Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Problémy pri monitorovaní

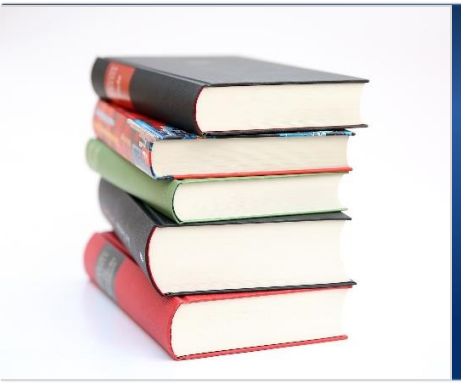
Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

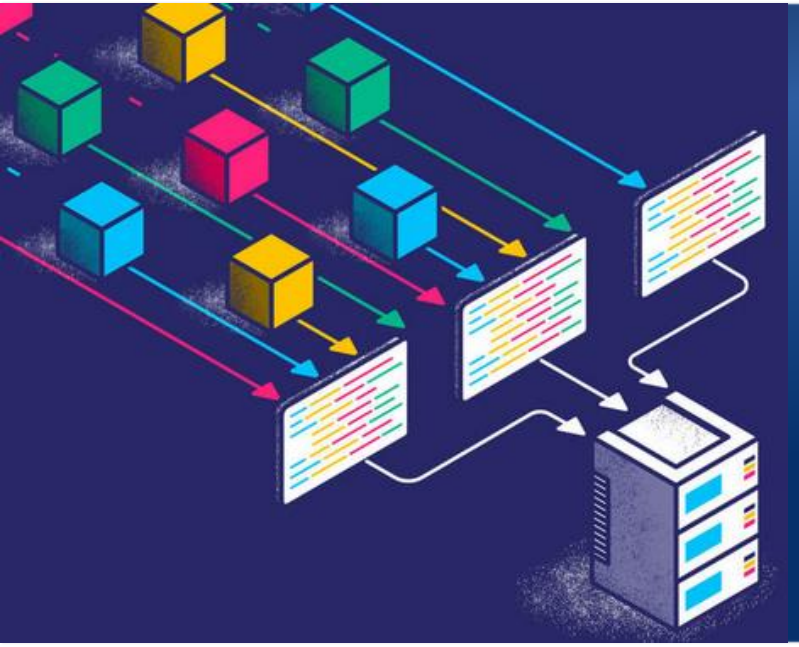
KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Ciele

- Pochopiť
  - aké problémy prinášajú pre monitorovanie bežne využívané sieťové protokoly a služby
    - Syslog,
    - NTP,
    - DNS,
    - HTTP and HTTPS,
    - email,
    - ICMP,
- Pochopiť
  - aké problémy prinášajú niektoré bezpečnostné technológie
    - ACL,
    - NAT,
    - šifrovanie,
    - tunelovanie,
    - P2P siete,
    - Tor,
    - a systémy pre rozkladanie záťaže



Bežné protokoly monitorovania

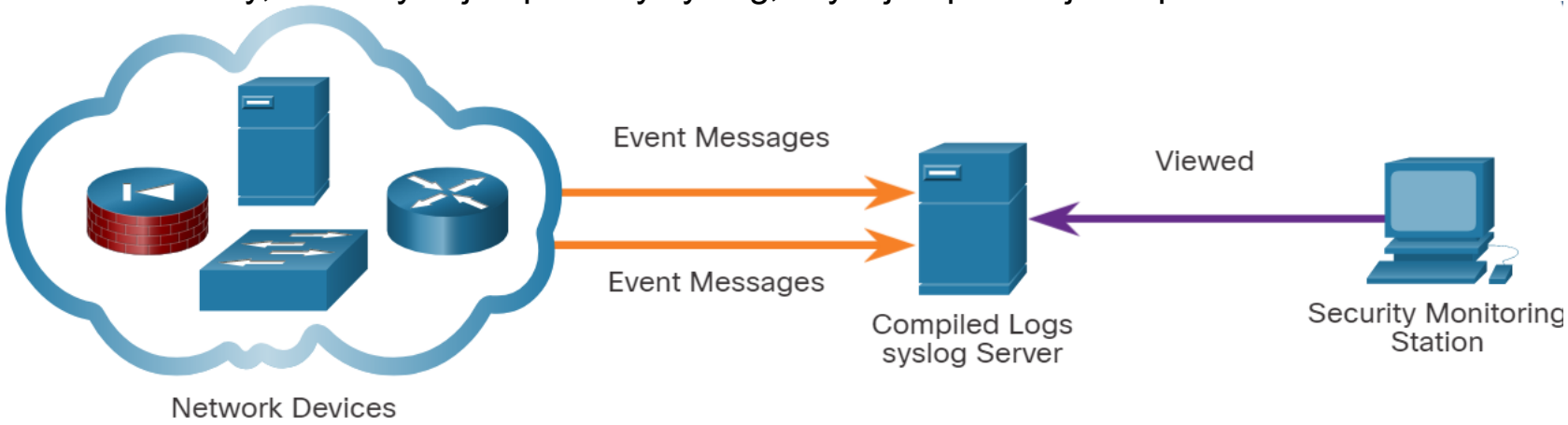
Správanie bežných sieťových protokolov
v kontexte monitorovania bezpečnosti

Syslog a NTP

- Syslog a Network Time Protocol (NTPv4, NTPv5 zatiaľ ako draft) sú **nevyhnutné** pre prácu **analytika** kybernetickej bezpečnosti.

Štandard syslog

- sa používa na zaznamenávanie správ udalostí zo sieťových zariadení a koncových bodov.
- umožňuje systémovo-neutrálne prostriedky na prenos, ukladanie a analýzu správ.
- Mnoho typov zariadení od mnohých rôznych dodávateľov môže použiť syslog na odosielanie záznamov protokolu na **centrálne servery**, ktoré spúšťajú **démona syslog**.
  - Táto centralizácia zhromažďovania protokolov pomáha s praktickým monitorovaním bezpečnosti.
  - Servery, na ktorých je spustený syslog, zvyčajne počúvajú na porte **UDP 514**.



Network Time Protocol (NTP)

- Správy Syslog sú zvyčajne označené časovou pečiatkou
- správy prichádzajú z mnohých zariadení => dôležité je, aby zariadenia zdieľali konzistentné časové hodiny – dosiahnuté pomocou NTP

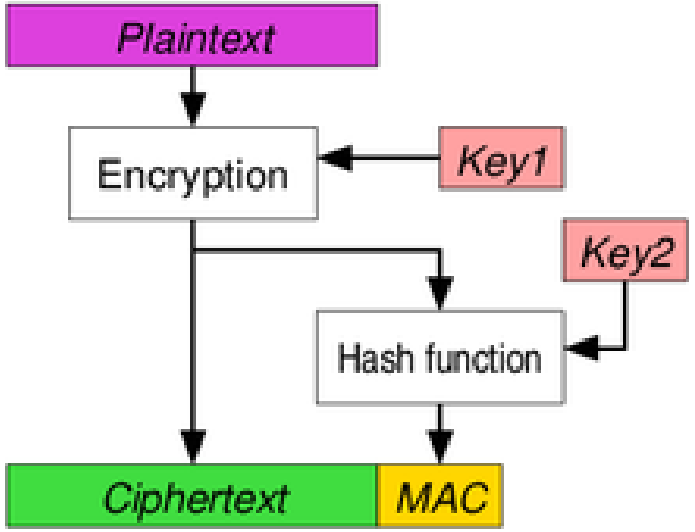
Network Time Security (NTS)

- Zabezpečená verzia NTP
  - s TLS a AEAD
- Authenticated Encryption with Associated Data (AEAD)
  - formou šifrovania, ktoré súčasne zaisťuje dôvernosť a autenticitu údajov

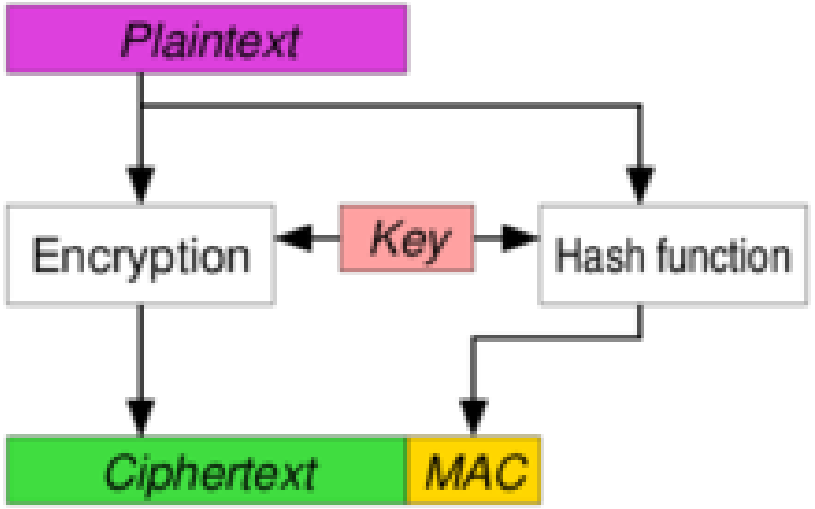
AEAD - Authenticated Encryption with Associated Data

- vyžadované napríklad sieťovými paketmi alebo rámcami, kde
  - **header** potrebuje viditeľnosť
  - **payload** potrebuje dôvernosť
  - a **oba** potrebujú integritu and autenticitu
- MAC = message authentication code

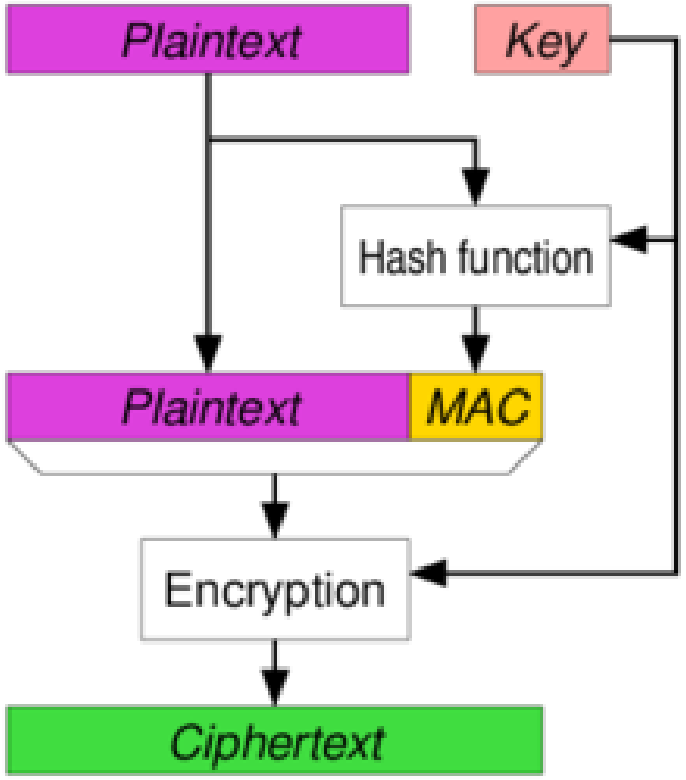
Encrypt-then-MAC (EtM)
used in SSHv2



Encrypt-and-MAC (E&M)
used in SSH



MAC-then-Encrypt (MtE)
used in TLS/SSL



https://en.wikipedia.org/wiki/Authenticated_encryption

Syslog útoky

ČO vie o protokole aj threat actor (TA):

- Syslog je dôležitý pre monitorovanie bezpečnosti
  - => syslog servery môžu byť cieľom pre aktérov hrozieb.

PREČO je to pre TA zaujímavé:

- Útočníci sa snažia utajiť, že dochádza k exfiltrácii údajov
  - dokončenie **exfiltrácie údajov** môže trvať dlho
    - kvôli veľmi pomalým spôsobom tajného odcudzenia údajov zo siete, ktoré používajú
- Preto realizujú útoky na servery syslog
  - ktoré obsahujú informácie, ktoré by mohli viesť k odhaleniu zneužitia

AKO TA útočí:

- Hackeri sa môžu pokúsiť o
  - zablokovanie prenosu údajov z klientov syslog na servery
  - narušenie alebo zničenie údajov záznamu
  - manipulovanie so softvérom, ktorý vytvára a prenáša logy

OBRANA:

- Implementácia syslog-u novej generácie (ng), tzv. syslog-ng
  - ponúka vylepšenia, ktoré môžu pomôcť zabrániť niektorým zneužitiam, ktoré sa zameriavajú na syslog

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

Zneužitie protokolov používaných pri monitorovaní

NTP útoky

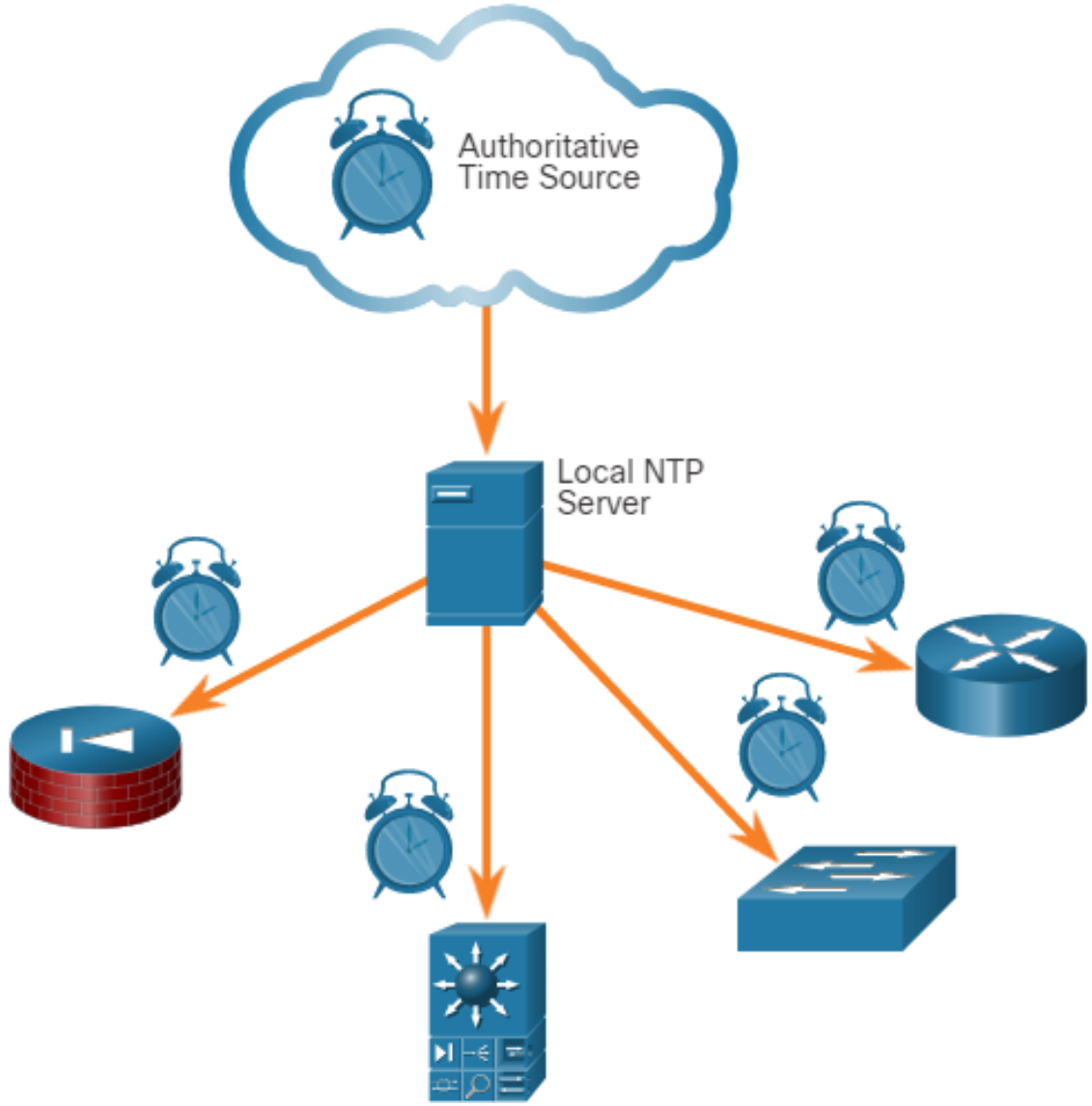
ČO vie o protokole aj threat actor (TA):

- NTP (udp, port 123) používa hierarchiu autoritatívnych zdrojov času
  - => na zdieľanie časových informácií medzi zariadeniami v sieti

PREČO a **AKO** TA útočí:

- Aktéri hrozieb sa môžu pokúsiť o
  - napadnutie **infraštruktúry** NTP
    - na poškodenie časových informácií používaných na koreláciu zaznamenaných sieťových udalostí
      - Expirovaný certifikát pre web… a ďalšie
  - použitie NTP systémov
    - na nasmerovanie DDoS útokov prostredníctvom zraniteľností v klientskom alebo serverovom softvéri

      = NTP amplifikačný útok



Zneužitie protokolov

NTP amplifikačný útok

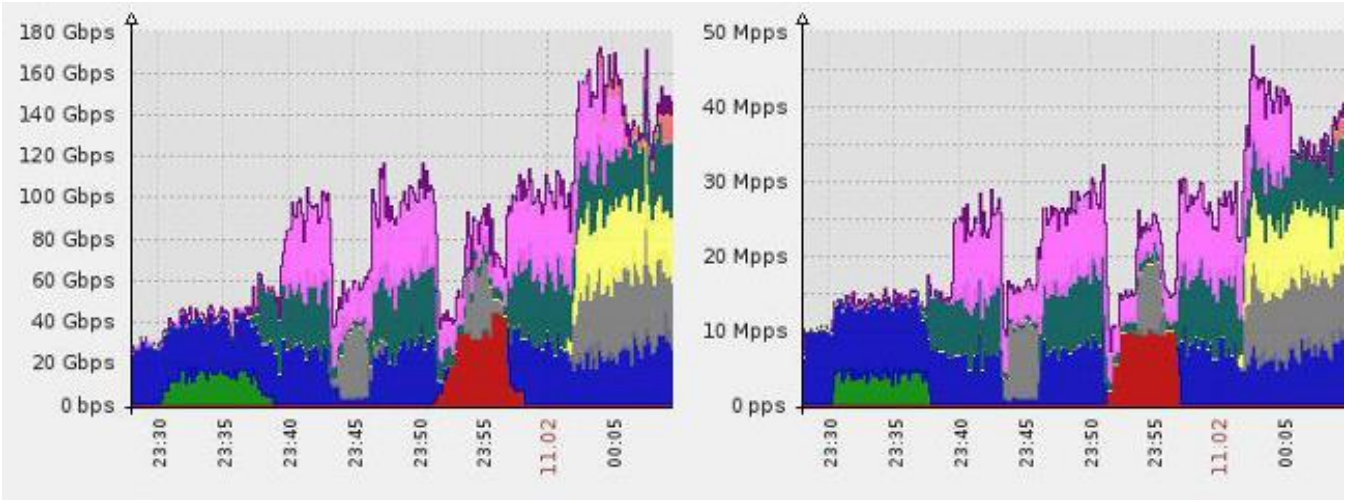
ČO využíva threat actor (TA):

- typ DDoS útoku
  - útočník využíva verejne prístupné NTP servery na zahltenie cieľa/obete UDP prenosom

AKO:

- Staršie verzie NTP podporujú okrem synchronizácie hodín aj službu monitorovania
  - umožňuje správcom dopytovať server NTP na počet prenosov
    - príkaz „get monlist“

      => pošle žiadateľovi zoznam posledných 600 zariadení
      - ktoré sa pripájajú k dopytovanému serveru
    - Odpoveď >> žiadosť
      - pomer veľkosti dopytu k veľkosti odpovede je medzi 20:1 a 200:1



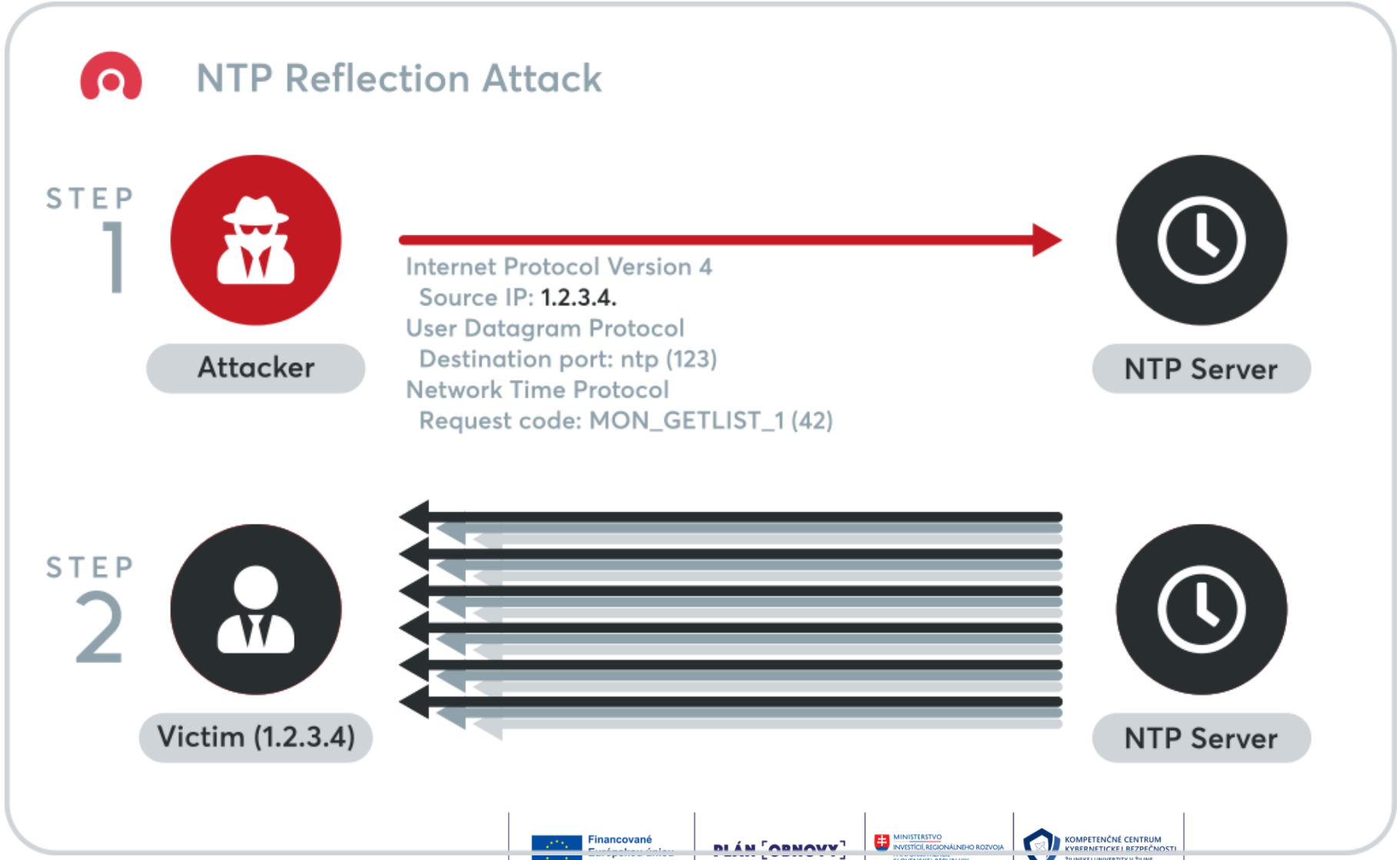
DÔSLEDOK:

- Útočník, ktorý ovláda 1 počítač s rýchlosťou 1 Gbps, by mohol efektívne nasmerovať 200 Gbps prevádzky na cieľový server

OBRANA:

- Náročné: zdanlivo legitímna prevádzka z platných serverov
- nadmerné poskytovanie a filtrovanie návštevnosti
- scrubbing (odkloniť a absorbovať)

NTP amplifikačný útok



Zneužitie bežných a legitímnych sieťových protokolov

DNS útoky

ČO využíva threat actor (TA):

- DNS zneužíva veľa typov malvéru
  - Napr. na komunikáciu s command-and-control (CnC) servermi a na exfiltráciu dát v prevádzke zamaskovanej ako bežné DNS dotazy

AKO TA realizuje útok:

- Malvér zakóduje ukradnuté údaje ako časť subdomény pri DNS dotazoch
  - pre doménu, kde je DNS server pod kontrolou útočníka
- Vyhľadanie DNS pre ‘long-string-of-exfiltrated-data.example.com’ by bolo preposlané na DNS server (kompromitovaný), ktorý spravuje doménu example.com
  - Server zaznamená ‘long-string-of-exfiltrated-data’ a odpovie späť na klienta kódovanou odpoveďou
  - Exfiltrované údaje sú zakódovaný text (v rámčeku hore)
  - Aktér hrozby zhromažďuje zakódované údaje, dekóduje ich, spojí, a získa prístup k celému súboru údajov

Zneužitie bežných a legitímnych sieťových protokolov

DNS

SOC analýza útoku:

- Je pravdepodobné, že časť subdomény takýchto žiadostí bude
  - **oveľa dlhšia** ako bežné požiadavky.
- Kybernetický analytik môže využiť **rozdelenie** dĺžok subdomén v rámci požiadaviek DNS
  - na vytvorenie matematického modelu, ktorý popisuje legitímne dĺžky domén (rozdelenie pravdepodobnosti)

OBRANA:

- Čo považovať za podozrivé:
  - DNS dotazy na **náhodne generované** názvy domén
  - **extrémne dlhé** náhodne sa objavujúce subdomény
    - Lepšie: matematický model pre dĺžky domén, ktoré sa odlišujú od legitímnych
  - najmä ak ich **výskyt** v sieti dramaticky **narastá**
- Na zistenie týchto stavov je možné **analyzovať DNS proxy logovacie záznamy**
- Alternatívne môžu byť na **blokovanie požiadaviek** na podozrivé CnC a zneužívanie domén použité služby ako *Cisco Umbrella passive DNS* a mnohé ďalšie.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Alternatívne riešenia od rôznych výrobcov

- **Palo Alto Networks – DNS Security**
  - **DNS Security** je súčasťou Palo Alto firewallov a Prisma Access. Poskytuje:
    - detekciu DNS tunelovania (analýza dĺžky subdomén, entropia, správanie)
    - blokovanie malvérových domén pomocou WildFire a ML
    - integráciu s **PAN Threat Intelligence Cloud**
- **Cloudflare Gateway / Cloudflare One**
  - Cloudflare má **DNS filtering** na úrovni edge siete:
    - analýza anomálií v DNS
    - blokovanie malvérových a C2 domén
    - pasívna DNS databáza od Cloudflare Research
    - detekcia náhodne generovaných domén (DGA)
- **Quad9 DNS**
  - Bezplatná služba zameraná na bezpečnosť:
    - DNS filtering na základe threat feedov (IBM X-Force, Packet Clearing House, atď.)
    - chráni pred malvérom, phishingom a C2 komunikáciou
    - vhodné pre menšie firmy alebo ako doplnok
- **Fortinet – FortiGuard DNS Filtering**
  - Fortinet poskytuje:
    - DNS filtering s reputáciou
    - detekciu DNS tunnelingu
    - integráciu so sandboxom FortiSandbox
- A iné
  - Infoblox BloxOne Threat Defense
  - Akamai Enterprise Threat Protector
  - DomainTools / Farsight DNSDB
  - Zscaler DNS Security
  - Trend Micro DNS filtering

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

Zneužitie bežných a legitímnych sieťových protokolov

HTTP (dnes už neaktuálne, uvedieme pre úplnosť)

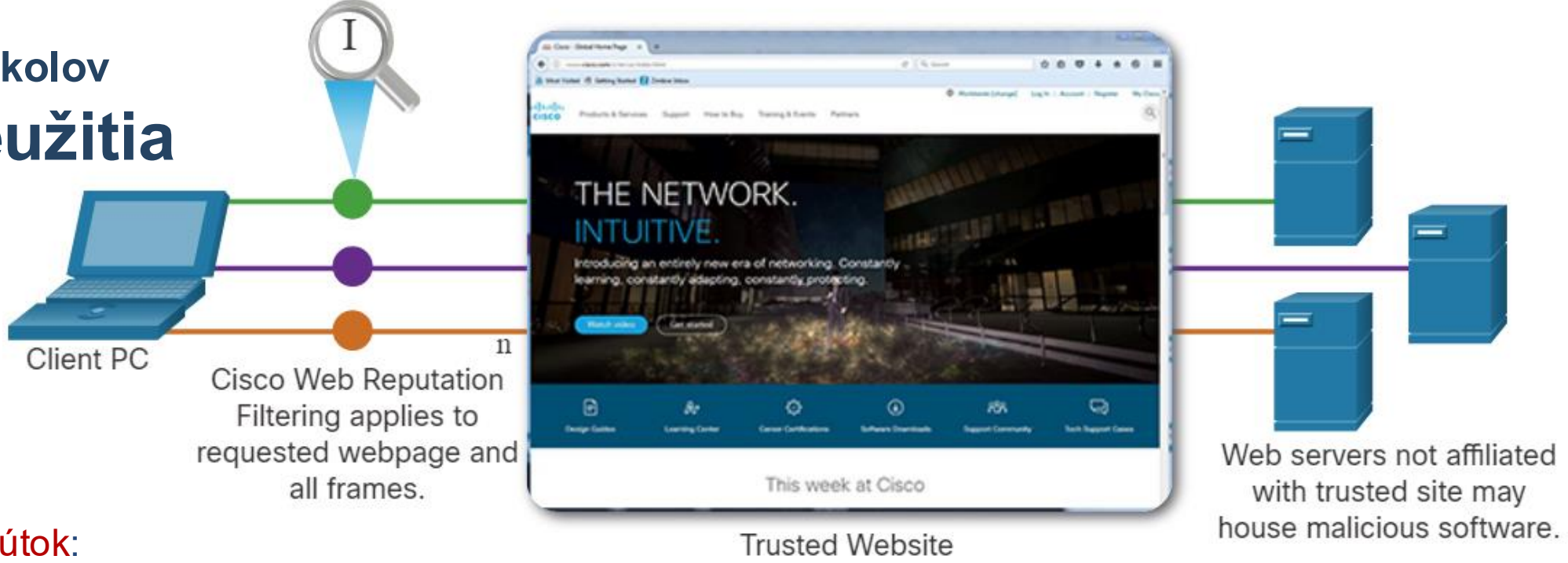
ČO vie o protokole každý... aj threat actor (TA):

- Hypertext Transfer Protocol (HTTP) je hlavný protokol siete World Wide Web.
- Všetky informácie prenášané v protokole HTTP sa prenášajú v obyčajnom texte zo zdrojového počítača do cieľa na internete.
- HTTP nechráni údaje pred zmenou alebo zachytením škodlivými stranami, čo predstavuje vážnu hrozbu pre súkromie, identitu a bezpečnosť informácií.
- Všetky aktivity prehliadania by sa mali považovať za rizikové.

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

Zneužitie protokolov

HTTP zneužitia



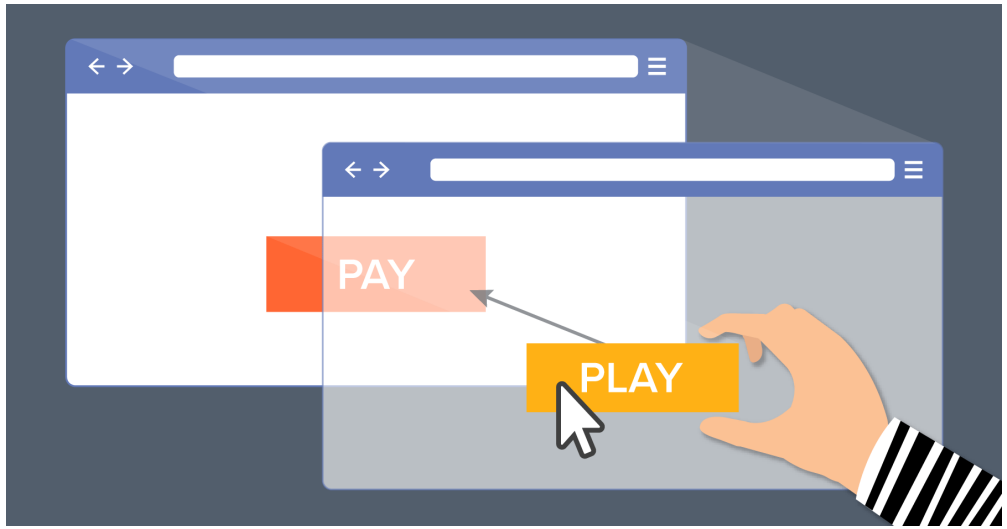
AKO TA realizuje útok:

- iFrame (inline frame) injection
  - aktér hrozby kompromituje webový server
  - a nasadí škodlivý kód
    => ktorý vytvorí neviditeľný iFrame na bežne navštevovanej webovej stránke.
- iFrame **sa načíta** => malware je **stiahnutý**
  - často z **inej adresy URL** ako z webovej stránky, ktorá obsahuje kód prvku iFrame.
- Služby zabezpečenia siete dokážu zistiť:
  - kedy sa webová lokalita pokúša odoslať obsah z nedôveryhodnej webovej lokality klientskému zariadeniu
    - aj keď je odoslaná z prvku iFrame.
  - Napr.: Cisco Web Reputation filtering, a ďalšie riešenia

OBRANA:

- používať HTTPs a zakázať iFrame v HTTP
  https://www.w3.org/TR/CSP2/#directive-frame-ancestors

HTTP a HTTPS



- **Content-Security-Policy** (CSP) s rámcovými predkami (frame-ancestors)
  - Hlavička HTTP CSP bola pôvodne vyvinutá na ochranu pred XSS a inými útokmi vkladania údajov
  - Poskytuje však aj direktívu rámcových predkov
    - na špecifikovanie zdrojov, ktoré majú povolené vložiť stránku
    - v prvku <frame>, <iframe>, <object>, <embed> alebo <applet>
    - Syntax je jednoduchá:

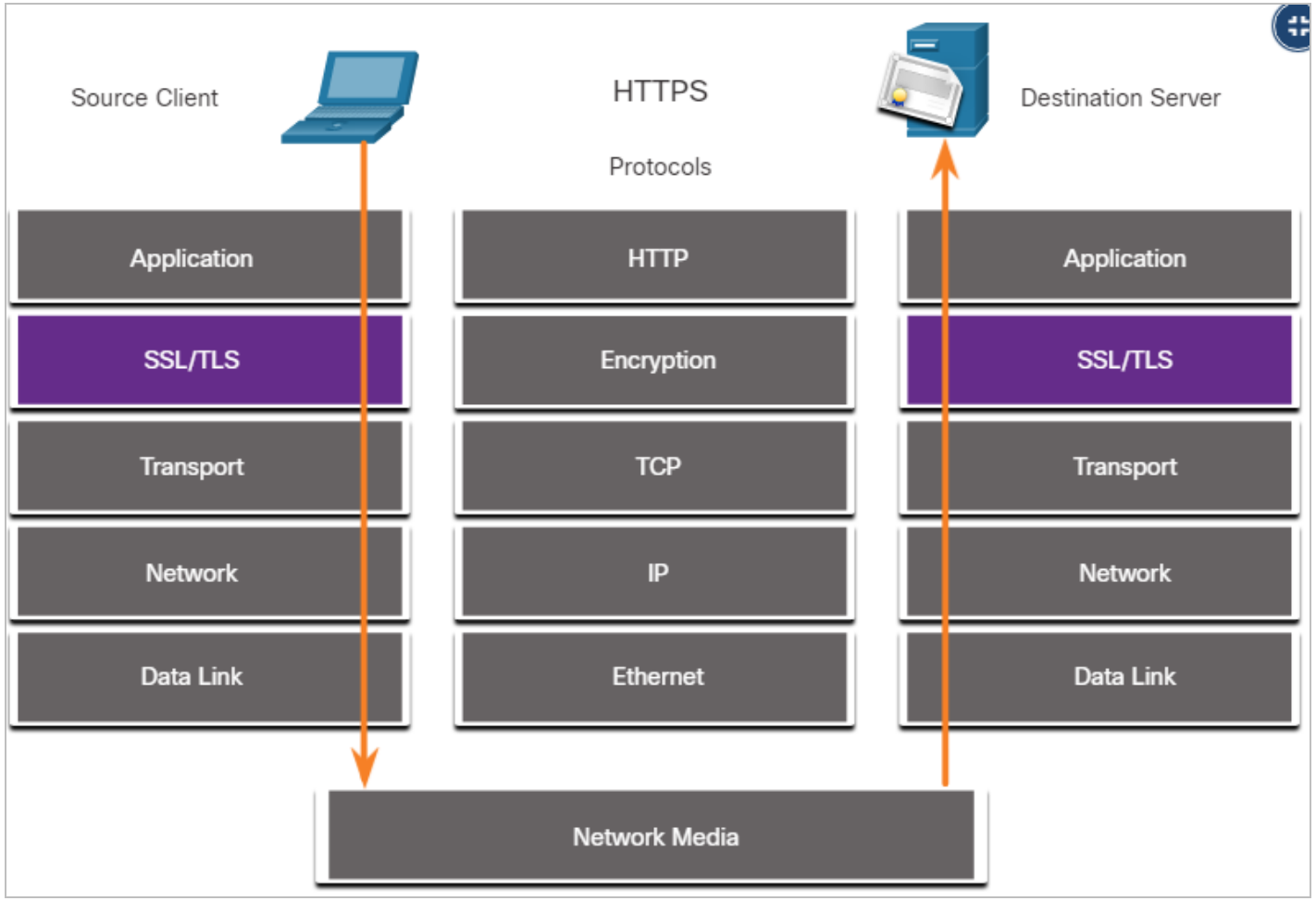
Content-Security-Policy: frame-ancestors <source1> <source2> ... <sourceN>;

Ochrana bežných a legitímnych sieťových protokolov

HTTPS

- implementovanie HTTPS-only
- HTTPS pridáva vrstvu šifrovania pomocou Secure Socket Layer (SSL)
- V dôsledku toho sú údaje HTTP nečitateľné
  - keď opúšťajú zdrojový počítač
  - až pokým sa nedostanú na server
- HTTPS **nie je mechanizmus na zabezpečenie webového servera**.
  - Zabezpečuje iba prenos protokolu HTTP počas prenosu

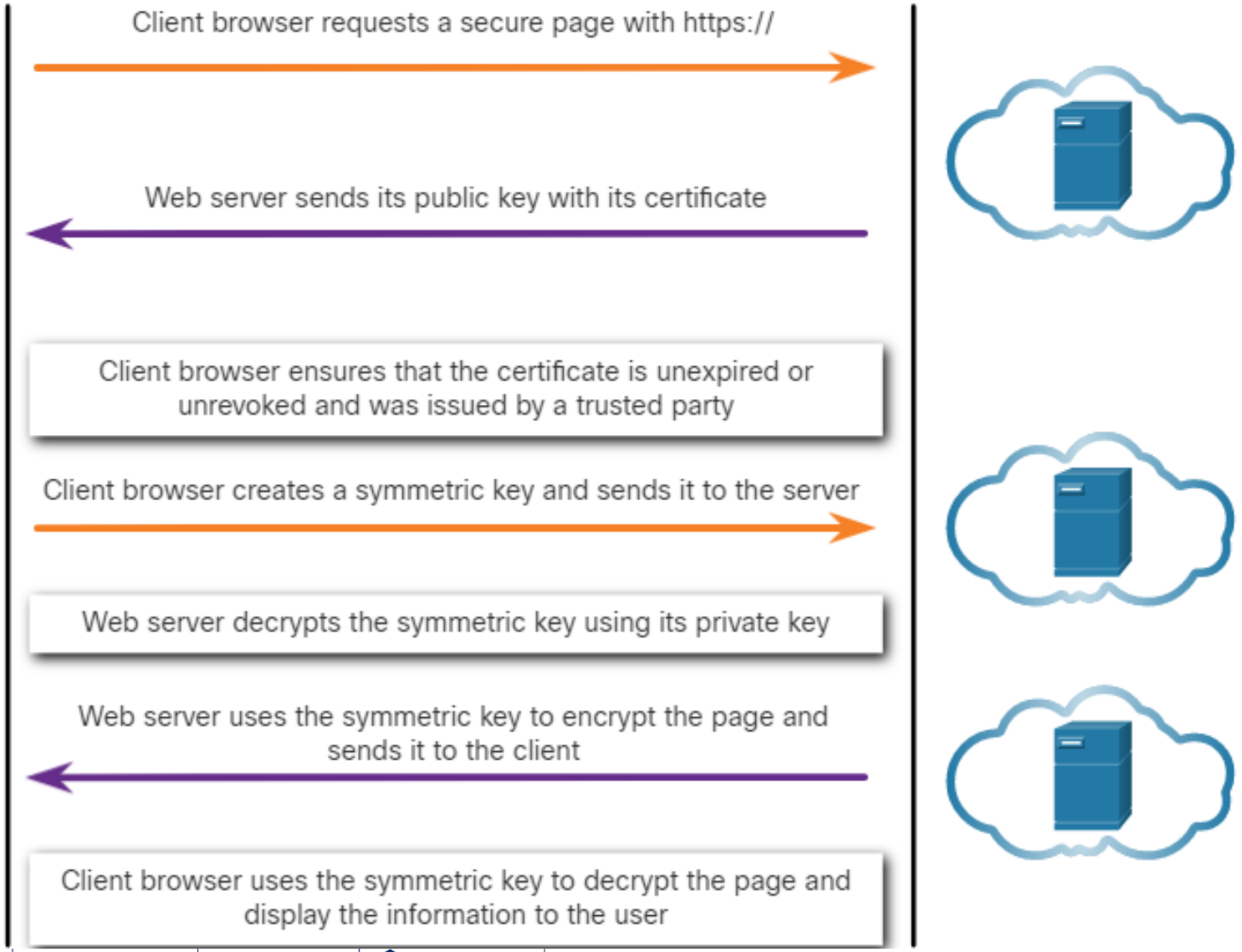
HTTPS Protocol Diagram



Problémy protokolov pre SOC analytikov

HTTPS

- šifrovaný prenos HTTPS **komplikuje** monitorovanie bezpečnosti siete
- Niektoré bezpečnostné zariadenia zahŕňajú dešifrovanie a kontrolu SSL
  - to však môže predstavovať problémy so spracovaním a ochranou súkromia
- HTTPS zvyšuje zložitosť pri zachytávaní paketov
  - kvôli dodatočným správam, ktoré sa podieľajú na vytváraní šifrovaného spojenia



Zneužitie bežných a legitímnych sieťových protokolov

Email protokoly

ČO využíva threat actor (TA):

- SMTP, POP3, IMAP
  - môžu aktéri hrozieb využiť na
    - šírenie malvéru
    - exfiltrovanie dát
    - poskytovanie kanálov malvérovým CnC serverom

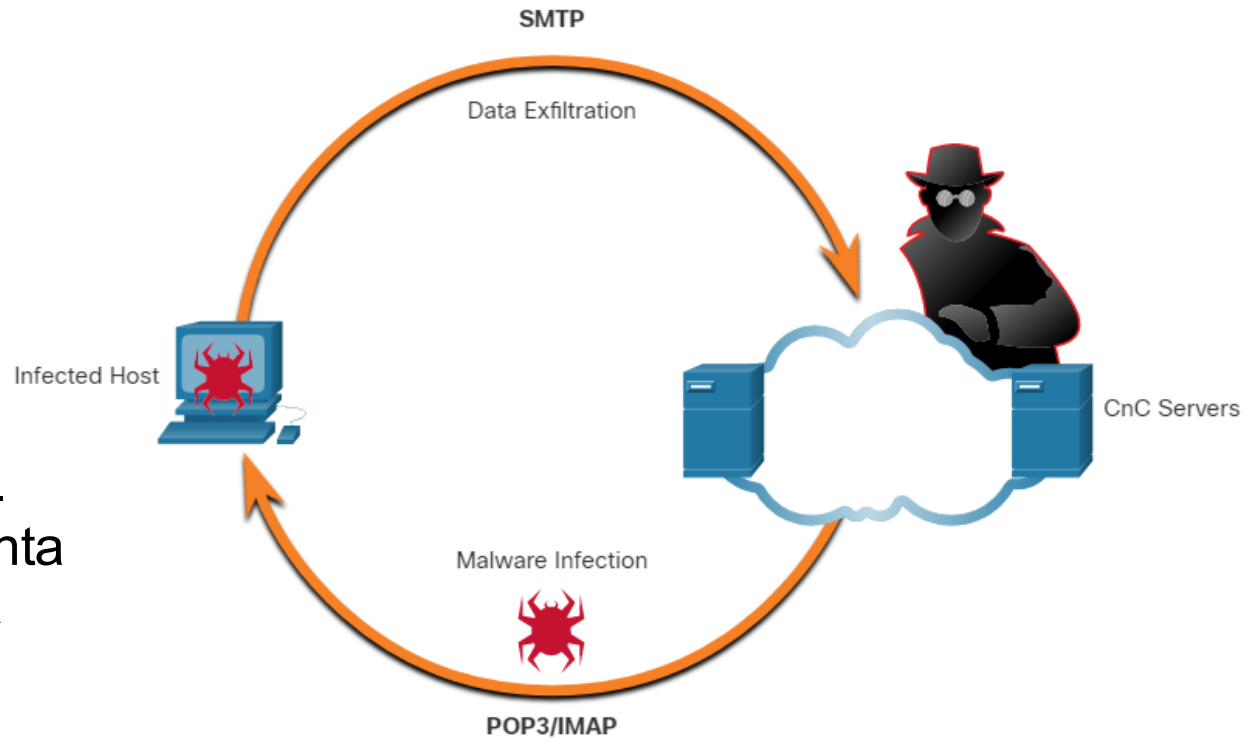
AKO TA realizuje útok:

- SMTP odosiela údaje z hostiteľa na poštový server a medzi poštovými servermi
  - Útočník môže využiť na exfiltráciu dát
- IMAP a POP3 sa používajú na sťahovanie e-mailových správ z poštového servera na klienta
  - Útočník môže zneužiť na stiahnutie malvéru na klienta

Možnosti SOC analýzy:

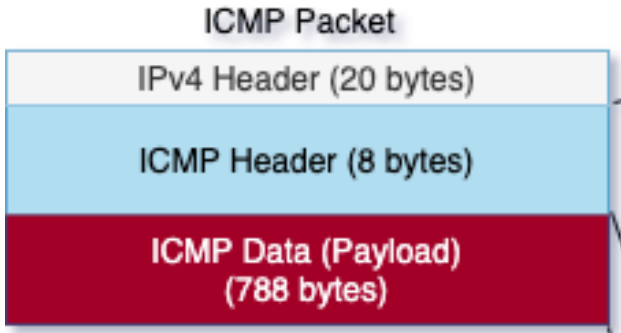
- Monitorovanie bezpečnosti dokáže identifikovať:
  - kedy sa malvérová príloha dostala do siete
  - Ktoré zariadenie bolo ako prvý infikované

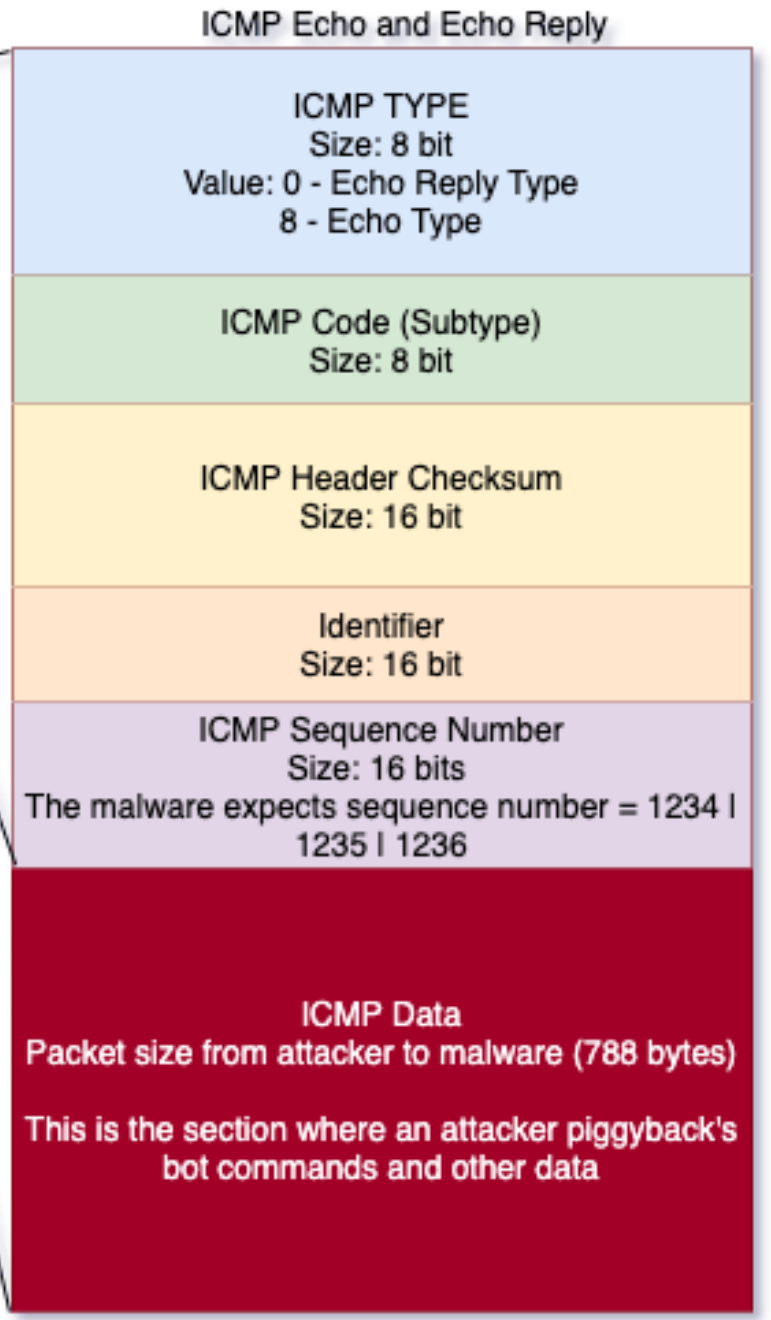
Hrozby e-mailového protokolu



Technológie a protokoly

ICMP





ČO využíva threat actor (TA):

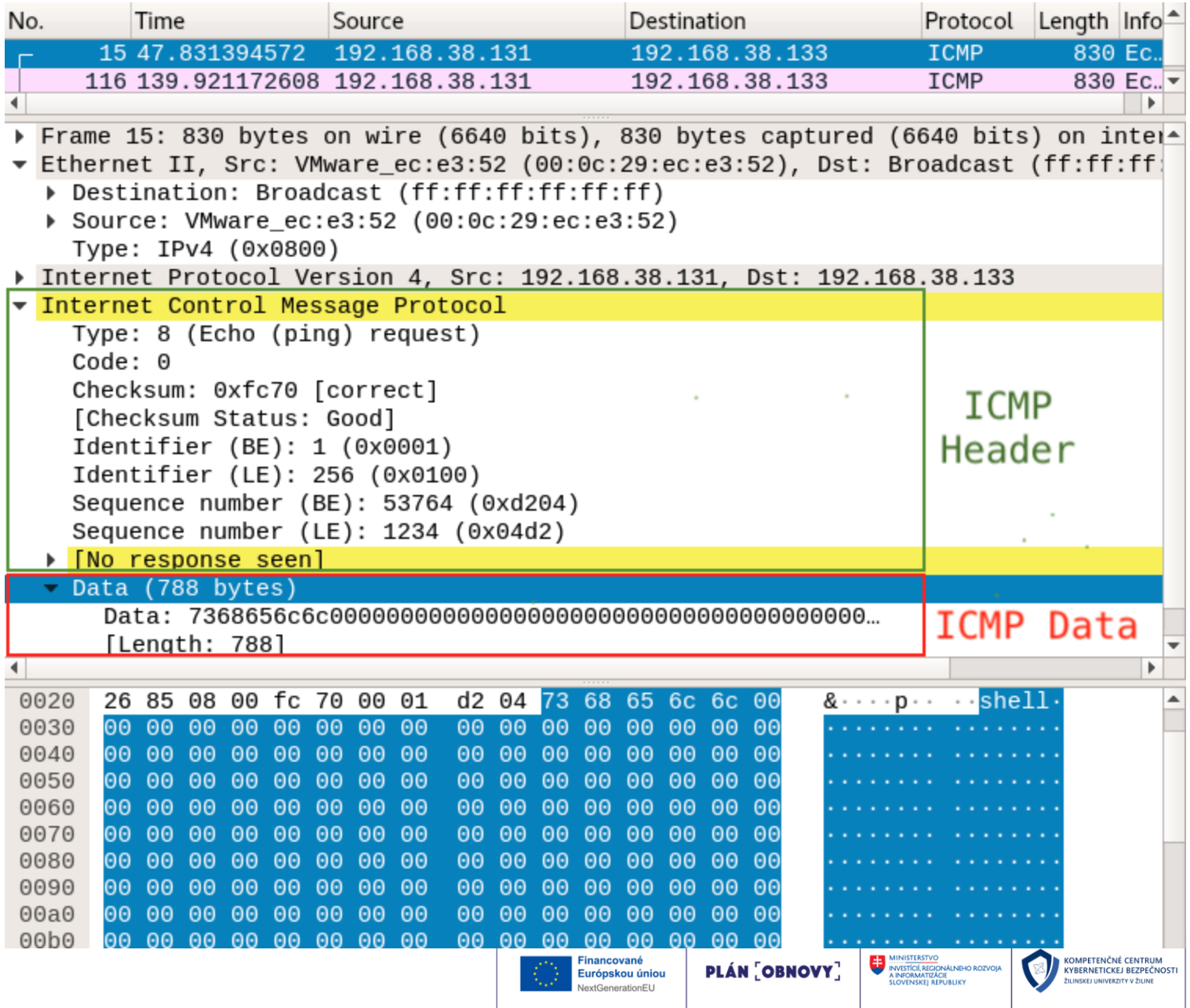
- ICMP môže byť použitý na
  - identifikovanie
    - zariadení v sieti
    - štruktúry siete
    - operačných systémov používaných v sieti
  - ako prostriedok pre rôzne typy DoS útokov.
  - na exfiltráciu dát
  - na prenos súborov z infikovaných hostiteľov k aktérom hrozieb pomocou vytvorených paketov (umelo vytvorené) = tunelovanie ICMP (niektoré typy malvéru)

OBRANA:

- **odmietnuť** službu **zvonku** siete
- Ale: ICMP prevádzka zvnútra siete je niekedy prehliadaná
  - a nemala by byť

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

ICMP tunneling analysis, backdoor at the end of ICMP tunnel



https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/backdoor-at-the-end-of-the-icmp-tunnel/

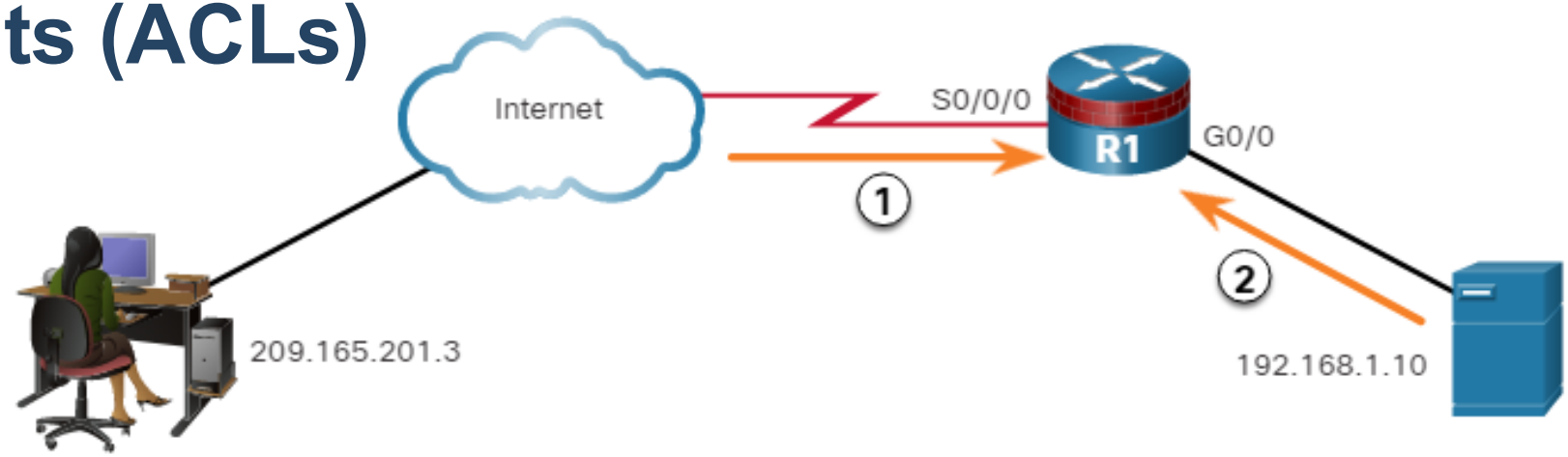
Bezpečnostné technológie

Ako bezpečnostné technológie ovplyvňujú schopnosť monitorovať bežné sieťové protokoly

Access control lists (ACLs)

- ACL a filtrovanie paketov:
  - sú technológie, ktoré prispievajú k množine sieťových bezpečnostných ochrán
- **source Quench**
  - pakety nie je možné posielať ďalej kvôli preťaženiu vyrovnávacej pamäte
  - TCP odosielateľ by mal zmenšiť svoje odosielacie okno, aby obmedzil odchádzajúci prenos.
- **parameter-problem**
  - nesprávne použitie IP Options

Zmiernenie zneužívania ICMP



1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

Zneužitie bezpečnostných technológií

ACLs

ČO využíva threat actor (TA):

- Útočníci môžu určiť, ktoré IP adresy, protokoly a porty sú povolené v daných ACL
  - buď skenovaním portov alebo penetračným testovaním, alebo prostredníctvom iných foriem prieskumu (reconnaissance attacks)

AKO TA realizuje útok:

- Útočníci môžu vytvárať pakety, ktoré používajú sfalšované zdrojové IP adresy (spoofed IP add)
- Aplikácie môžu vytvárať spojenia
  - na ľubovoľných portoch
  - s manipulovaným zavedeným príznakom v segmentoch TCP (established tag)

Problém pre obrancov:

- ACL pravidlá sa nedajú napísať tak, aby predvída všetky vznikajúce techniky manipulácie s paketmi
  - nedostatky bezpečnostných opatrení založených na pravidlách

OBRANA:

- S cieľom odhaliť manipuláciu s paketmi a reagovať na ňu, je potrebné:
  - sofistikovanejšie správanie
  - prijať kontextové opatrenia
  - zahrnúť ďalšie sieťové prvky do obrany

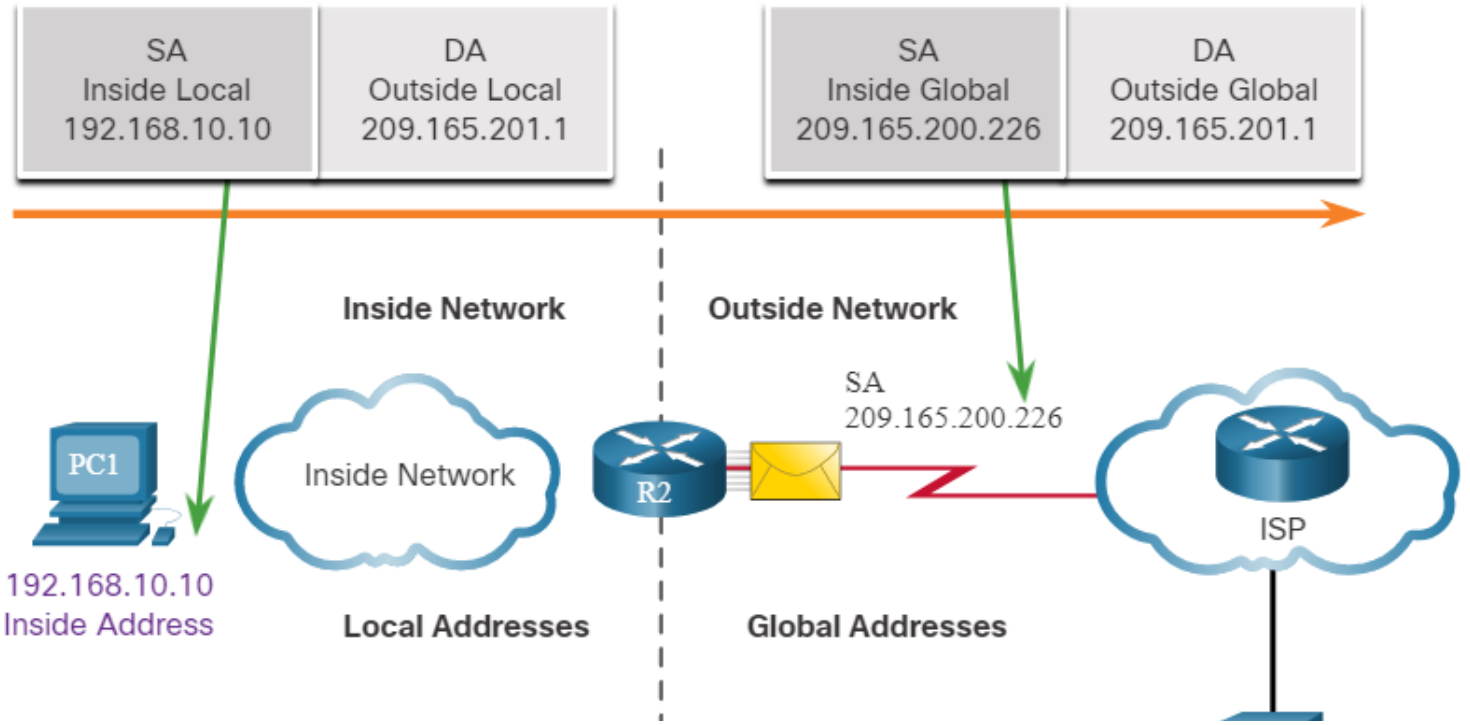
Pokročilé riešenia:

- Next Generation FW (NGFW)
- Antimalware Protection (AMP)
  - Ochrana pred vírusmi a škodlivým softvérom
- Email Security Appliance (ESA)
  - Filtrovanie nevyžiadaných e-mailov skôr, ako sa dostanú do koncového bodu
- Web Security Appliances (WSA)
  - Filtrovanie webových stránok a blacklisting
- Network Admission Control (NAC)
  - Vykonávať rozhodnutia o prístupe k sieti
  - Pripájať sa môžu iba autorizované a vyhovujúce systémy

NAT a PAT

PROBLÉM pre SOC analytikov:

- Tieto technológie môžu skomplikovať monitorovanie bezpečnosti
- Ak je PAT v platnosti, môže byť ťažké **logovať konkrétne vnútorné zariadenie**, ktoré požaduje a prijíma prenos, keď vstúpi do siete.
- Tento problém je prítomný aj v súvislosti s údajmi NetFlow
  - Toky NetFlow sú **jednosmerné** a sú definované adresami a portami, ktoré identifikujú



- PAT (Port Address Translation) prekladá viac interných IP → na jednu verejnú IP → rôzne porty.
- V logoch mimo perimetra (napr. upstream smerovač, NetFlow z ISP) sa vnútorná IP stratí.
- NetFlow je jednosmerný a používa iba IP + porty, takže bez doplnkových informácií nevieme spätne dohľadať pôvodnú internú IP.

Možné RIEŠENIA:

- Nič moc
- Byť si vedomý...
- Vykonávať monitorovanie v rámci našej siete (nie za NAT)

Financované Európskou úniou NextGenerationEU

Riešenia problému s NAT/PAT používané v SOC

1. **NAT logovanie (NAT logging / PAT translation logging)**
   - Najdôležitejší mechanizmus. Firewall / router loguje **mapovania**
   - Vendor riešenia:
     - Cisco ASA / FTD – NAT/PAT logging (connection build)
     - Palo Alto – Traffic Logs + NAT Logs (NAT Policy match logs)
     - Fortinet – Forward Traffic + NAT Translation logs
     - Check Point – NAT Session logs
     - Juniper SRX – Security Flow NAT logging
   - => SOC nástrojom tým umožníme korelovať verejný port späť na interné zariadenie.

2. **Exportovanie NAT informácií cez NetFlow/IPFIX**
   - **IPFIX** (rozšírený nástupca NetFlow) podporuje **NAT event recordy**. To znamená, že zariadenie môže posielať do SIEMu *aj preklady NAT/PAT*.
   - Vendor riešenia:
     - Cisco ASA – NSEL (NetFlow Security Event Logging)
     - Palo Alto – IPFIX NAT translations
     - Fortinet – IPFIX with NAT translation fields
   - Tieto NAT Eventy obsahujú napr.:
     - Original inside IP + port
     - Translated public IP + port
     - NAT rule number
     - Session ID
   - => SIEM tak vie spárovať flow s pôvodným zariadením.

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

Riešenia problému s NAT/PAT používané v SOC

3. Využívanie firewall session logs

- Keďže firewall *vidí oba smery komunikácie* (inside → outside), vie logovať celú session, vrátane NAT prekladu.

- V SIEM-e potom robíme koreláciu:
  - flow log (z perimeteru)
  - session log (z firewallu)
  - NAT translation event

- => Presné priradenie interného klienta.

4. Kombinácia DHCP logov a NAT logov

- Ak NAT log hovorí "192.168.1.50 → public_IP:port", ale 192.168.1.50 je pridelené dynamicky:
- potrebujeme aj **DHCP logy** na dohľadanie konkrétneho zariadenia / MAC adresy.

- => Bežný SOC workflow:
  NAT Log → interná IP → DHCP Log → hostname/MAC → používateľ

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

Riešenia problému s NAT/PAT používané v SOC

5. DNS logy pre doplnenie kontextu

- V SOC sa často na zistenie atribútov pri PAT používa aj:
  - DNS query logy
  - DNS proxy logy
- Pretože zariadenie pred vytvorením TCP session často robí DNS dotaz → ktorý už obsahuje internú IP.

6. Proxy (Web proxy) s autentifikáciou

- Ak organizácia používa proxy pre web požiadavky (napr. BlueCoat, Zscaler, Squid):
  - klient sa autentifikuje
  - proxy robí NAT za seba (nepoužíva sa PAT na firewall zar.)
  - logy obsahujú **užívateľské meno, internú IP** aj cieľ
- => riešenie aj pre web-based C2 a exfiltráciu, keďže moderné proxy poskytujú aj SSL inspection, kategorizáciu domén, reputáciu, blokovanie malvérových domén, sandboxing sťahovaných súborov,
- => Útočníkovi je oveľa ťažšie schovať C2 do HTTPS

7. Flow export z vnútornej strany (distribuovaný NetFlow)

- Ak chceme znížiť závislosť od NAT na perimetri:
  - nasadíme **NetFlow/ IPFIX na vnútornej sieti**
  - korelujeme vnútorné flow → NAT flow → externé flow
- Vendor riešenia:
  - Cisco FTD/Firewall inside interface flow
  - Palo Alto – inside zone IPFIX
  - Juniper – flow from trust zone

Čo proxy nedokáže úplne eliminovať

1. Non-web C2 stále prejde

- Proxy rieši len webový (HTTP/HTTPS) kanál.
  Útok môže bežať cez:
  - DNS tunneling
  - ICMP
  - Tor
  - custom TCP/UDP protokoly
  - TLS bez SNI alebo s domain fronting
  - cloud API (napr. AWS S3 endpoints) mimo HTTP proxy

2. Proxy nefunguje, ak klient obíde proxy

- Ak zariadenie:
  - má admin práva
  - používa hardcoded C2
  - používa vlastný TLS stack
  - alebo ide "direct" do internetu
    → Proxy to neuvidí (pokiaľ nevynucujeme transparent intercept + firewall rules).

3. Proxy môže mať problém sledovať QUIC/HTTP3

- HTTP/3 (QUIC/UDP) je problém, pretože väčšina proxy SSL inspection funguje iba pre TLS/HTTPS (TCP).

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

Problém so SNI v SOC

- SNI (Server Name Indication) je rozšírenie protokolu TLS, ktoré umožňuje klientovi už na začiatku šifrovaného spojenia prezradiť, ku ktorému hostname / doméne sa chce pripojiť.
- **Prečo existuje SNI?**
  - Keď sa cez HTTPS pripája klient na server, komunikácia je šifrovaná.

    Problém:
  - TLS handshake prebieha **predtým**, než sa nadviaže šifrované spojenie.
  - Server preto *nevie*, pre ktorú doménu má poslať certifikát (ak hostuje viac domén na jednej IP).
  - **SNI to rieši tým, že klient pošle názov domény už pri začiatku TLS handshaku.**
- SNI obsahuje jedno pole: **hostname (napr. www.example.com)**
  - Toto pole je *nešifrované* v klasickom TLS 1.2 / 1.3 → a teda viditeľné pre:
    - firewall
    - proxy
    - IDS/IPS
    - útočníka na ceste
    - sieťový monitoring
- **Prečo je SNI dôležité pre SOC?**
  - SOC analytici ho využívajú na:
    - **1. Identifikáciu cieľovej domény v šifrovanom HTTPS**
      - Napriek šifrovaniu v SOC vidíme, kam sa zariadenie pripája.
    - **2. Detekciu C2 komunikácie**
      - Malvér často komunikuje na podozrivé alebo novo registrované domény.
        SNI ich odhalí, aj keď je payload šifrovaný.
    - **3. Web filtering a kategorizáciu**
      - Proxy a firewally kategorizujú prevádzku podľa domény v SNI.
- **Nevýhody / obmedzenia SNI**
  - Niektoré malvéry SNI **schválne neodosielajú** (→ “TLS handshake anomaly”).
  - Útočníci môžu použiť **ESNI** (starší predchodca) **/ ECH** (Encrypted Client Hello, finálne riešenie, ktoré sa dnes používa/zavádza) na skrytie SNI.
  - Niektoré VPN protokoly SNI vôbec nepoužívajú → SOC tam nevidí doménu.

Problém s domain fronting pre SOC analýzy

- **Domain fronting** je technika, ktorú útočníci (ale aj legitímne aplikácie v minulosti) používajú na **skrytie skutočného cieľa komunikácie** pri HTTPS spojení.
- Používa sa najmä na:
  - **schovanie C2 komunikácie** (Command & Control)
  - obchádzanie cenzúry
  - obchádzanie firewallov a web filtrácie
- **Ako domain fronting funguje (jednoducho):**
- Pri HTTPS spojení sú 2 dôležité hostnames:
  - **SNI** (Server Name Indication) – viditeľný v nezašifrovanom TLS handshaku
  - **Host header** – skutočný cieľ v HTTP požiadavke (už šifrovaný)
- Pri domain frontingu sa tieto dve hodnoty **nezhodujú**.

- Útočník nastaví:
  - **SNI:** www.google.com
  - **Host header:** malicious-c2.example.com (skutočné C2)
- Firewall vidí iba SNI → vyhodnotí prenos ako komunikáciu na Google → *povolí*.
- Ale po nadviazaní TLS spojenia proxy/CDN na edge serveri presmeruje požiadavku na skutočný C2 server, ktorý je hostovaný za rovnakou CDN infraštruktúrou.
- **Dnes je domain fronting obmedzený**
  - Väčšina veľkých cloud providerov ho už **zakázala**:
    - Google – **blokuje od 2018**
    - Amazon CloudFront – **zakázal 2018**
    - Microsoft Azure – obmedzil
    - Cloudflare – obmedzené, ale *isté formy techník stále existujú*
- Útočníci však našli náhradné techniky.

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

Ako v SOC detegovať domain fronting?

- Domain fronting sa dá odhaliť podľa:
  - chýbajúceho / prázdneho SNI
  - podozrivého SNI (veľké známe domény, napr. google.com)
  - TLS handshake anomálií
  - abnormálneho objemu dát na SNI, ktoré bežne neumožňuje upload
  - porovnania SNI s IP-adresou (napr. google SNI, ale IP nepatrí Google)
  - EDR alertov (Cobalt Strike beaconing)

- **Nový problém pre SOC:**

  ECH (Encrypted Client Hello) – moderná techniku, ktorá má SNI úplne skryť pred firewallom (a je to pre SOC veľký problém).

ECH ako veľký problém pre SOC

- ECH = **Encrypted Client Hello**
  Nová technológia v TLS 1.3, ktorá **šifruje celý Client Hello**, vrátane:
  - SNI (Server Name Indication)
  - ALPN
  - supported cipher suites
  - extensions
- Dôležité:
  - Doteraz bolo SNI *nezašifrované* → firewall mohol vidieť, na akú doménu sa klient pripája.
  - S ECH je SNI **skryté**.

- **Ako ECH funguje (jednoducho):**
  - Prehliadač použije ECH public key publikovaný cez DNS HTTPS record.
  - Celý ClientHello (vrátane SNI) zašifruje.
  - Firewall vidí len “outer SNI” – väčšinou CDN doménu (napr. cloudflare.com).
  - Skutočná doména je ukrytá v encrypted ClientHello.

Čo to znamená pre SOC:

- **S ECH je detekcia výrazne ťažšia:**
  - Nevieme v SOC vidieť skutočnú doménu
  - firewall vidí len prístup na CDN (napr. Cloudflare, Fastly…)
  - Deep packet inspection je bez ECH key zbytočný
  - hrozby typu C2 over CDN, domain hiding, QUIC útoky sú efektívnejšie
- Útočníkom to **prinavracia možnosti domain frontingu**, hoci v inej forme.

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

Problém s modernými C2 kanálmi v SOC

Dnes je veľmi aktuálne mať čo najlepšie IOC charakteristiky moderných C2 kanálov, a sledovať vývoj.

Náhradné techniky útočníkov po zákaze domain frontingu

1. Domain hiding (iné ako domain fronting)

- SNI je *pravdivé* (napr. cdn.cloudflare.net)
- skutočný C2 je hostovaný *na tej istej CDN infraštruktúre*
- žiadny rozdiel medzi SNI a Host header → firewallu nič nesvieti
- **Výhoda pre útočníka:**
  Vyzerá to ako úplne legitímna komunikácia cez veľkú CDN.

2. C2 cez legitímne cloud služby (C2 over SaaS / C2 over cloud)

- Najčastejšie:
  - Cloudflare Workers / Pages
  - AWS API Gateway
  - Google Apps Script
  - Firebase
  - Dropbox
  - Telegram Bot API
  - Discord Webhooks
  - GitHub Gists
  - Slack API
- **Výhoda:**
  Protokol aj infraštruktúra je legitímna → ťažké blokovať bez poškodenia biznisu.

3. C2 cez CDNs (C2 via CDN / CDN proxying)

- Útočník použije CDN edge node ako **relay**.
  Najčastejšie používané:
  - Cloudflare
  - Fastly
  - Akamai
  - Firewally vidia iba CDN IP → nie skutočný backend.

4. C2 cez Encrypted DNS (DoH/DoT tunneling)

- DNS over HTTPS (DoH) slúži ako **tunnel** pre C2.
- **Podozrivé:**
  - veľa dát cez DoH
  - komunikácia s neštandardnými DoH endpointmi
  - exfiltrácia cez DNS payloady
- A mnohé ďalšie

Encryption, Encapsulation, a Tunneling

PROBLÉMY pre SOC analytikov:

- **Encryption** => problémy s monitorovaním bezpečnosti tým, že podrobnosti o paketoch sú nečitateľné
- **VPN** vytvára virtuálne point-to-point spojenie medzi sieťami cez verejné zariadenia
  - Encryption
    - je súčasťou technológií VPN -- IPsec sa používa na prenášanie šifrovanej prevádzky
    - robí prenos nečitateľným pre iné zariadenia okrem koncových bodov VPN

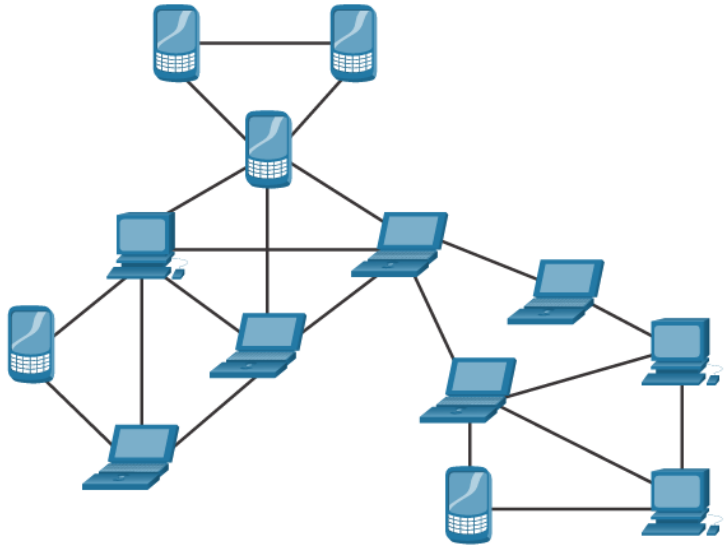
Ďalšie PROBLÉMY:

- Podobnú technológiu môžu použiť aktéri hrozieb (s malvérom) na vytvorenie
  - **virtuálneho point-to-point** spojenia **medzi interným klientom** (obeť) a zariadením **aktéra hrozieb**
  - šifrovaný tunel, ktorý funguje na **známom a dôveryhodnom protokole**
    - Aktér hrozby ho používa na exfiltráciu údajov zo siete

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

Zneužívanie sieťových technológií aktérmi hrozieb

Peer-to-Peer Networking



- P2P
  - používatelia pracujú v roli **klienta aj servera**
  - je vo svojej podstate **dynamický**
    - pripojenie k mnohým cieľovým IP adresám
    - môže tiež použiť dynamické číslovanie portov
- typy P2P aplikácií/operácií
  - zdieľanie súborov
    - **BitTorrent**
  - zdieľanie procesora
    - poskytnúť cykly procesora distribuovaným výpočtovým úlohám
    - príklady:
      - výskum rakoviny
      - pátranie po mimozemšťanoch
      - vedecký výskum
  - Instant messaging
    - Legitímna aplikácia v rámci organizácií, ktoré majú geograficky rozložené projektové tímy
  - **Bitcoin** je P2P operácia

PROBLÉM:

- Aktivita P2P siete sa môže vyhnúť firewallovej ochrane
- Známy a častý vektor šírenia malvéru

OBRANA:

- P2P aplikácie na zdieľanie súborov by nemali byť povolené v podnikových sieťach
- Používať špecializované aplikácie pre IM (platforma Cisco Webex, MS Teams, Zoom Team Chat, Slack, a iné), ktoré sú bezpečnejšie ako tie, ktoré využívajú verejné servery

Peer-to-Peer Networking

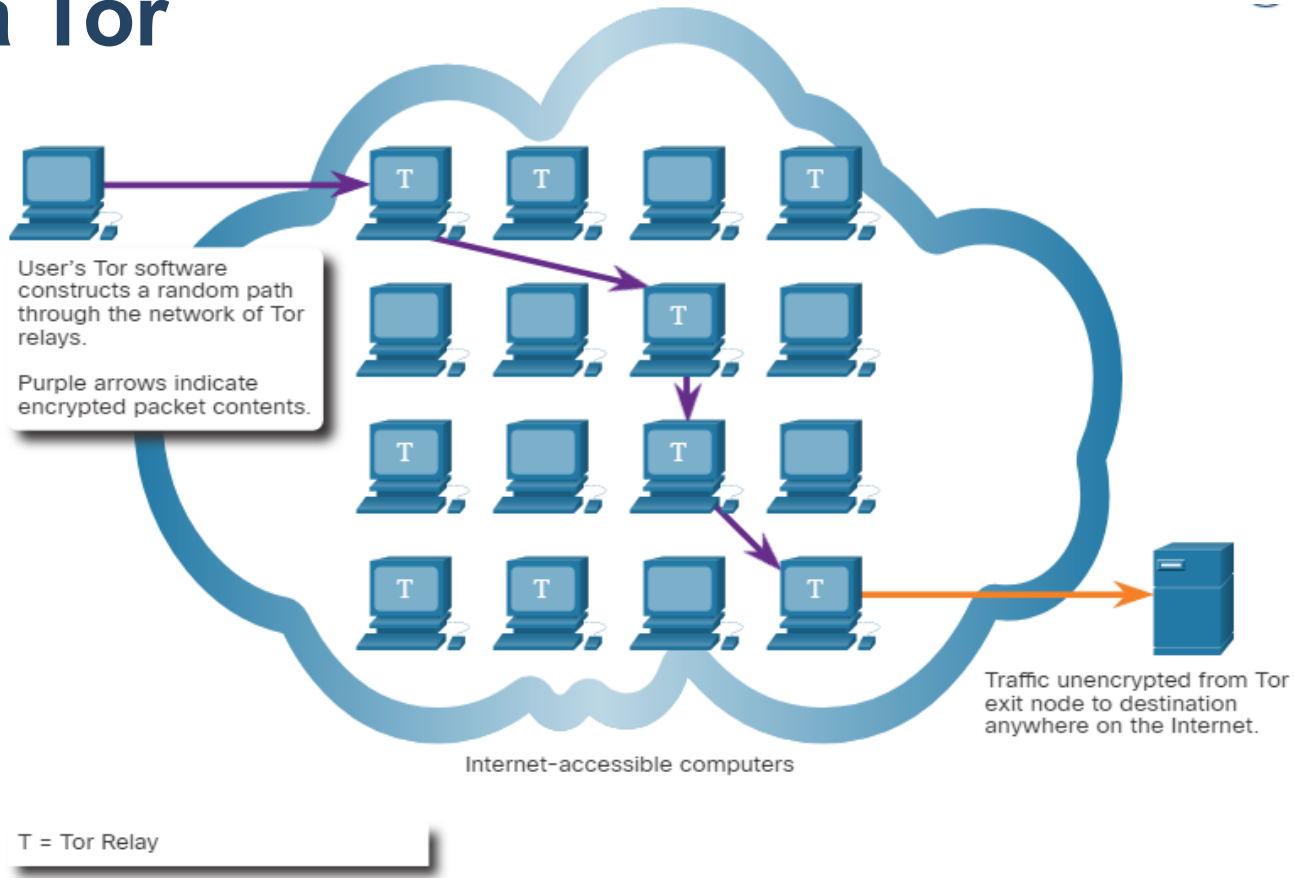
OBRANA:

- P2P aplikácie na zdieľanie súborov by nemali byť povolené v podnikových sieťach
- Používať špecializované aplikácie pre IM (platforma Cisco Webex, MS Teams, Zoom Team Chat, Slack, a iné), ktoré sú bezpečnejšie ako tie, ktoré využívajú verejné servery

- OBRANA - PREČO TO FUNGUJE (zatiaľ):
  - nemajú P2P prenos dát → všetko ide cez centrálne servery
  - poskytujú audit logy
  - sú monitorovateľné SIEM-om
  - integrujú sa s DLP
  - umožňujú blokáciu file sharingu
  - majú riadený onboarding / offboarding používateľov

Peer-to-Peer Networking a Tor

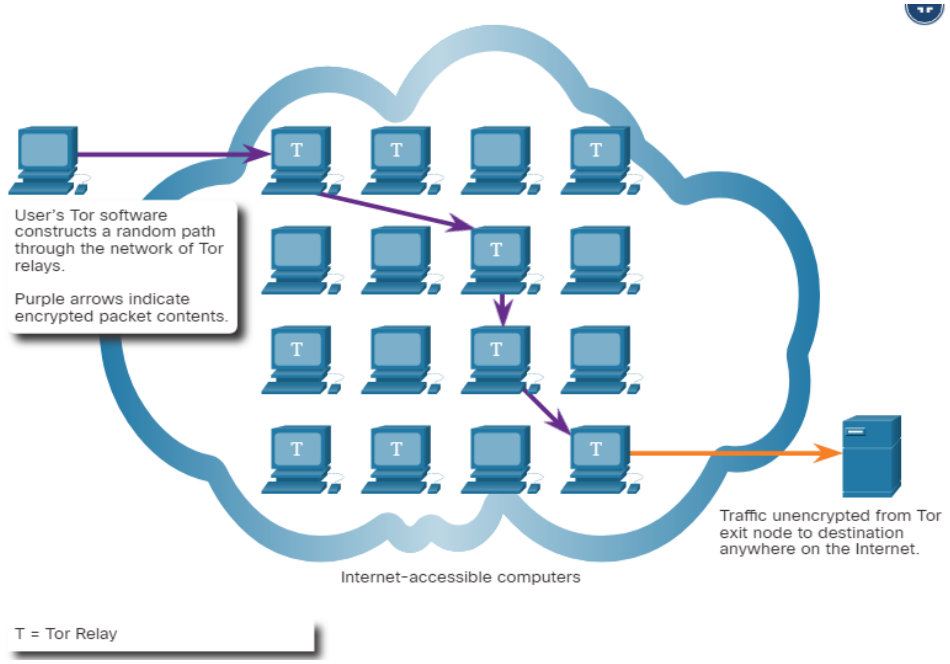
- Tor (The Onion Router)
  - softvérová platforma
  - sieť P2P používateľov/uzlov
  - používatelia fungujú ako internetové smerovače (Tor relays)
  - umožňuje používateľom anonymne prehliadať internet
    - je potrebný špeciálny prehliadač
- Keď začne prehliadanie webu, prehliadač vytvorí end-to-end cestu cez ToR sieť, pričom sa využíva:
  1. **Šifrovanie** - na zabezpečenie súkromia údajov v rámci siete Tor
  2. **Autentifikácia -** aby klienti vedeli, že komunikujú s tými Tor relays, s ktorým chcú (po ceste do cieľa),
  3. **Podpisy** - aby sa zabezpečilo, že všetci klienti poznajú rovnakú sadu Tor relays



Zneužívanie sieťových technológií aktérmi hrozieb

Peer-to-Peer Networking a Tor

- všetky pripojenia v Tor sieti používajú **TLS** šifrovanie
  - **PROBLÉM pre SOC analýzu**: pozorovatelia sa nemôžu pozrieť dovnútra, aby zistili, pre ktorý okruh je daná bunka určená
- Klient Tor vytvorí **dočasný šifrovací kľúč** s každým Tor relay v danom spojení/ceste
  - tieto extra vrstvy šifrovania znamenajú
    - že len výstupný Tor relay môže čítať pakety
  - Po skončení spojenia/komunikácie obe strany zničia kľúč, ktorý použili pre dané spojenie
    - **PROBLÉM pre SOC analýzu**: logovanie prevádzky a následný prieskum Tor relay pre zistenie kľúča nefunguje
- žiadne zariadenie nepozná celú cestu k cieľu
  - informácie o smerovaní sú čitateľné iba pre zariadenie, ktoré ich práve v tej chvíli potrebuje
- na konci cesty Tor sieťou, sieťová prevádzka dosiahne svoj cieľ, a pre odpoveď:
  - sa **znova vytvorí** šifrovaná cesta (layered path)



ĎALŠIE PROBLÉMY pre SOC analytikov:

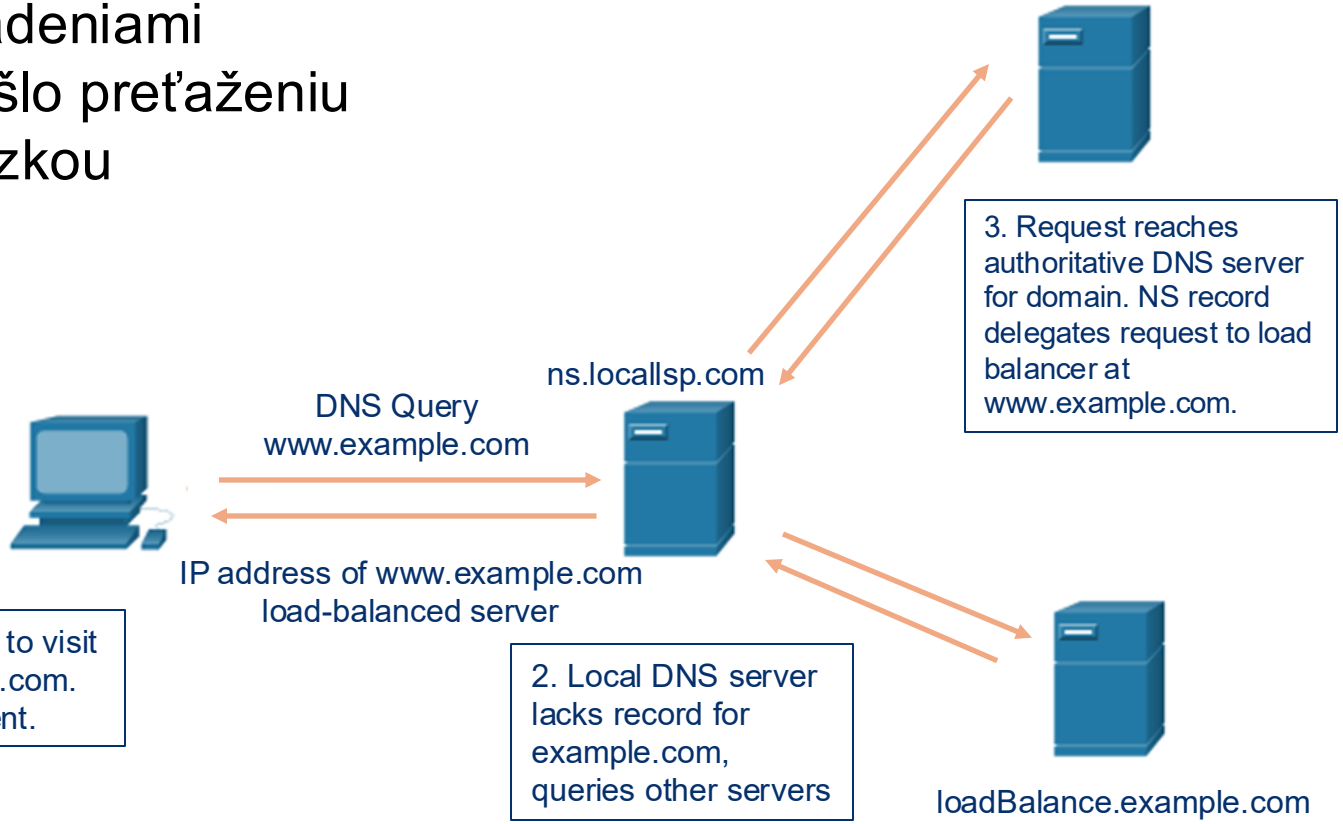
- Tor je široko používaný zločineckými organizáciami na "dark net"
- Tor býva použitý ako komunikačný kanál pre malvér CnC
- Vyhne sa tak obrane, ktorú obrancovia konfigurujú na bezpečnostných zariadeniach – tzv. blacklisting
  - *cieľová IP adresa* Tor prevádzky Tor je skrytá vďaka šifrovaniu
    - známy je len ďalší next-hop Tor uzol

Load Balancing

Vyvažovanie záťaže s delegovaním DNS

Čo vieme o tejto legitímnej sieťovej technológii:

- rieši rozdelenie prevádzky medzi zariadeniami alebo sieťovými cestami, aby sa predišlo preťaženiu sieťových zdrojov príliš veľkou prevádzkou
- Jedným zo spôsobov, ako to dosiahnuť, sú techniky využívajúce DNS
  - Odoslaním sieťovej prevádzky na také zdroje, ktoré:
    - majú rovnaký názov domény
    - ale viacero IP adries



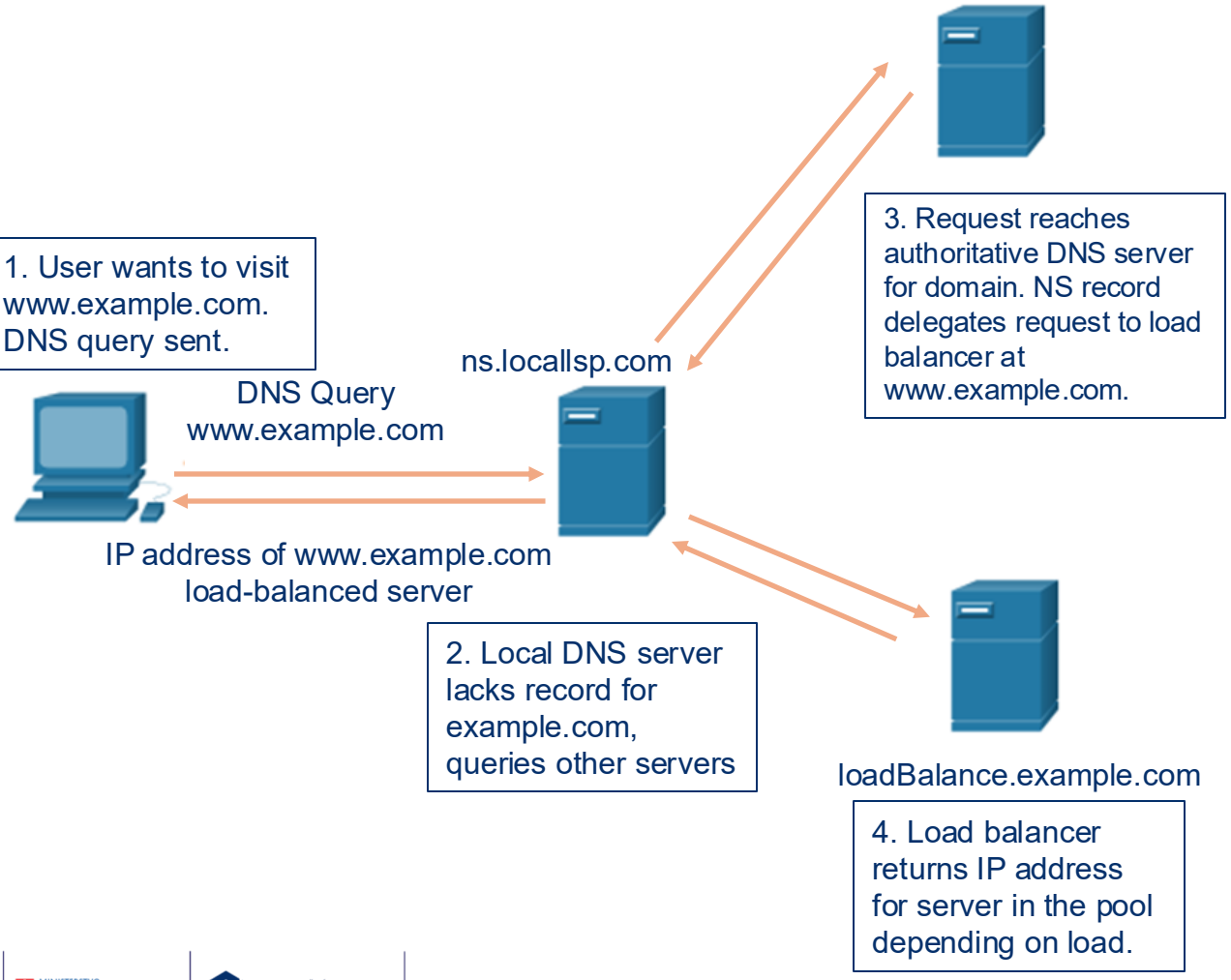
Rozdelenie výkonu

Vyvažovanie záťaže s delegovaním DNS

- V niektorých prípadoch môže rozdeľovanie prevádzky na viaceré servery, ktoré sú geograficky vzdialené, spôsobiť že:
  - výsledkom je **jedna internetová transakcia**
    - v ktorej sa ale vyskytujú **viaceré/odlišné IP adresy** v prichádzajúcich paketoch

  PROBLÉM pre SOC analytika:
    - to pri SOC analýze a monitorovaní môže spôsobiť, že sa v zachytávaní paketov objavia podozrivé charakteristiky
- Aby sa rozdeľovala prevádzka medzi také servery, ktoré vedia ešte obslúžiť požiadavky:
  - Používa sa tzv. **load balancing manager (LBM)**
    - ten používa sondu na testovanie:
      - výkonnosti rôznych ciest
      - funkčnosť rôznych zariadení
    - aby zistil, že servery fungujú, a vyhol sa odosielaniu prevádzky na zdroj, ktorý nie je dostupný

  PROBLÉM pre SOC analytika:
    - Tieto sondy sa môžu javiť ako podozrivá prevádzka
      - ak si SOC analytik neuvedomuje, že táto prevádzka je súčasťou prevádzky LBM



Riešenia pre SOC pri problémoch s Load Balancingom

Problém pre SOC	Príčina	Riešenie	Prínos pre SOC
Viaceré IP adresy v jednej transakcii	Geo-distribuované servery, CDN	**SIEM integrácia logov z load balancera** (F5, Citrix, Cloudflare,..)	SOC vidí presne, ktorý backend poskytol odpoveď.
Podozrivé health-check sondy	LBM testuje servery a linky	**Whitelisting IP rozsahov LBM a health-check uzlov** (AWS, Cloudflare, Azure)	Znižuje falošné poplachy, sondy sa označia ako legitímne.
Zmeny IP adries pri requestoch	DNS, Anycast alebo CDN routing	**DNS & CDN awareness** (Cisco Umbrella, Infoblox, DNSDB, Recorded Future)	SOC vie, že IP rotácia je normálna pre CDN.
Nemožnosť rozlíšiť podozrivú prevádzku od LB trafficu	Load balancer skrýva backendy	**NDR/NTA riešenia** (Corelight, Darktrace, Stealthwatch, ExtraHop)	Učia sa model správania LB, automaticky potláčajú false positives.
Nejasný tok requestov v aplikácii	LB → viacero backendov → rôzne lokality	**APM/Observability** (Datadog, Dynatrace, Elastic APM, New Relic)	SOC vidí celú cestu requestu (end-to-end tracing).
Podozrivé anomálie v packet capture	LBM preposiela traffic podľa dostupnosti	**SIEM korelácia a enrichment** (Sentinel, Splunk ES, Elastic SIEM)	Automaticky spája LB logy s network trafficom.
Nejasný NetFlow pri LB	Load balancer mení smerovanie podľa health checkov	**Enhanced Flow telemetry** (F5 IPFIX, Citrix AppFlow, Cisco NSEL)	Flow obsahuje informácie o backend serveri – viac kontextu pre SOC.
False positives pri failover udalostiach	LB presmeruje traffic na iný server	**Monitoring failover udalostí v SIEM**	SOC vie, že zmena bola legitímna, nie útok.

Zhrnutie

SOC monitorovanie je komplikované nielen útokmi, ale aj vlastnosťami bežných protokolov a bezpečnostných technológií. Úspech závisí od kombinácie **logov, kontextu, whitelisting-u a inteligentnej korelácie udalostí**.

Zhrnutie
- Bežné sieťové protokoly – problémy pre SOC

Protokol	Hlavný problém
Syslog	UDP môže stratiť logy, nesprávne zoradenie udalostí
NTP	Nesynchronizovaný čas → nesprávna korelácia logov
DNS	Exfiltrácia dát, C2, náhodné alebo dlhé subdomény
HTTP/HTTPS	Šifrovanie skrýva obsah, SOC vidí len IP, port, veľkosť
Email (SMTP/IMAP/POP3)	Phishing, malvér v prílohách, šifrované správy
ICMP	Tunelovanie dát, ale blokovanie bráni diagnostike

Zhrnutie
- Bezpečnostné technológie – problémy pre SOC

Technológia	Hlavný problém
ACL	Môžu vytvárať slepé miesta, maskovať laterálny pohyb
NAT / PAT	Menia zdroj IP/port → ťažké identifikovať interné zariadenia
Šifrovanie / VPN	Skrytie obsahu → SOC vidí len metaúdaje
Tunelovanie / Tor	Anonymizácia zdroja → SOC falošne hodnotí prevádzku
P2P siete	Skrytá prevádzka → riziko šírenia malvéru
Load balancery	Rotujúce IP, health-check sondy → falošné anomálie

Zhrnutie
- Bezpečnostné technológie – problémy pre SOC

- **Kľúčové odporúčania pre SOC**
  - Logy protokolov a bezpečnostných zariadení centralizovať do SIEM
  - Whitelist / tagovanie interných a infraštruktúrnych IP
  - Detekcia anomálií na základe správania, nie len IP/port
  - Používať metadata, TLS fingerprinting a APM/observability nástroje
  - Vzdelávať analytikov o špecifikách protokolov a technológií

Spoločná reflexia

1. Aké problémy prináša NTP pre monitorovanie?

- A) NTP neposkytuje časovú synchronizáciu
  B) Nesprávna synchronizácia vedie k nesprávnej korelácii logov
  C) NTP šifruje všetky pakety, SOC ich nemôže čítať
  D) NTP je iba pre lokálne siete a nie je relevantné

2. Prečo môže byť DNS zneužité na C2 (C&C) alebo exfiltráciu dát?

- A) DNS používa TCP, ktoré je vždy monitorované
  B) DNS dotazy sú vždy šifrované
  C) Útočník môže generovať podozrivé subdomény alebo tunelovať dáta cez DNS
  D) DNS neumožňuje záznamy typu TXT

3. Prečo HTTPS komplikuje detekciu útokov?

- A) HTTPS je pomalý protokol
  B) Šifrovanie TLS skrýva obsah, SOC vidí len IP a port
  C) HTTPS nefunguje cez NAT
  D) HTTPS vždy generuje logy

4. Aké výzvy prináša emailová komunikácia pre SOC?

- A) Email nikdy neobsahuje prílohy
  B) Phishing, malvér v prílohách, šifrované správy a spam
  C) Email je vždy šifrovaný a SOC ho nemôže monitorovať
  D) Email nevyžaduje NAT

5. Prečo je ICMP problematické v SOC?

- A) ICMP neexistuje v IPv6
  B) ICMP funguje len na localhost
  C) ICMP automaticky šifruje pakety
  D) ICMP môže byť zneužité na tunelovanie dát, ale úplné blokovanie môže narušiť diagnostiku

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

Problémy pri monitorovaní

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

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

Jana.Uramova@fri.uniza.sk