<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Mrežna i sistemska sigurnost </CISSP>

Summary

- Sistemska sigurnost
- Mrežna sigurnost
- Mrežni napadi i odbrane

Lekcija 1. Sistemska sigurnost

- Uvod
- Klasifikacija operativnih sistema
- TCB

Uvod

- Sistemska sigurnost je mnogo više od:
  - administratorskih naloga
  - korisničkih naloga
  - prava pristupa
  - dijeljenja resursa i sl.
- Odnosi se na OS u cjelini bez aplikativnog sloja
  - Aplikativni sloj može ugroziti sistem

Klasifikcija operativnih sistema

- 1983, DoD - Trusted computer system evaluation criteria (TCSEC)", poznata još kao "Orange Book
- Definiše sljedeće klase operativnih sistema:
  - Klasa D – minimalna zaštita (MS DOS, Windows 95, 98)
  - Klasa C1 – Diskretna zaštita (UNIX)
  - Klasa C2 – Kontrolisana zaštita pristupa (UNIX, Linux, Windows NT, 2000, XP, 7, 8, 10)
  - Klasa B1 – Uključuje elemente povjerljivosti
  - Klasa B2 i B3 - Strukturna i hijerarhijska zaštita sa elementima uzbunjivanja
  - Klasa A1 – Vrhunski sistemi (uglavnom vojna rješenja i real time sistemi gdje se radi o ljudskim životima)

TCB

- Trusted Computing Base
- Hardver+Firmware+Softver
  - Dijelovi navedenih elemenata namijenjenih održavanju sigurnosne politike
- Potrebno kao uslov za samu sigurnost

Lekcija 2. Mrežna sigurnost

- Uvod
- TCP/IP sigurnost
- Firewall

Uvod

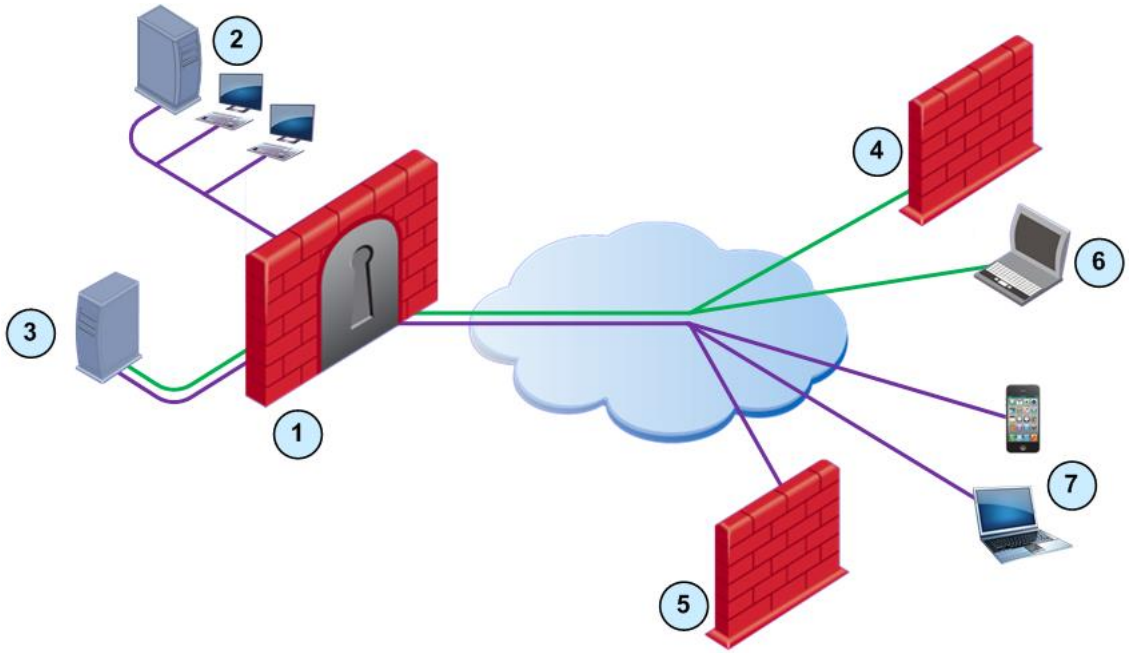
- Mrežna rasprostranjenost
- Protokoli nisu dizajnirani sa elementima sigurnosti
  - U početku
- Greške u postojećim protokolima
- Sve učestali mrežni napadi
  - DoS
  - DDoS

TCP/IP sigurnost

- IP adresa identifikuje hosta, a portovi razgraničavaju rad različitih procesa unutar host okruženja
- Adress spoofing
  - Lažiranje destinacijske adrese
- Primjeri TCP/IP ranjivosti
  - Gubitak izvorne rute
  - Krađa sesija
    - Session hijacking
  - SYN flooding

Firewall

- Razdvaja LAN i WAN
  - Softverski i hardverski
- Kompletan sadržaj mrežnih paketa je podložan prolasku firewall
  - Primjena lokalnih sigurnosnih politika
  - Osnova funkcija je nadgledanje i filtriranje TCP/IP paketa
  - Provjera destinacijskih i izvornih adresa
  - Provjera sadržaja paketa
  - Logiranje/auditing/alarmiranje
- Problemi
  - Mala zaštita za unutarnji saobraćaj
  - Otežavanje poslovnih procesa
  - Implementacija novih servisa



Lekcija 3. Mrežni napadi

- Zašto dolazi do mrežnih napada?
- Ko je glavni krivac?
- Napad
- Zaključak

Zašto dolazi od mrežnih napada?

- Uskraćivanje mrežnih usluga i servisa
  - www
  - Email
  - ...
- Prikrivanje pravog razloga napada
    - Krađa
    - Špijunaža
- Politički razlozi:
  - Information warfare

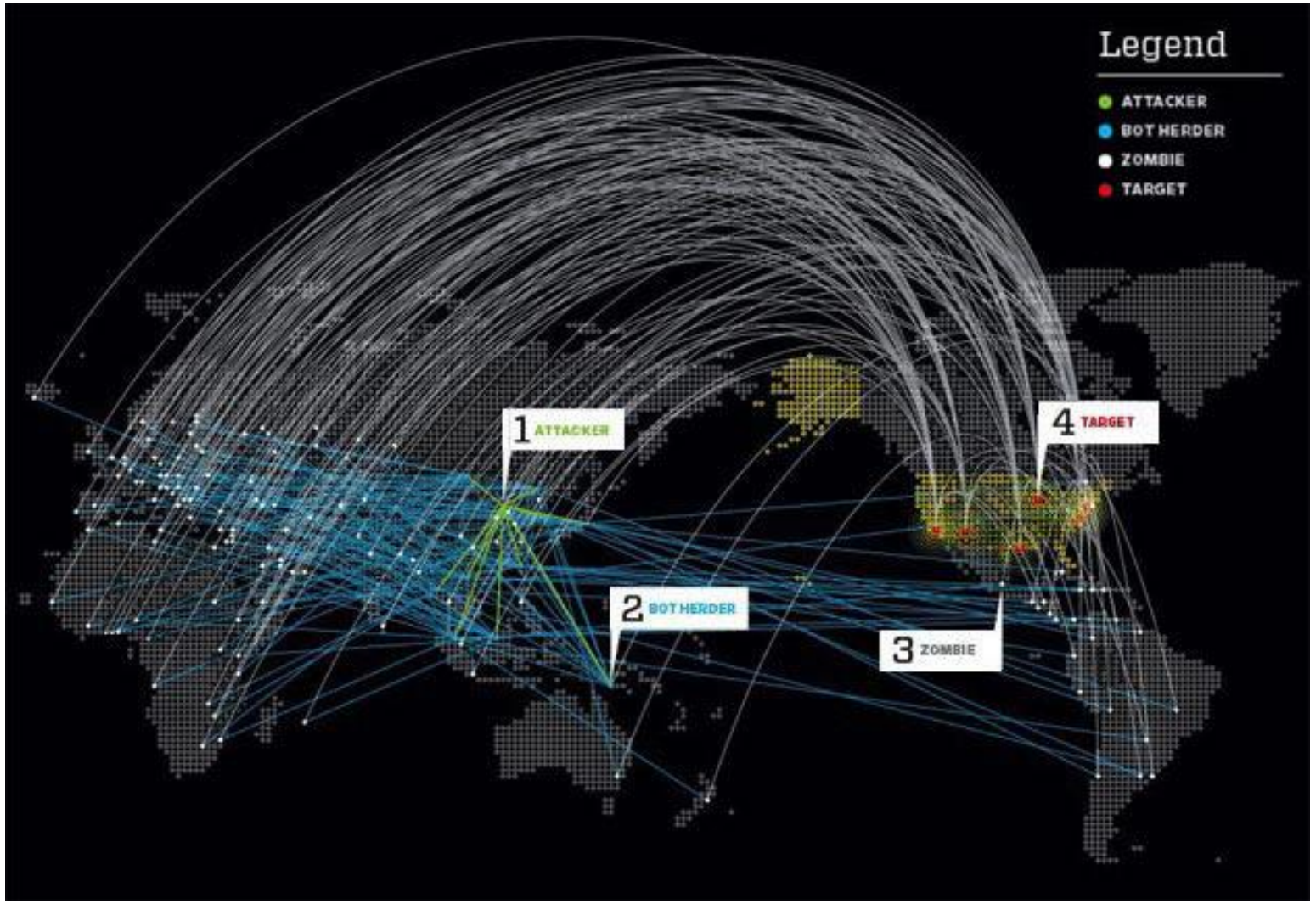
Koje glavni krivac?

- Čovjek
  - Psihologija
  - Naivnost
  - Neznanje
- Protokoli
  - Loše dizajnirani i implementirani mrežni protokoli
- Tehnologija
  - Propusti u softverskim i hadrverskim komponentama

Napadi

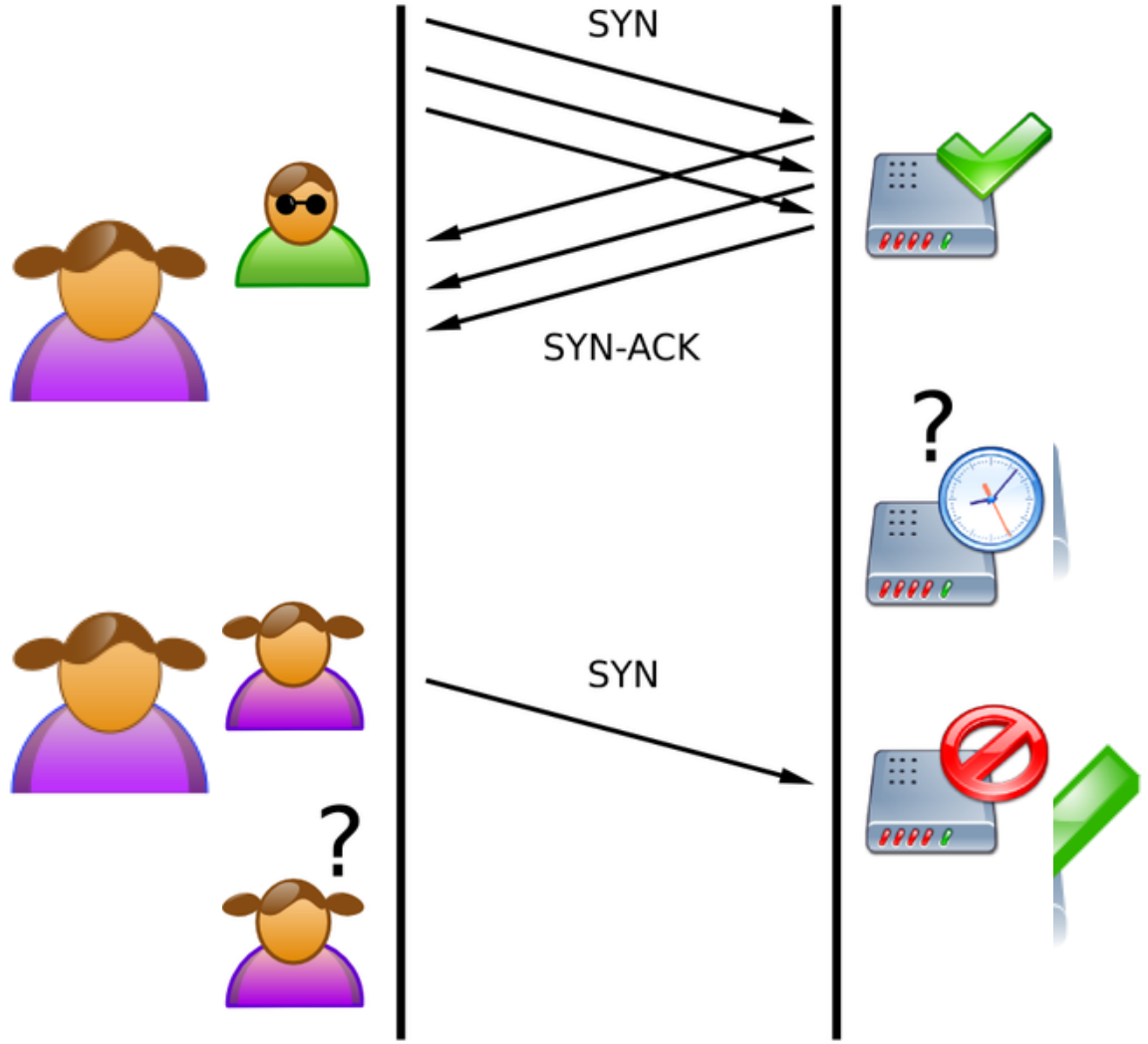
- DoS/DDoS
- SYN Flooding
- ARP Poisoning
- Smurfing (obsolete)

DoS/DDoS



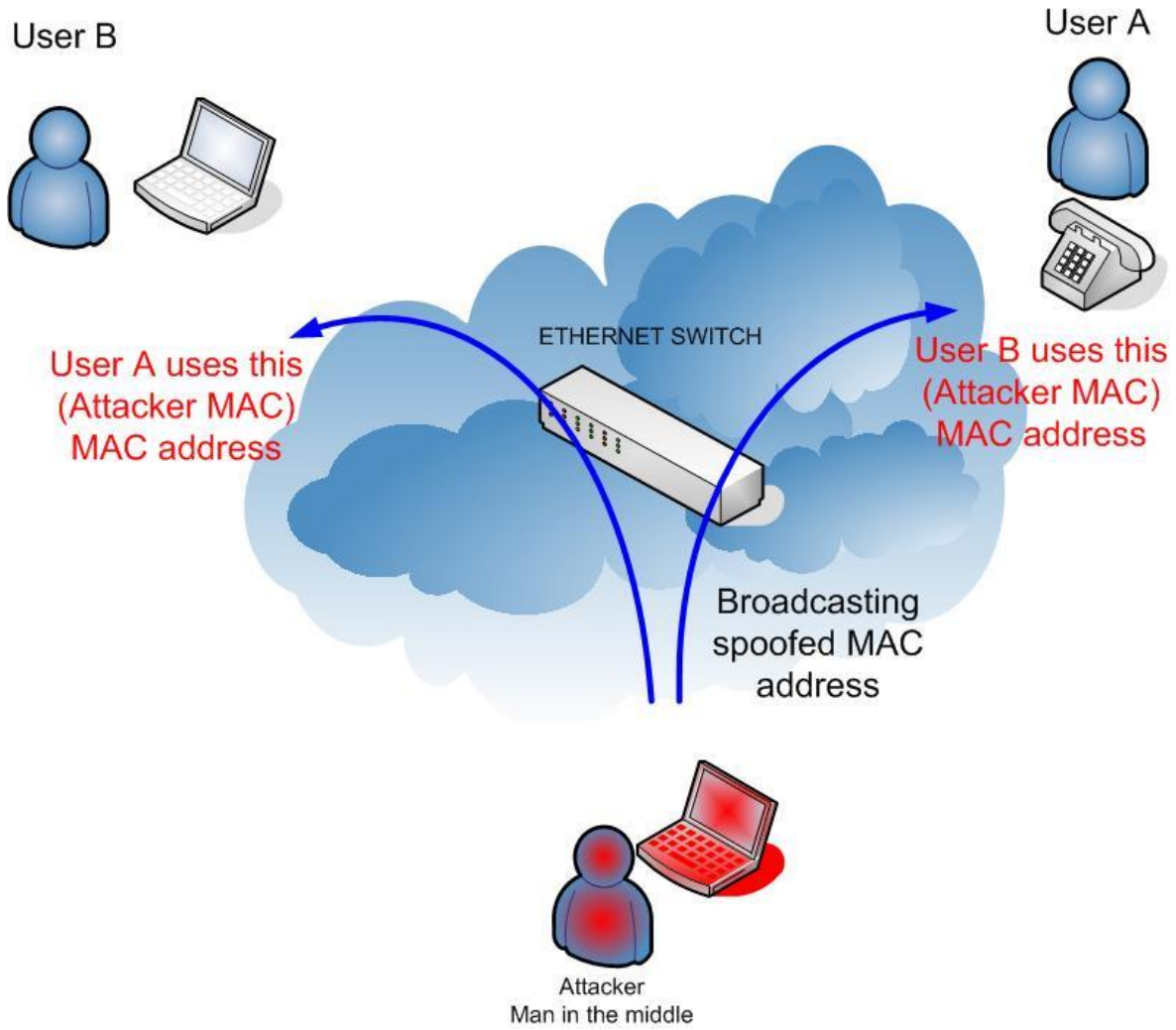
SYN Flooding

- Jedna vrsta DoS napada
- Odbrana
  - SYN Cookies
  - Timeframe limit



ARP Poisoning

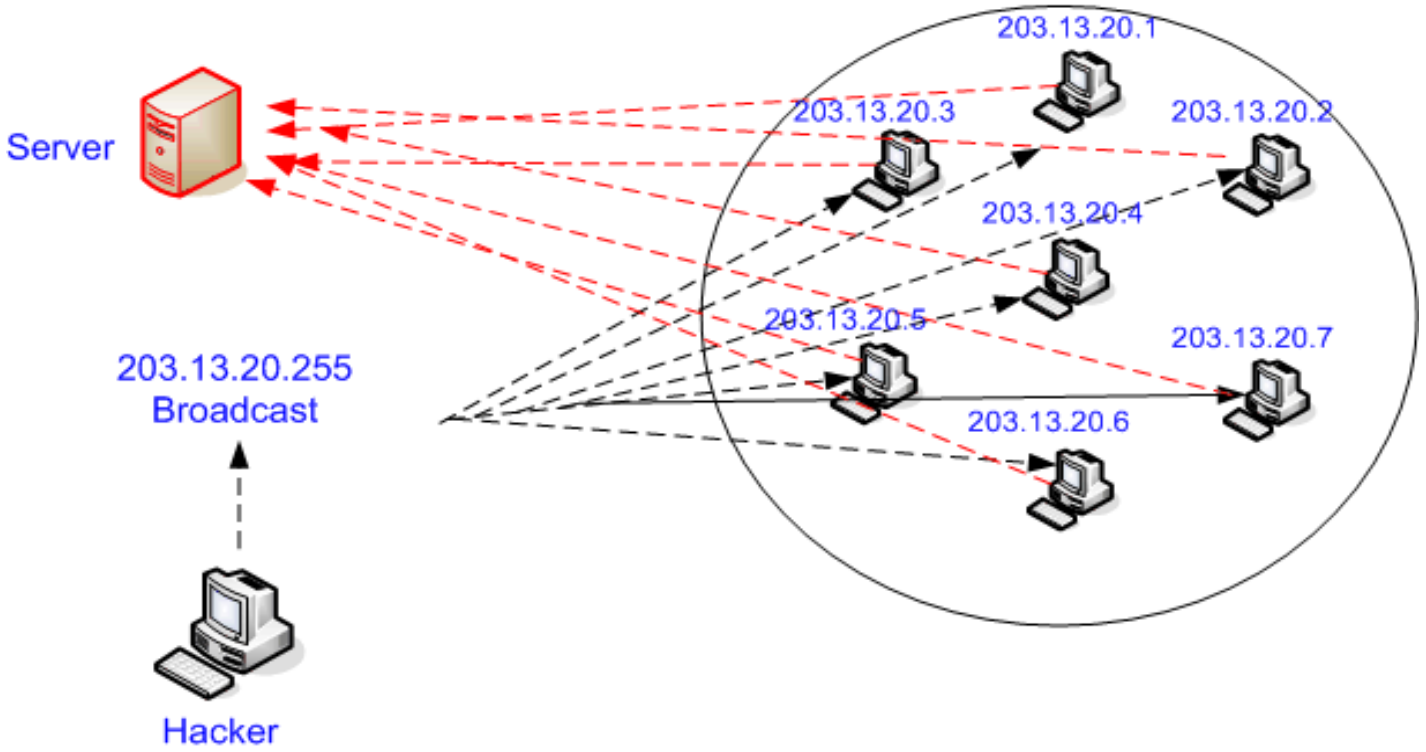
- Odbrana
  - IP2MAC mapiranje
  - Softver za detekciju
  - OS konfiguracija



Smurfing

Jako „popularan“ napad druge polovine 90‘tih

- Vrsta DoS napada
- *ICMP echo request issue*



Zaključak

- Sistem management
- Filtering mrežnog saobraćaja
- Monitoring
- Intrusion detekcija
- Enkripcija

Pitanja