Kybernetická bezpečnosť

II.

Metódy podvodu

- Shoulder Surfing and Dumpster Diving
  - Pozorovanie ponad rameno a prehľadávanie odpadu
- Odcudzenie identity a hoax
- Piggybacking, tailgating

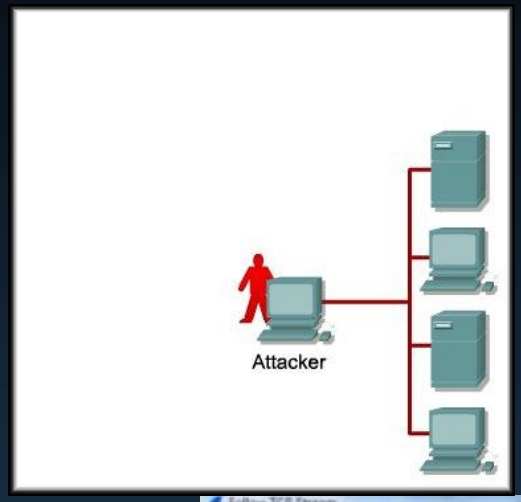
- On-line, e-mail a web-based podvody

Ochrana proti podvodu

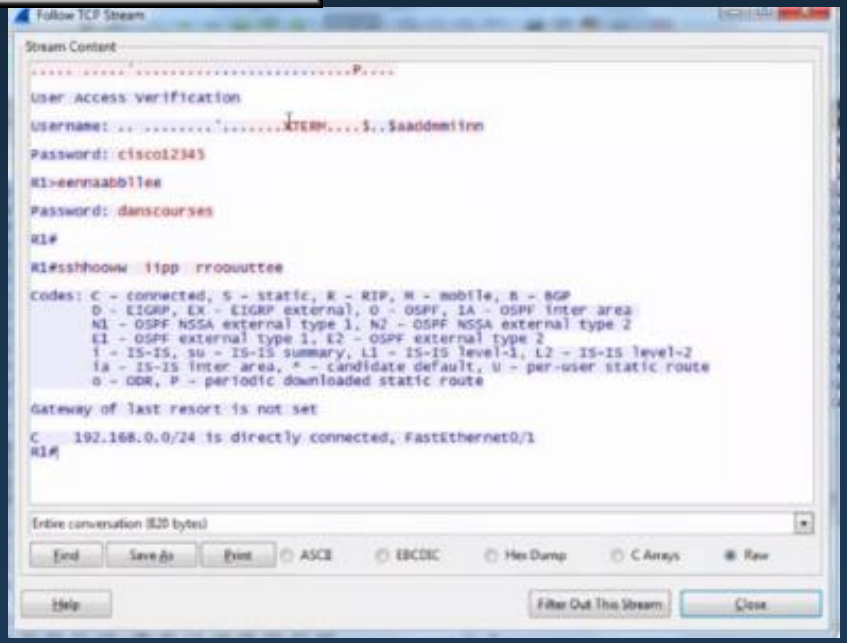
- Nikdy neposkytujte dôverné informácie ani poverenia prostredníctvom e-mailu, chatu, osobne alebo telefonicky neznámym stranám.
- Odolať nutkaniu kliknúť na lákavé e-maily a odkazy na webové stránky.
- Dávajte pozor na neiniciované alebo automatické sťahovanie.
- Zaviesť politiky a vzdelávať zamestnancov o týchto pravidlách.
- Pokiaľ ide o bezpečnosť, dajte zamestnancom pocit vlastníctva.
- Nepodliehajte tlaku od neznámych osôb

Útoky

- DoS, DDoS
  - Obmedzenie služby



- Sniffing
  - Ňuchač



Útoky

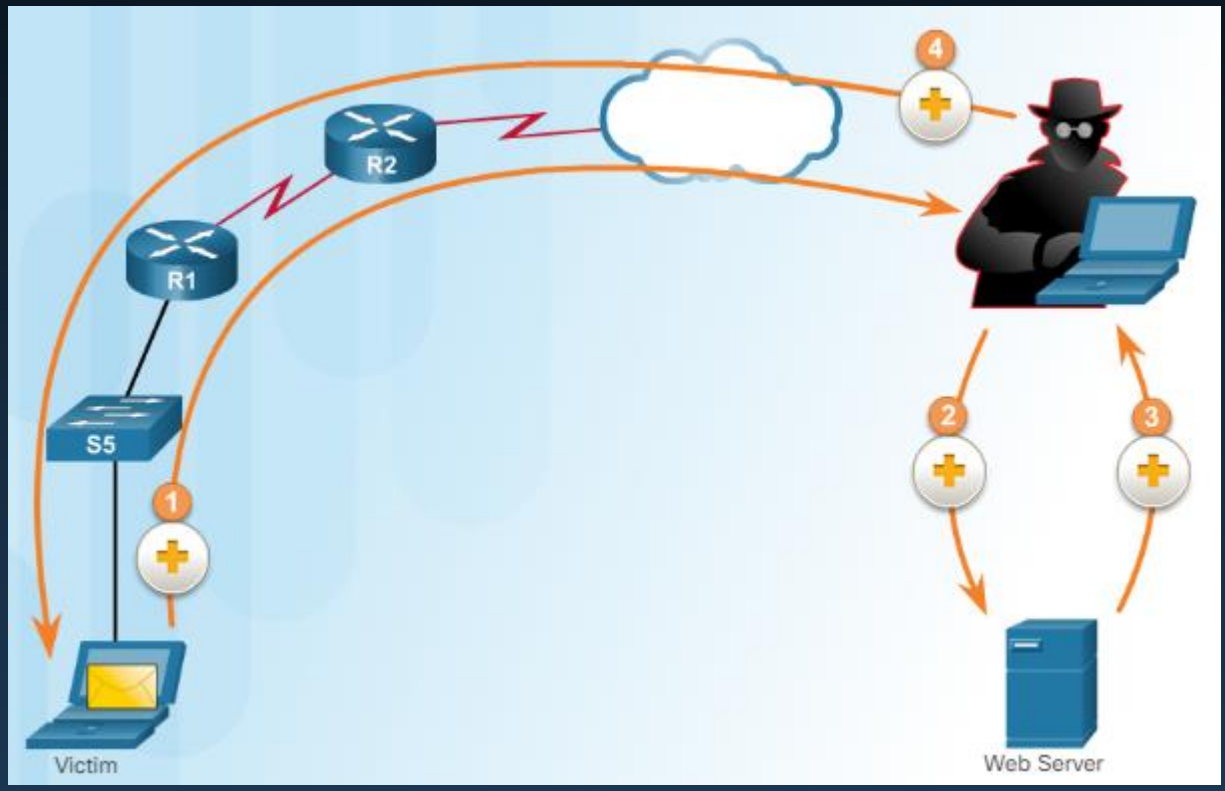
- Spoofing
  - MAC
  - IP
  - ARP
  - DNS

    - Nastavenie pasce
    - Obchádzanie autentifikácie

- Používa sa v spojení s iným typom útoku napr. MitM

Útoky

- MitM
- MitMo



Útoky

- Zero-Day Attacks
  - Zneužitie novej hrozby

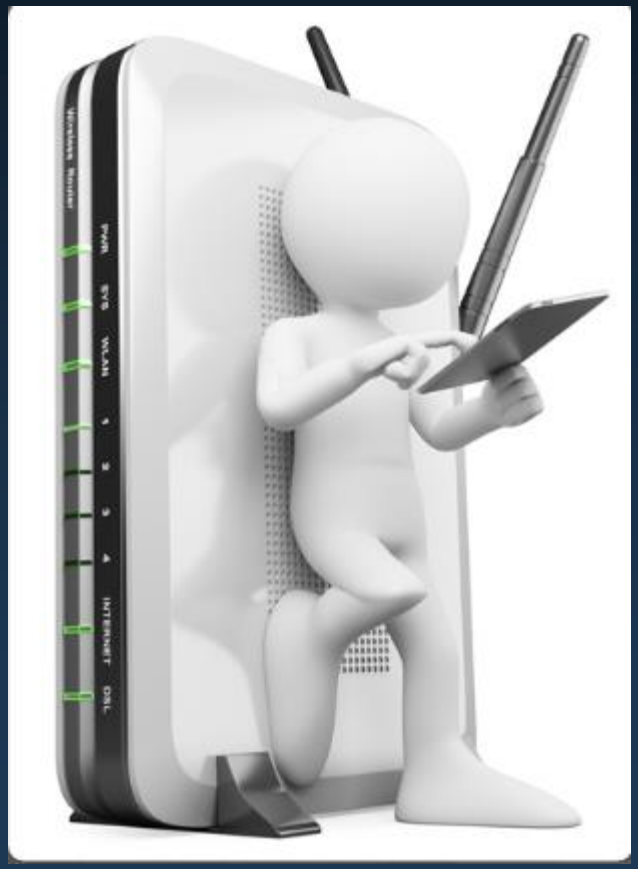
- KeyLogger
  - Odchytávanie stlačených kláves

Útoky

- Ochrana proti útokom
  - Firewall
  - Blokovanie ICMP
  - Logovanie
  - Autentifikácia

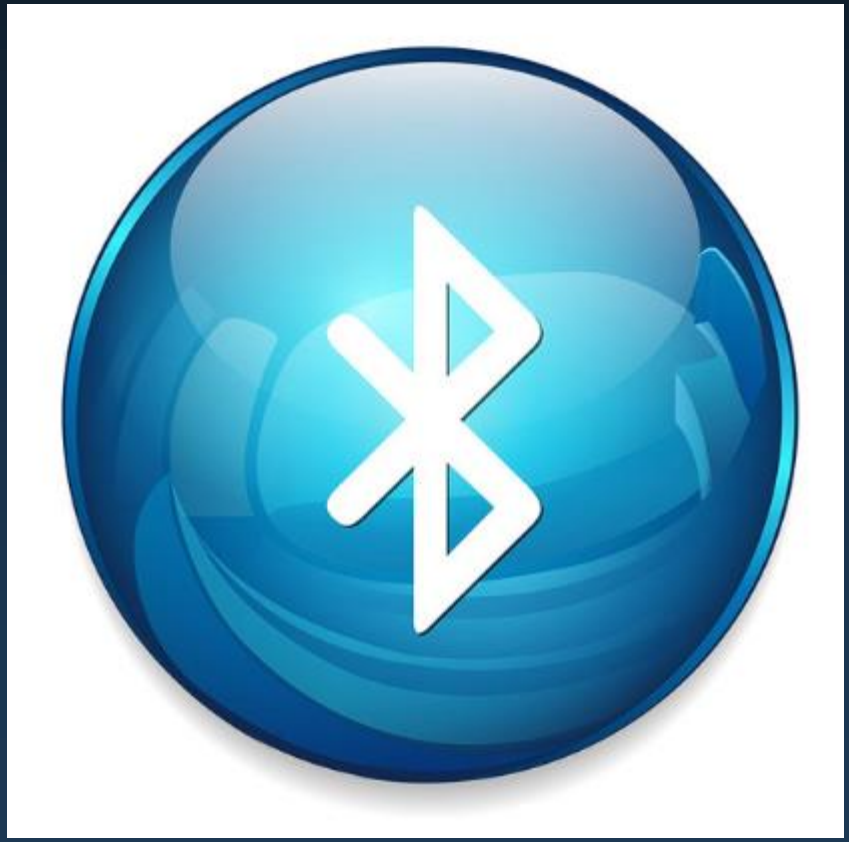
Mobilné útoky

- Greyware a SMiShing
  - Skrytá funkcionalita aplikácií
  - Phishing pomocou SMS
- Nelegálne AP
  - Útočná mobilná sieť
  - Často nevyžaduje autentifikáciu



- Zablokovanie RF
  - Prekrytie signálu silnejším

- BlueJacking a BlueSnarfing
  - Zneužitie Bluetooth



Mobilné útoky

- Útoky WEP a WPA
  - Využíva známe chyby a slabiny WiFi

- Zabezpečenie mobilných zariadení a sietí
  - Skryté vysielanie SSID
  - WPA2
  - Filtre na MAC adresy
  - Overovanie RADIUS

Aplikačné útoky

- Cross-Site Sripting - XSS
- Injektovanie kódu
  - XML
  - SQL
- Buffer overflow
- Vzdialené spustenie kódu
- ActiveX a Java

- Využívajú sa slabiny web aplikácií