SYSTEMS LABORATORY

Curs 19

Securitatea LAN
Atacuri de rețea

RL
crunch it connected

Cybersecurity in 2023

RL
crunch it connected

- Exploits
  - Pegasus – zero-click exploit for iOS 16.0.3
    - https://en.wikipedia.org/wiki/Pegasus_(spyware)
  - SpinOK - 190 Adroid apps, 300 M downloadss
- Data breach
  - Twitter – 220M records (emails)
  - Shields Health Care Group – 2.3M records (medical and financial)
- DDoS
  - Blizzard – Diablo IV down 25.06.2023
  - Swiss gov websites – 15.06.2023

Recapitulare: Clasificarea atacurilor

- Internetul nu este un loc sigur
- Rețeaua locală poate fi oricând ținta unui atac:
  - De recunoaștere
    - Ping sweep
    - Sniffing
    - Port scan
  - De DoS (Denial of Service) sau DDoS (Distributed DoS)
    - Smurf attack
    - SYN flood
  - De acces
    - Atacarea unei parole (cu dicționar sau brute-force)
    - Buffer overflow
    - Man-in-the-middle

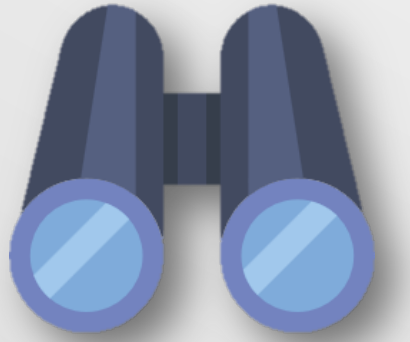
Atacuri de recunoaștere

- Scop
- nmap
- tcpdump
- Wireshark
- whois

RL
crunch it connected

Atacuri de recunoaștere

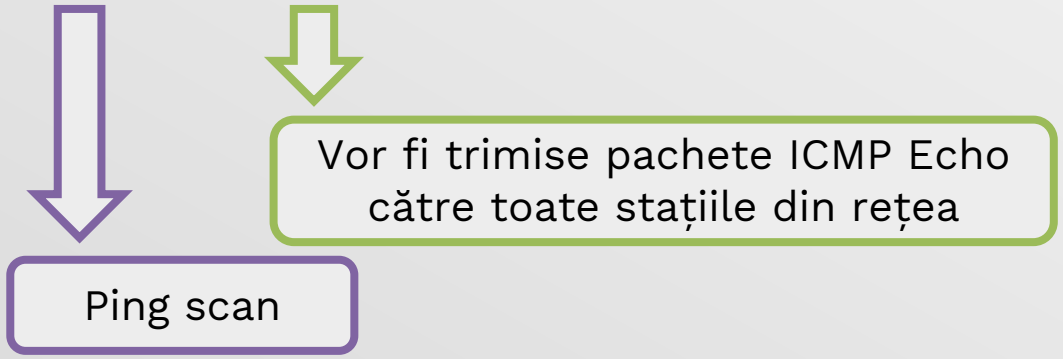
- Constau în recoltarea informațiilor despre o anumită rețea
- Se caută orice informație utilă care poate fi folosită în desfășurarea unui atac ulterior
- Exemple de informații utile unui atacator:
  - IP-urile stațiilor dintr-o rețea
  - Serviciile ce rulează pe fiecare stație
  - Locația serviciilor în care utilizatorii rețelei au încredere
  - Vulnerabilități în versiunile serviciilor



Utilitare de recunoaștere: nmap

- Permite scanarea stațiilor din rețea
- Poate descoperi:
  - Stațiile active (**Ping Scan**)

```
attacker# nmap -sP 141.85.227.0/24
```



- Informații despre sistemul de operare

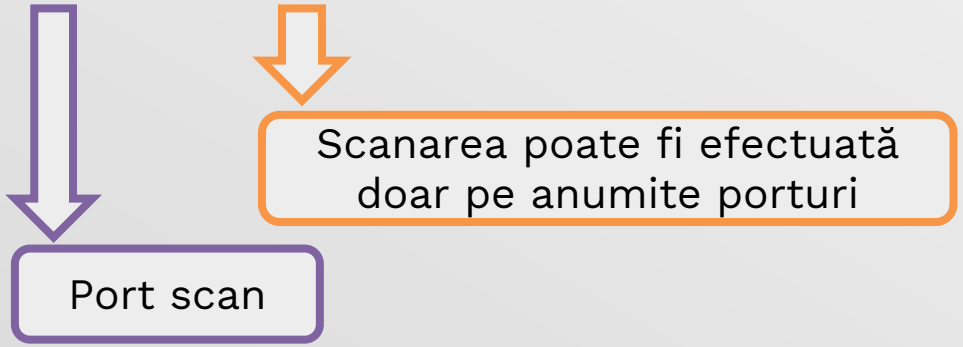
```
attacker# nmap -O 141.85.227.116
```

Utilitare de recunoaștere: nmap

RL
crunch it connected

- Permite scanarea stațiilor din rețea
- Poate descoperi:
  - Informații despre porturile deschise (**Port Scan**)

```
attacker# nmap -sP -p T:21-25,80 141.85.227.0/24
```



  - Informații despre servicii și versiunea acestora (**Service Scan**)

```
attacker# nmap -sV 141.85.227.118
```

Utilitare de recunoaștere: nmap


```
attacker# nmap -sV elf.cs.pub.ro

[…]
Interesting ports on elf.cs.pub.ro (141.85.227.116):
Not shown: 993 closed ports
PORT      STATE    SERVICE            VERSION
22/tcp    open     ssh                OpenSSH 5.5p1 Debian 6 (protocol 2.0)
25/tcp    open     smtp               Postfix smtpd
80/tcp    open     http               Apache httpd 2.2.16 ((Debian))
443/tcp   open     ssl/http           Apache httpd 2.2.16 ((Debian))
6881/tcp  filtered bittorrent-tracker
6969/tcp  open     http               BitTornado tracker T-0.3.18
20222/tcp open     ssh                OpenSSH 5.1p1 Debian 5 (protocol 2.0)
MAC Address: 00:18:51:6C:1F:9E (SWsoft)
Service Info: Host:  elf.cs.pub.ro; OS: Linux
[…]
```

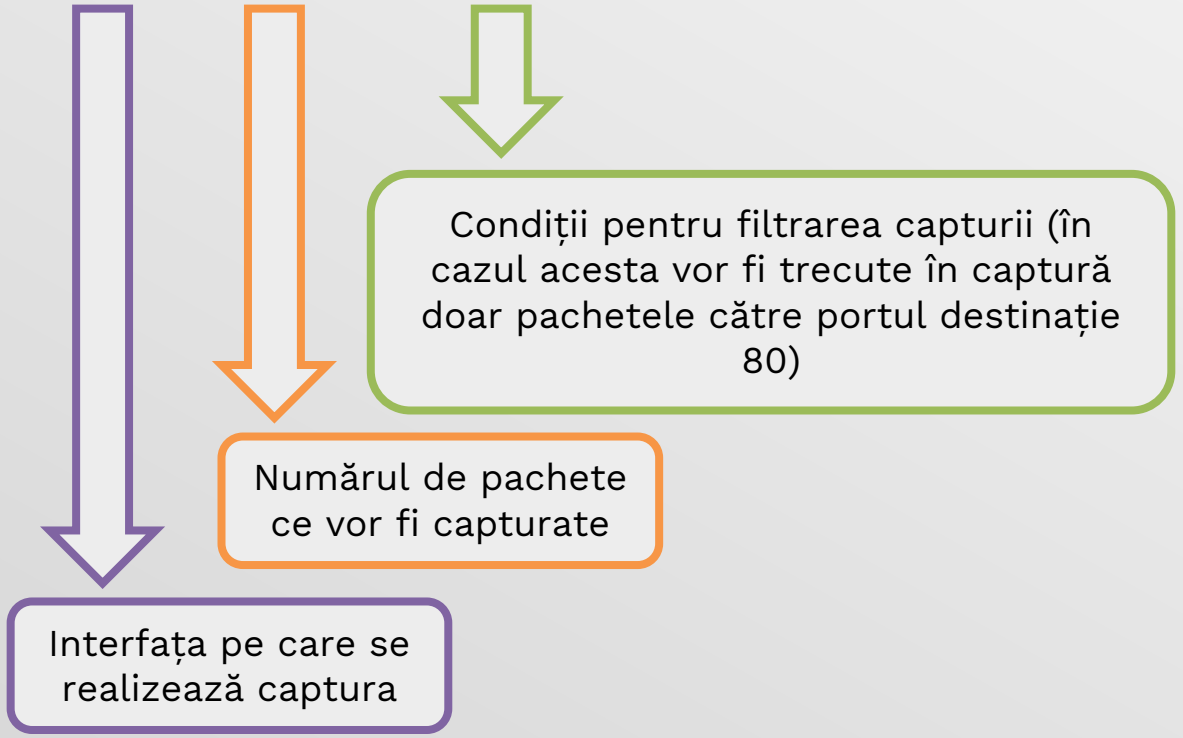
Utilitare de recunoaștere: Wireshark

- Permite interceptarea și analiza traficului de rețea
- Necesită trecerea interfeței de rețea în mod promiscuous
  - În acest mod este primit orice trafic (chiar și cel care nu este destinat stației locale)
  - Utilizează formatul libpcap
    - Permite deschiderea fișierelor de captură libpcap ale altor utilitare (tcpdump, dynagen)

Utilitare de recunoaștere: tcpdump

- Folosit pentru captura din linie de comandă a traficului

```
attacker# tcpdump -i eth0 -c 10 dst port 80
```



Utilitare de recunoaștere: whois

RL
crunch it connected

- Utilitar pentru serviciul **whois**
  - Permite obținerea informațiilor despre un domeniu

```
Registrant:
        Dns Admin
        Google Inc.
        Please contact contact-admin@google.com 1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6502530000 Fax: +1.6506188571

    Domain Name: google.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        DNS Admin
        Google Inc.
        1600 Amphitheatre Parkway
         Mountain View CA 94043
        US
        dns-admin@google.com +1.6506234000 Fax: +1.6506188571
```

Utilitare de recunoaștere: host

RL
crunch it connected

- Utilitar pentru serviciul **DNS**
  - Permite obținerea informațiilor despre serverele de nume și de mail ale unui domeniu

```
attacker# host -t MX pub.ro
pub.ro mail is handled by 5 mail.pub.ro.
pub.ro mail is handled by 50 relay.roedu.net.
```

```
attacker# host -t NS pub.ro
pub.ro name server pub.pub.ro.
pub.ro name server ns1.roedu.net.
pub.ro name server pub2.pub.ro.
```

Atacuri DoS

- Identificare
- DDoS
- Smurf attack
- TCP SYN flood
- CAM overflow

RL
crunch it connected

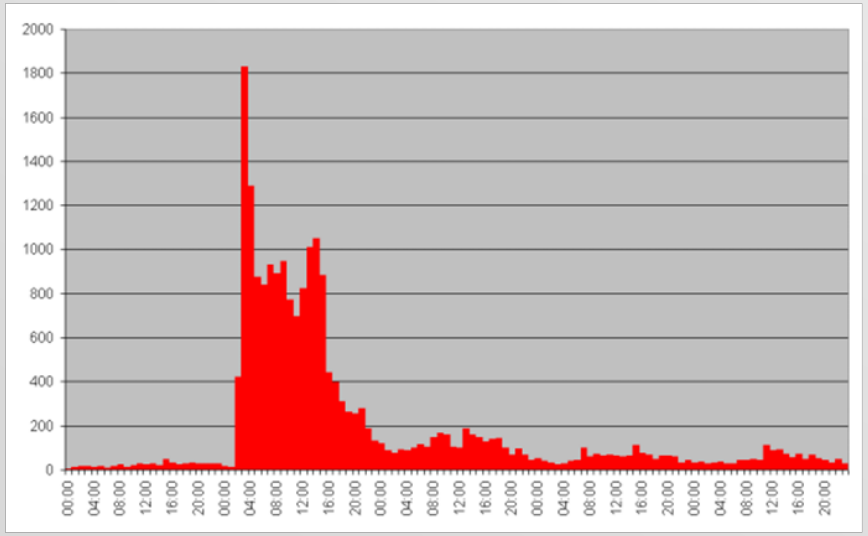
Identificare atacuri DoS

- Denial of service
- Se trimite un număr mare de cereri pentru a preveni procesarea cererilor normale
- Din cauza încărcării există inclusiv riscul ca aplicația să întâmpine o eroare și să se oprească
- Atacurile DoS se recunosc măsurând traficul în condiții normale
  - Apariția unei anomalii poate indica un atac DoS

Atacuri DDoS

RL
crunch it connected

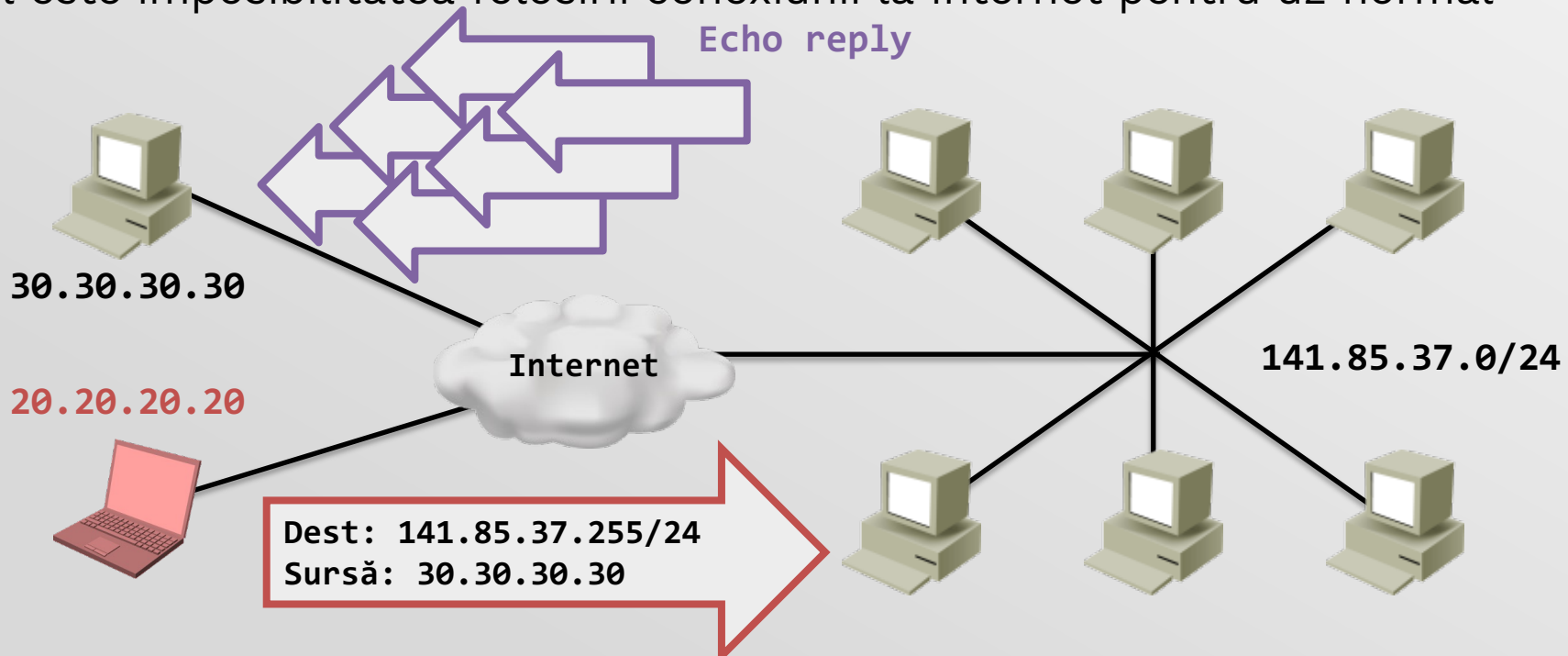
- Constau în trimiterea cererilor de la mai multe sisteme către o singură țintă
- Atacurile DoS/DDoS sunt dificil de identificat
  - Nu se poate determina mereu care sunt cereri valide și care reprezintă un atac
  - Exemplu de trafic valid cu rezultat de DoS: Slashdot effect



Exemplu de Slashdot effect

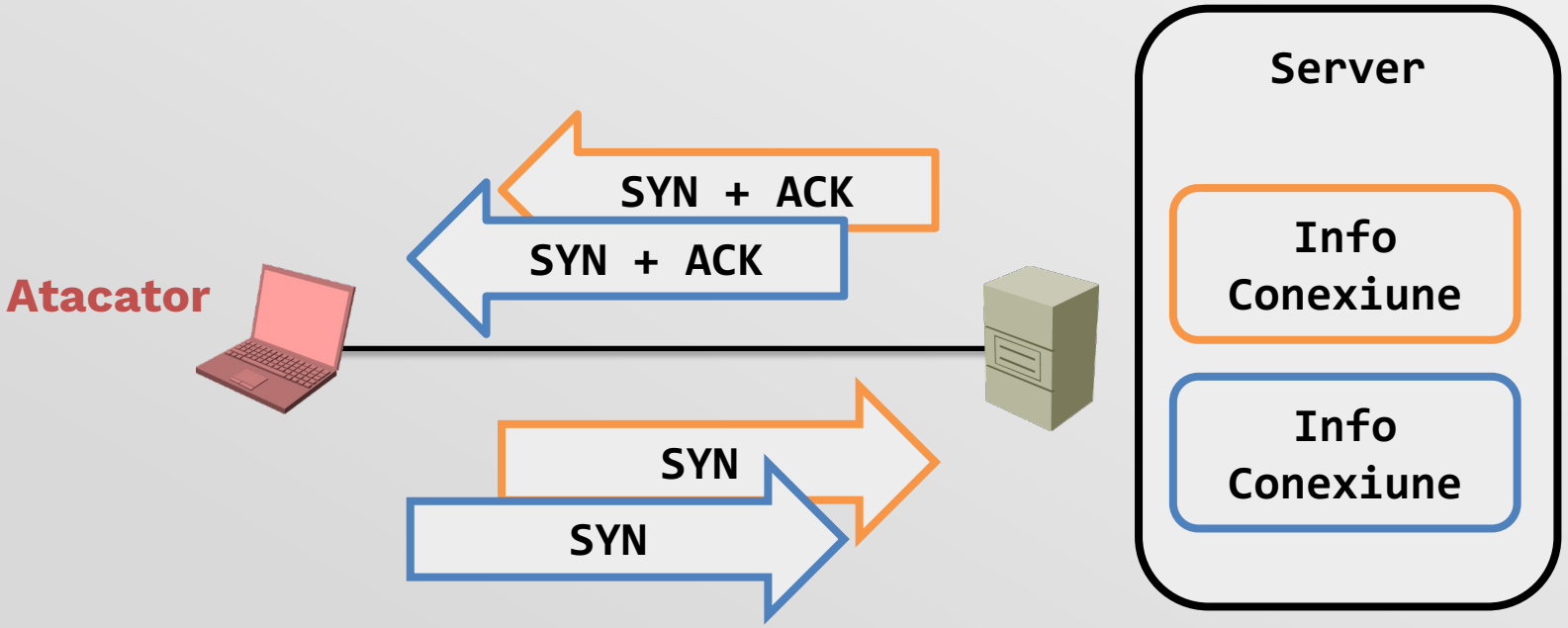
Smurf attack

- Ping-uri către o adresă de broadcast cu o adresă sursă spoofed
- Toate stațiile din rețeaua respectivă vor răspunde către sursă
- Dacă rețeaua este mare stația țintă poate să primească mai mult trafic decât poate procesa
  - Efectul este imposibilitatea folosirii conexiunii la Internet pentru uz normal



TCP SYN flood

- Atacatorul inițiază un număr mare de conexiuni TCP cu un server, fără a termina handshake-ul inițial (conexiuni half-open)
- Respectivele conexiuni epuizează resursele serverului
  - Acesta nu mai poate procesa cereri valide



CAM Overflow

RL
crunch it connected

- Ce este tabela CAM?
  - **R:** Tabelă folosită de switch-uri pentru a reține prin ce port se ajunge la o anumită adresă MAC
- Memoria unui switch nu e nelimitată:
  - Tabela CAM se poate umple
  - Dacă se umple, switch-ul va lucra în regim de hub
- Un atacator poate trimite un volum mare de cadre cu adrese MAC spoofed
- Ce adrese MAC trebuie falsificate pentru acest atac?
  - **R:** Switch-ul învață adresele MAC sursă, deci acestea trebuie falsificate
- Cum se poate opri acest atac?
  - **R:** Limitarea numărului de adrese ce pot fi învățate pe un port.

Atacuri acces

- Spargere de parole
- MITM
- Social engineering
- Exploatarea încrederii
- Buffer overflow
- VLAN hopping
- Atacuri STP

RL
crunch it connected

Spargere parole

RL
crunch it connected

- Parolele trimise în clar (Telnet) pot fi obținute prin **sniffing**
- Parolele cărora li s-a obținut hash-ul pot fi sparte prin:
  - **Brute force** (se încearcă toate combinațiile ce folosesc un set de simboluri)
  - **Dictionary attack** (se încearcă toate cuvintele din dicționar împreună cu permutări simple)
  - **Cryptanalysis attack** (**Rainbow tables**)
- Brute force / dictionary attack pot fi aplicate direct pe serviciul de autentificare, fără a avea hash-ul:
  - Ușor de blocat prin adăugarea de limitări la autentificare (de exemplu blocarea contului pentru 10 minute la 3 eșuări de autentificare în decurs de un minut)

Rainbow Tables

- Atac de criptanaliză
- Pentru spargere se pot folosi tabele de hash-uri precalculate → necesar prea mare de spațiu
- **Rainbow tables** mențin punctele de pornire pentru lanțuri de hash-uri

- Ideea este să se folosească spațiu pentru a economisi timp de rulare

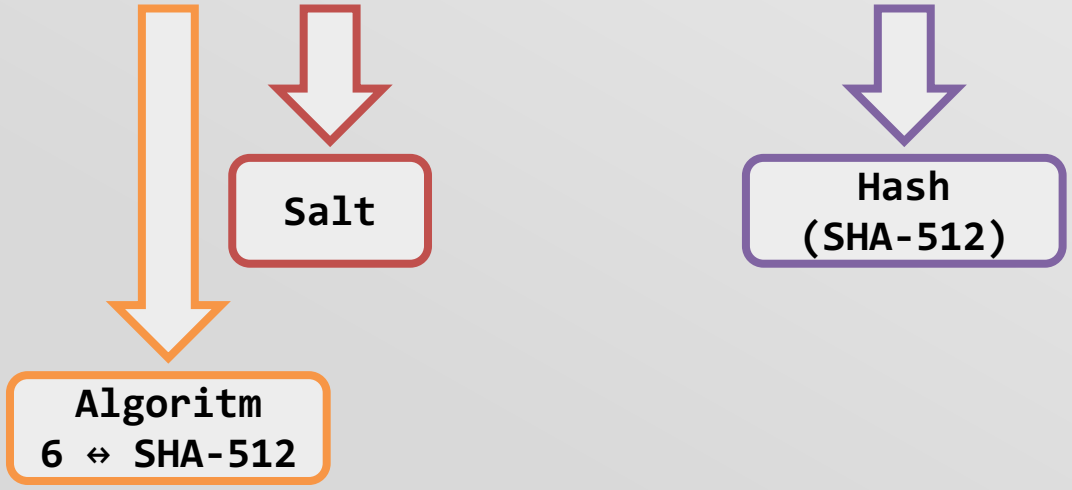
- Rainbow tables publice se pot obține de pe Internet
  - www.freerainbowtables.com (are 4178 de GB)

Spargere parole - Salting

RL
crunch it connected

- Metodă de prevenire a atacurilor ce folosesc **rainbow tables**
- Se folosește un segment suplimentar, generat aleator, ce este concatenat la parola utilizatorului înainte de hashing
- Segmentul aleator crește dimensiunea tabelelor necesare pentru spargere
- Exemplu:

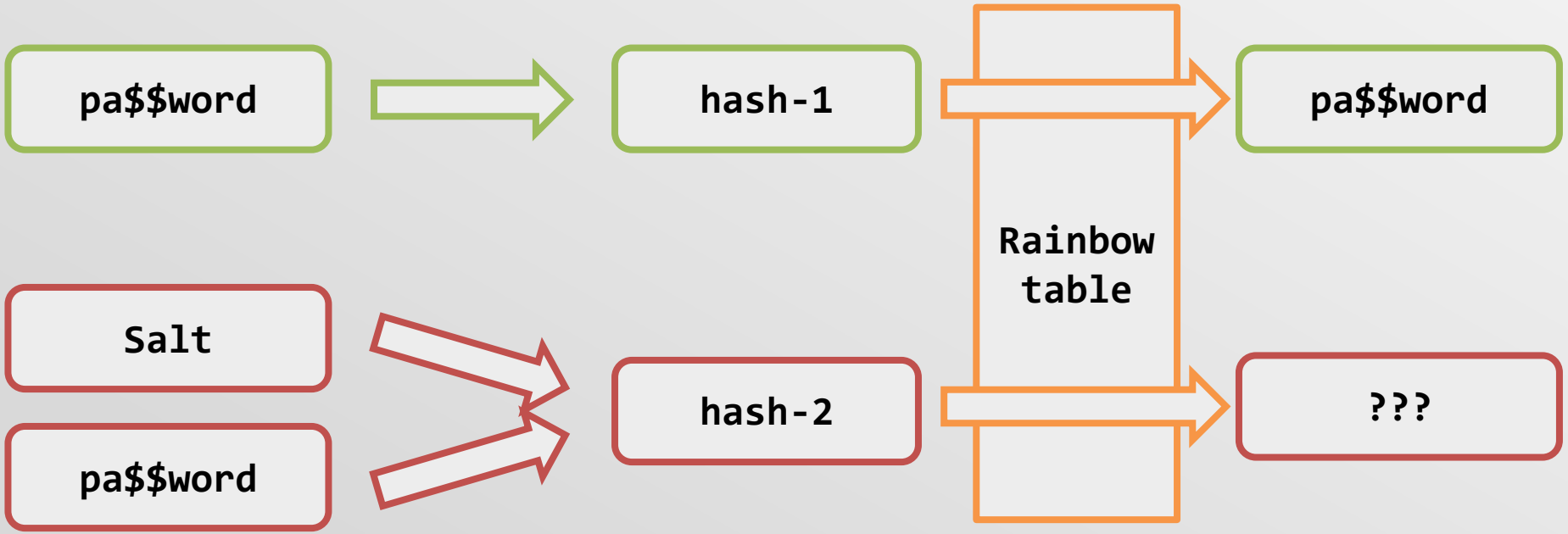
```
/etc/shadow:
        trudy:$6$/tKy92iM$/.cIxbEX49qHpZt74D5L0W1vXO2fJuXjyXJnsT0.M… […]
```



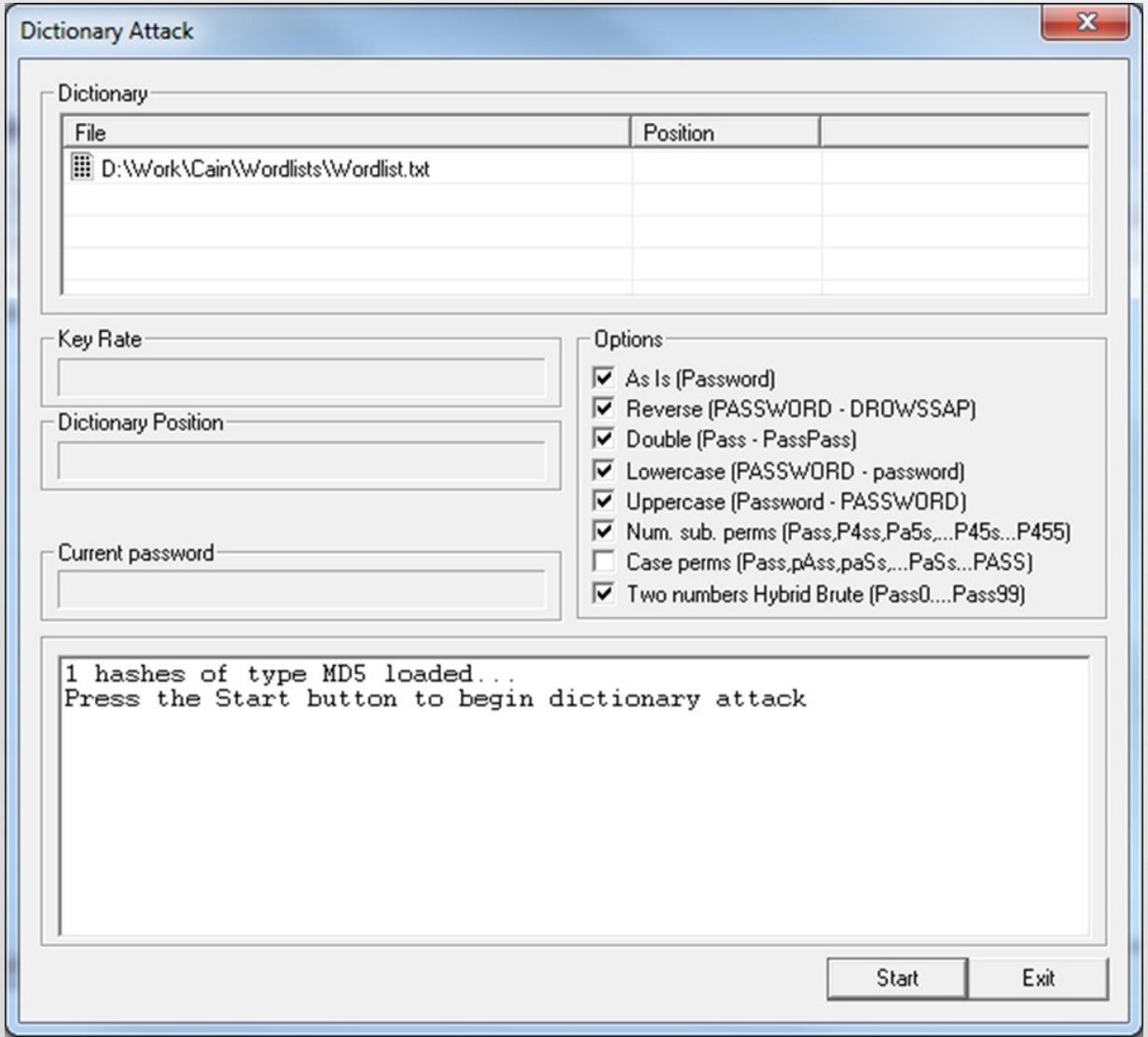
Spargere parole - Salting

RL
crunch it connected

- Folosirea unui salt nu previne atacurile prin **rainbow tables**, doar crește dimensiunea necesară a acestora



Spargere parole cu Cain



Un **dictionary attack** încearcă și variații simple ale cuvântului de bază

MITM

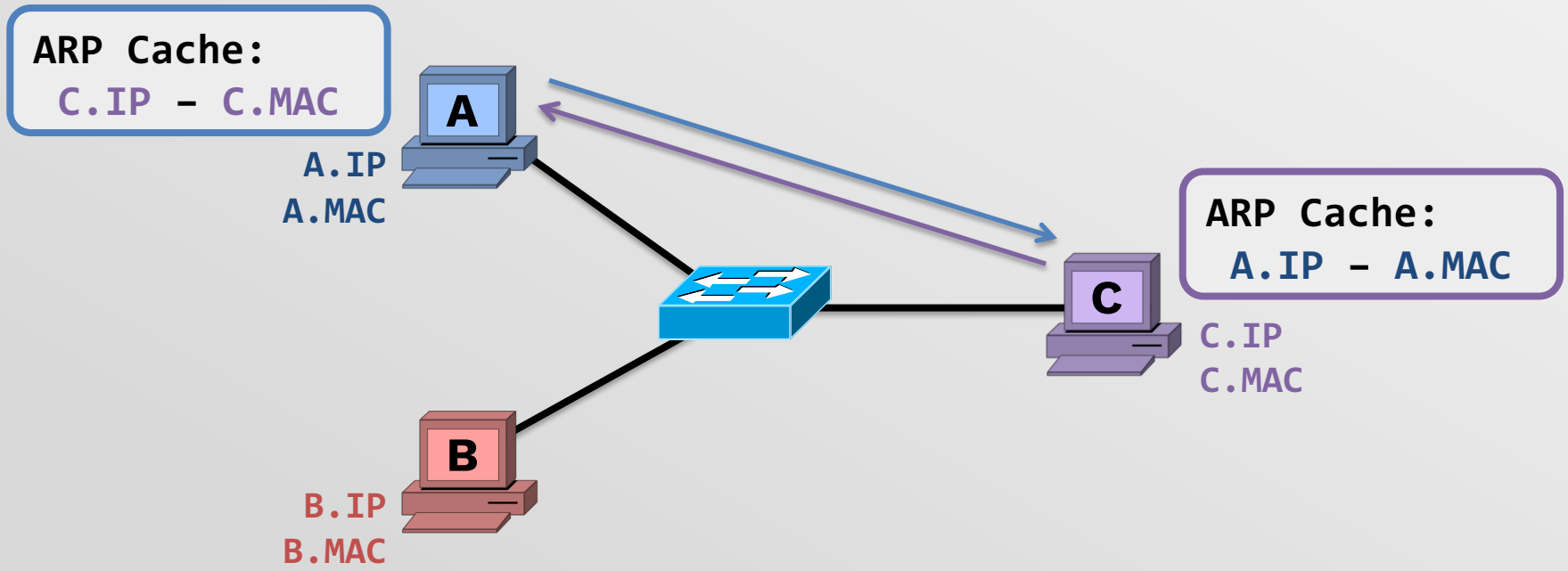
- **Man in the Middle**
- Traficul dintre două entități este interceptat și rutat de un atacator
  - Exemplu: traficul între o stație și default gateway

- Exemplu de MITM: **ARP Poisoning**
  - Se bazează pe faptul că protocolul ARP nu face autentificare
  - O stație poate minți referitor la adresa sa de nivel 3

  - Exemplu de program pentru ARP Poisoning: Cain

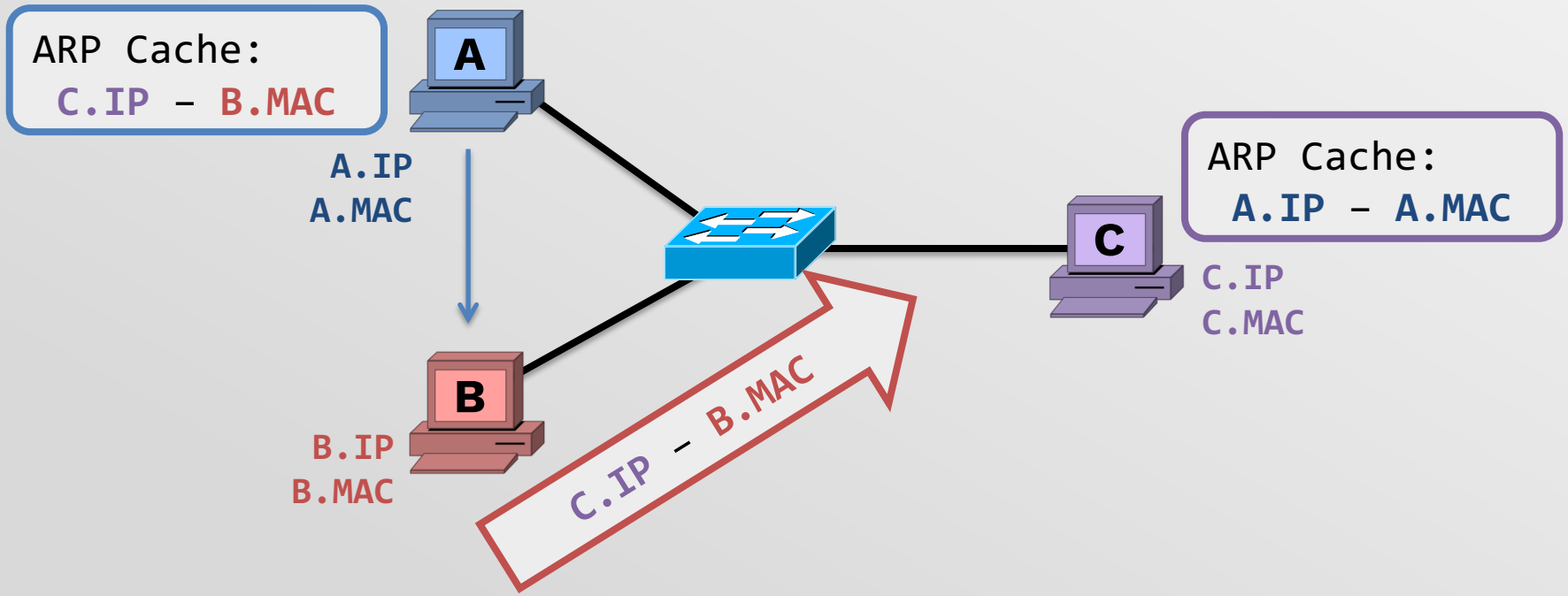
MITM – Stare inițială

- Rețeaua operează normal înaintea atacului
- Stația **A** are informații corecte despre stația **C**



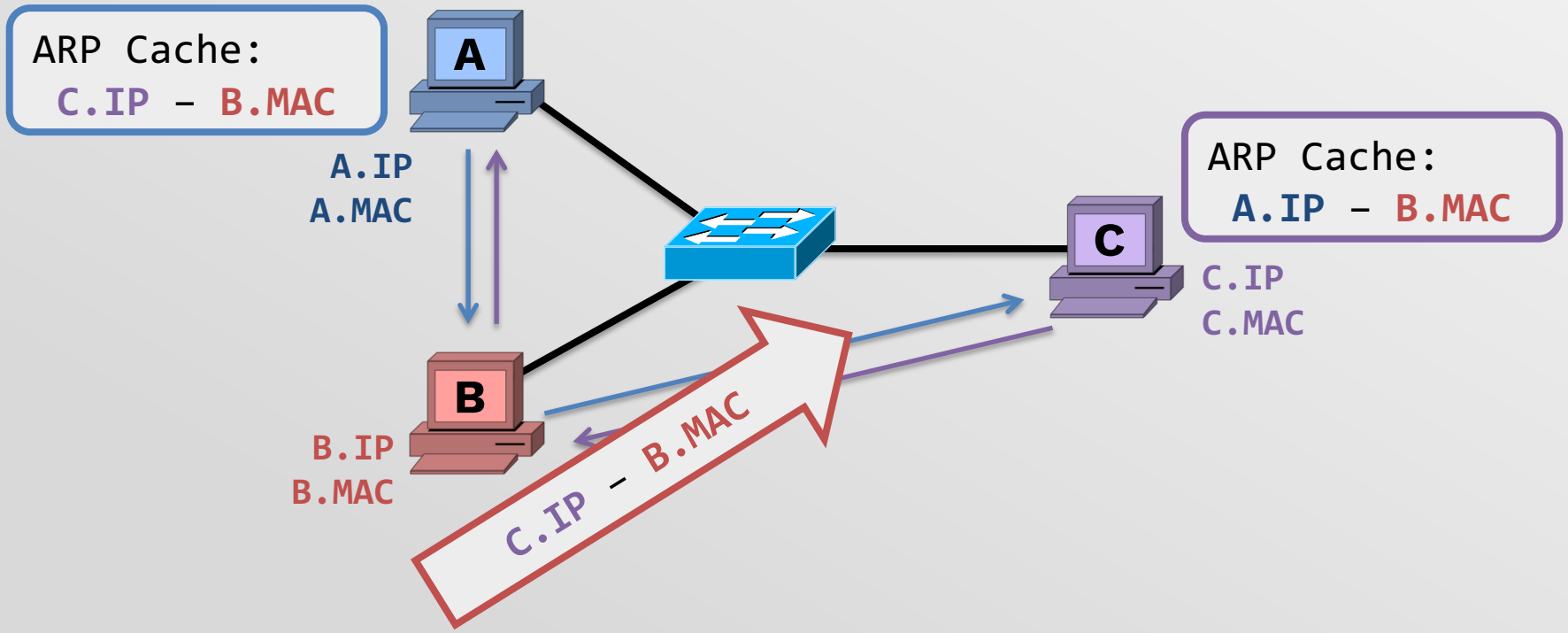
MITM – Atac

- **B** dorește să intercepteze traficul dintre **A** și **C**
  - Trimite un mesaj ARP către **A** cu conținutul **C.IP** – **B.MAC**
  - La primirea mesajului, **A** schimbă conținutul cache-ului (chiar dacă nu a solicitat mesajul în prealabil)
  - **B** va ”ruta” corect traficul de la **A**



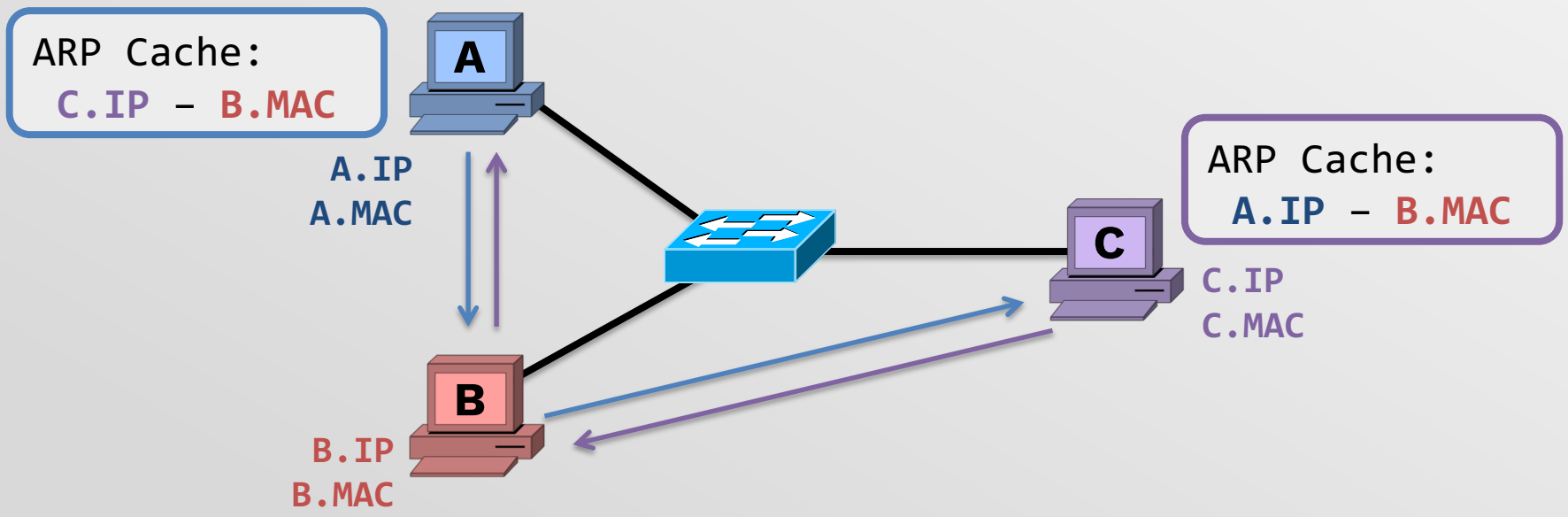
MITM – Atac

- **B** dorește să intercepteze traficul dintre **C** și **A**
  - Trimite un mesaj ARP către **C** cu conținutul **A.IP** – **B.MAC**
  - La primirea mesajului, **C** schimbă conținutul cache-ului (chiar dacă nu a solicitat mesajul în prealabil)



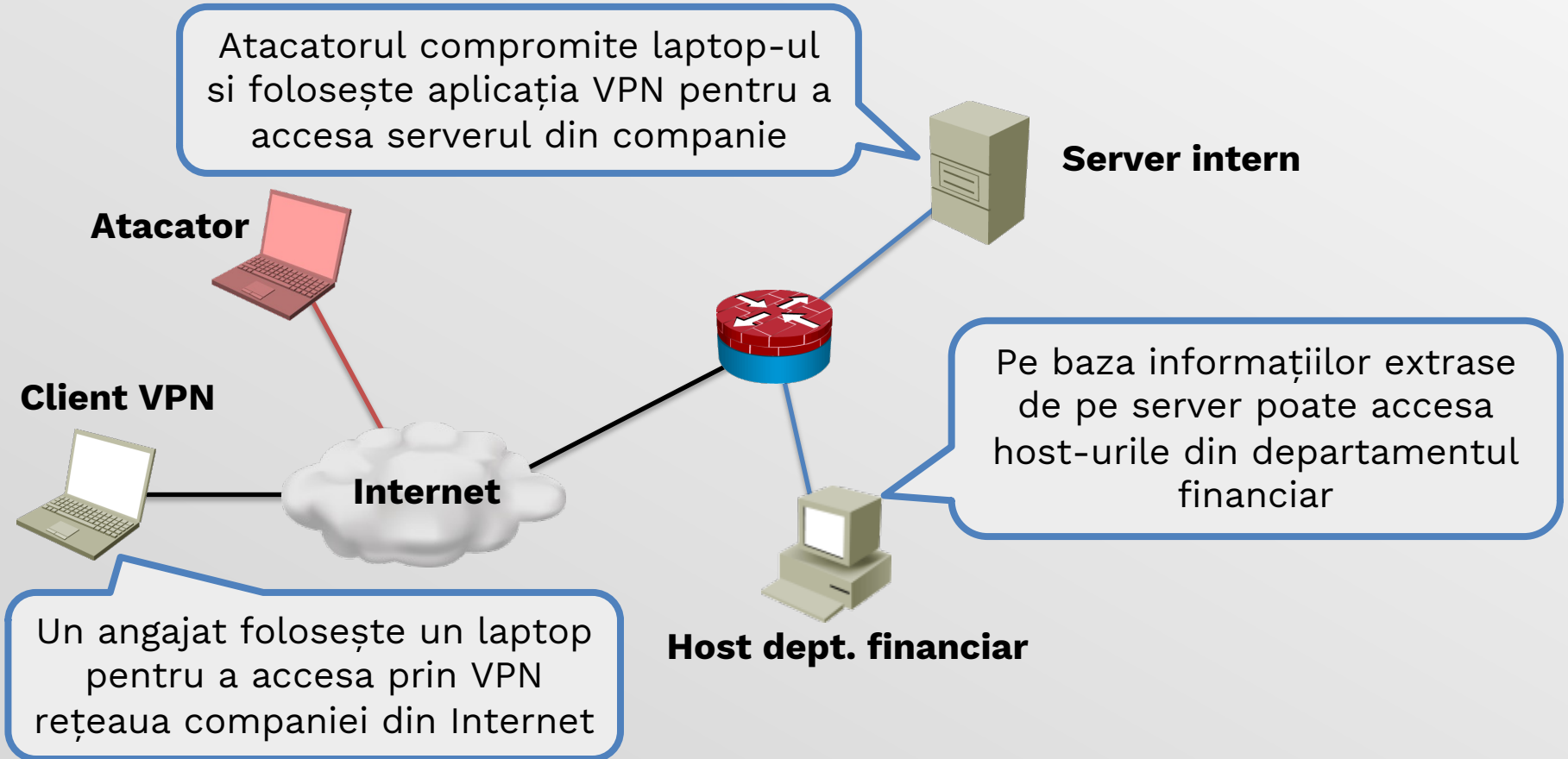
MITM – Stare finală

- **A** și **C** vor crea cadrele cu adresa lui **B** în antetul de nivel 2
- Switch-ul va comuta cadrele respective către atacator



Exploatarea încrederii

- Inițial este compromis un sistem din rețea
- Sistemul compromis este folosit pentru a ataca mai departe rețeaua



Social engineering

RL
crunch it connected

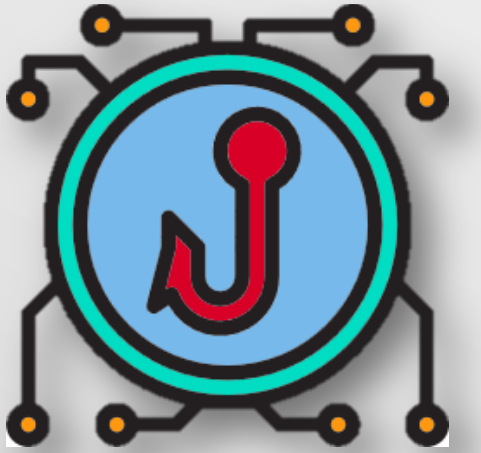
- Se bazează pe extragerea informațiilor confidențiale de la oameni
  - Parole sau detalii financiare
- Atacatorul trebuie să convingă potențialele ținte că este de încredere
- Este probabil ca ținta respectivă să nu fie de profil tehnic și să aibă încredere în autoritatea atacatorului
  - Atacatorul se poate da drept un membru al echipei tehnice

Social engineering

RL
crunch it connected

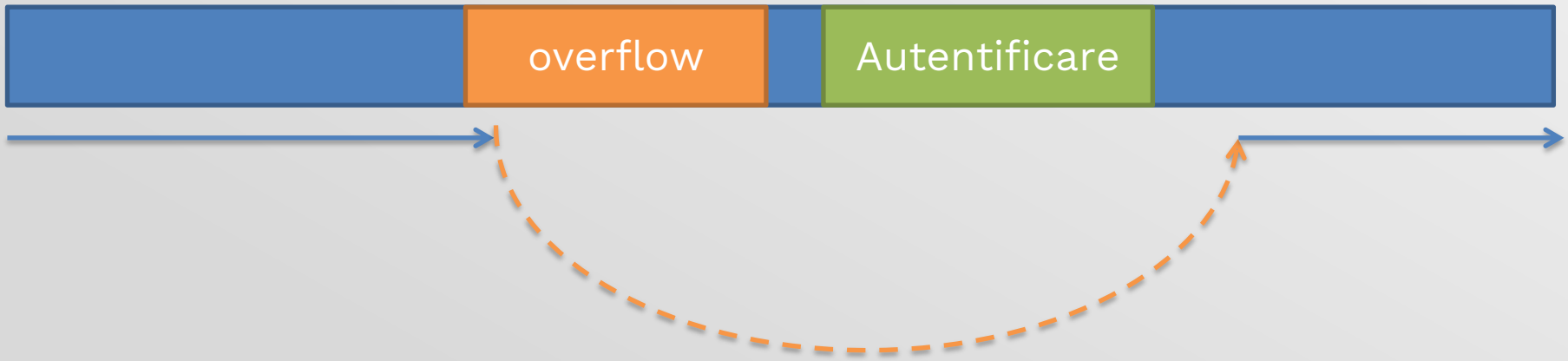
- Oamenii nu sunt conștienți de valoarea informației pe care o posedă și vor să ajute
- Social engineering poate evita orice tip de securitate
  - Este necesară realizarea de ședințe de instruire pentru angajații non-tehnici

- Exemplu: phishing



Buffer overflow

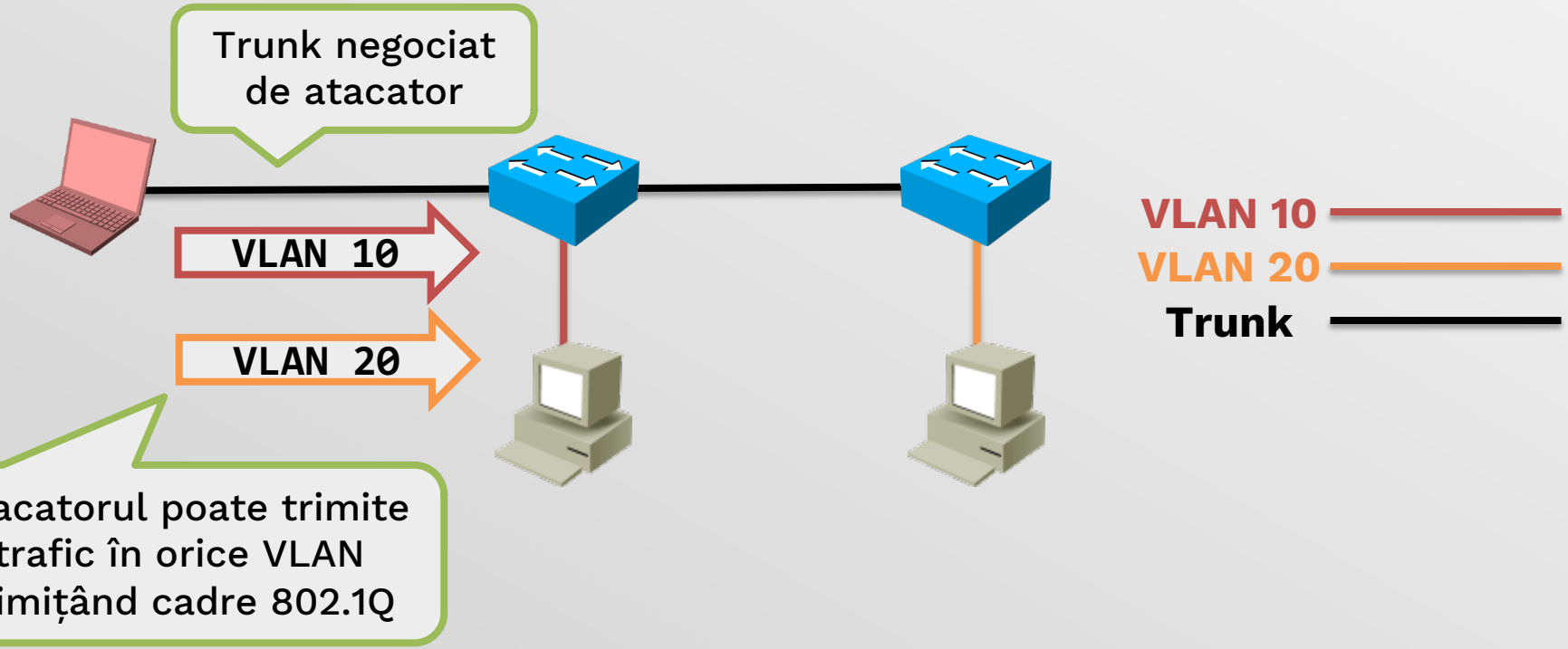
- Scriere de informație peste un buffer alocat
  - Permite executarea de cod de atac sau crash-uirea aplicației
- Exemplu: scrierea în afara unui vector alocat pe stivă în C poate permite suprascrierea adresei de întoarcere din funcție
  - Atacatorul poate provoca astfel sărirea peste o funcție de verificare, obținând acces în sistem fără autentificare



Flux modificat printr-un atac tip buffer overflow

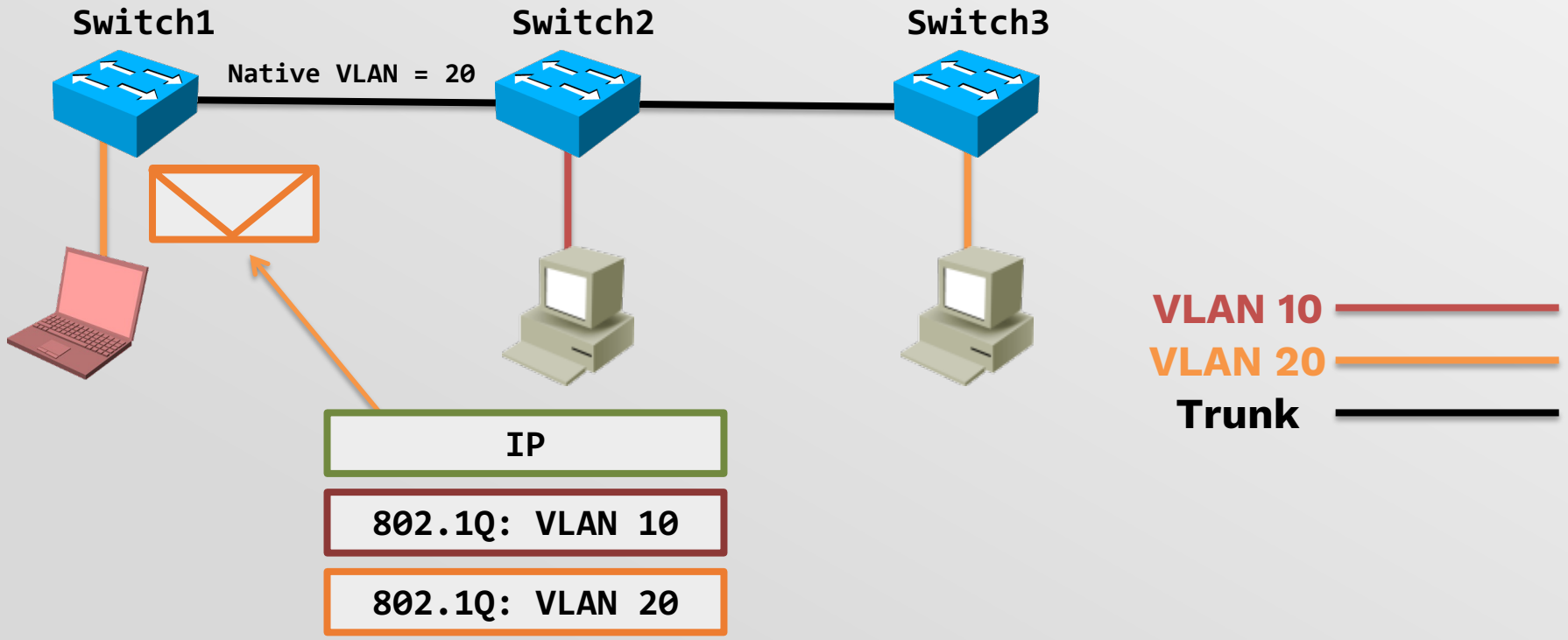
VLAN Hopping

- Switch spoofing:
  - Sistemul atacatorului negociază o legătură trunk cu switch-ul (prin DTP)
  - Atacatorul poate ulterior trimite trafic în orice VLAN



VLAN Hopping

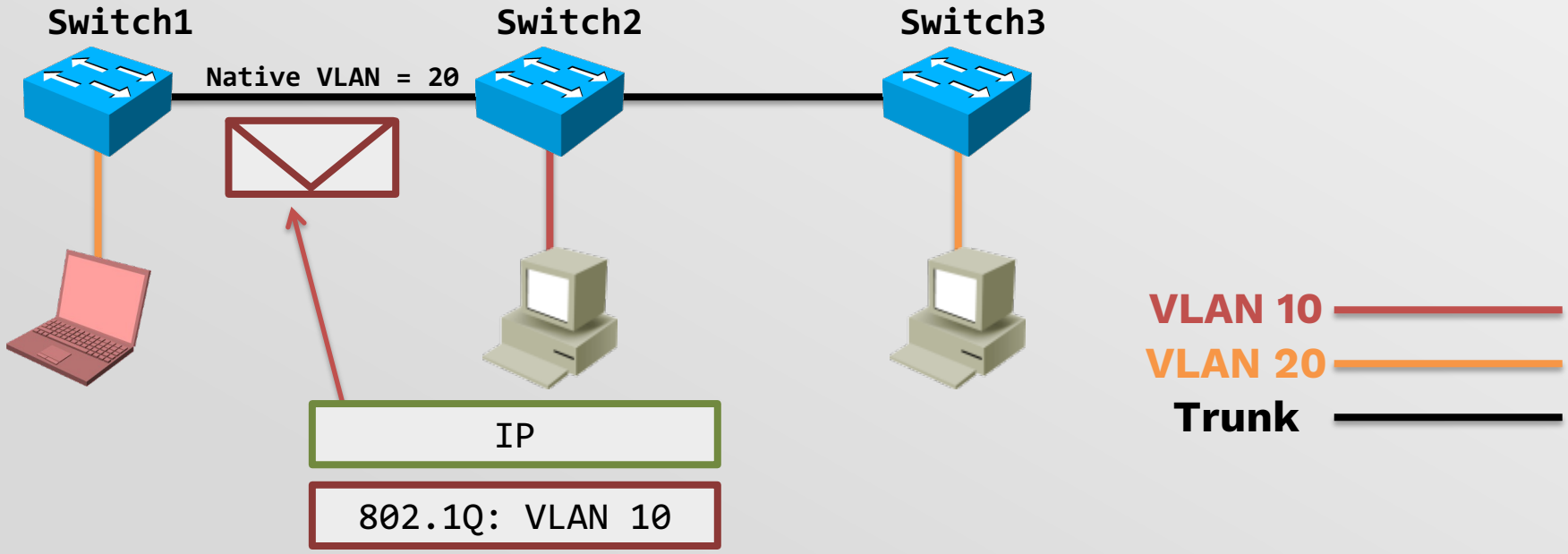
- Double tagging:
  - Simplu de realizat deoarece nu necesită implementarea **DTP** pe atacator
  - Tehnică folosită și de ISP-uri în **802.1Q tunneling**
  - VLAN-ul nativ de pe trunk trebuie să fie același cu VLAN-ul atacatorului



VLAN Hopping

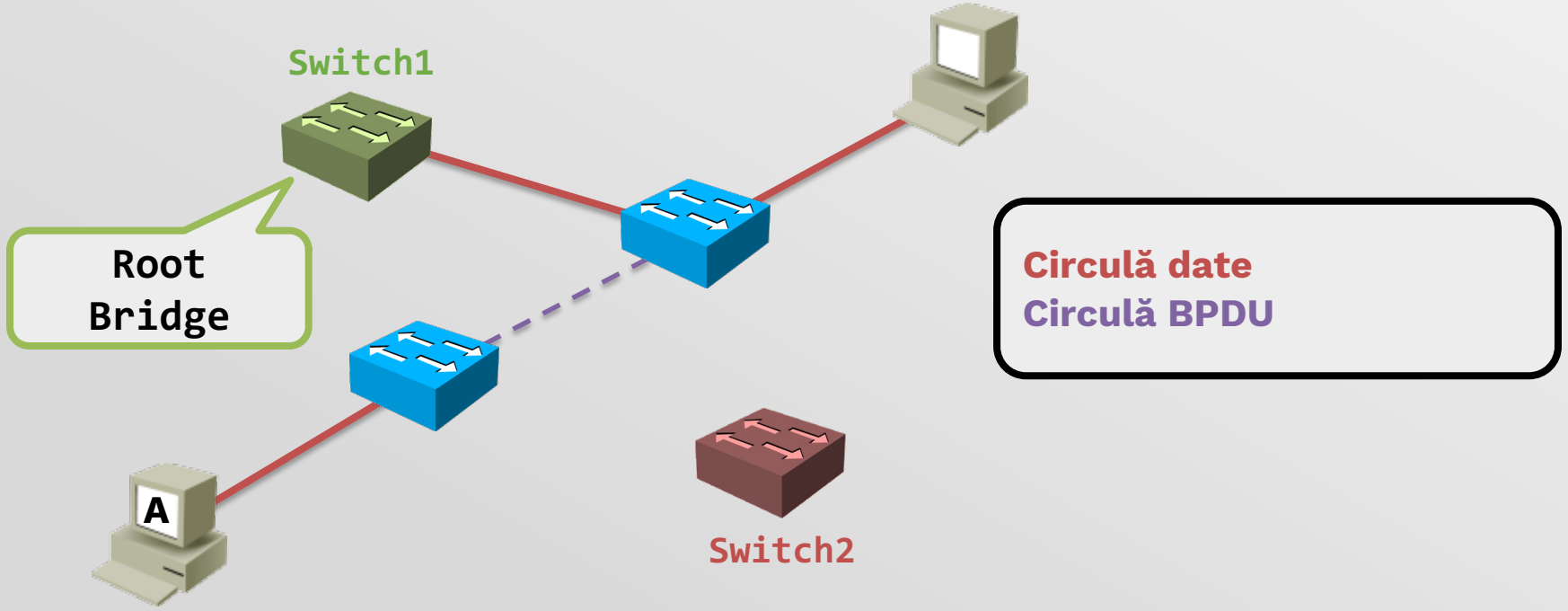
RL
crunch it connected

- Double tagging:
  - Switch-ul înlătură tag-ul de **VLAN 20** și trimite cadrul mai departe pe trunk
  - Switch-ul 2 va vedea tag-ul 10 și va trimite mai departe cadrul pe **VLAN 10**



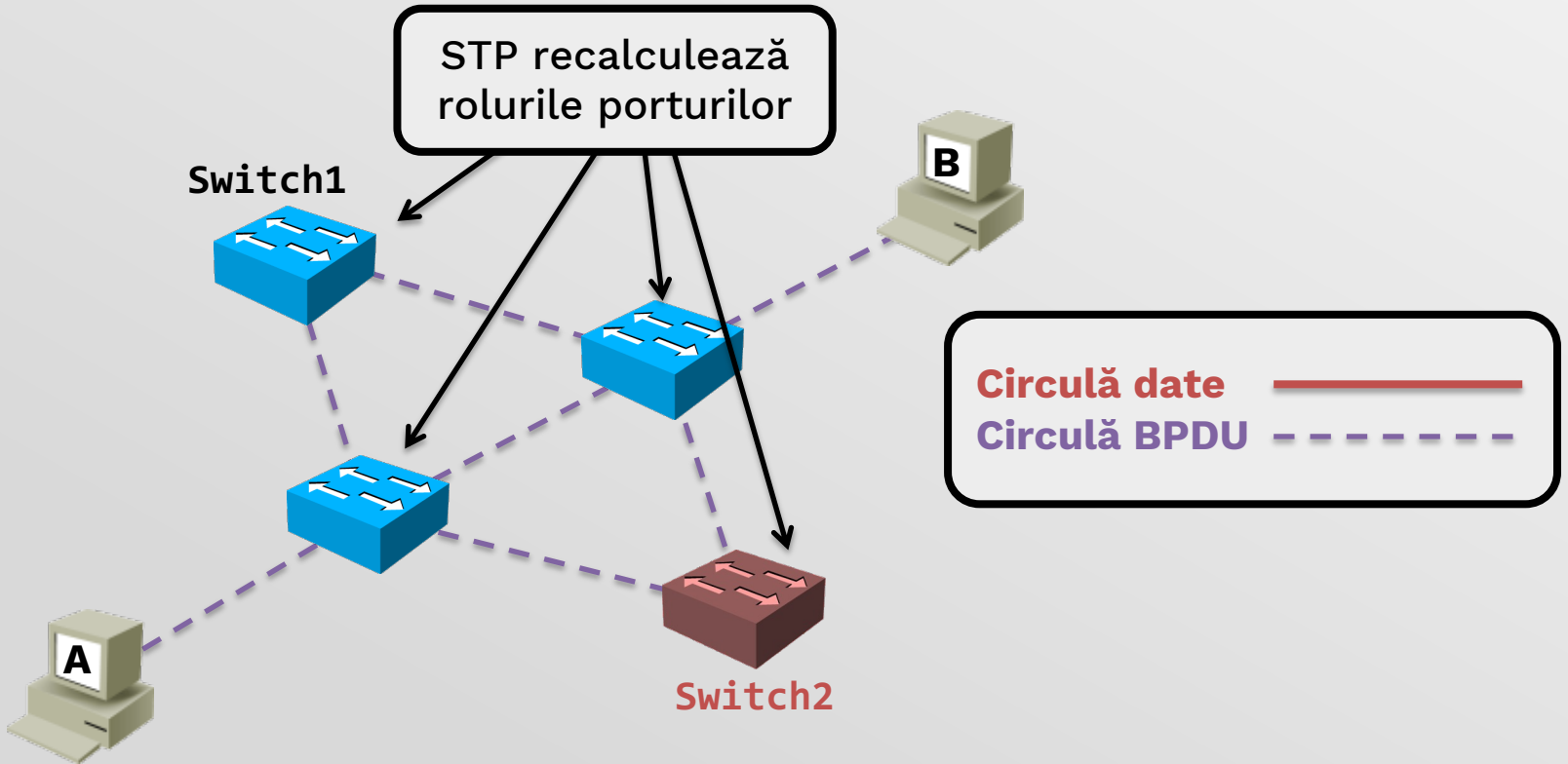
Atacuri STP

- Protocolul STP nu folosește autentificare → vulnerabil
- Un atac STP are de obicei următorii pași:
  1. Conectare la rețeaua de switch-uri
  2. Trimiterea de BPDU-uri cu BID mic
  3. Devenire root bridge



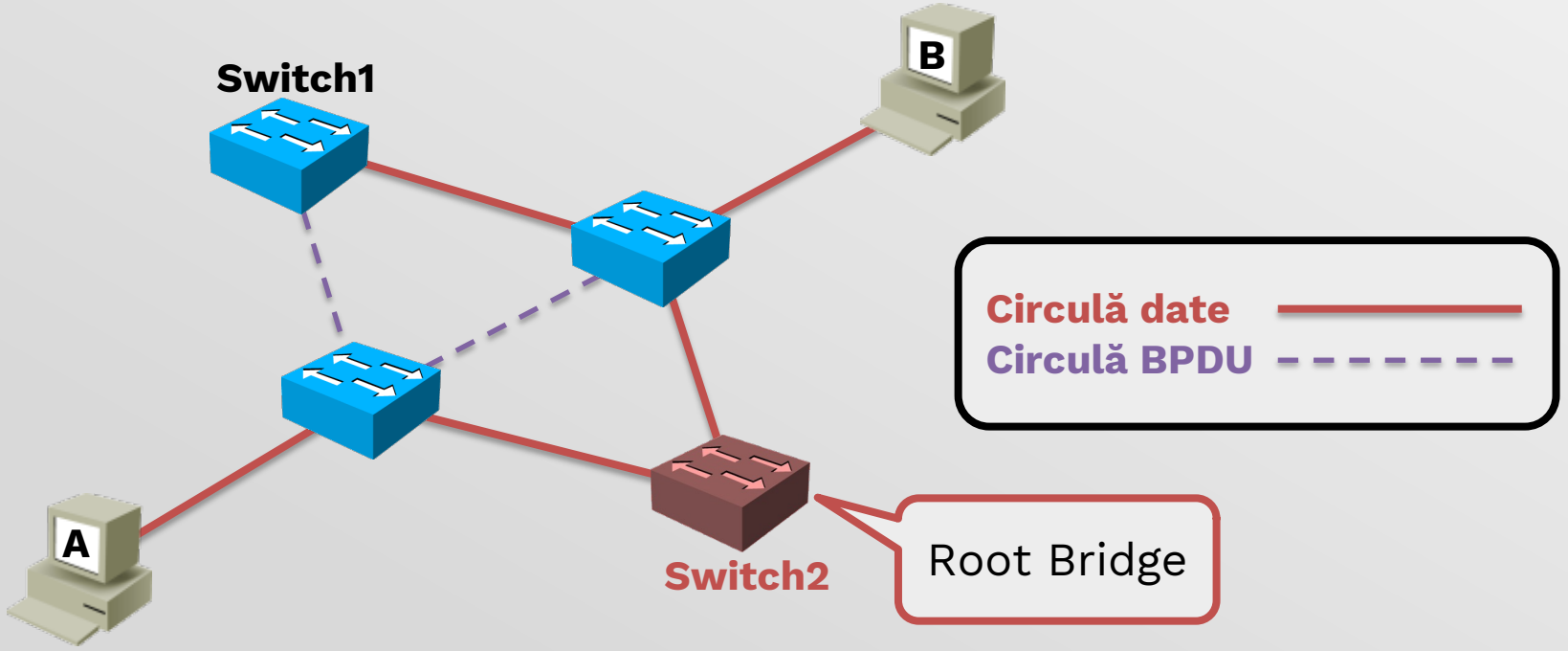
Atacuri STP

- Traficul dintre **A** și **B** trece prin **Switch1**
- **Switch2** este sistemul folosit de atacator (Linux cu Yersinia)
- **Switch2** e conectat la rețea și anunță BPDU-uri cu BID=1 (prioritate 0)



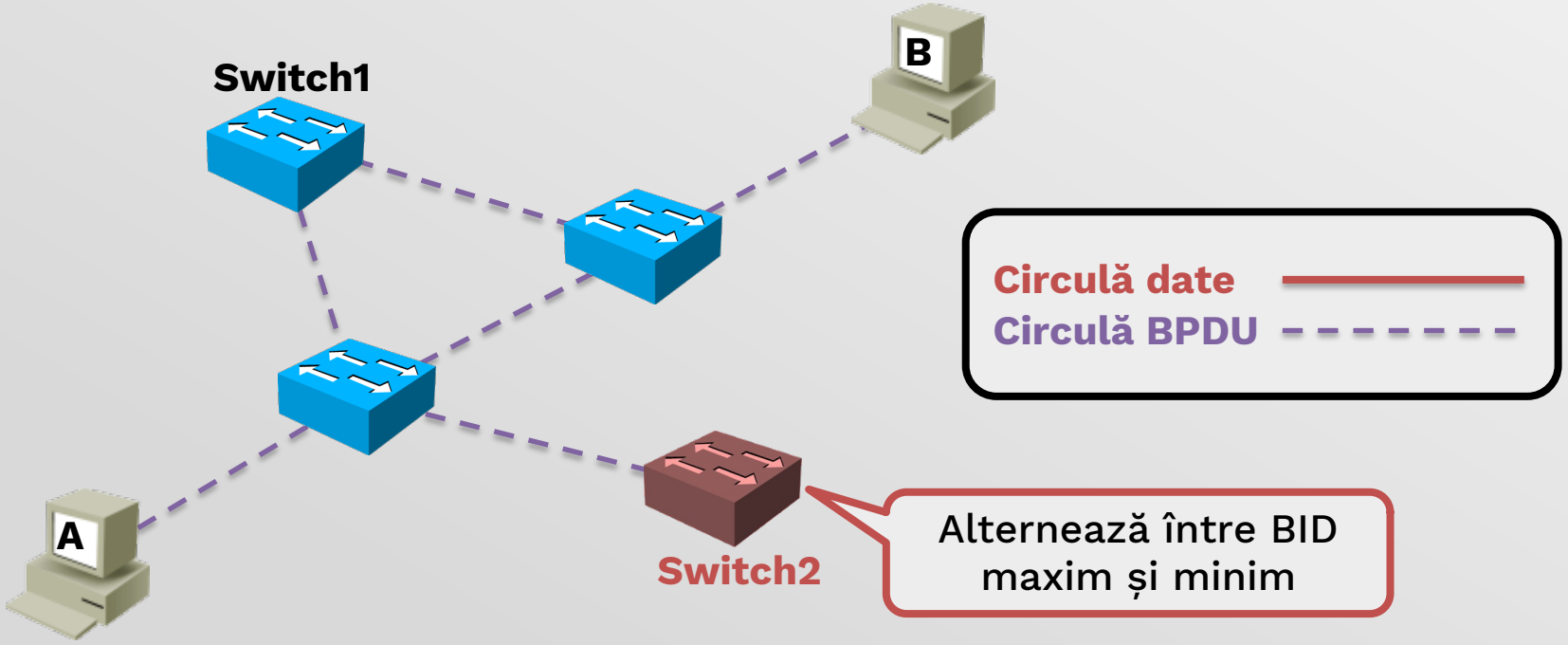
Atacuri STP

- Traficul dintre **A** și **B** trece acum prin **Switch2**
- Atacatorul poate porni o captură de trafic pe **Switch2** pentru a analiza comunicația dintre **A** și **B**
- Soluții pentru protejarea STP: RootGuard, BPDU Guard, BPDU Filter



Atacuri STP

- STP reconverge imediat dacă se detectează BID-uri noi
- Switch-ul atacatorului își poate schimba continuu BID-ul pentru a forța recalcularea STP
- Porturile nu ajung niciodată să transmită date (denial of service)
- Suficientă o singură legătură la rețea pentru a implementa atacul



Atacuri cu cod executabil

- Viruși
- Troieni
- Viermi

RL
crunch it connected

Viruși

- Cod executabil atașat unui program sau executabil
- Codul trebuie să fie rulat de un utilizator pentru a avea efect

- Se propagă prin:
  - Atașamente de e-mail
  - Fișiere descărcate infectate
  - Partajări de fișiere în rețeaua locală
  - Stick-uri USB

Troieni

RL
crunch it connected

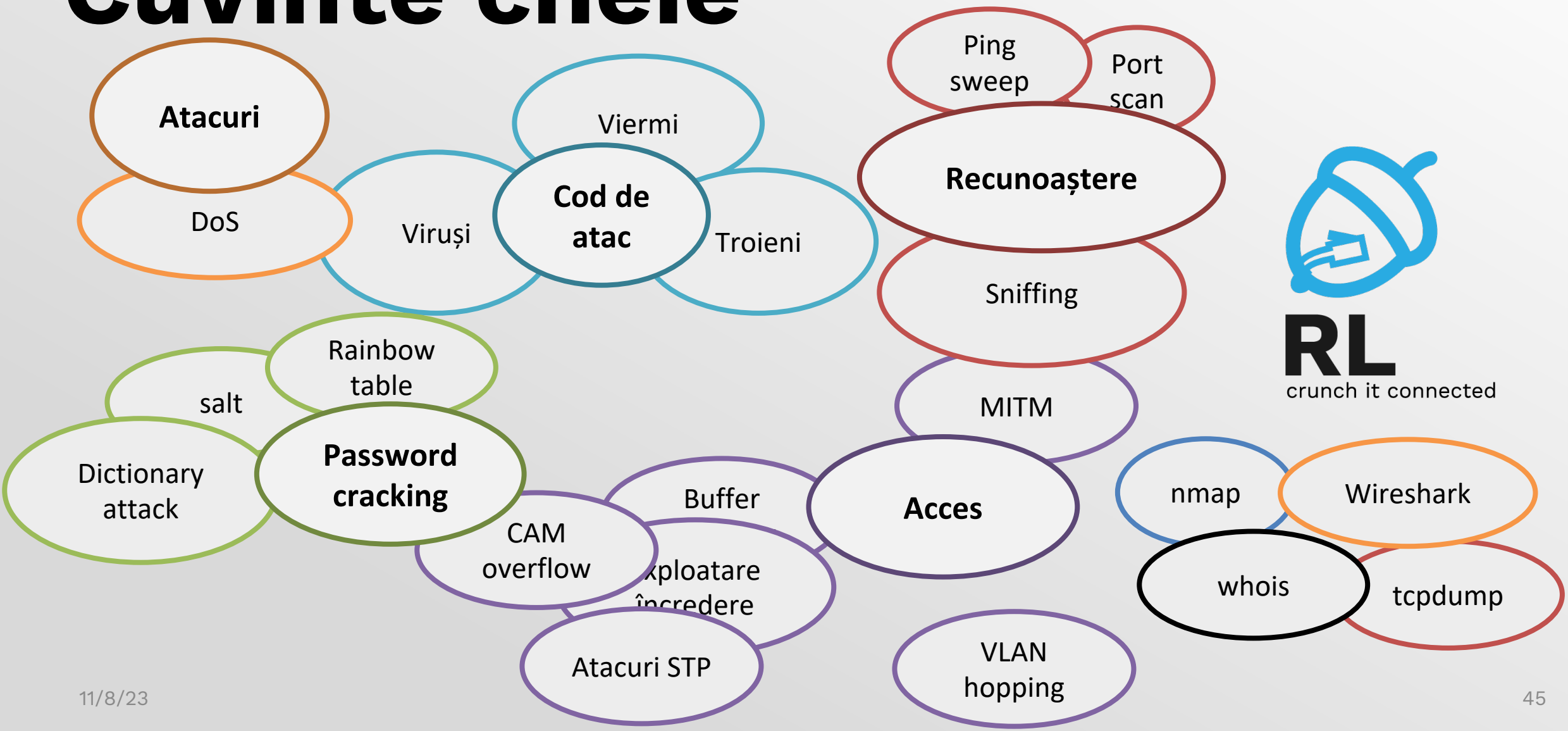
- Cod executabil atașat unei aplicații
- Spre deosebire de viruși, care au un efect direct, troienii au un efect subtil
  - Deschidere backdoor
- Sunt mult mai greu de detectat decât virușii

Viermi

RL
crunch it connected

- Cod executabil ce folosește vulnerabilități pentru a se răspândi
- Spre deosebire de viruși nu necesită intervenția directă a unui utilizator
- Răspândire foarte rapidă
- Dificil de înlăturat
- Au adesea scopul de a partaja resurse de procesare, stocare sau conexiune internet (de exemplu botnet de trimitere spam)

Cuvinte cheie



Atacuri în 2016

RL
crunch it connected

- Los Angeles Hospital Hit (February 2016)
  - Răscumpărare plătită pentru recuperarea conturilor de email și informațiilor pacienților
  - https://www.theguardian.com/technology/2016/feb/17/ los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center
- IRS Security Breach (February 2016)
  - accesarea datelor personale a peste 700 000 de americani
  - http://www.usatoday.com/story/money/2016/02/26/ cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/
- Mossack Fonseca Leak (May 2016)
  - publicarea a 2.6 TB de documente private
  - http://www.bbc.com/news/world-latin-america-36232142
- Banner Health (August 2016)
  - pierderea datelor personale a 3.7 milioane de pacient,i
  - http://www.securityweek.com/37-million-exposed-banner-health-breach
- Bitfinex Heist (August 2016)
  - furtul a echivalentului de 72 milioane USD
  - http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP
- Suma medie a cererilor de răscumpărare: 679$ (față de 342$ în 2015)

Câteva întâmplări din 2017

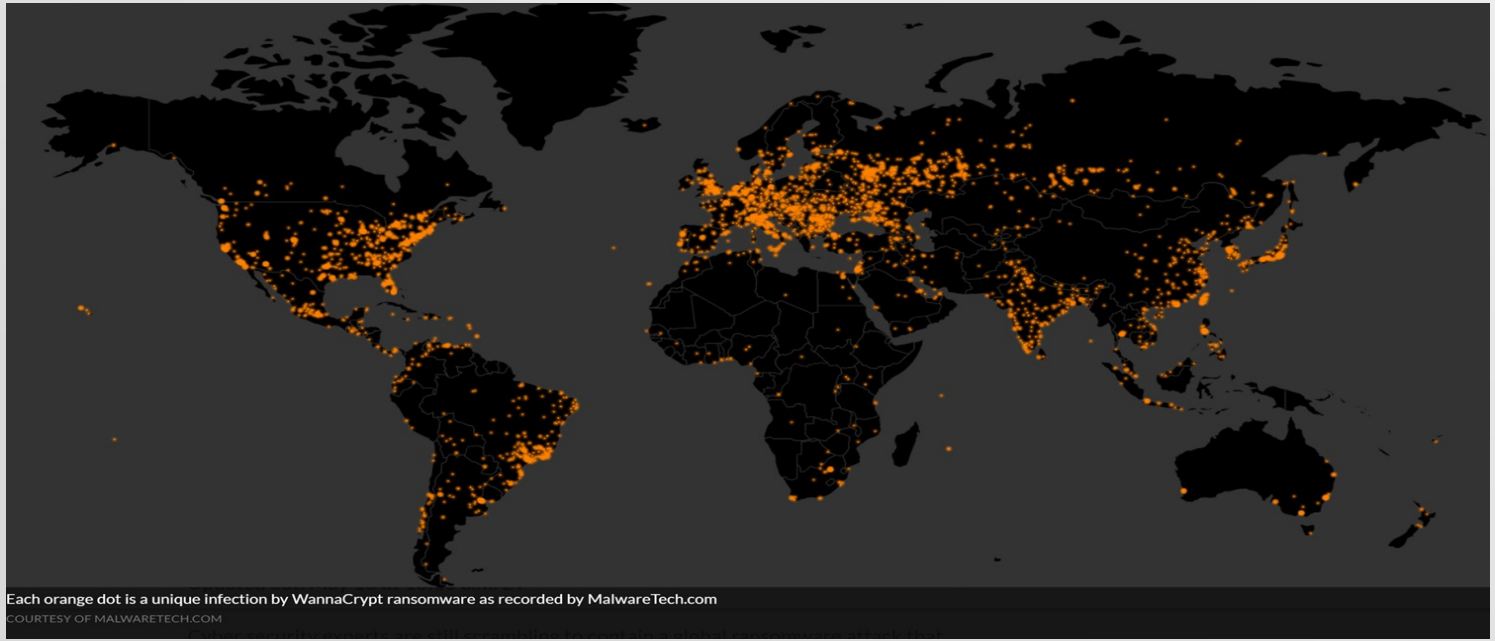
RL
crunch it connected

- Yahoo: 3 miliarde de conturi compromise
  - 2 atacuri (2013 & 2014) dezvăluite total în 2017 după achiziția Verizon
  - http://www.wired.co.uk/article/hacks-data-breaches-2017
- Equifax: datele personale pentru 200.000 de persoane
  - 200.000 nume, Social Security, carduri de credit, permisuri de conducere
  - http://www.wired.co.uk/article/hacks-data-breaches-2017
- 14.04: Shadow Brokers publică EternalBlue (NSA)
  - Utilizat în Ransomware: WannaCry (12.05), Petya (27.06)
- 07.03: Wikileaks CIA „Vault 7”
  - 8761 documente posibil aparținând CIA
  - Vulnerabilități iOS, Android, Windows, smart TV
- Compania republicană Deep Root Analytics a stocat datele a 200.000.000 votanți pe un server Amazon nesecurizat
  - 1.1Tb date: nume, data nașterii, adresa, telefon, etnia și religiozitatea
  - https://www.wired.com/story/2017-biggest-hacks-so-far/

WannaCry

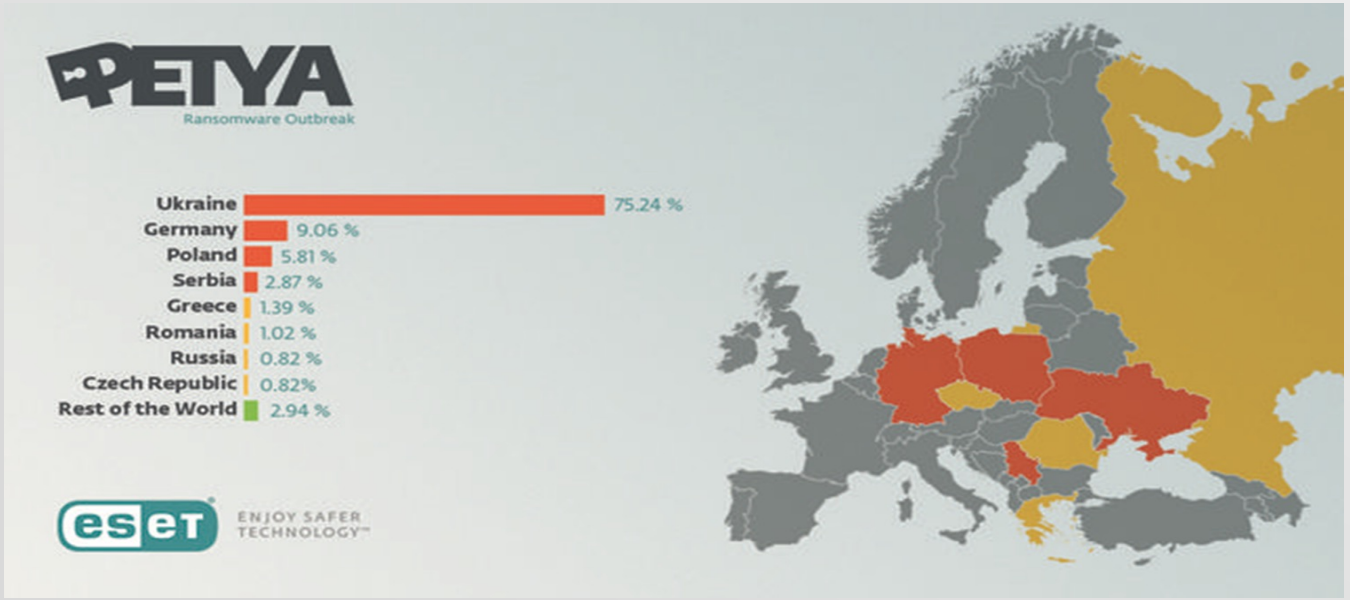
RL
crunch it connected

- 12 mai: WannaCry atacă mii de ținte, inclusiv spitale în UK
- 52 bitcoins ($130.000); sursă probabilă: Coreea de Nord
- Utilizează EternalBlue, o vulnerabilitate Shadow Brokers pentru care Microsoft a publicat un patch în martie 2017



Petya

- 27-29 iunie: Petya/NotPetya/Nyetya/Goldeneye
- Focus: Ucraina
- Alte victime: US Pharma Merck, Danish shipping Maersk, Russian oil giant Rosnoft



Tendințe 2017

RL
crunch it connected

- Costurile ransomware:
  - 2015: **$ 325.000.000** | 2017: **$5.000.000.000**
  - 2019: o firmă atacată la 19 secunde – mai ales spitalele
  - https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Cybersecurity în 2018

- Ransomware (2017) a fost înlocuit cu malware care folosesc CPU-ul pentru minat de cryptocurrencies
- **GDPR** se aplică începând cu Mai 2018
- Aspecte legate de privacy într-un scandal politic unde **Facebook** este acuzat că a fost folosit să influențeze cursa prezidențială din US (aprox. 87.000.000 utilizatori)

Spectre and Meltdown

RL
crunch it connected

- Vulnerabilitate de nivel Hardware
- Ofera posibilitatea de a citi zone de memorie protejate
- Patch-urile implementate aduc un overhead de pana la 30%

Data breaches 2018

- 30 Noiembrie 2018 – 500.000.000 informații compromise într-un atac cibernetic asupra lanțului de hoteluri **Marriott International**
- Martie 2018 – 150.000.000 date compromise într-un atac asupra **MyFitnessPal**
- August 2018 – 2.000.000 date au fost compromise de la **T-Mobile**

Cybersecurity în 2019

- Researchers find 540 million Facebook user records on exposed servers
  - https://techcrunch.com/2019/04/03/facebook-records-exposed-server/?guccounter=1

Cybersecurity in 2020

RL
crunch it connected

- Email Scams on the Rise
  - https://www.securitymagazine.com/articles/93194-new-research-shows-significant-increase-in-phishing-attacks-since-the-pandemic-began-straining-corporate-it-security-teams
- crimeware-as-a-service
  - Emotet, Dharma and Trickbot
  - https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/

Cybersecurity in 2020

- Android Joker malware growing in volume
  - https://arstechnica.com/information-technology/2020/09/joker-the-malware-that-signs-you-up-for-pricey-services-floods-android-markets/#:~:text=Known%20as%20Joker%2C%20this%20family,contact%20lists%2C%20and%20device%20information
- Tesla hacked with Raspberry Pi
  - https://www.wired.com/story/tesla-model-x-hack-bluetooth/

Cybersecurity in 2021

RL
crunch it connected

- Colonial Pipeline
  - 2.3 M USD
  - https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
- Twitch Data Dump
  - https://kotaku.com/twitch-says-malicious-third-party-was-behind-hack-1847815516
- Microsoft Exchange Server Attack
  - https://geeks.lk/microsoft-warns-of-a-new-rare-fileless-malware-hijacking-windows-computers/