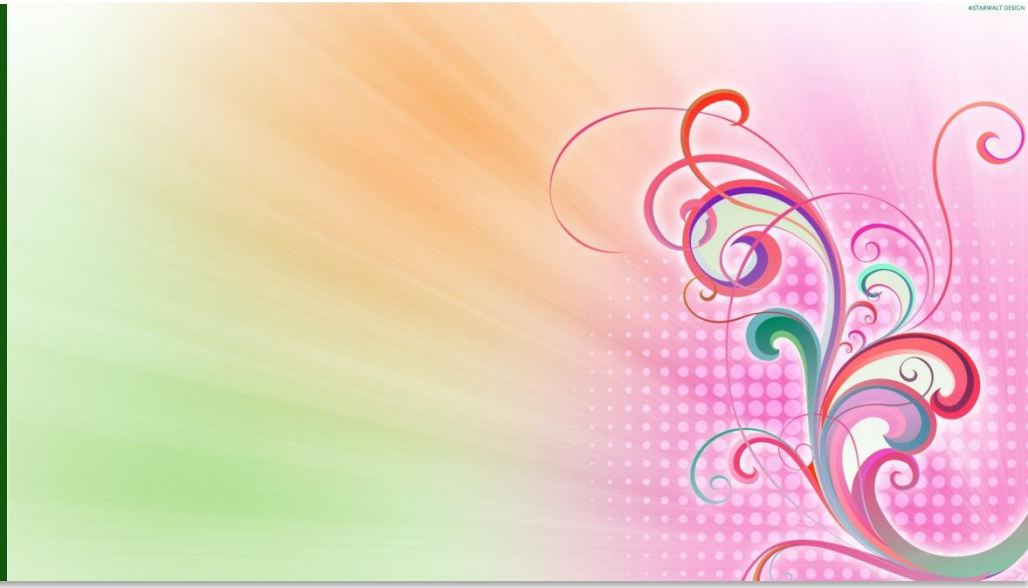
Curs 6: Network-Security

Retele WAN

Silviu Vasile
vsl@fmi.unibuc.ro

Network Security



Obiective

- Identificarea vulnerabilităților în rețelele “enterprise”
- Tipuri de atacuri
- Tehnici de prevenire ale atacurilor
- Securizarea routerelor
- Cisco SDM
- Administrarea fișierelor de pe ruter

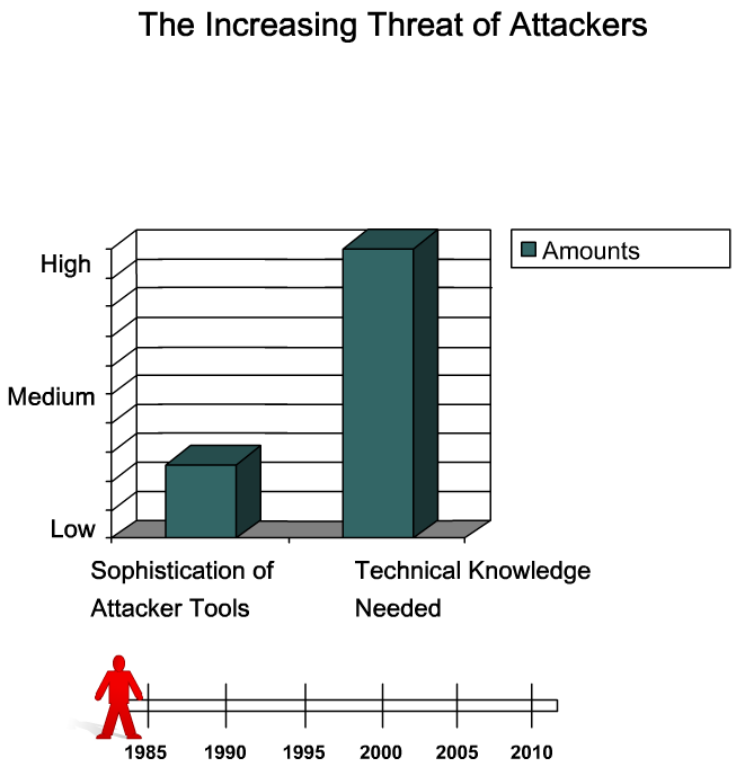
Concepte din securitatea rețelelor

Importanţa securităţii

- Compromiterea securității unei reţele poate avea consecinţe grave
- Securizarea unei rețele constă în găsirea unui echilibru între izolarea completă și expunerea la vulnerabilități, ținând cont de evoluția cerințelor acesteia:
  - e-business,
  - aplicații online
  - rețele wireless

Terminologii

- White hat
- Hacker
- Black hat
- Cracker
- Phreaker
- Spammer
- Phisher

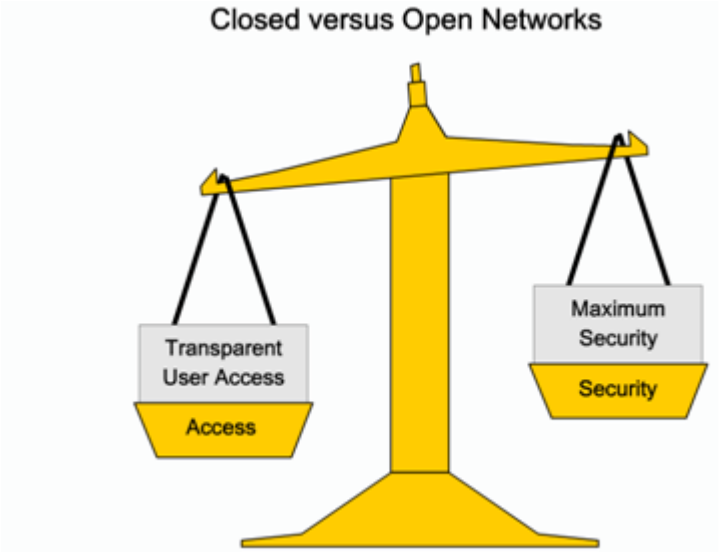


Etapele unui atac

- Footprint analysis (reconnaissance)
- Extinderea numărului de informaţii aflate despre o reţea
- Manipularea utilizatorilor pentru a obţine accesul la o reţea
- Extinderea privilegiilor atacatorului în reţea
- Obţinerea mai multor parole
- Crearea de backdoors
- Folosirea sistemului compromis pentru a ataca alte reţele

Reţele Open vs reţele Closed

- Echilibru între nivelul de acces şi cel de securitate
  - open
  - restrictive
  - closed

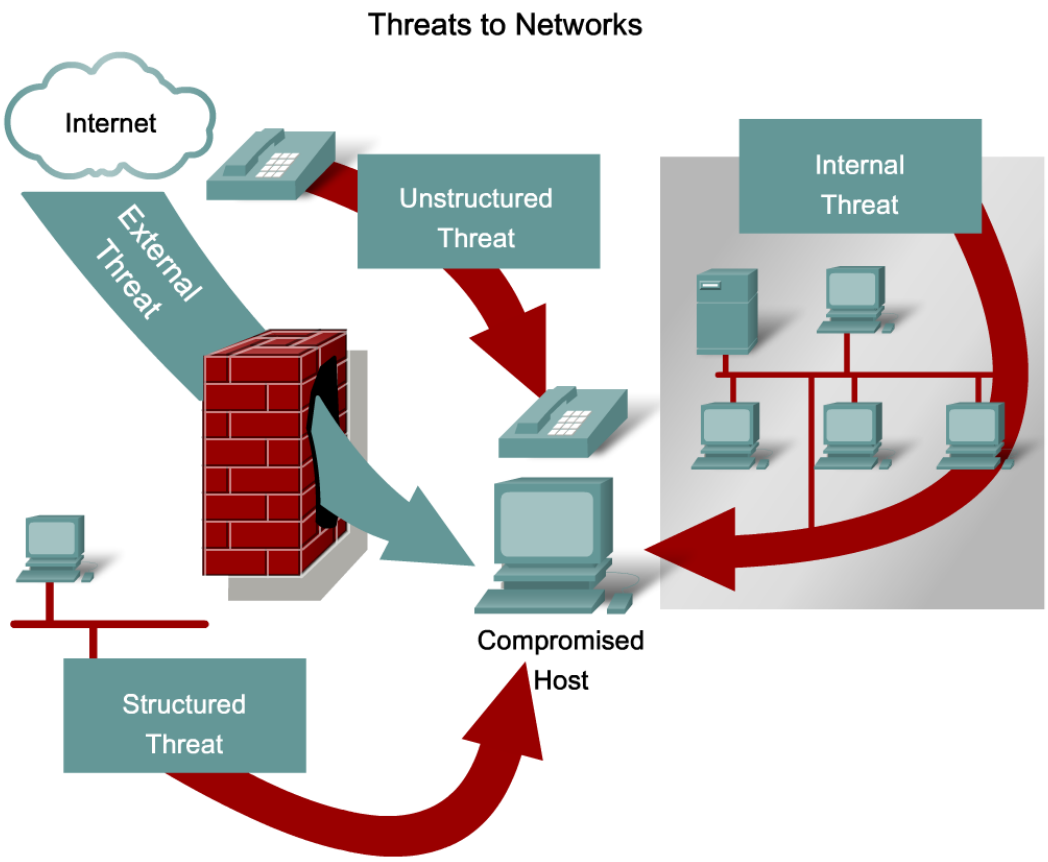


Ameninţări comune (1)

- Vulnerabilităţi
  - tehnice
  - de configuraţie
  - în politicile de securitate
- Ameninţări ale infrastructurii fizice
  - hardware
  - de mediu
  - electrice
  - de administrare
- Social engineering

Ameninţări comune (2)

- Ameninţările unei rețele
  - nestructurate
  - structurate
  - externe
  - interne



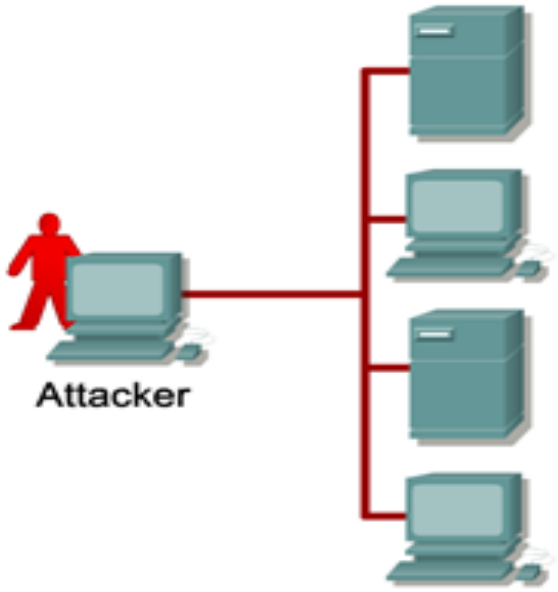
Tipuri de atacuri

Reconnaissance

Access

Denial of Service

Viermi, viruşi, cai troieni



Reconnaissance

- Adunarea neautorizată de informaţii despre sisteme, servicii şi vulnerabilităţi
  - Internet information queries
    - nslookup, whois
  - Ping sweeps
    - fping, gping
  - Port scans
  - Packet sniffers
    - Wireshark, Cain and Abel

Access

- Compromiterea sistemelor la care nu există acces public
  - atacuri de parole
    - brute force
    - rainbow table
    - trojan horse
    - packet sniffer
  - trust exploitation
    - compromiterea unui host de încredere din reţea şi folosirea acestuia pentru a porni alte atacuri către acea reţea
  - port redirection
  - man in the middle

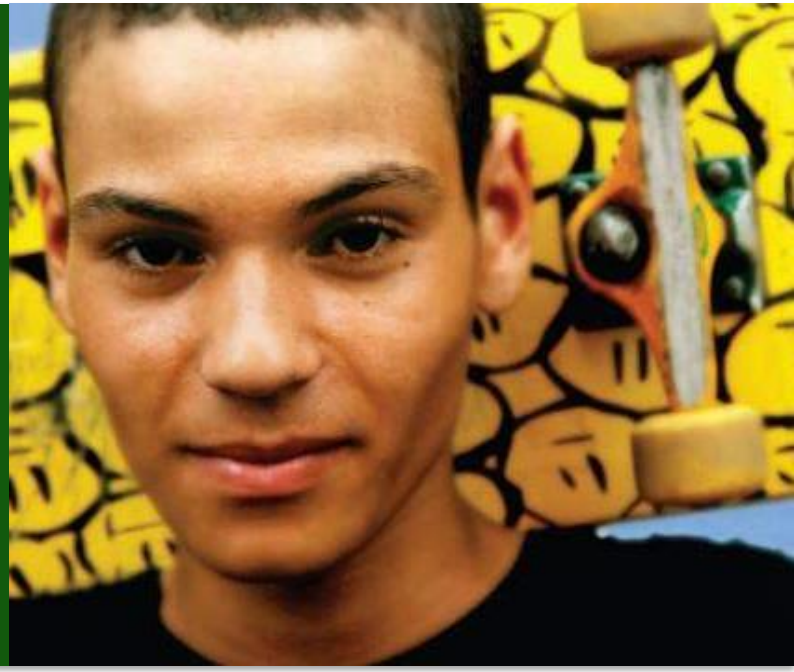
Denial of Service

- Întreruperea funcţionării unor sisteme sau a unor servicii
  - Ping of death
    - modifică header-ul unui pachet ping pentru a indica dimensiuni foarte mari
  - SYN flood
    - exploatează TCP 3-way handshake
    - trimite multe SYN REQ, dar nu răspunde la SYN ACK ale victimei
  - DDoS
    - sute de mii de atacuri Distributed DoS ce duc la saturarea conexiunilor
    - Smurf attack

Atacuri Software

- Viermi
  - **autoinstalare** prin exploatarea vulnerabilităților cunoscute ale unui sistem (ex: deschiderea unui mail cu ataşament)
  - mecanism de **propagare**
  - **extindere** a privilegiilor atacatorului
- Viruşi
  - software ataşat de un alt program executabil pentru a executa o anumită funcție pe hostul atacat
- Trojan Horses
  - aplicaţie propriu-zisă creată să se asemene cu o aplicaţie cunoscută în scopul exploatării unui host sau a unei rețele

Tehnici de prevenire



Tehnici de prevenire

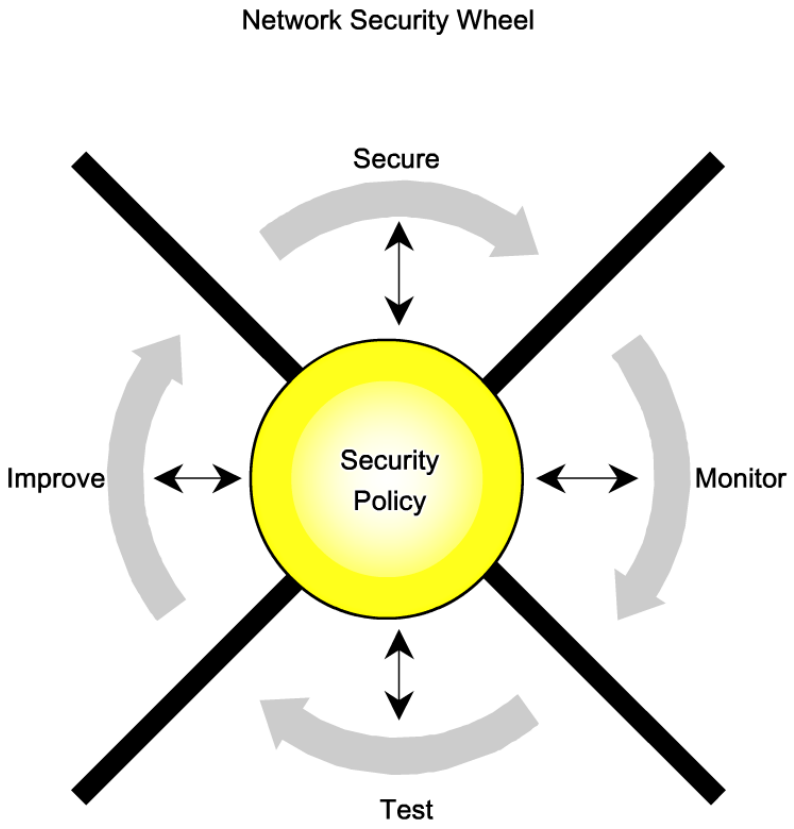
- Device hardening
- Antiviruşi
- Firewall
- Patch-uri pentru SO-uri
- IDS
- IPS

Aplicaţii şi echipamente pentru securitate

- Soluţii pentru controlul ameninţărilor
  - Cisco ASA 5500 Series Adaptive Security Appliances
  - Integrated Services Routers (ISR)
  - Network Admission Control
  - Cisco Security Agent for Desktops
  - Cisco Intrusion Prevention Systems (Cisco IPS 4200 Series Sensors)
- Soluţii pentru comunicaţii sigure (VPN)
  - rutere Cisco ISR cu soluţie Cisco IOS VPN
  - Cisco 5500 ASA
  - switch-uri Cisco Catalyst 6500

Network Security Wheel

- Pas 1: Securizare
- Pas 2: Monitorizare
- Pas 3: Testare
- Pas 4: Îmbunătăţire



Politică de securitate

- “A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.”

  (RFC 2196, Site Security Handbook)

- Protejează oamenii şi informaţia
- Set de reguli pentru comportamente aşteptate
- Permite monitorizarea, probarea şi investigarea
- Defineşte consecinţele nerespectării regulilor

Componentele unei politici de securitate

- Statement of authority and scope
- Acceptable use policy (AUP)
- Identification and authentication policy
- Internet access policy
- Campus access policy
- Remote access policy
- Incident handling procedure

Securizarea ruterelor

Categorii de securizare

- Securizare fizică
- Updatare IOS
- Back-up pentru fișierul de configurare și IOS
- Securizare în vederea eliminării exploatării potențiale a serviciilor si port-urilor neutilizate

Cisco IOS Security

- Pas 1: Securizarea folosind parole criptate
- Pas 2: Securizarea accesului remote
- Pas 3: Logarea activităţii pe ruter
- Pas 4: Securizarea serviciilor vulnerabile
- Pas 5: Securizarea protocoalelor de rutare
- Pas 6: Filtrarea traficului

Pas1: Securizarea router-ului

- Configurarea securităţii de bază

- Configurarea de utilizatori

```
Router(config)#username cisco password ccna
```

- Criptarea parolelor de tip 7

```
Router(config)#service password-encryption
```

- Parole criptate md5

```
Router(config)#enable secret P4r014.cr1pt4t4
```

- Lungimea minimă a parolelor

```
Router(config)#security passwords min-length 15
```

Pas2: Securizarea accesului remote (1)

- Stabilirea unei rețele dedicate de management
  - doar echipamente de rețea și host-uri destinate administrării
  - VLAN separat sau rețea fizică separată
- Criptarea traficului între host-ul de administrare și router
  - se pot utiliza filtre pentru permiterea accesului exclusiv al unor anumite host-uri la router prin protocolul utilizat (SSH)

– Controlarea accesului pe VTY

```
Router(config)#line vty 0 4
Router(config-line)#no transport input
Router(config-line)#transport input ssh
```

– Comenzi adiționale pentru securizarea liniilor VTY

```
Router(config)#service tcp-keepalives-in
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 3 0
```

Pas2: Securizarea accesului remote (2)

- Configurarea SSH

- Configurarea parametrilor routerului

```
Router(config)#hostname R2
```

- Configurarea domeniului

```
R2(config)#ip domain-name cisco
```

- Generarea cheilor asimetrice (se recomandă lungimea minimă de *1024*)

```
R2(config)#crypto key generate rsa
```

- Configurarea bazei de date locale de autentificare și a liniilor VTY

```
R2(config)#username student secret cisco
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
```

- Configurarea timeout-urilor

```
R2(config)#ip ssh time-out 15
R2(config)#ip ssh authentication-retries 2
```

Pas3: Logarea activității pe ruter

- Syslog
  - se recomandă trimiterea log-urilor către un host dedicat si securizat
  - exemplu de aplicație pentru un server de syslog: Kiwi Syslog Daemon
  - mai multe nivele de logging:
    - 0 – mesaje de instabilitate ale sistemului
    - 7 – mesaje de debug cu informații generale despre router
- Service timestamps
  - folosirea unui server de NTP pentru sincronizarea ceasului pe echipamente

Pas4: Securizarea serviciilor vulnerabile

- Servicii ce trebuie dezactivate în general:

```
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no service finger
no ip http server
no snmp server
```

- Servicii ce permit anumite tipuri de pachete si configurarea remote:

```
no cdp run
no service config
no ip source-route
```

- Securizarea interfețelor:

```
shutdown (interfețe neutilizate)
no ip directed-broadcast
no ip proxy-arp
```

- Cisco auto secure: specificații ale interfețelor, banner, parole, SSH, IOS firewall features

Pas5: Securizarea protocoalelor de rutare(2)

- EIGRP

```
Router(config)#key chain EIGRP_KEY
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string cisco
Router(config)#interface serial0/0
Router(config-if)#ip authentication mode eigrp 1 md5
Router(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
```

- OSPF

```
Router(config)#router ospf 1
Router(config-router)#area 0 authentication message-digest
Router(config)#interface serial0/0
Router(config-if)#ip ospf message-digest-key 1 md5 cisco
Router(config-if)#ip ospf authentication message-digest
```

Cisco SDM

Cisco Router and Security Device Manager (SDM)

- Instrument de management al rețelei web-based
- Se poate instala atât pe router cât și pe PC
- Preinstalat “by default” pe toate ruterele Cisco ISR
- Conține wizard-uri inteligente
- ACL management
- VPN crypto map editor
- Cisco IOS CLI preview
- Ruter lock down

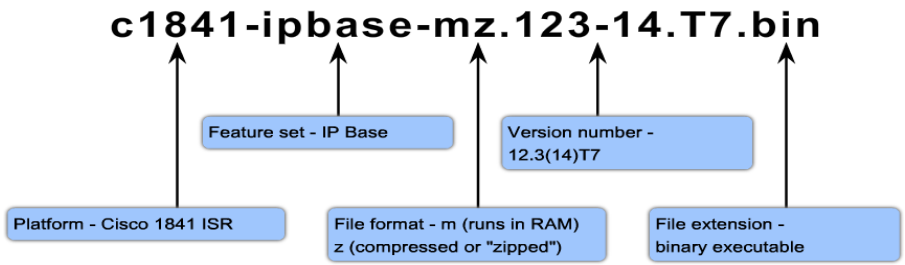
Configurarea routerului pentru SDM

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication-local
Router(config)#username student privilege 15 secret cisco
Router(config)#line vty 0 4
Router(config-if)#privilege level 15
Router(config-if)#login local
Router(config-if)#transport input telnet ssh
```

Administrarea fișierelor de pe router

Administrarea IOS

- Convenția de denumire a Cisco IOS



- Back-up pe server TFTP

```
R#copy flash: tftp:
```

- Upgrade IOS de pe server TFTP

```
R#copy tftp: flash:
```

- Restaurare IOS (IOS-ul curent nu este funcțional)

```
rommon1>IP_ADDRESS=
rommon2>IP_SUBNET_MASK=
rommon3>DEFAULT_GATEWAY=
rommon4>TFTP_SERVER=
rommon5>TFTP_FILE=
rommon6>tftpdnld
```

- Restaurare IOS folosind Xmodem (transfer IOS prin cablu consolă)

```
rommon1>xmodem -c  nume IOS
```

Password recovery

- Necesită acces fizic la portul de consolă al echipamentului

- Pas 1. Repornirea ruter-ului
- Pas 2. Apăsarea “break” în primele 60s de la pornirea ruterului pentru a intra in ROMmon
- Pas 3. Schimbarea valorii registrului de config astfel încât la bootare să se ignore fișierul de configurare

```
rommon>confreg 0x2142
```

- Pas 4. Reboot și intrare în modul privilegiat (enable)
- Pas 5. Copy startup-config în running-config
- Pas 6. Resetarea parolei, modificarea registrului de configurare la 0x2102 (default), no shutdown pe interfețele ce vor fi folosite

Multumesc!