ**
- **XM Cyber**
- **Caldera**

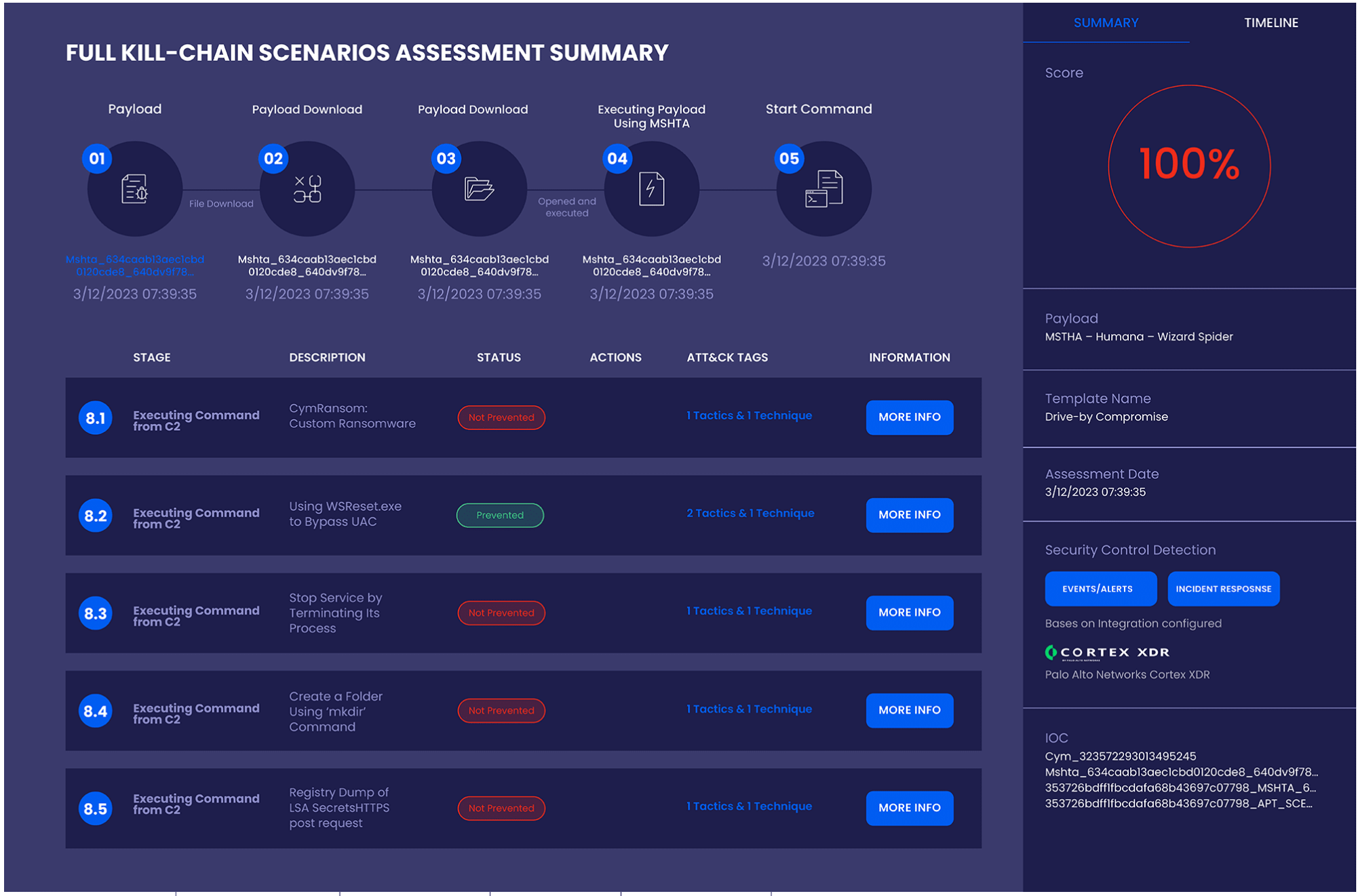
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ukážka z prostredia

Cymulate

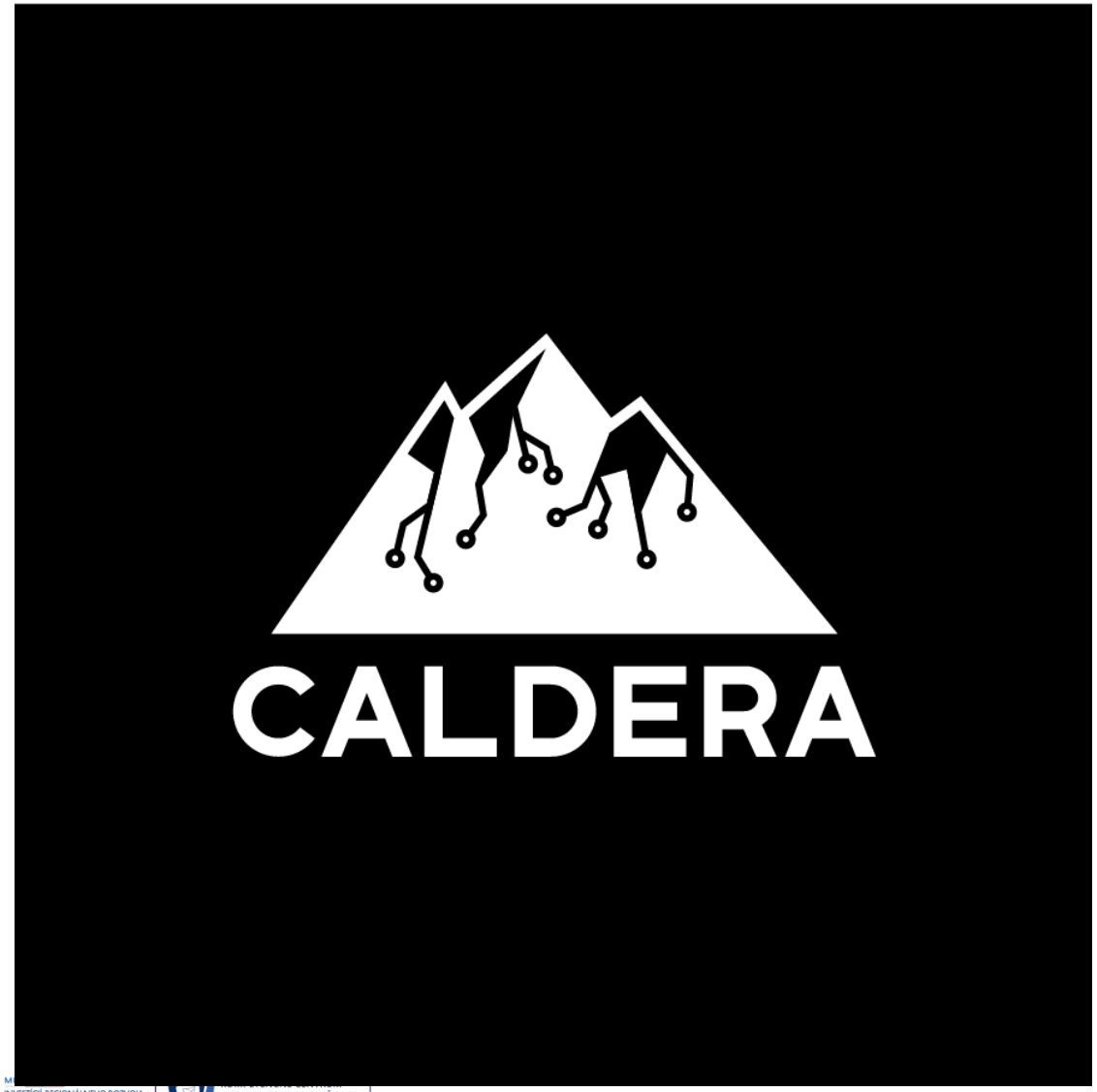
Príklad ktorý obsahuje viacero krokov, pričom jeden z nich bol úspešne zachytený EDR/XDR riešením.

Vpravo je možné vidieť integráciu s platformou Palo Alto Cortex XDR.



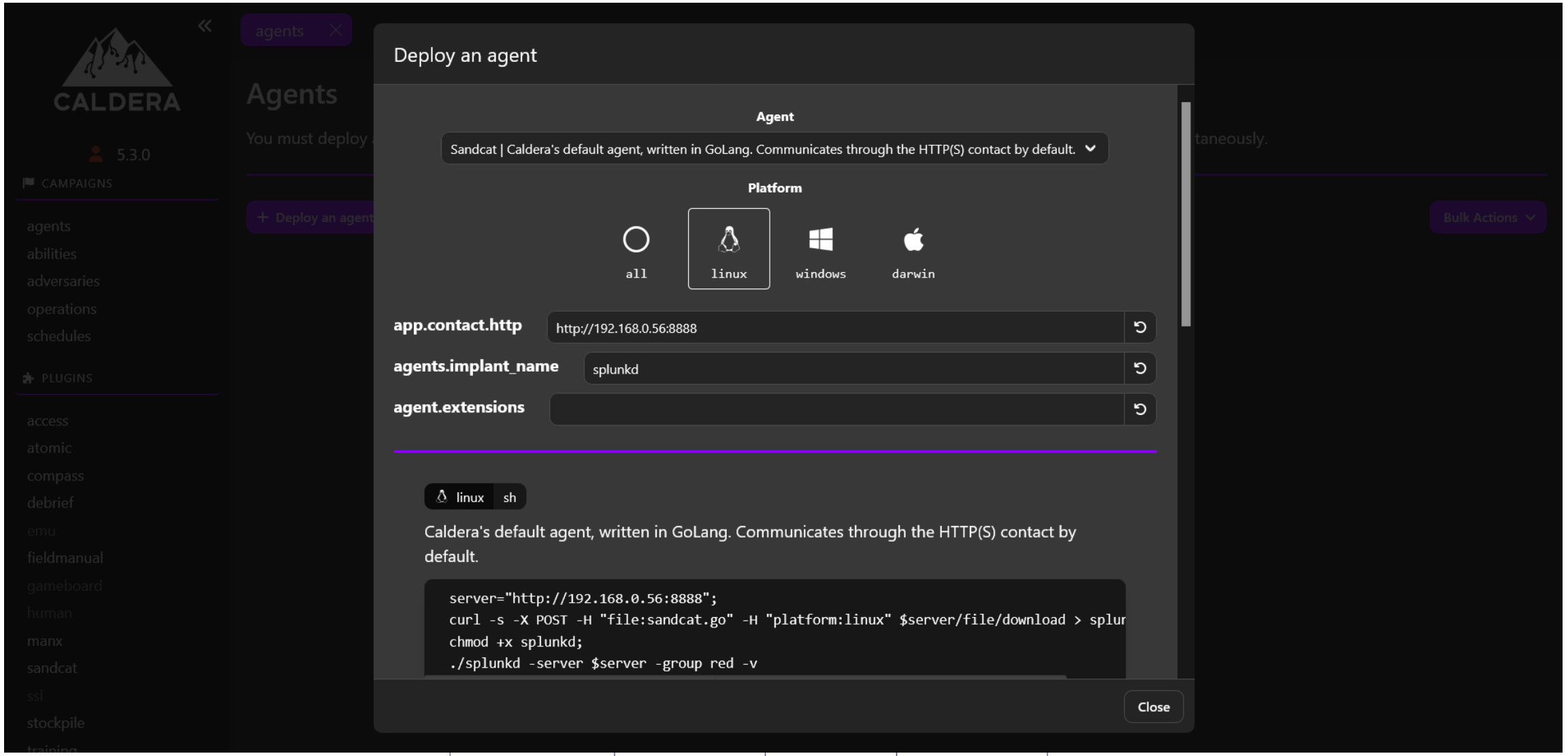
Čo je Caldera

- Rámec pre emuláciu útočníkov a automatizáciu red-team aktivít
- Postavené nad MITRE ATT&CK — mapovanie TTP
- Klient–server model: C2 server + agenti
- Podporuje automatické emulácie, asistuje red team a pomáha pri incident response



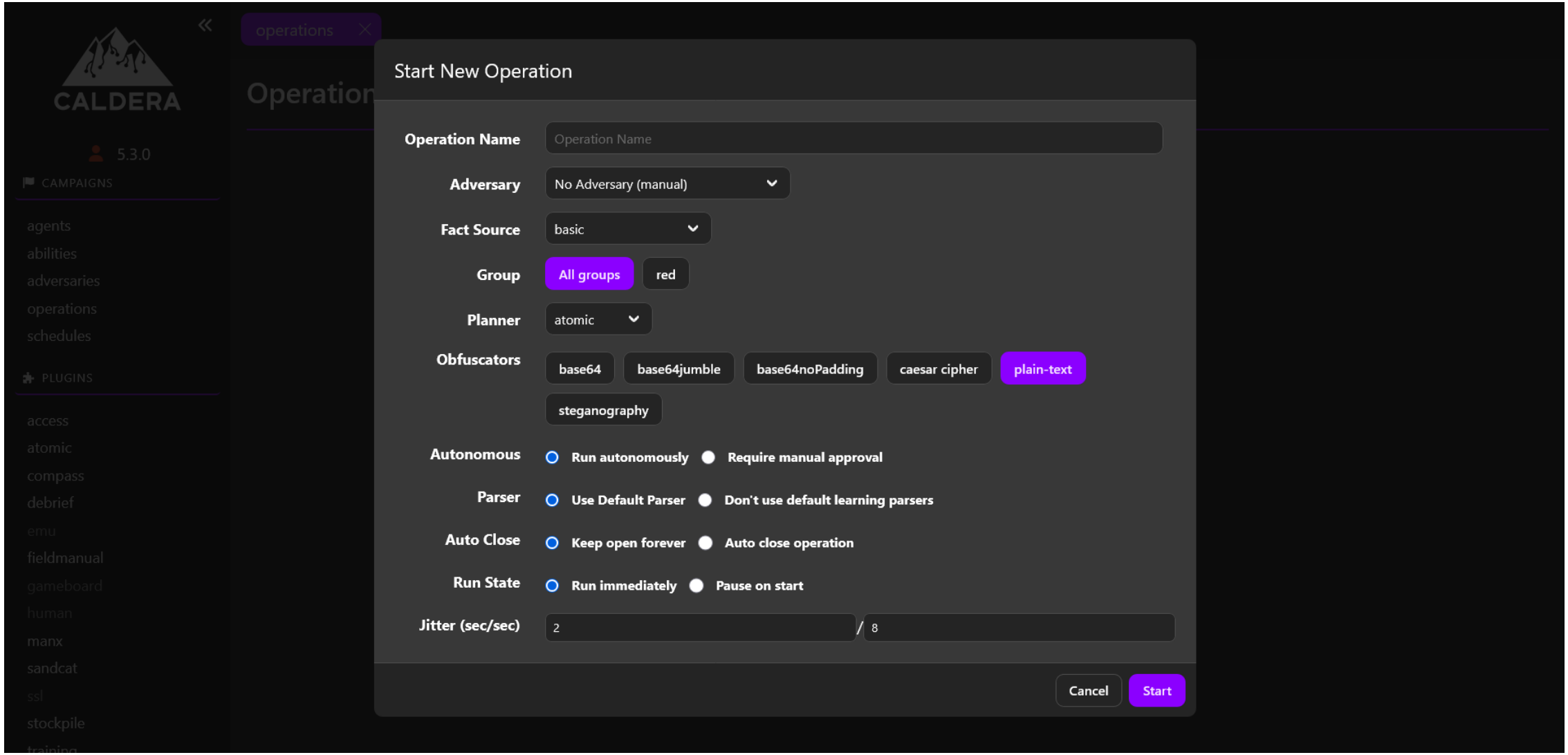
Caldera

Nasadenie agenta



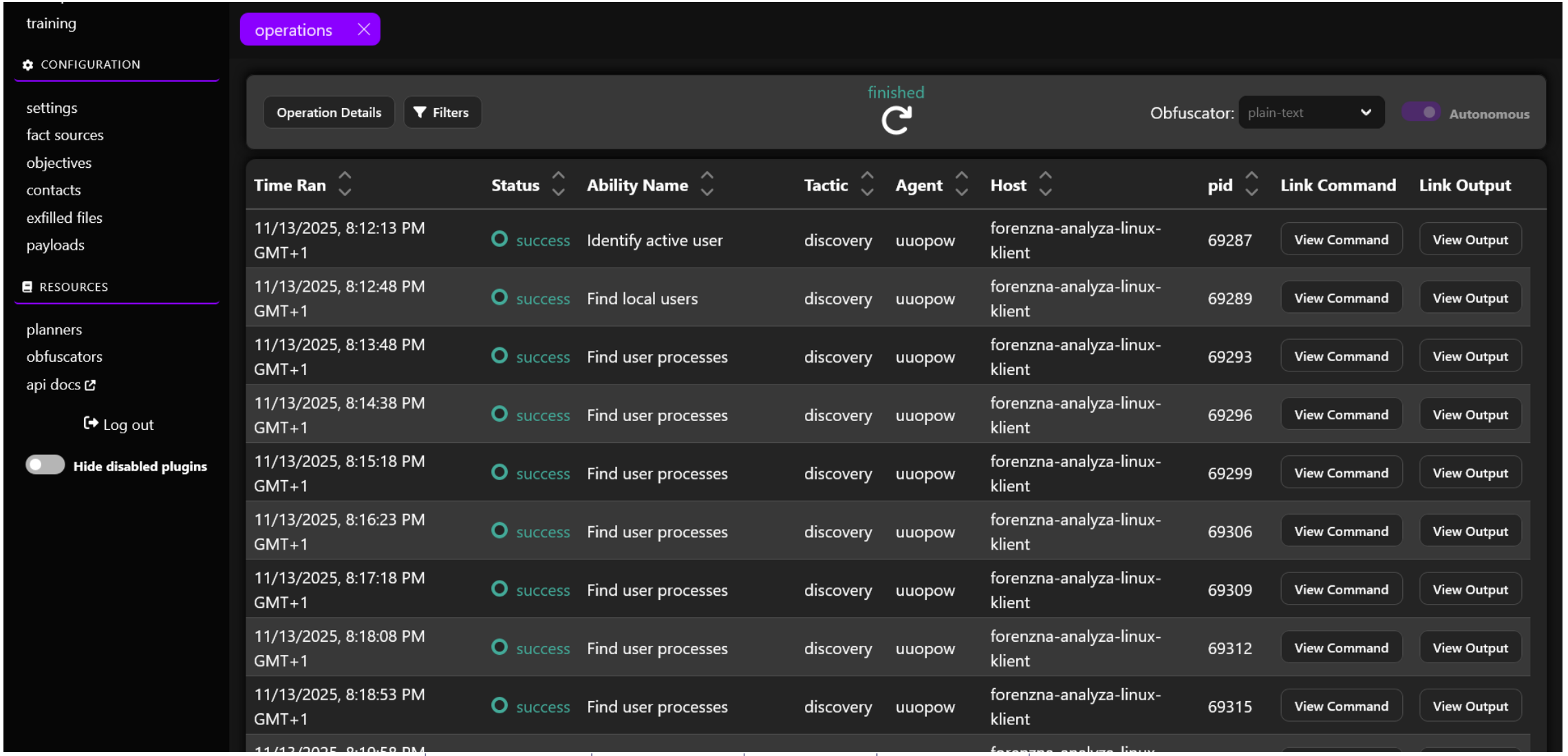
Caldera

Operácie



Caldera

Výsledky operácie

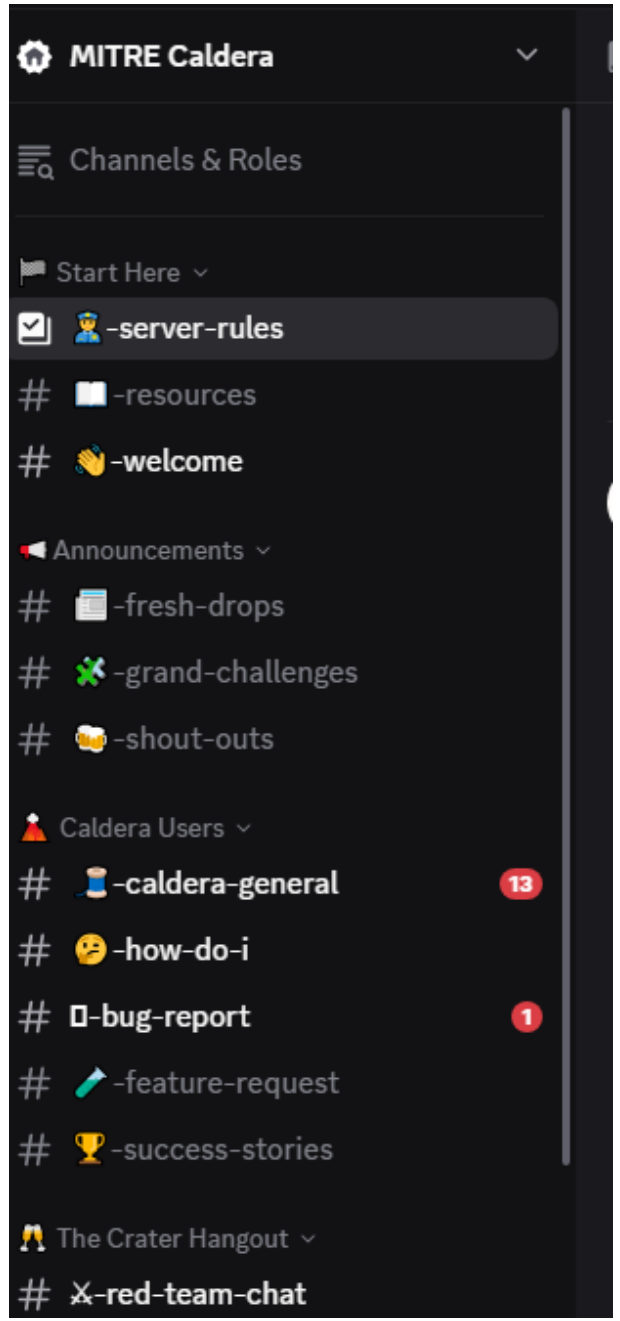


Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
11/13/2025, 8:12:13 PM GMT+1	success	Identify active user	discovery	uuopow	forenzna-analyza-linux-klient	69287	View Command	View Output
11/13/2025, 8:12:48 PM GMT+1	success	Find local users	discovery	uuopow	forenzna-analyza-linux-klient	69289	View Command	View Output
11/13/2025, 8:13:48 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69293	View Command	View Output
11/13/2025, 8:14:38 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69296	View Command	View Output
11/13/2025, 8:15:18 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69299	View Command	View Output
11/13/2025, 8:16:23 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69306	View Command	View Output
11/13/2025, 8:17:18 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69309	View Command	View Output
11/13/2025, 8:18:08 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69312	View Command	View Output
11/13/2025, 8:18:53 PM GMT+1	success	Find user processes	discovery	uuopow	forenzna-analyza-linux-klient	69315	View Command	View Output

Odkazy

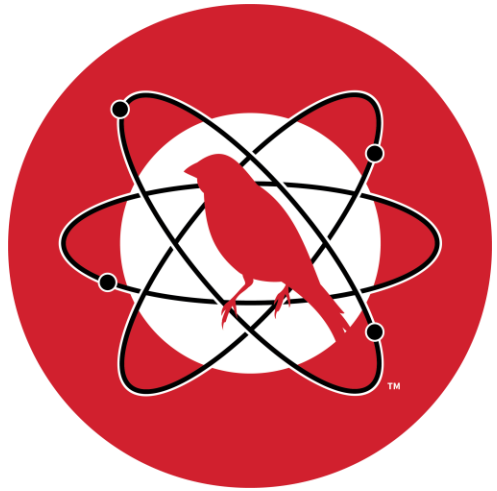
Discord:

- https://discord.com/invite/mJsTuhZ88T



C3. Emulácia TTP

- **Atomic Red Team™**
  - Knižnica malých testov, ktoré umožňujú testovať detekčné mechanizmy
  - Open-source riešenie pravidelne udržiavané komunitou
  - Podporované OS: Windows, Linux a macOS
  - Existuje PowerShell modul Invoke-AtomicRedTeam



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Farebné položky v matici označujú, že pre danú techniku existuje aspoň jeden atomic test

Úvod do ATT&CK taktík a techník

Enterprise taktiky

- Taktiky predstavujú „**prečo**" pri technike alebo podtechnike ATT&CK. Ide o taktický cieľ útočníka – dôvod, pre ktorý vykonáva danú aktivitu
- Útočník môže napríklad sledovať dosiahnutie prístupu k prihlasovacím údajom
- **14 hlavných fáz útoku**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

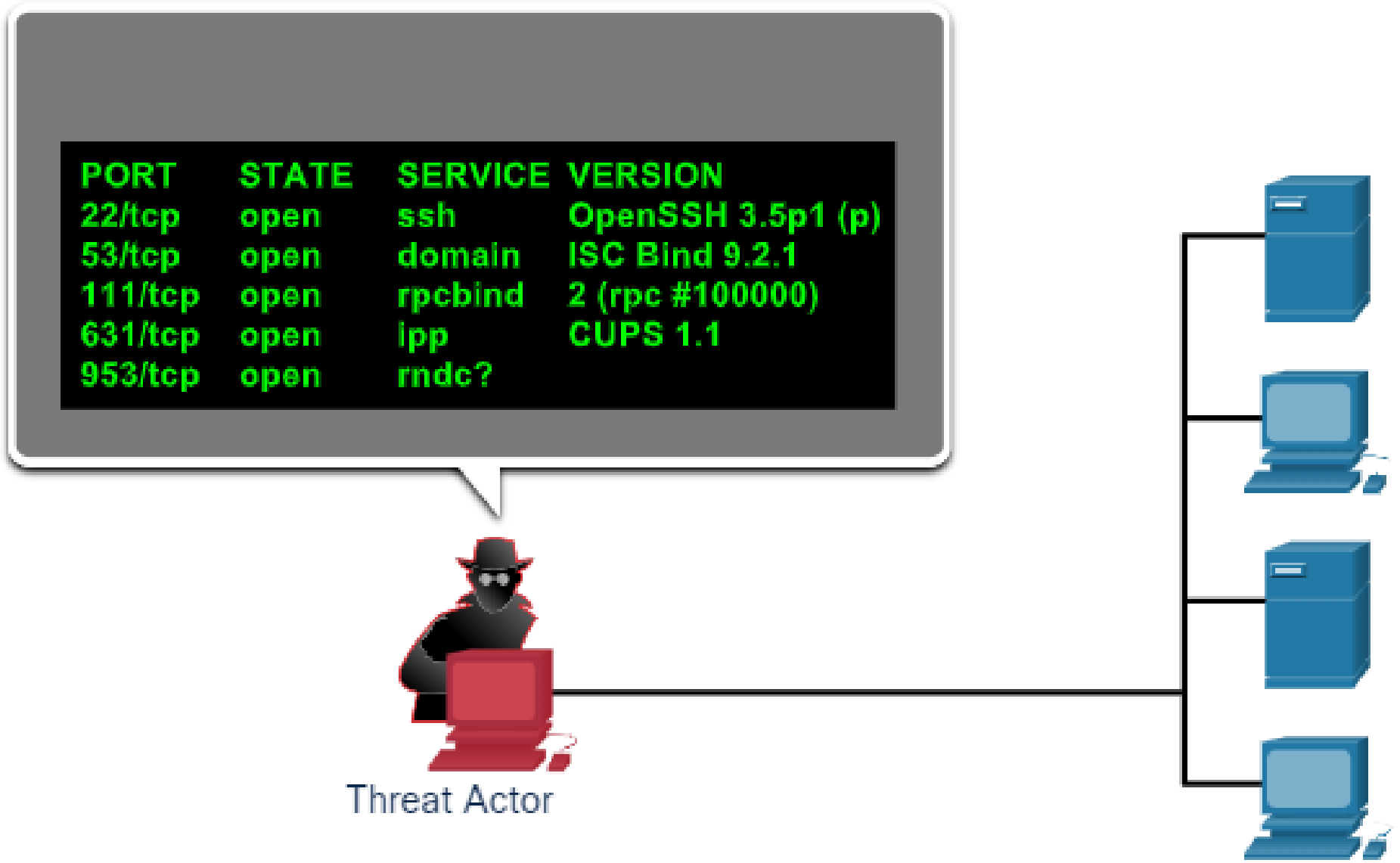
TA0043 – Reconnaissance (Prieskum)

- Prieskum - zbieranie informácií o cieli
- Pasívne i aktívne metódy
  - OSINT - získavanie verejných informácií
  - Skenovanie portov
  - DNS enumerácia
- Mapovanie:
  - Infraštruktúry
  - Zamestnancov
  - Technológií
- Útočník buduje detailný profil cieľa pred vlastným útokom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Úvod do ATT&CK taktík a techník

Úvod do ATT&CK taktík a techník



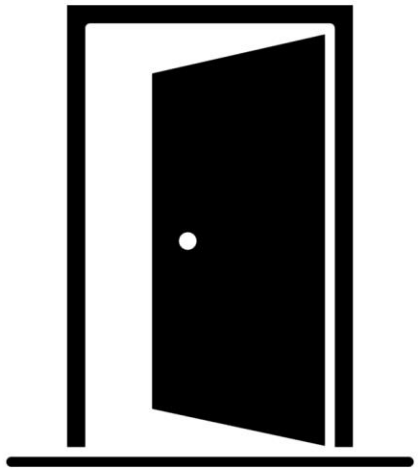
TA0042 – Resource Development (Vývoj zdrojov)

- Vývoj zdrojov - Príprava infraštruktúry
- Vytvorenie vlastnej infraštruktúry (servery, C2)
- Nákup domén a falošných účtov
- Nákup prípadne výtváranie ďalšieho malvéru a nástrojov
- Všetky potrebné zdroje sú pripravené pred prvotným dopadom na cieľ

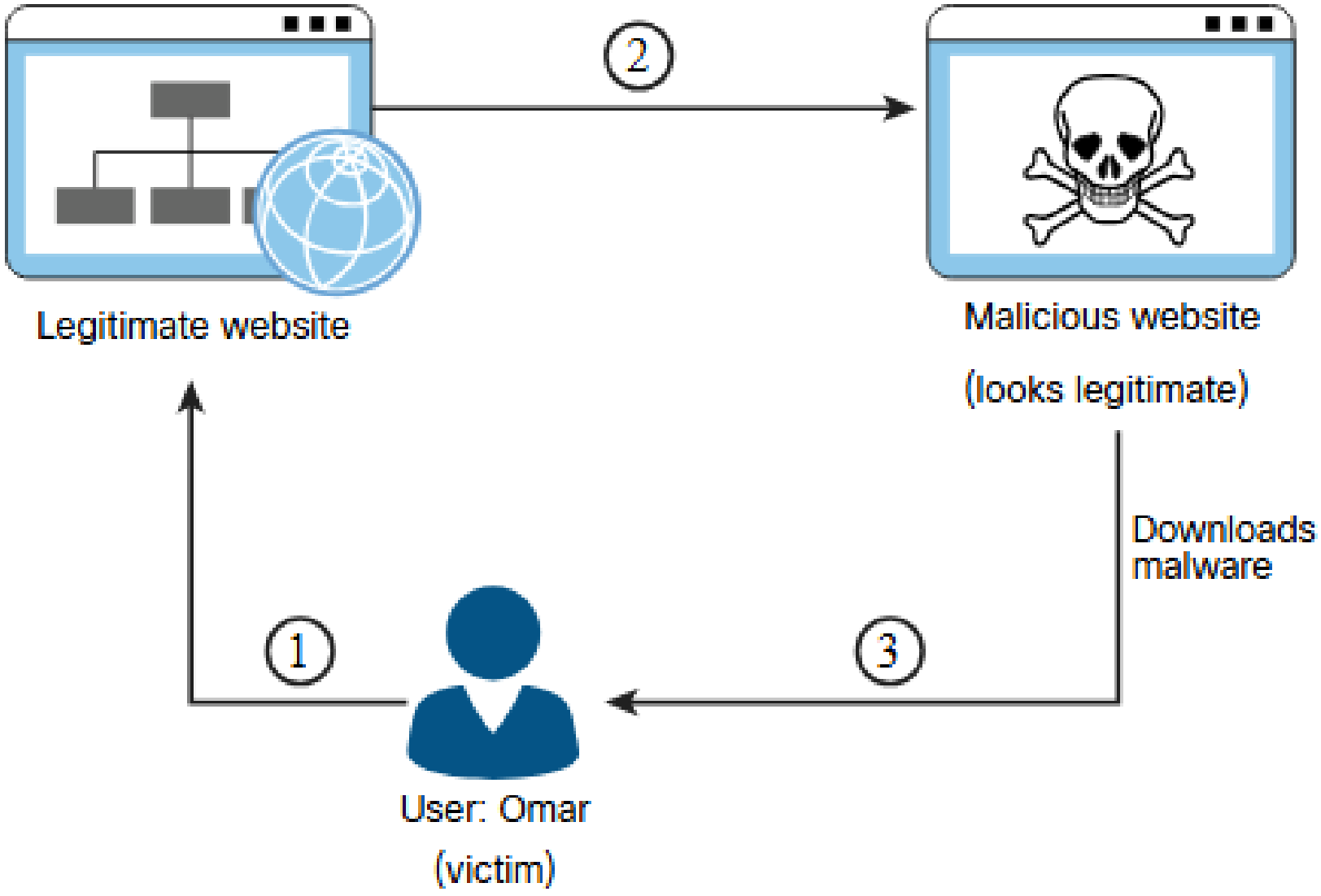
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

TA0001 – Initial Access (Počiatočný prístup)

- Počiatočný prístup - Vstup do siete
- Phishing kampane a sociálna manipulácia
- Zneužitie verejne dostupných (web) aplikácií
- Kompromitácia používateľských účtov a zneužitie zraniteľností
- Prvý vstup do siete - kritická fáza pre ďalší pokrok útočníka

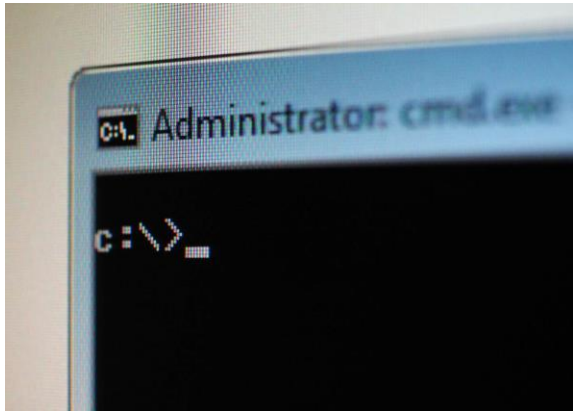


Úvod do ATT&CK taktík a techník



TA0002 – Execution (Vykonanie)

- Po získaní prvotného prístupu útočník spúšťa svoj škodlivý kód na kompromitovanom systéme
- Vykonanie je fáza, v ktorej sa plány útočníka stávajú reálnymi akciami
- PowerShell skripty, Bash príkazy, vykonávanie binárnych súborov a injektovanie do legit. procesov
- Spustenie makier v dokumentoch (Word, Excel)
- Útočník maskuje aktivity pomocou legitímnych nástrojov (PowerShell, WMI, LSASS)
- Typ vykonávaného kódu je špecificky zacielený na dosiahnutie útočníkových cieľov



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

TA0003 – Persistence (Perzistencia)

- Po získaní prístupu a vykonaniu kódu si útočník zabezpečuje dlhodobú kontrolu nad systémom
- Perzistencia umožňuje útočníkovi zostať v systéme aj po reštarte, zmene hesiel alebo bezpečnostných záplatách
- Útočník skrýva „persistence“ mechanizmy hlboko v systéme (aby boli ťažšie objaviteľné pri auditoch)
- Cieľom je vytvoriť si "**zadné vrátka**" pre prípadnú budúcu re-infekciu

- Windows: modifikácia registrov, vytvorenie nových používateľských účtov
- Linux: cron joby, SSH kľúče, modifikácie shell profilov

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

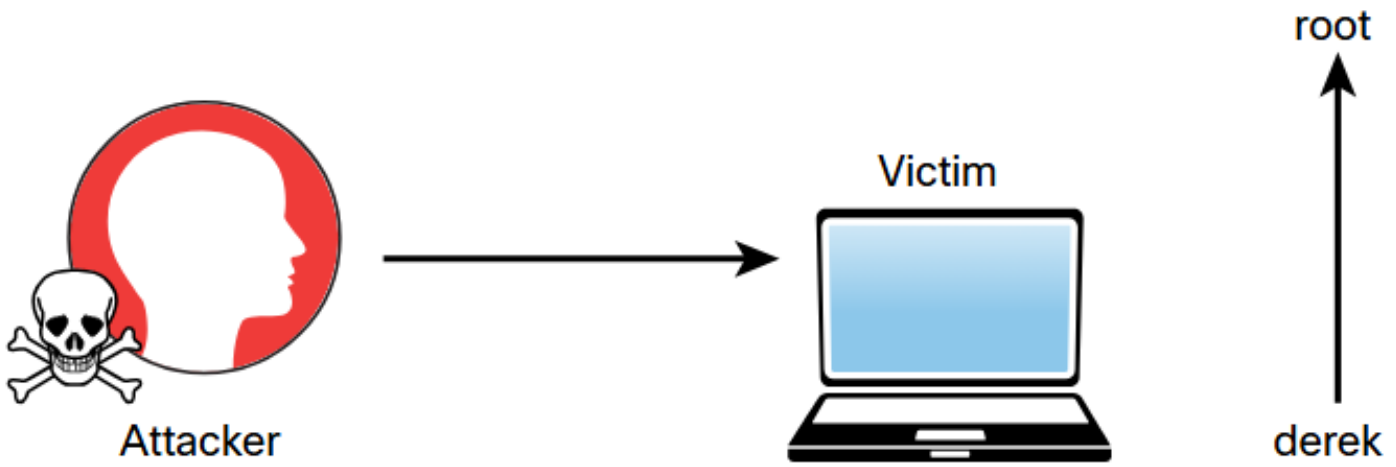
TA0004 – Privilege Escalation (Eskalácia privilégií)

- V mnohých prípadoch útočník nemá administrátorské práva pri počiatočnom prístupe
- Kompromitovaný účet je zvyčajne bežný užívateľský účet s obmedzenými oprávneniami
- Zneužívanie zraniteľností v jadre operačného systému (kernel exploity)
- Nesprávne konfigurácie súborov a služieb (SUID bity v Linuxe, chybné ACL v OS Windows)
- Legitímne nástroje ako sudo, UAC bypass techniky alebo Windows Token Impersonation
- Po úspešnej eskalácii môže útočník robiť operácie vyžadujúce administrátorské práva

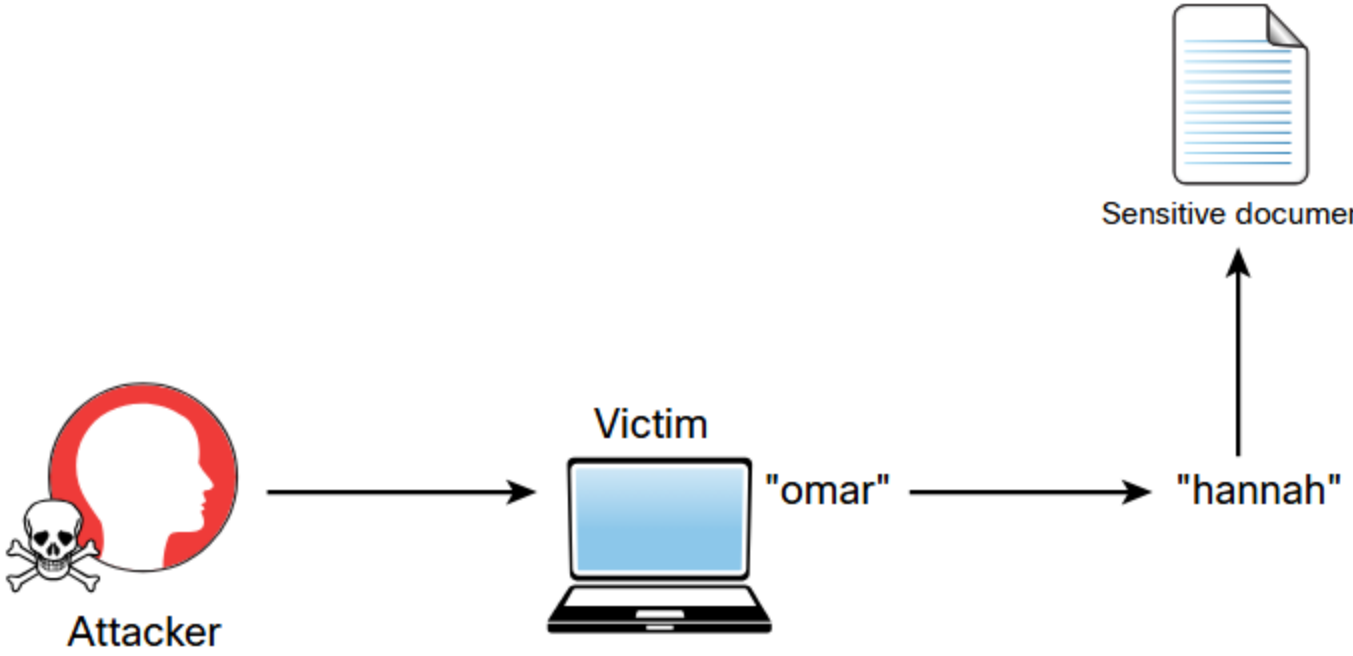
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Eskalácia privilégií

- Vertikálna



- Horizontálna



TA0005 – Defense Evasion (Obchádzanie obrany)

- Obfuskácia kódu – kód sa stáva ťažšie čitateľný pre analytikov, znižuje sa šanca že antivírus zakročí
- Vypínanie bezpečnostných nástrojov (antivírus, firewall)
- Mazanie a modifikácia log súborov - vymazanie stôp svojich aktivít
- Injektovanie kódu do legitímnych procesov (explorer.exe, svchost.exe) a Living off the land binaries (LOLBins)
- **Aktivity sa javia ako legitímna systémová aktivita** - detekcia je oveľa ťažšia

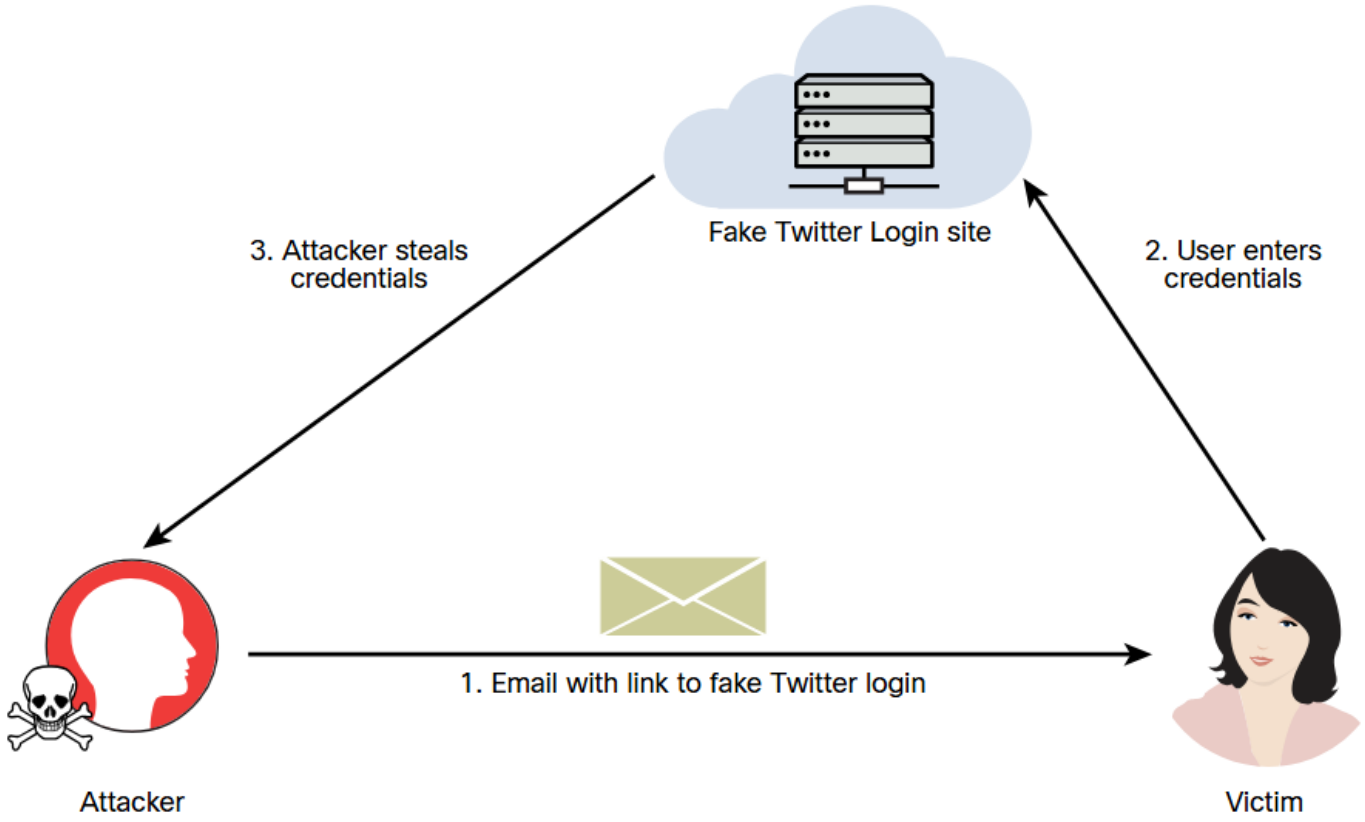
TA0006 – Credential Access (Prístup k prihlasovacím údajom)

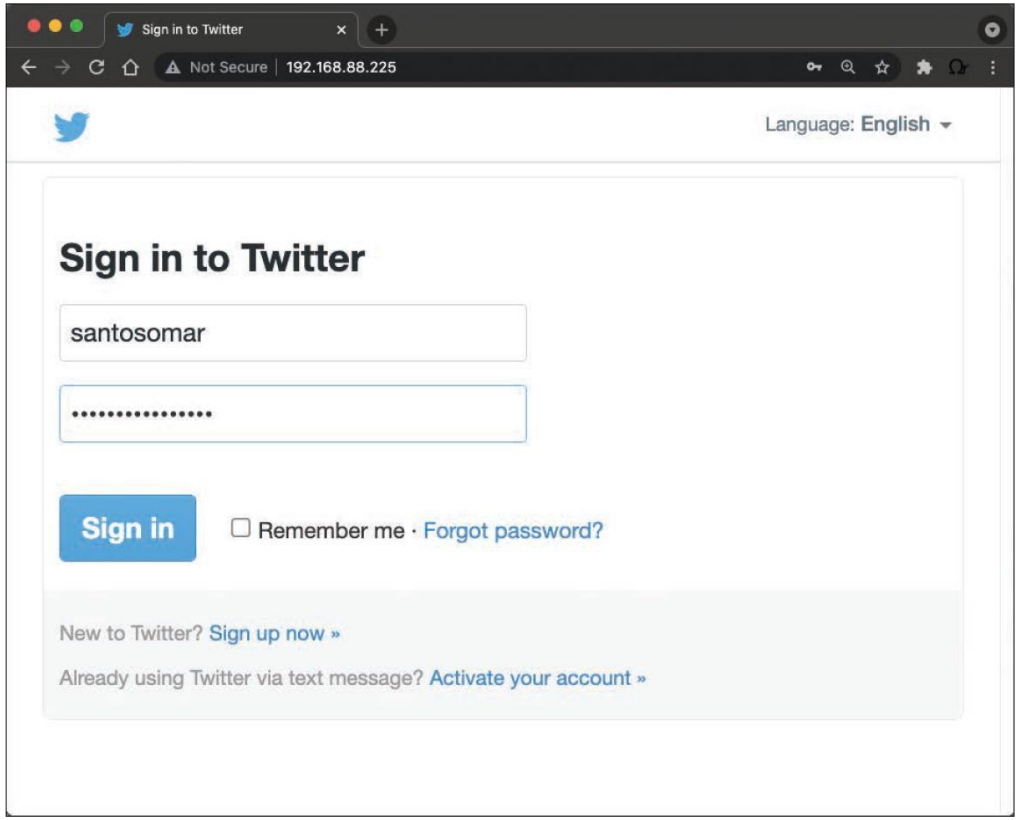
- Získanie prihlasovacích údajov je jednou z najcennejších vecí pre útočníka
- Ak má útočník platnú kombináciu užívateľského mena a hesla, môže sa priamo prihlásiť bez ďalšej exploitácie
- **Získané údaje sú používané na laterálny pohyb**

- Zaznamenávanie všetkých stlačení klávesnice (Keylogging)
- Extrakcia hesiel a hashov z pamäte (LSASS procesu, SAM databázy, Credentials Manager)
- Útok pomocou slovníka a hrubou silou proti slabým heslám, phishing a extrakcia uložených hesiel z prehliadačov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Úvod do ATT&CK taktík a techník





TA0007 – Discovery (Zisťovanie)

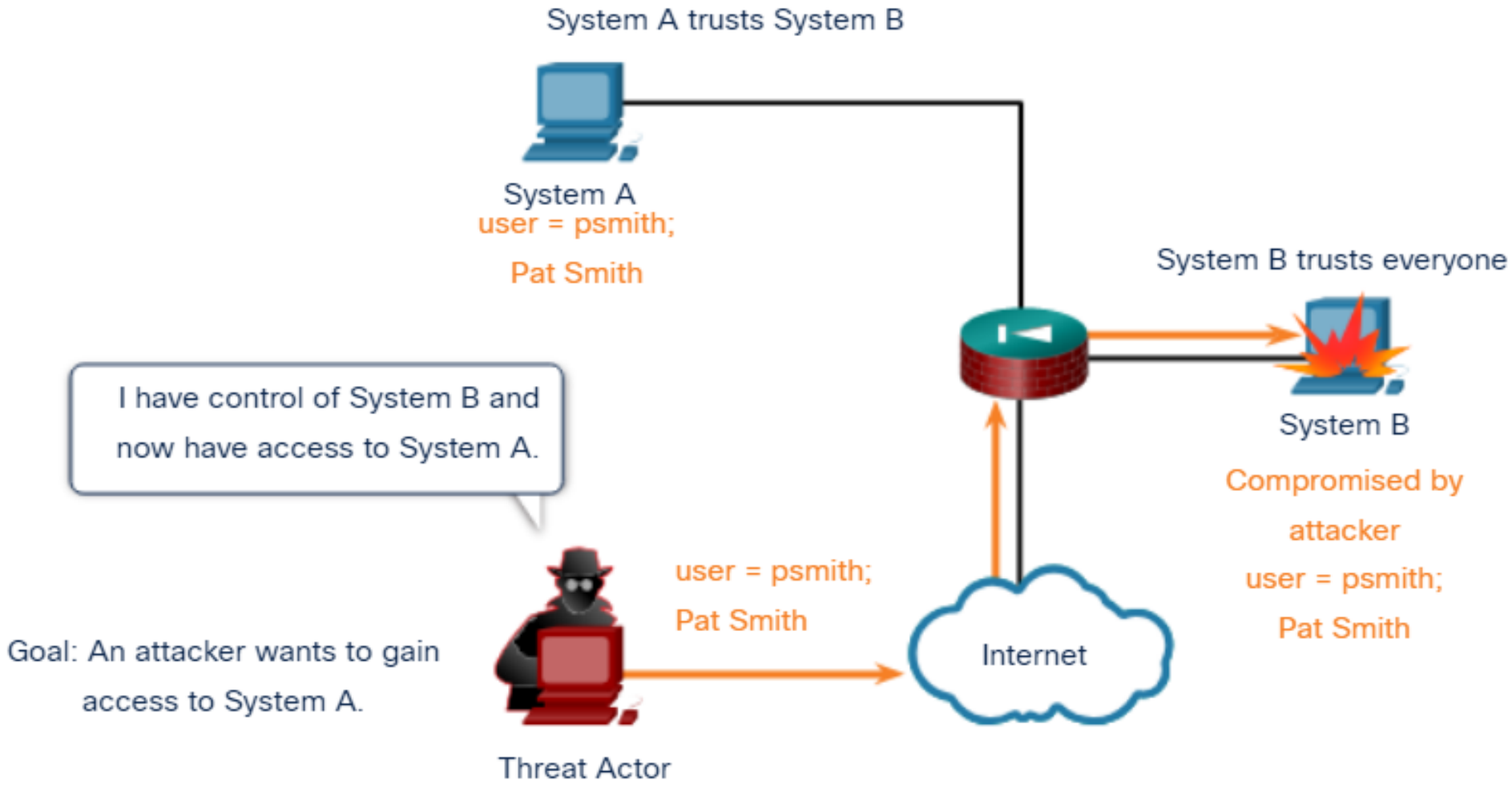
- Po získaní kontroly nad systémom potrebuje útočník identifikovať prostredie
- Enumerácia užívateľov a skupín (príkazy `net user` a `net group`)
- Identifikácia zdieľaných zdrojov (`net share`), mapovanie sieťovej topológie (`tracert, route`)
- Detekcia bezpečnostných softvérov a firewall pravidiel
- Tieto informácie sú kritické pre úspešný laterálny pohyb a cielenie na cenné systémy

TA0008 – Lateral Movement (Laterálny pohyb)

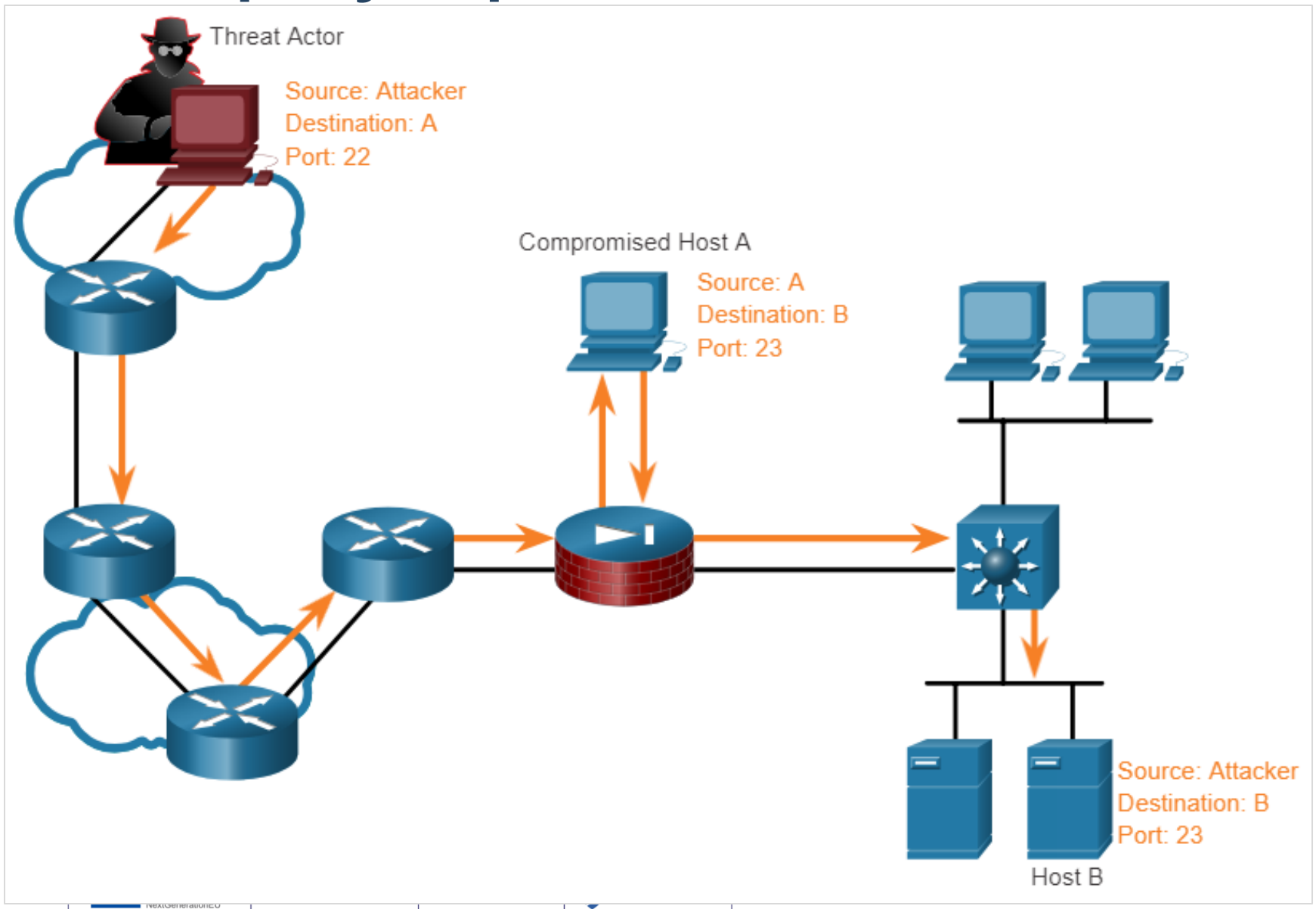
- Laterálny pohyb je proces rozširovania kontroly z počiatočného systému na ďalšie servery v sieti
- Cieľom je dostať sa k citlivejším systémom - databázové servery, súborové servery, doménové radiče
- Zneužitie získaných prihlasovacích údajov - ak má útočník heslo s administrátorskými právami
- Zneužitie trust vzťahov medzi systémami (Kerberos delegation, trust exploity)
- RDP, PSExec, WMI alebo SMB protokoly na priame vykonávanie príkazov
- Útočník sa snaží vyhnúť detekcii - minimalizuje množstvo logov a maskuje svoju aktivitu ako legitímnu komunikáciu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad 1 laterálneho pohybu po sieti



Príklad 2 laterálneho pohybu po sieti



TA0009 – Collection (Zber dát)

- Po získaní prístupu k viacerým systémom prichádza zber dát - agregácia citlivých informácií
- Typ zbieraných dát závisí od motivácie útočníka: finančné údaje, obchodné tajomstvá, osobné údaje
- Zbieranie z rôznych zdrojov - súbory na diskoch, e-maily, databázy
- Sieťová komunikácia (sniffing)
- Systémové informácie ako konfigurácie, prihlasovacie údaje alebo bezpečnostné objekty
- Zbierané dáta sú kategorizované, centralizované a pripravené na prenos mimo siete

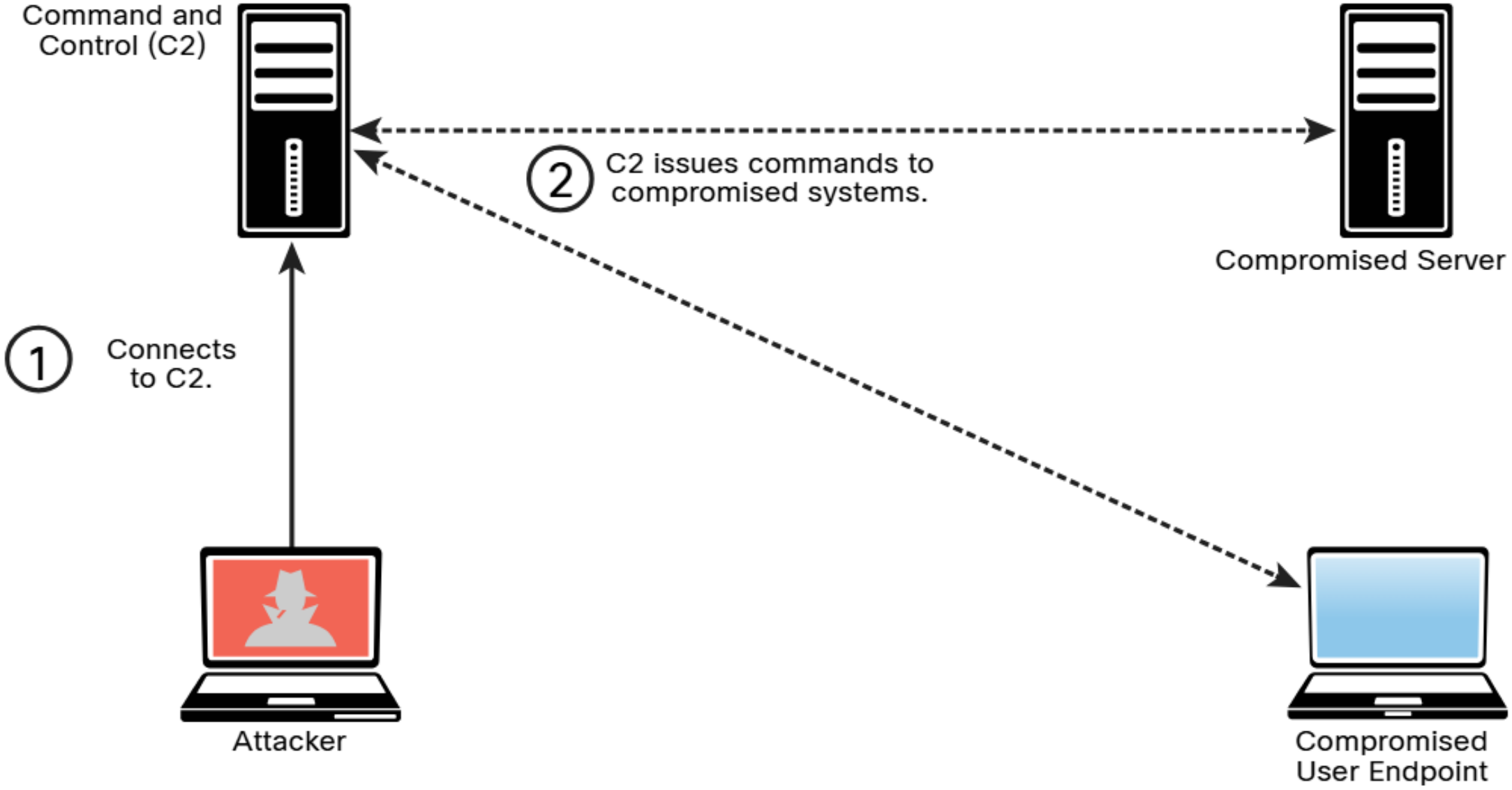
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

TA0011 – Command and Control

- Počas kampane musí útočník komunikovať so svojimi kompromitovanými systémami
- Command and Control (C2) infraštruktúra je komunikačný kanál medzi útočníkom a kompromitovanými systémami
- Útočník vytvára C2 kanály, ktoré sú šifrované a skryté - používa legitímne protokoly (HTTPS, DNS)
- C2 infraštruktúra je umiestnená na serveroch, ktoré útočník kontroluje (Cloud, poskytovatelia VPS)
- Cez tieto kanály útočník posiela príkazy, prijíma odpovede a dáta, alebo orchestruje komplexné operácie
- C2 komunikácia sa maskuje ako legitímna prevádzka

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako funguje C2 server



TA0010 – Exfiltration (Exfiltrácia)

- Exfiltrácia je fáza, v ktorej útočník odvádza ukradnuté dáta mimo siete do svojich serverov
- Práve tieto dáta sú finálnym cieľom útočníka - budúce zisky pochádzajú z ich predaja, vydierania alebo špionáže
- Použitie legitímnych protokolov (HTTPS, FTP, DNS)
- Kompresia a šifrovanie dát - zníženie veľkosti a skrytie obsahu
- Prenos dát v menších veľkostiach = vyhnúť sa anomáliám v šírke pásma
- Cloudové úložiská (Google Drive, Dropbox, OneDrive) slúžia na skrytie aktivít

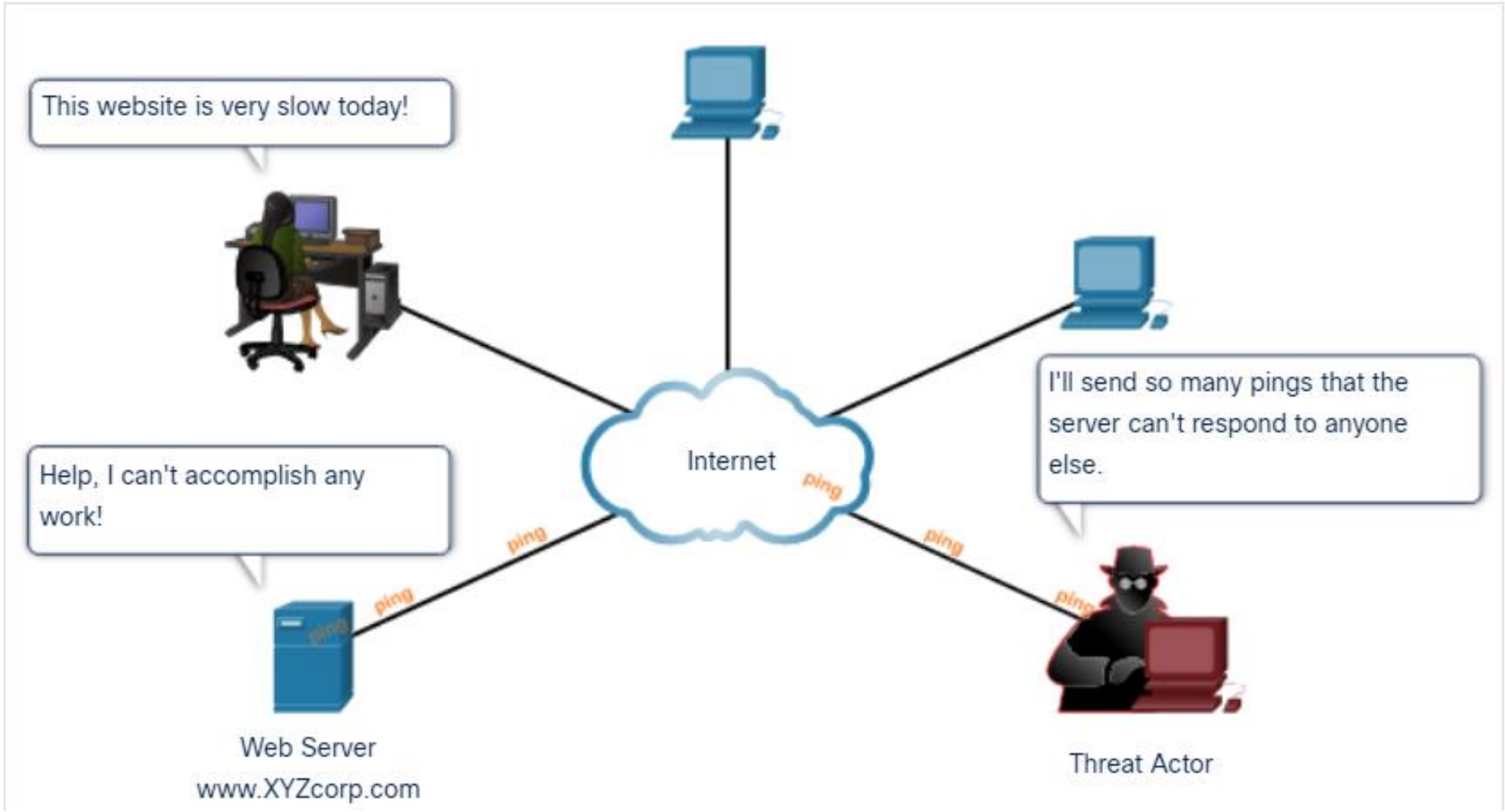
Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

TA0040 – Impact (Dopad)

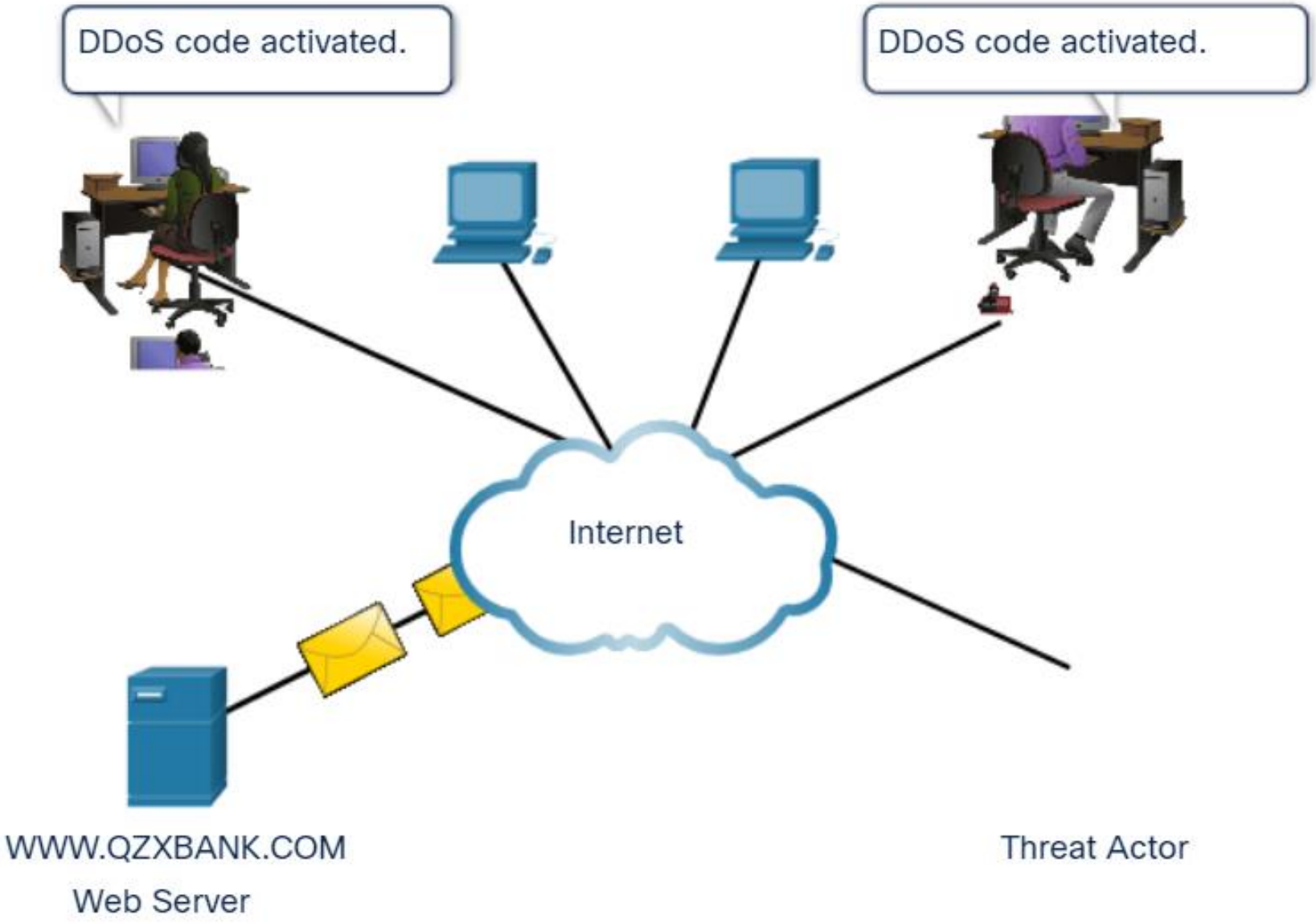
- Dopad je posledná a najviditeľnejšia fáza útoku - moment, keď sa útočníkova aktivita stáva evidentná
- Táto fáza predstavuje dopad na dostupnosť, integritu a dôvernosť systémov a dát organizácie
- Ransomvér - šifrovanie kritických dát a vydieranie za ich odšifrovanie
- DoS a DDoS útoky na narušenie dostupnosti online služieb
- Deštruktívny malvér na fyzické zmazanie dát alebo sabotáž infraštruktúry
- Modifikácia dát na narušenie integrity alebo ovplyvňovanie fyzických systémov (SCADA, ICS)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Úvod do ATT&CK taktík a techník



Úvod do ATT&CK taktík a techník



Certfikácie a ďalšie vzdelávanie v oblasti ofenzívnej bezpečnosti

Certifikácie

- **OffSec**
  - OSCP+ (PEN-200: Penetration Testing with Kali Linux)
  - OSED (EXP-301: Windows User Mode Exploit Development)
  - OSWA (WEB-200: Web Attacks with Kali Linux)
  - OSEP (PEN-300: Evasion Techniques and Breaching Defenses)

- **Zero-Point Security**
  - Certified Red Team Operator (CRTO)
  - CRTO II

Certifikácie

- **Burp Suite**
  - Burp Suite Certified Practitioner (BSCP)

- **GIAC (SANS)**
  - GPEN – GIAC Penetration Tester
  - GRTP - GIAC Red Team Professional
  - GWAPT - GIAC Web Application Penetration Tester
  - GX-PT - GIAC Experienced Penetration Tester

Certfikácie a ďalšie vzdelávanie v oblasti ofenzívnej bezpečnosti

Kurz / Certifikácia	Približná cena (EUR)
OSCP+/OSED/OSEP	*~1 560 € (OSCP+ cena $1 699)*
Burp Suite Certified Practitioner (BSCP)	*~90 € (skúška $99)*
GIAC GPEN / GRTP / GWAPT	*~930 € (základná cena za skúšku)* *~6 400 – 8 000€ (celý kurz + skúška)*

Ďalšie vzdelávanie

- **HTB Academy**
  - Kurzy sa platia tzv. Cubes (tie si viete dokúpiť alebo ich získať v CTF)
  - Pokrýva rôzne oblasti, či už Penetračného testovania alebo Red Teamingu
  - https://academy.hackthebox.com/
- **PortSwigger Academy**
  - Zadarmo, pokrýva web applikácie
  - Od začiatočníkov až po profesionálov
  - https://portswigger.net/web-security

HACKTHEBOX

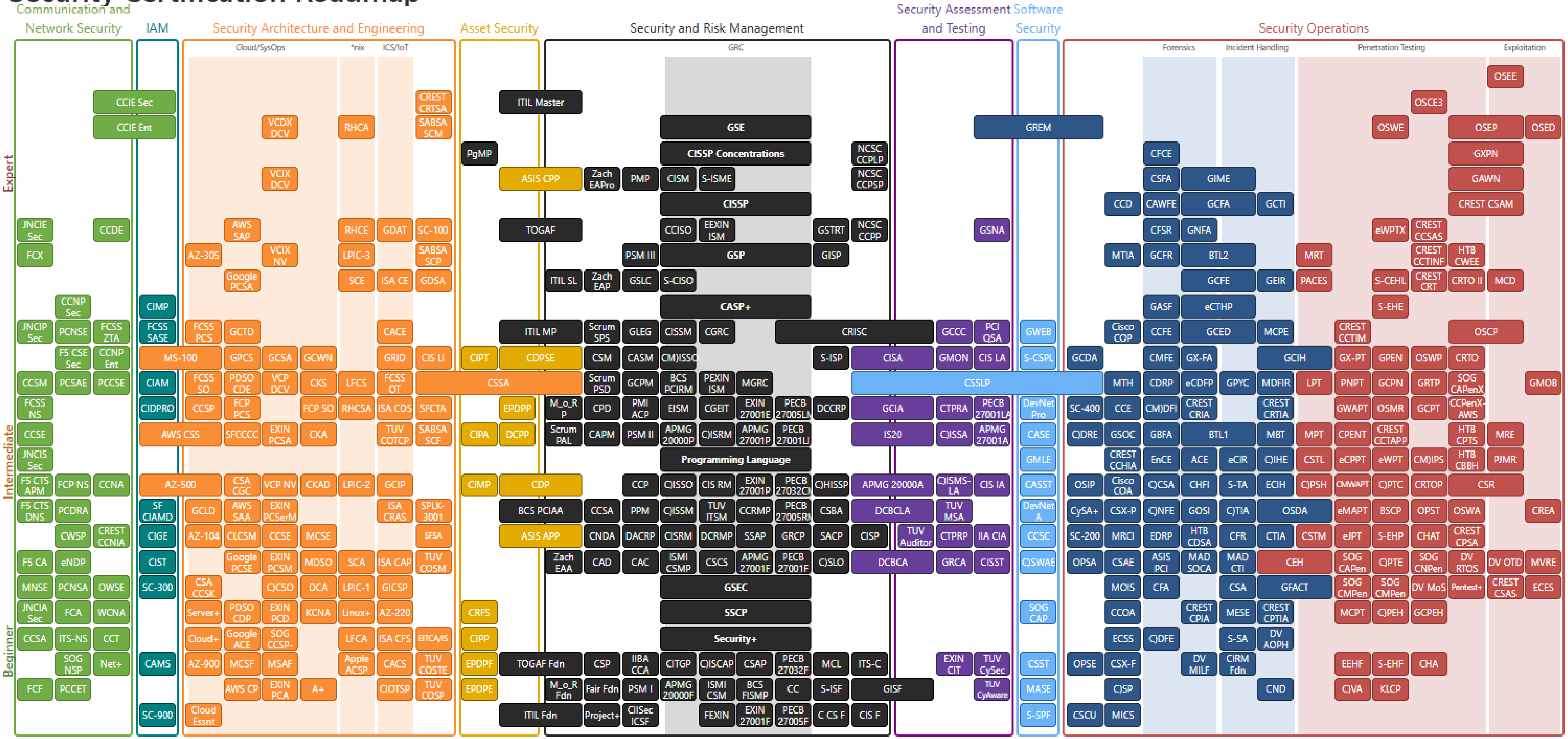
Ďalšie vzdelávanie

- **Cisco Ethical Hacker**
  - Kurz vhodný pre úplných začiatočníkov
- **HackTricks**
  - https://book.hacktricks.wiki/en/index.html
- **Game of Active Directory (GOAD)**
  - Lab pre testovanie Active Directory zraniteľností a miskonfigurácii
  - https://github.com/Orange-Cyberdefense/GOAD

HackTricks

Ďalšie možnosti certifikácie ☺

Security Certification Roadmap



481 certifications listed | July 2024

Odkaz na Security Certification Roadmap

- https://pauljerimy.com/security-certification-roadmap/

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Bezpečnostné testovanie a ofenzívne zručnosti

Zvyšovanie povedomia o KB a testovanie bezpečnosti (Blok VIII)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk