PREPARAZIONE DI UN ATTACCO IN RETE: “ENUMERATION”

Corso di Laurea Magistrale in Ingegneria Informatica

A.A. 2015/2016

Prof. Simon Pietro Romano

spromano@unina.it

COME SI PREPARA UN ATTACCO DI RETE?

- Concetti vitali per chiunque si voglia preparare, con cognizione di causa, a sferrare un attacco in una rete di calcolatori:
  - *footprinting:*
    - l'arte di raccogliere informazioni in rete
      - la cosiddetta "network reconnaissance"
  - *scanning:*
    - ispezione minuziosa del "perimetro" di attacco, alla ricerca di potenziali punti di ingresso
  - *enumeration:*
    - 'probing' dei servizi identificati, al fine di identificare potenziali vulnerabilità

ENUMERATION vs SCANNING

- La principale differenza tra le tecniche di enumeration e quelle di scanning risiede nel più alto livello di intrusività delle prime:
  - l'enumerazione richiede:
    - la creazione di connessioni "attive" verso i sistemi analizzati
    - l'invio di "query" esplicite verso i servizi individuati in fase di scanning
- Per sua natura, l'enumeration è:
  - ☹ più pericolosa delle altre tecniche di raccolta delle informazioni
    - accesso a dati di dettaglio sui servizi individuati
  - ☺ più "tracciabile" e, quindi, più facilmente rilevabile da parte dei sistemi di sicurezza di cui l'organizzazione target è (auspicabilmente!) dotata

INFORMAZIONI RICERCATE

- Nomi di account utente
  - per pilotare eventuali attacchi di tipo “password guessing”
- Risorse condivise mal configurate
  - es: cartelle di file system condivise e non protette opportunamente
- Versioni meno recenti di moduli software, potenzialmente “bacate”
  - es: web server vulnerabili ad attacchi del tipo “buffer overflow”

CARATTERISTICHE DELL'ENUMERATION

- Le tecniche di enumeration sono strettamente collegate alle caratteristiche specifiche delle piattaforme hardware/software oggetto di analisi
- Esse, dunque, dipendono fortemente dai dati raccolti in fase di scanning
  - molto spesso, le fasi di scanning e di enumeration coesistono (e vengono condotte in maniera sequenziale) nel medesimo tool
  - fase 1:
    - scansione delle porte (scanning)
  - fase 2:
    - "banner grabbing" sui servizi trovati attivi, al fine di determinare il tipo di sistema operativo in esecuzione sul target (enumeration)

SERVICE FINGERPRINTING

- Il passo successivo al “port scanning”
  - una volta individuate le porte aperte…
  - …si passa all’analisi dettagliata dei servizi ad esse associati:
    - versione, eventuali revisioni, livello di “patch” applicato
- Tipicamente condotto in maniera atuomatizzata sfruttando le tecniche messe a disposizione da tool quali *nmap*
- Gli attaccanti tipicamente si affidano alle tecniche cosiddette “manuali” solo in caso di requisiti di estrema robustezza dell’attacco rispetto alla possibilità di essere tracciato

VERSION SCANNING CON NMAP

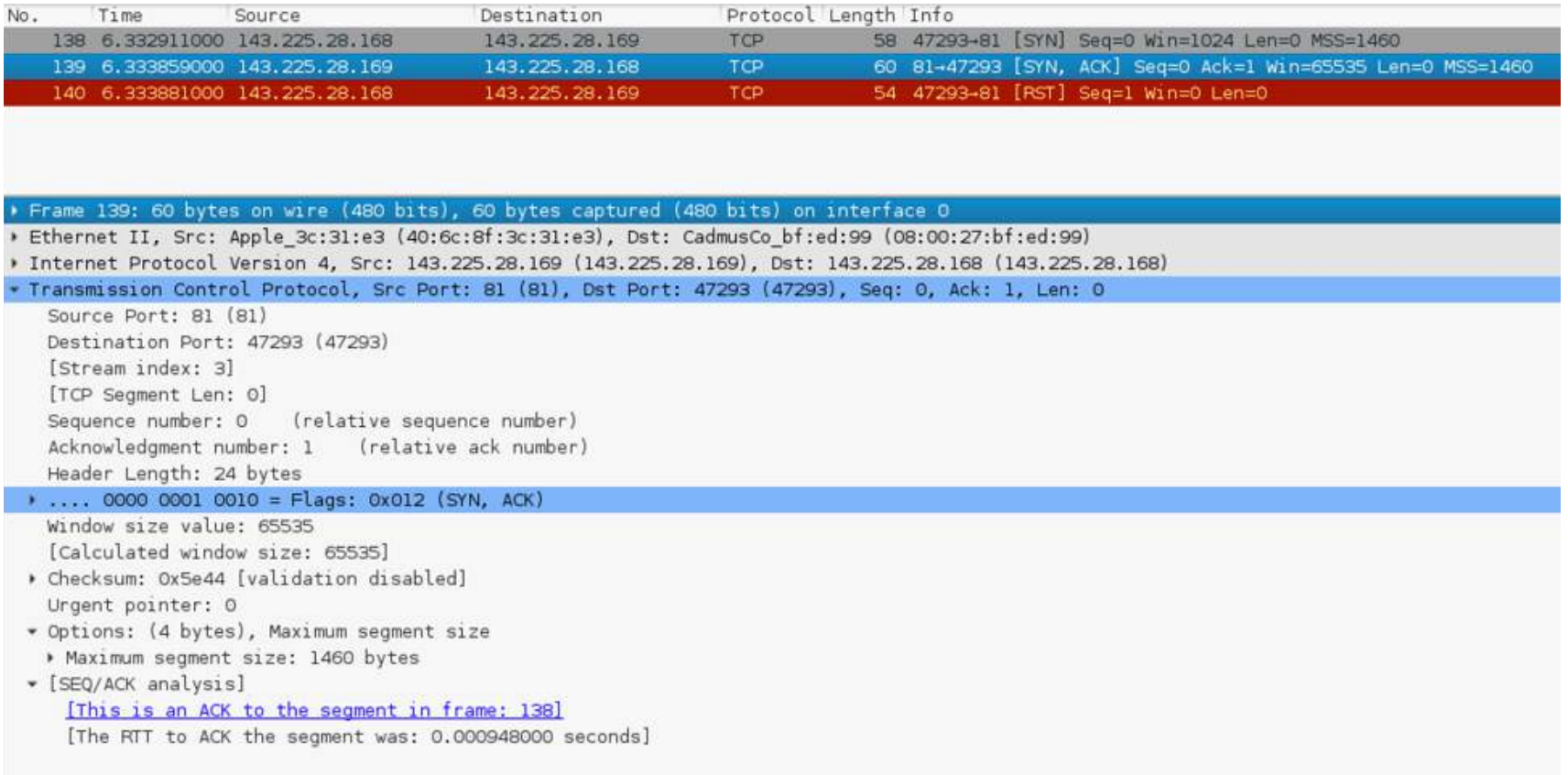
- Impiego dello switch “-sV”
  - interroga le porte aperte, sollecitando feedback e confrontando le risposte con un database di “firme” associate ai singoli servizi ed alle relative versioni/ implementazioni
  - consente di scoprire servizi in ascolto su porte “non di default”

“SCANNING” vs “ENUMERATION” CON *nmap*

```
root@kali:~# nmap -sS 143.225.28.169 -p 81

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-05 06:45 EDT
Nmap scan report for 143.225.28.169
Host is up (0.0013s latency).
PORT   STATE SERVICE
81/tcp open  hosts2-ns
MAC Address: 40:6C:8F:3C:31:E3 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
root@kali:~# nmap -sV 143.225.28.169 -p 81

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-05 06:45 EDT
Nmap scan report for 143.225.28.169
Host is up (0.00068s latency).
PORT   STATE SERVICE VERSION
81/tcp open  http    Apache httpd 2.4.4 ((Unix) PHP/5.4.16 OpenSSL/1.0.1e mod_perl/2.0.8-dev Perl/v5.16.3)
MAC Address: 40:6C:8F:3C:31:E3 (Apple)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds
```

Presenza di un server HTTP in ascolto sulla porta 81!

DIETRO LE QUINTE: “SCANNING”



No.	Time	Source	Destination	Protocol	Length	Info
138	6.332911000	143.225.28.168	143.225.28.169	TCP	58	47293→81 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	6.333859000	143.225.28.169	143.225.28.168	TCP	60	81→47293 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
140	6.333881000	143.225.28.168	143.225.28.169	TCP	54	47293→81 [RST] Seq=1 Win=0 Len=0

```
▸ Frame 139: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Apple_3c:31:e3 (40:6c:8f:3c:31:e3), Dst: CadmusCo_bf:ed:99 (08:00:27:bf:ed:99)
▸ Internet Protocol Version 4, Src: 143.225.28.169 (143.225.28.169), Dst: 143.225.28.168 (143.225.28.168)
▾ Transmission Control Protocol, Src Port: 81 (81), Dst Port: 47293 (47293), Seq: 0, Ack: 1, Len: 0
    Source Port: 81 (81)
    Destination Port: 47293 (47293)
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 24 bytes
  ▸ .... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
    Window size value: 65535
    [Calculated window size: 65535]
  ▸ Checksum: 0x5e44 [validation disabled]
    Urgent pointer: 0
  ▾ Options: (4 bytes), Maximum segment size
    ▸ Maximum segment size: 1460 bytes
  ▾ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 138]
      [The RTT to ACK the segment was: 0.000948000 seconds]
```

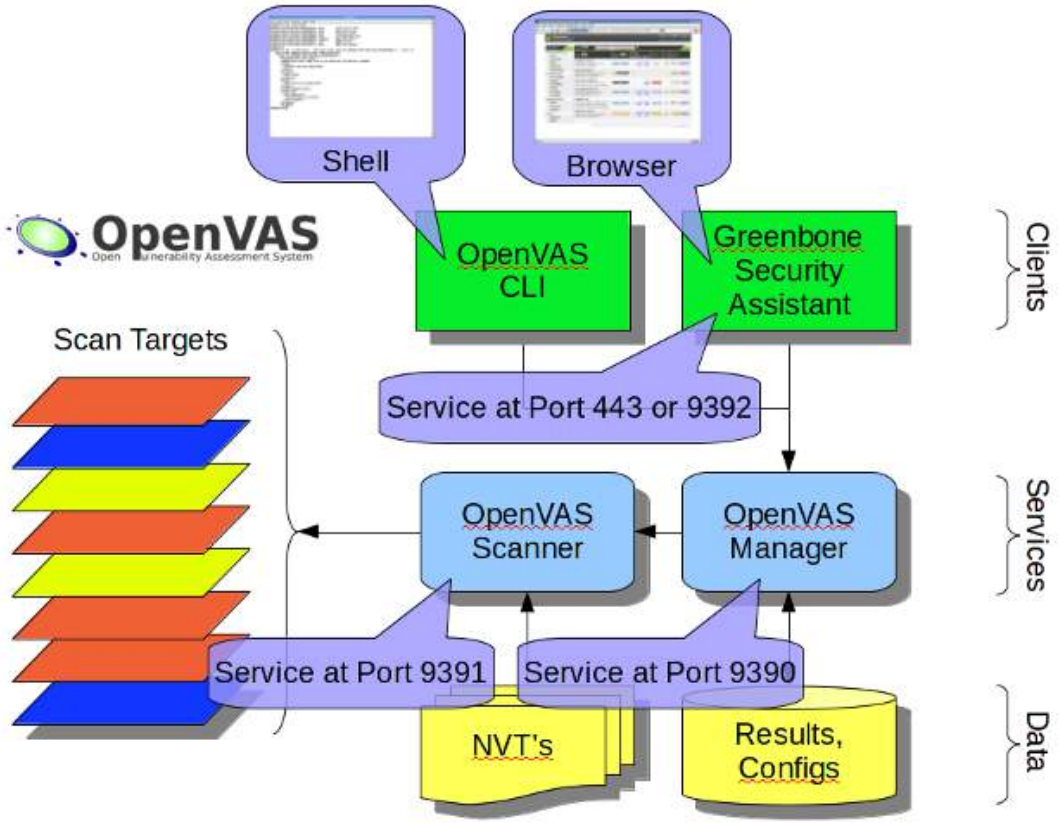
DIETRO LE QUINTE: “ENUMERATION”

No.	Time	Source	Destination	Protocol	Length	Info
98	4.641790000	143.225.28.168	143.225.28.169	TCP	58	49769→81 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
99	4.642583000	143.225.28.169	143.225.28.168	TCP	60	81→49769 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
100	4.642590000	143.225.28.168	143.225.28.169	TCP	54	49769→81 [RST] Seq=1 Win=0 Len=0
104	4.742019000	143.225.28.168	143.225.28.169	TCP	58	49770→81 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
105	4.742915000	143.225.28.169	143.225.28.168	TCP	60	81→49770 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
106	4.742931000	143.225.28.168	143.225.28.169	TCP	54	49770→81 [RST] Seq=1 Win=0 Len=0
108	4.881624000	143.225.28.168	143.225.28.169	TCP	74	59451→81 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2772176 TSecr=0 WS=1024
109	4.882600000	143.225.28.169	143.225.28.168	TCP	78	81→59451 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=330830057 TSecr=2772176 SACK_PERM=1
110	4.882629000	143.225.28.168	143.225.28.169	TCP	66	59451→81 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=2772176 TSecr=330830057
111	4.883466000	143.225.28.169	143.225.28.168	TCP	66	[TCP Window Update] 81→59451 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=330830057 TSecr=2772176
244	10.88972500	143.225.28.168	143.225.28.169	HTTP	84	GET / HTTP/1.0
245	10.89056800	143.225.28.169	143.225.28.168	TCP	66	81→59451 [ACK] Seq=1 Ack=19 Win=131744 Len=0 TSval=330836055 TSecr=2773678
246	10.89234800	143.225.28.169	143.225.28.168	HTTP	460	HTTP/1.1 302 Found (text/html)
247	10.89236500	143.225.28.168	143.225.28.169	TCP	66	59451→81 [ACK] Seq=19 Ack=395 Win=30720 Len=0 TSval=2773678 TSecr=330836056
248	10.89238100	143.225.28.169	143.225.28.168	TCP	66	81→59451 [FIN, ACK] Seq=395 Ack=19 Win=131744 Len=0 TSval=330836056 TSecr=2773678
249	10.89277000	143.225.28.168	143.225.28.169	TCP	66	59451→81 [FIN, ACK] Seq=19 Ack=396 Win=30720 Len=0 TSval=2773678 TSecr=330836056
250	10.89279100	143.225.28.169	143.225.28.168	TCP	66	[TCP Out-Of-Order] 81→59451 [FIN, ACK] Seq=395 Ack=19 Win=131744 Len=0 TSval=330836056 TSecr=2773678
251	10.89279100	143.225.28.168	143.225.28.169	TCP	78	[TCP Dup ACK 249#1] 59451→81 [ACK] Seq=20 Ack=396 Win=30720 Len=0 TSval=2773679 TSecr=330836056 SLE=395 SRE=
252	10.89297400	143.225.28.169	143.225.28.168	TCP	66	81→59451 [ACK] Seq=396 Ack=20 Win=131744 Len=0 TSval=330836057 TSecr=2773678
253	10.96664200	143.225.28.168	143.225.28.169	TCP	74	59452→81 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2773697 TSecr=0 WS=1024
254	10.96763400	143.225.28.169	143.225.28.168	TCP	78	81→59452 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=330836130 TSecr=2773697 SACK_PERM=1
255	10.96764700	143.225.28.168	143.225.28.169	TCP	66	59452→81 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=2773697 TSecr=330836130
256	10.96825900	143.225.28.169	143.225.28.168	TCP	66	[TCP Window Update] 81→59452 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=330836130 TSecr=2773697
257	10.96855600	143.225.28.168	143.225.28.169	HTTP	84	GET / HTTP/1.0
258	10.96925200	143.225.28.169	143.225.28.168	TCP	66	81→59452 [ACK] Seq=1 Ack=19 Win=131744 Len=0 TSval=330836131 TSecr=2773697
259	10.97052300	143.225.28.169	143.225.28.168	HTTP	460	HTTP/1.1 302 Found (text/html)
260	10.97053900	143.225.28.168	143.225.28.169	TCP	66	59452→81 [ACK] Seq=19 Ack=395 Win=30720 Len=0 TSval=2773698 TSecr=330836132
261	10.97056600	143.225.28.169	143.225.28.168	TCP	66	81→59452 [FIN, ACK] Seq=395 Ack=19 Win=131744 Len=0 TSval=330836132 TSecr=2773697
262	10.97086000	143.225.28.168	143.225.28.169	TCP	74	59453→81 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2773698 TSecr=0 WS=1024
263	10.97105900	143.225.28.169	143.225.28.168	TCP	66	[TCP Out-Of-Order] 81→59452 [FIN, ACK] Seq=395 Ack=19 Win=131744 Len=0 TSval=330836132 TSecr=2773698
264	10.97106400	143.225.28.168	143.225.28.169	TCP	78	59452→81 [ACK] Seq=19 Ack=396 Win=30720 Len=0 TSval=2773698 TSecr=330836132 SLE=395 SRE=396
265	10.97138200	143.225.28.169	143.225.28.168	TCP	78	81→59453 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=330836133 TSecr=2773698 SACK_PERM=1
266	10.97139400	143.225.28.168	143.225.28.169	TCP	66	59453→81 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=2773698 TSecr=330836133
267	10.97140300	143.225.28.169	143.225.28.168	TCP	66	[TCP Dup ACK 263#1] 81→59452 [ACK] Seq=396 Ack=19 Win=131744 Len=0 TSval=330836133 TSecr=2773698
268	10.97152000	143.225.28.168	143.225.28.169	HTTP	106	GET / HTTP/1.1
269	10.97188800	143.225.28.169	143.225.28.168	TCP	66	[TCP Window Update] 81→59453 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=330836133 TSecr=2773698
270	10.97189300	143.225.28.169	143.225.28.168	TCP	66	81→59453 [ACK] Seq=1 Ack=41 Win=131712 Len=0 TSval=330836133 TSecr=2773698
271	10.97248600	143.225.28.169	143.225.28.168	HTTP	322	HTTP/1.1 302 Found
272	10.97249100	143.225.28.168	143.225.28.169	TCP	66	59453→81 [ACK] Seq=41 Ack=257 Win=30720 Len=0 TSval=2773698 TSecr=330836134
273	10.97273400	143.225.28.168	143.225.28.169	TCP	66	59452→81 [FIN, ACK] Seq=19 Ack=396 Win=30720 Len=0 TSval=2773698 TSecr=330836133
274	10.97274600	143.225.28.168	143.225.28.169	TCP	66	59453→81 [FIN, ACK] Seq=41 Ack=257 Win=30720 Len=0 TSval=2773699 TSecr=330836134

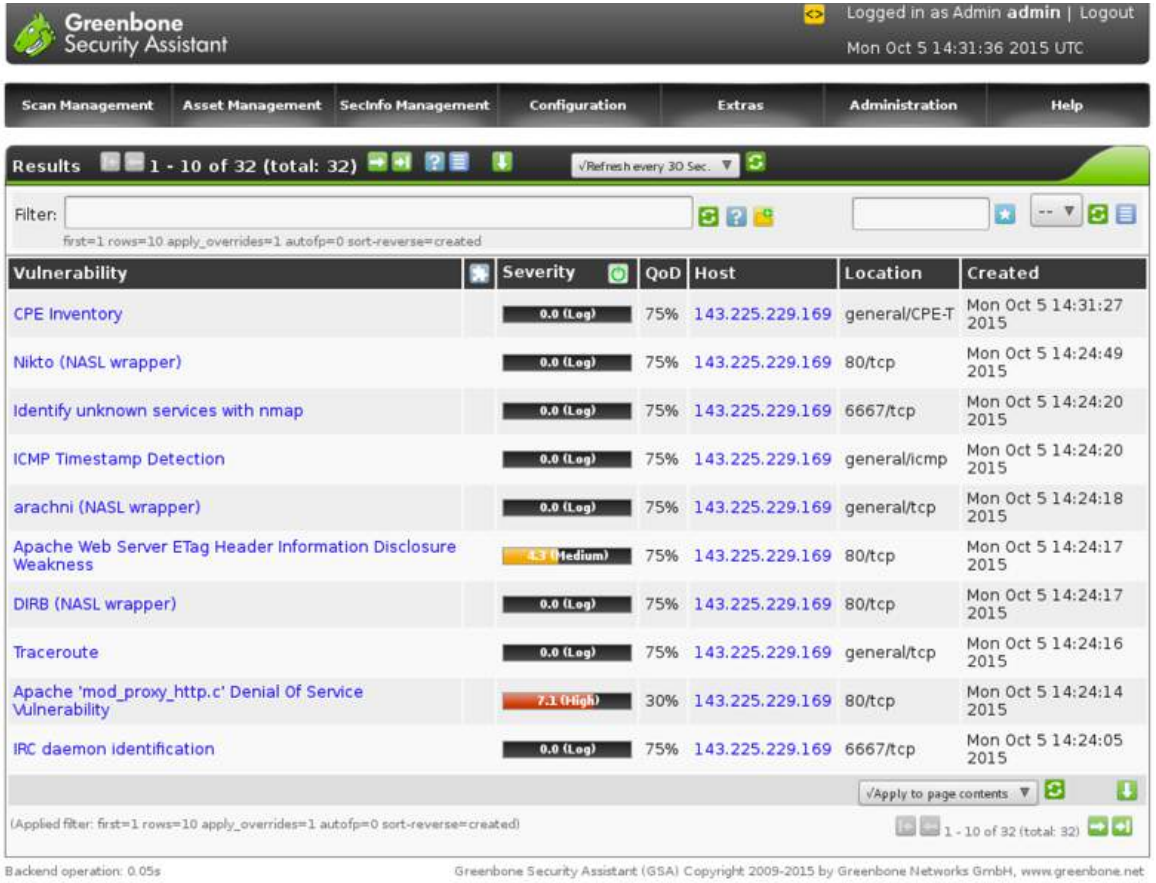
VULNERABILITY SCANNERS

- Tipicamente utilizzati quando non ci si preoccupa più di tanto di coprire le tracce dell'attività di scanning
- Basati sulla raccolta e l'aggiornamento di "signatures" di vulnerabilità note relative a tutti i tipi di processi potenzialmente in ascolto su una porta di rete:
  - sistema operativo, servizi di rete, applicazioni web, basi di dati, ecc.
- Moltissimi strumenti disponibili allo scopo, sia in ambito commerciale, sia nella comunità open source
  - es: OpenVAS → Open Vulnerability Assessment System

OpenVAS: ARCHITETTURA GENERALE



OpenVAS IN AZIONE



OpenVAS: REPORTISTICA

Scan Report

October 5, 2015

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 143.225.229.169". The scan started at Mon Oct 5 14:23:40 2015 UTC and ended at Mon Oct 5 14:31:28 2015 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

. . . continued from previous page . . .

A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result
Information that was gathered:
Inode: 11278888
Size: 434

Impact
Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution
OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.
Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method
Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.
Details:Apache Web Server ETag Header Information Disclosure Weakness
OID:1.3.6.1.4.1.25623.1.0.103122
Version used: $Revision: 1218 $

References
CVE: CVE-2003-1418
BID:6939
Other:
URL:https://www.securityfocus.com/bid/6939
URL:http://httpd.apache.org/docs/mod/core.html#fileetag
URL:http://www.openbsd.org/errata32.html
URL:http://support.novell.com/docs/Tids/Solutions/10090670.html

NMAP SCRIPTING ENGINE (NSE)

- Un'interfaccia che consente agli utenti *nmap* di estenderne le potenzialità attraverso script realizzati in linguaggio *Lua*
  - invio e ricezione di dati, creazione di report, ecc.
- Moltissimi script disponibili di default:
  - network discovery, rilevamento della versione dei servizi di rete, scoperta di backdoor, sfruttamento di vulnerabilità (*exploit*)

BANNER GRABBING

- La forma più semplice di enumerazione:
  - mi collego ad un servizio remoto…
  - …ne "osservo" l'output
- Una attività foriera di informazioni estremamente utili:
  - tipo di servizio attivo, versione del servizio, presenza di plugin e/o moduli aggiuntivi, ecc.
- Eseguibile manualmente con due utilissimi strumenti:
  - *telnet*
  - *netcat*

BANNER GRABBING CON NETCAT

```
root@kali:~# vim snippet.txt
root@kali:~# nc -nvv -o banners.txt 143.225.28.169 80 < snippet.txt
(UNKNOWN) [143.225.28.169] 80 (http) open
HTTP/1.1 302 Found
Date: Mon, 05 Oct 2015 15:30:05 GMT
Server: Apache/2.4.4 (Unix) PHP/5.4.16 OpenSSL/1.0.1e mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.4.16
Location: http:///xampp/
Content-Length: 131
Connection: close
Content-Type: text/html

<br />
<b>Notice</b>:  Undefined index: HTTP_HOST in <b>/Applicati
 sent 17, rcvd 394
```

```
root@kali:~# more snippet.txt
GET / HTTP/1.0


root@kali:~#
```

```
root@kali:~# more banners.txt
> 00000000 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 30 0a 0a # GET / HTTP/1.0..
> 00000010 0a                                              # .
< 00000000 48 54 54 50 2f 31 2e 31 20 33 30 32 20 46 6f 75 # HTTP/1.1 302 Fou
< 00000010 6e 64 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 30 # nd..Date: Mon, 0
< 00000020 35 20 4f 63 74 20 32 30 31 35 20 31 35 3a 33 30 # 5 Oct 2015 15:30
< 00000030 3a 30 35 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a # :05 GMT..Server:
< 00000040 20 41 70 61 63 68 65 2f 32 2e 34 2e 34 20 28 55 #  Apache/2.4.4 (U
< 00000050 6e 69 78 29 20 50 48 50 2f 35 2e 34 2e 31 36 20 # nix) PHP/5.4.16
< 00000060 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 31 65 20 6d # OpenSSL/1.0.1e m
< 00000070 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 38 2d 64 65 # od_perl/2.0.8-de
< 00000080 76 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a # v Perl/v5.16.3..
< 00000090 58 2d 50 6f 77 65 72 65 64 2d 42 79 3a 20 50 48 # X-Powered-By: PH
< 000000a0 50 2f 35 2e 34 2e 31 36 0d 0a 4c 6f 63 61 74 69 # P/5.4.16..Locati
< 000000b0 6f 6e 3a 20 68 74 74 70 3a 2f 2f 2f 78 61 6d 70 # on: http:///xamp
< 000000c0 70 2f 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 # p/..Content-Leng
< 000000d0 74 68 3a 20 31 33 31 0d 0a 43 6f 6e 6e 65 63 74 # th: 131..Connect
< 000000e0 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 # ion: close..Cont
< 000000f0 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 # ent-Type: text/h
< 00000100 74 6d 6c 0d 0a 0d 0a 3c 62 72 20 2f 3e 0a 3c 62 # tml....<br />.<b
< 00000110 3e 4e 6f 74 69 63 65 3c 2f 62 3e 3a 20 20 55 6e # >Notice</b>:  Un
< 00000120 64 65 66 69 6e 65 64 20 69 6e 64 65 78 3a 20 48 # defined index: H
< 00000130 54 54 50 5f 48 4f 53 54 20 69 6e 20 3c 62 3e 2f # TTP_HOST in <b>/
< 00000140 41 70 70 6c 69 63 61 74 69 6f 6e 73 2f 58 41 4d # Applications/XAM
< 00000150 50 50 2f 78 61 6d 70 70 66 69 6c 65 73 2f 68 74 # PP/xamppfiles/ht
< 00000160 64 6f 63 73 2f 69 6e 64 65 78 2e 70 68 70 3c 2f # docs/index.php</
< 00000170 62 3e 20 6f 6e 20 6c 69 6e 65 20 3c 62 3e 37 3c # b> on line <b>7<
< 00000180 2f 62 3e 3c 62 72 20 2f 3e 0a                   # /b><br />.
root@kali:~#
```

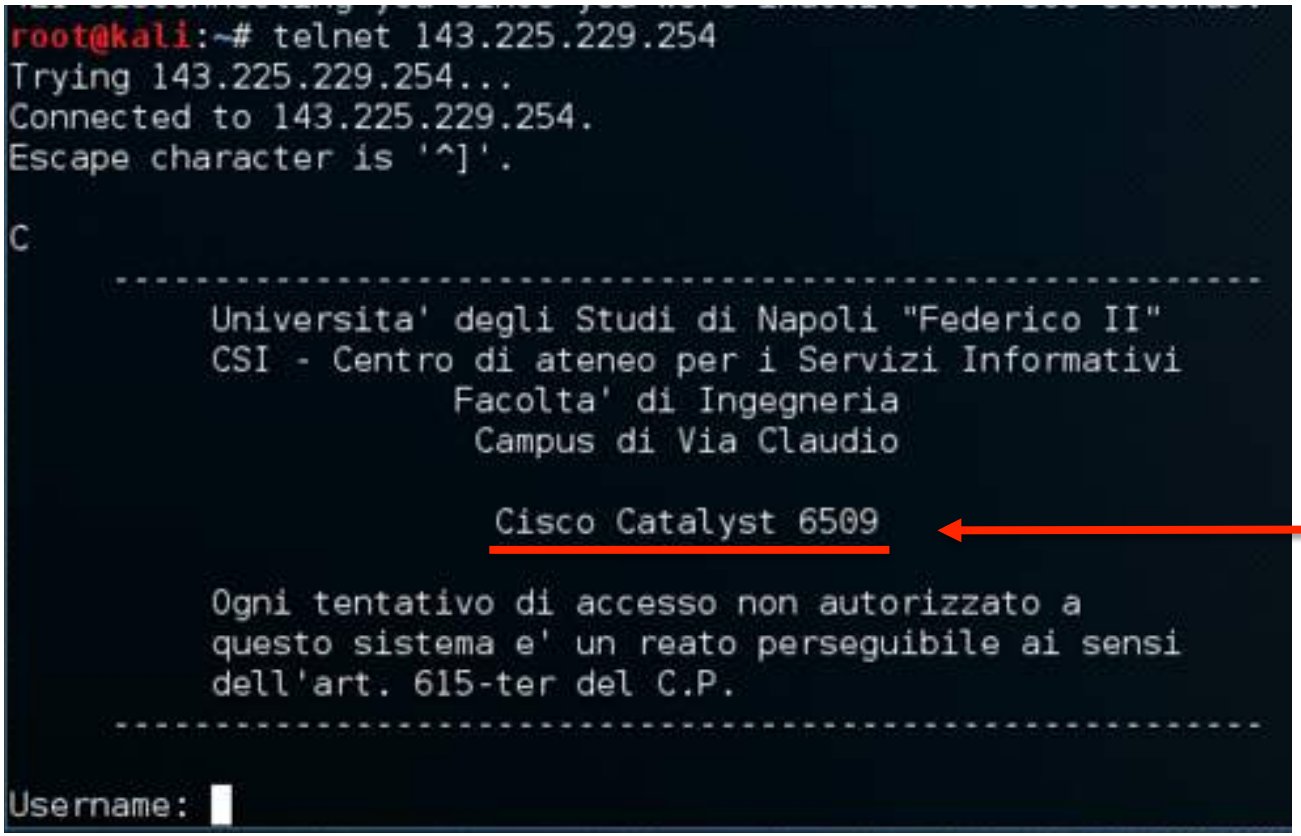
SERVIZI DI RETE COMUNI: FTP (PORTA TCP 21)

```
root@kali:~# ftp ftp.unina.it
Connected to ftp.unina.it.
220 ftp.unina.it NcFTPd Server (free educational license) ready.
Name (ftp.unina.it:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-You are user #3 of 50 simultaneous users allowed.
230-
230 Logged in anonymously.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
drwxr-xr-x   2 ftpuser  ftpusers   1808 Sep  5  2011 images
-rw-r--r--   1 ftpuser  ftpusers  28319 Sep  6  2011 index.html
-rw-r--r--   1 ftpuser  ftpusers  24855 Jan 14  2011 index2.html
-rw-r--r--   1 ftpuser  ftpusers  28252 Sep  5  2011 indexprova.html
-rw-r--r--   1 ftpuser  ftpusers  28305 Sep  5  2011 indexprova.html-2
drwxr-xr-x  10 ftpuser  ftpusers    360 May  2  2011 pub
226 Listing completed.
ftp>
```

FTP: CONTROMISURE

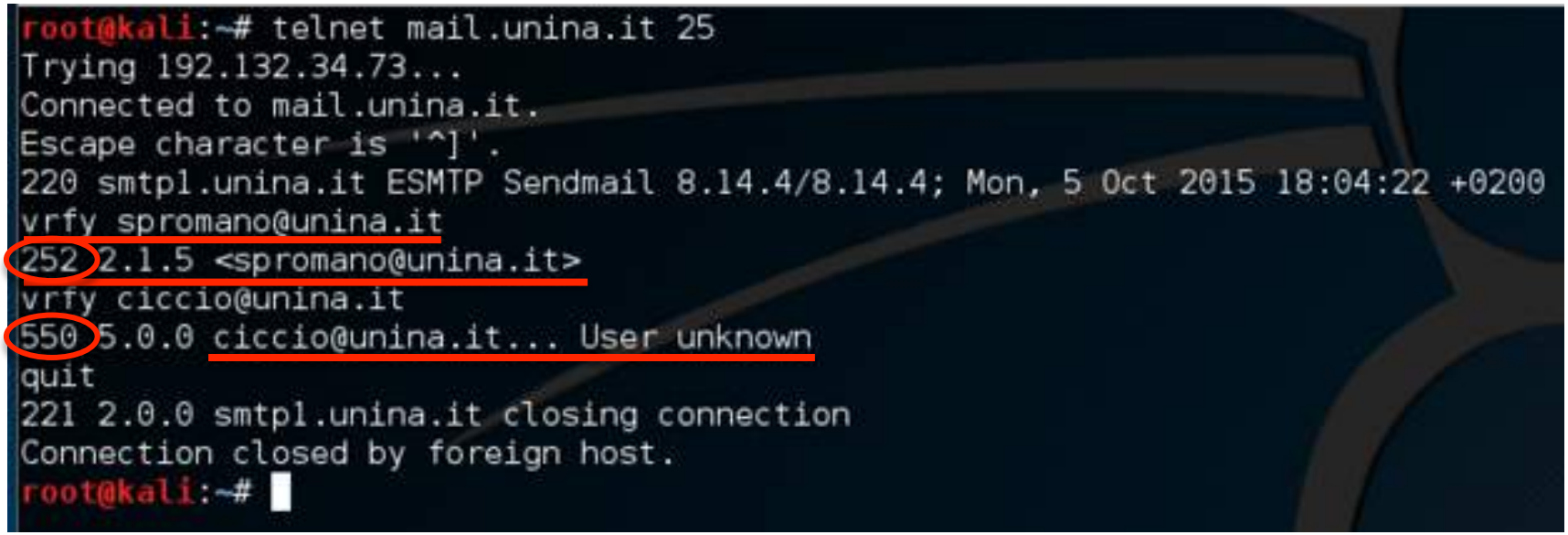
- FTP (File Transfer Protocol) è uno di quei servizi che oggi sono considerati talmente insicuri da suggerire, come unica contromisura, la loro dismissione!
- Alternativa al servizio “plain”:
  - Secure FTP (SFTP)
    - basato sulla codifica SSH (Secure Shell)
- Nel caso in cui si ritenga di voler comunque offrire accesso in FTP ai propri utenti, occorre(rebbe) come minimo seguire alcuni accorgimenti di base:
  - es: non consentire in alcun modo il login “anonimo”...

SERVIZI DI RETE COMUNI: TELNET (PORTA TCP 23)



NB: a volte, è il banner stesso a dirci che tipo di sistema stiamo contattando!

SERVIZI DI RETE COMUNI: SMTP (PORTA TCP 25)



- Una rudimentale forma di “account enumeration”!
  - “spromano” è un utente valido…
  - …“ciccio” NO!

SERVIZI DI RETE COMUNI: DNS (UDP/TCP, PORTA 53)

```
root@kali:~# fierce -dns unina.it
DNS Servers for unina.it:
        dscna1.unina.it
        dscna2.unina.it

Trying zone transfer first...
        Testing dscna1.unina.it
                Request timed out or transfer not allowed.
        Testing dscna2.unina.it
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
143.225.5.200   apps.unina.it
192.132.34.4    web.unina.it
192.132.34.5    vftp.unina.it
192.132.34.8    pmx1n.unina.it
192.132.34.9    pmx3.unina.it
192.132.34.12   ssoiam.unina.it

Subnets found (may want to probe here using nmap or unicornscan):
        127.0.0.0-255 : 1 hostnames found.
        143.225.148.0-255 : 1 hostnames found.
        143.225.163.0-255 : 2 hostnames found.
        143.225.172.0-255 : 1 hostnames found.
        143.225.19.0-255 : 1 hostnames found.
        143.225.200.0-255 : 1 hostnames found.
        143.225.215.0-255 : 1 hostnames found.
        143.225.5.0-255 : 1 hostnames found.
        143.225.58.0-255 : 1 hostnames found.
        172.29.0.0-255 : 1 hostnames found.
        192.132.34.0-255 : 78 hostnames found.
        192.133.28.0-255 : 7 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 96 entries.

Have a nice day.
```

- Problema principale:
  - Zone Transfer
    - cfr. lezione sul footprinting…
- Anche con Zone Transfer disabilitato:
  - reverse lookup, brute forcing, ecc.
- Moltissimi tool per automatizzare il tutto:
  - es: *fierce*

SERVIZI DI RETE COMUNI: TFTP (UDP/TCP, PORTA 69)

- Trivial File Transfer Protocol (TFTP)
  - la forma più semplice di trasferimento file in rete
  - tipicamente configurato per lavorare sulla porta 69 UDP
  - ipotesi di base:
    - per scaricare un file dal server, ne devi conoscere il nome…
    - …l'autenticazione non serve!
- Difficilmente abilitato sui nodi di rete proprio a causa dei suoi scarsissimi (pressocché assenti) requisiti di sicurezza…
- …ma ancora ampiamente diffuso, anche su router e switch!
- Tipici nomi di file di configurazione disponibili sui router:
  - *"running-config"*, "*startup-config"*, "*config", "cisco-config"*, ecc.

SERVIZI DI RETE COMUNI: Finger (UDP/TCP, PORTA 79)

- Il modo classico di fornire, in maniera automatizzata, informazioni sugli utenti nella rete Internet dei primi tempi (quando tutti erano più buoni…)
- Tipicamente disabilitato nei moderni sistemi di rete

```
[root$]finger -l @target.example.com
[target.example.com]
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
On since Sun Mar 28 11:01 (PST) on tty1 11 minutes idle
     (messages off)
On since Sun Mar 28 11:01 (PST) on ttyp0 from :0.0
   3 minutes 6 seconds idle
No mail.
plan:
John Smith
Security Guru
```

```
root@kali:~# finger @143.225.28.244

Integrated port
Printer Type: Lexmark T644
Print Job Status: No Job Currently Active
Printer Status: 0 Ready
root@kali:~#
```

SERVIZI DI RETE COMUNI: HTTP (TCP, PORTA 80)

- Approccio “manuale”: il solito *netcat*
  - già il metodo HEAD fornisce un bel po’ di dati utili…

```
root@kali:~# nc www.unina.it 80
HEAD / HTTP/1.1
Host: www.unina.it

HTTP/1.1 301 Moved Permanently
Date: Mon, 05 Oct 2015 18:05:28 GMT
Set-Cookie: JSESSIONID=9310ADFCD08E953244C280103B7A52BB.node_staging11; Path=/; HttpOnly
Set-Cookie: GUEST_LANGUAGE_ID=it_IT; Expires=Tue, 04-Oct-2016 18:05:33 GMT; Path=/
Set-Cookie: COOKIE_SUPPORT=true; Expires=Tue, 04-Oct-2016 18:05:33 GMT; Path=/
Location: http://www.unina.it/home;jsessionid=9310ADFCD08E953244C280103B7A52BB.node_staging11
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 336
Connection: close
```

```
root@kali:~# nc www.unina.it 80
HEAD /home;jsessionid=9310ADFCD08E953244C280103B7A52BB.node_staging11 HTTP/1.1
Host: www.unina.it

HTTP/1.1 200 OK
Date: Mon, 05 Oct 2015 18:06:25 GMT
Set-Cookie: COOKIE_SUPPORT=true; Expires=Tue, 04-Oct-2016 18:06:31 GMT; Path=/
Liferay-Portal: Liferay Portal Enterprise Edition 6.1.20 EE (Paton / Build 6120 / July 31, 2012)
ETag: "0"
Set-Cookie: COOKIE_SUPPORT=true; Expires=Tue, 04-Oct-2016 18:06:31 GMT; Path=/
Content-Type: text/html;charset=UTF-8
Content-Length: 32
Connection: close
```

MICROSOFT RPC (MSRPC): TCP, PORTA 135

- Remote Procedure Call (RPC) endpoint mapper:
  - utilizzato per fornire informazioni circa la presenza di servizi/applicazioni sulla macchina (Microsoft) target

```
root@kali:~# nmap 143.225.XXX.XXX --script=msrpc-enum
```

```
Host script results:
| msrpc-enum:
|
|     uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d
|     tcp port: 49152
|     ip_addr: 0.0.0.0
|
|     uuid: 4b112204-e19-11d3-b42b-0000f81feb9f
|     ncalrpc: LRPC-51de3ed2060d22ec0d
```

```
|     netbios: \\GREEN-PC
|     uuid: b58aa02e-2884-4e97-8176-4ee06d794184
|     ncacn_np: \pipe\trkwks
```

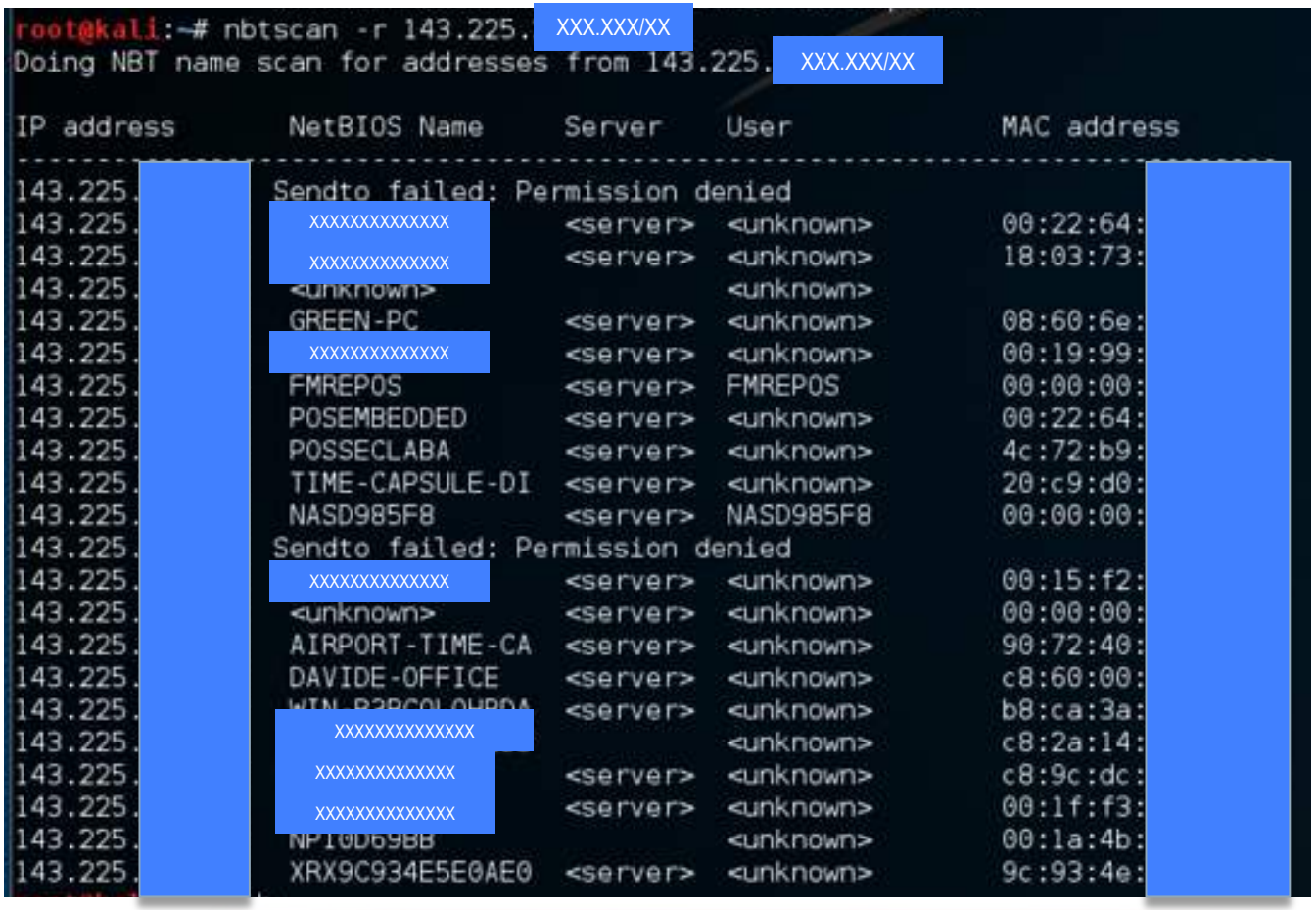
NETBIOS NAME SERVICE: UDP, PORTA 137

- NetBIOS Name Service (NBNS):
  - un sistema dei nomi distribuito per reti Microsoft
  - non più necessario, da Windows 2000 in poi, perché rimpiazzato dall'approccio standard (DNS)…
  - …ma ancora abilitato di default in quasi tutte le distribuzioni di Windows
- L'enumerazione è in questo caso banale:
  - si inviano in rete semplici messaggi di "poll" UDP indirizzati alla porta 137

NETBIOS NAME SERVICE: I TOOL

- **“net view”**
  - identifica tutti i domini Microsoft in una rete, o tutti i computer in un dominio
- **“nltest”**
  - identifica i *Domain Controller* (depositari delle informazioni di autenticazione!) di uno specifico dominio
- **“nbtstat”**
  - consente di collegarsi a singole macchine in un dominio per prelevarne la “tabella dei nomi”:
    - nome del sistema, nome del dominio cui il sistema appartiene, utenti attivi sul sistema, servizi attivi, indirizzo MAC, ecc.
- **“nbtscan”** (anche per Linux…)
  - effettua le operazioni di nbtsat su un’intera rete

NBTSCAN: UN ESEMPIO



NETBIOS NAME SERVICES: CONTROMISURE

- Restringere (o negare) l'accesso alla porta 137 UDP
- Per evitare che dati sugli utenti appaiano nelle tabelle NETBIOS:
  - disabilitare i servizi "Alerter" e "Messenger" sui singoli host del dominio
    - Services Control Panel
- Per evitare che si possa accedere ai servizi NETBIOS da Internet:
  - disabilitare il servizio NETBIOS su TCP/IP nelle proprietà delle singole schede di rete di cui è dotato il proprio host

NETBIOS SESSION ENUMERATION: TCP 139/445

- Il principale tallone di Achille per sistemi Windows
  - "null session (o anonymous connection) attack"!
- Un exploit del protocollo SMB (Server Message Block):
  - la base per i servizi Microsoft di condivisione di file e di stampa:

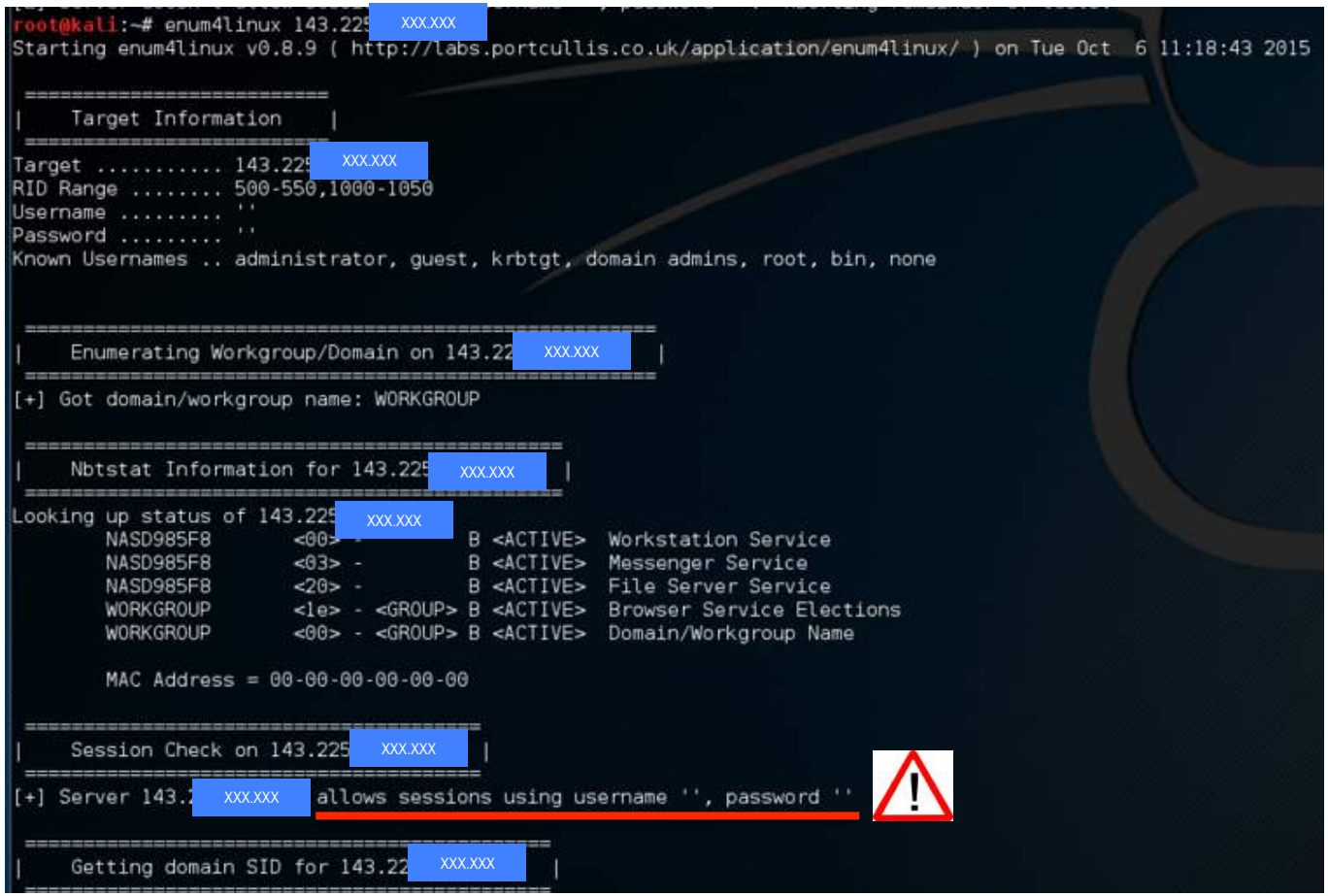
```
C:\>net use \\192.168.202.33\IPC$ "" /u:""
```

    - sintassi simile a quella del comando per "montare" un drive di rete
    - utilizzato per:
      - collegarsi alla risorsa condivisa (nascosta) di Inter Process Communication **(IPC$)**
      - come utente "anonimo" **(/u:"")**
      - con password "null" **("")**
  - in caso di successo, l'attaccante ha a disposizione un canale aperto per "spillare" informazioni sensibili dal sistema target:
    - informazioni di rete, cartelle condivise, utenti, gruppi, chiavi di registro, ecc.

NULL SESSION: I TOOL “ALL-IN-ONE”

- Un insieme di strumenti preconfezionati per:
  - stabilire una null session con il target
  - recuperare quante più informazioni possibile dal target sfruttando la sessione stabilita
- Ambiente Windows:
  - Winfingerprint: http://winfingerprint.sourceforge.net/winfingerprint.php
  - NBTenum: http://nbtenum.sourceforge.net/
- Ambiente Linux:
  - enum4linux: http://tools.kali.org/information-gathering/enum4linux

ENUM4LINUX IN AZIONE…



SMB NULL SESSION: CONTROMISURE

- Porte TCP utilizzate: 139 e 445 (quest'ultima da Win2000 in poi)
  - soluzione più immediata:
    - filtrare le porte TCP (ed UDP) 139 e 445 su tutti i dispositivi di accesso perimetrali della propria rete
- Sui singoli host:
  - disabilitare i servizi SMB
    - "unbinding" del client WINS (TCP/IP) dall'interfaccia di rete, tramite il Tab "Bindings" del pannello di controllo relativo al networking
  - per sistemi successivi a Windows NT4 Service Pack3:
    - configurazione del flag "RestrictAnonymous" nel registro di sistema
      - una "facility" concepita ad hoc per prevenire l'enumerazione di informazioni sensibili sfruttando "null sessions"
    - NB: soluzione comunque "aggirabile" da parte di alcuni dei tool di attacco più potenti!

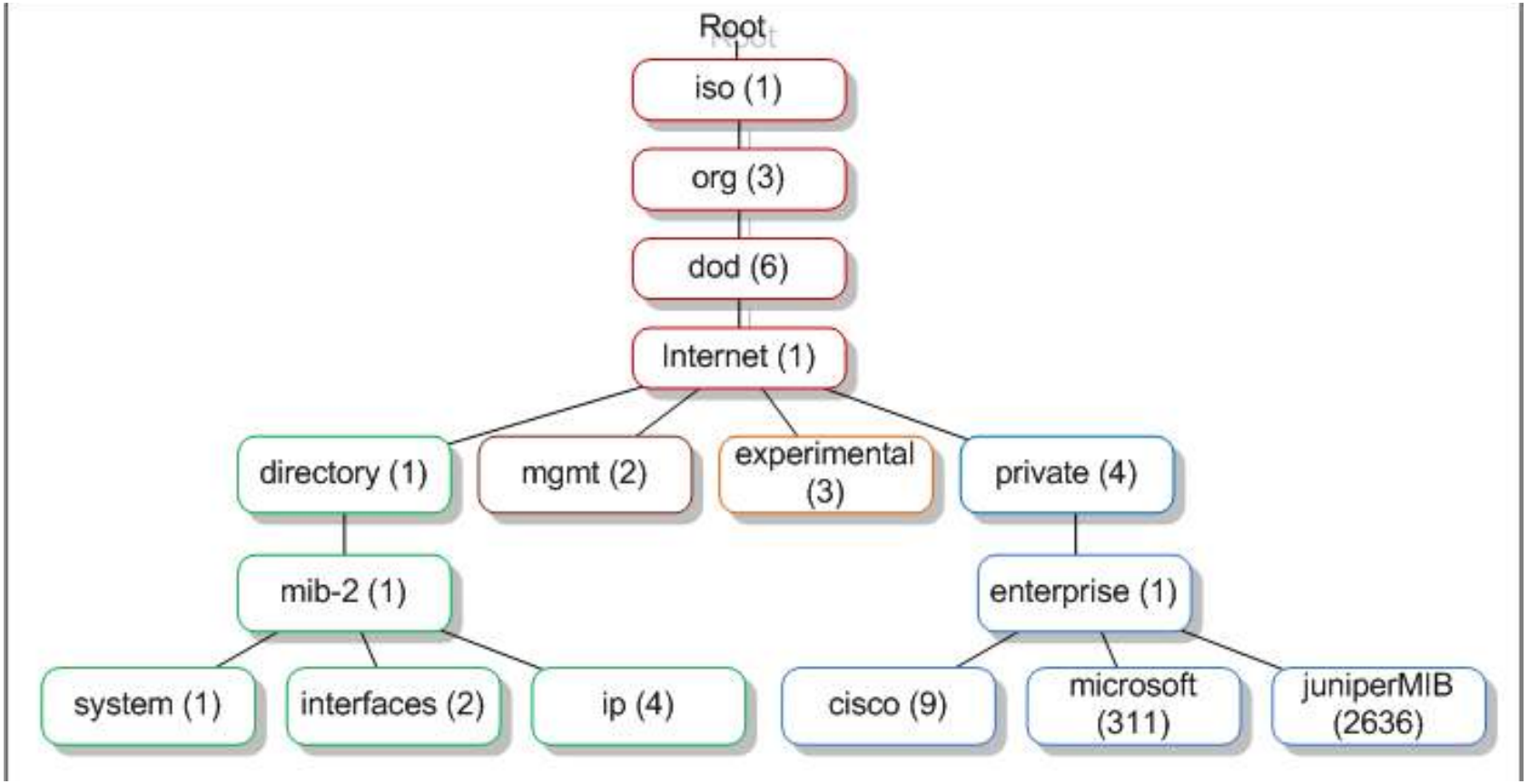
SNMP ENUMERATION: UDP, PORTA 161

- Simple Network Management Protocol…
- …aka “Security Not My Problem” (almeno per le versioni 1 e 2 del protocollo)!
- Un protocollo concepito per fornire informazioni “intime” circa i dispositivi di rete
- Dotato di un semplice meccanismo di autenticazione basato su password
  - spesso configurato in maniera fin troppo lasca
    - es: password di default per accedere a dispositivi SNMP in modalità read-only:
      - “public”
  - dati contenuti in un’apposita struttura chiamata MIB (Management Information Base)
    - moltissime informazioni vengono pubblicate nella parte “proprietaria” della MIB da parte dei singoli produttori di dispositivi:
      - es: sistemi Windows NT → nomi degli account utente

ALLA RICERCA DI DISPOSITIVI SNMP-ENABLED

```
MacBookPro-spromano:logs spromano$ sudo nmap -sU -p161 --script snmp-brute --script-args snmplist=community.lst 192.168.1.0/24

Starting Nmap 6.40-2 ( http://nmap.org ) at 2015-10-07 08:52 CEST
Nmap scan report for 192.168.1.64
Host is up (0.77s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
| snmp-brute:
|   admin - Valid credentials
|_  public - Valid credentials
MAC Address: B0:E8:92:76:34:13 (Seiko Epson)

Nmap scan report for 192.168.1.79
Host is up (0.84s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 40:F3:08:8D:52:4A (Murata Manufactuaring Co.)

Nmap scan report for 192.168.1.253
Host is up (0.041s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 9E:97:26:D0:5C:0E (Unknown)

Nmap scan report for 192.168.1.254
Host is up (0.0083s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 9C:97:26:D0:5C:0E (Technicolor)

Nmap scan report for 192.168.1.76
Host is up (0.000071s latency).
PORT    STATE  SERVICE
161/udp closed snmp

Nmap done: 256 IP addresses (5 hosts up) scanned in 58.27 seconds
```

LA MIB SNMP


Root
iso (1)
org (3)
dod (6)
Internet (1)
directory (1)
mgmt (2)
experimental (3)
private (4)
mib-2 (1)
enterprise (1)
system (1)
interfaces (2)
ip (4)
cisco (9)
microsoft (311)
juniperMIB (2636)

A PASSEGGIO NELLA MIB

```
[root]# snmpwalk -c public -v 2c 192.168.1.60

system.sysDescr.0 = Linux wave 2.6.10 mdk #1 Sun Apr 15 2008 i686
system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.linux
system.sysUpTime.0 = Timeticks: (25701) 0:04:17.01
system.sysContact.0 = Root <root@localhost> (configure /etc/snmp/snmp.
conf)system.sysName.0 = wave
system.sysLocation.0 = Unknown (confi gure /etc/snmp/snmp.conf)system.
sysORLastChange.0 = Timeticks: (0)

[output truncated for brevity]
```

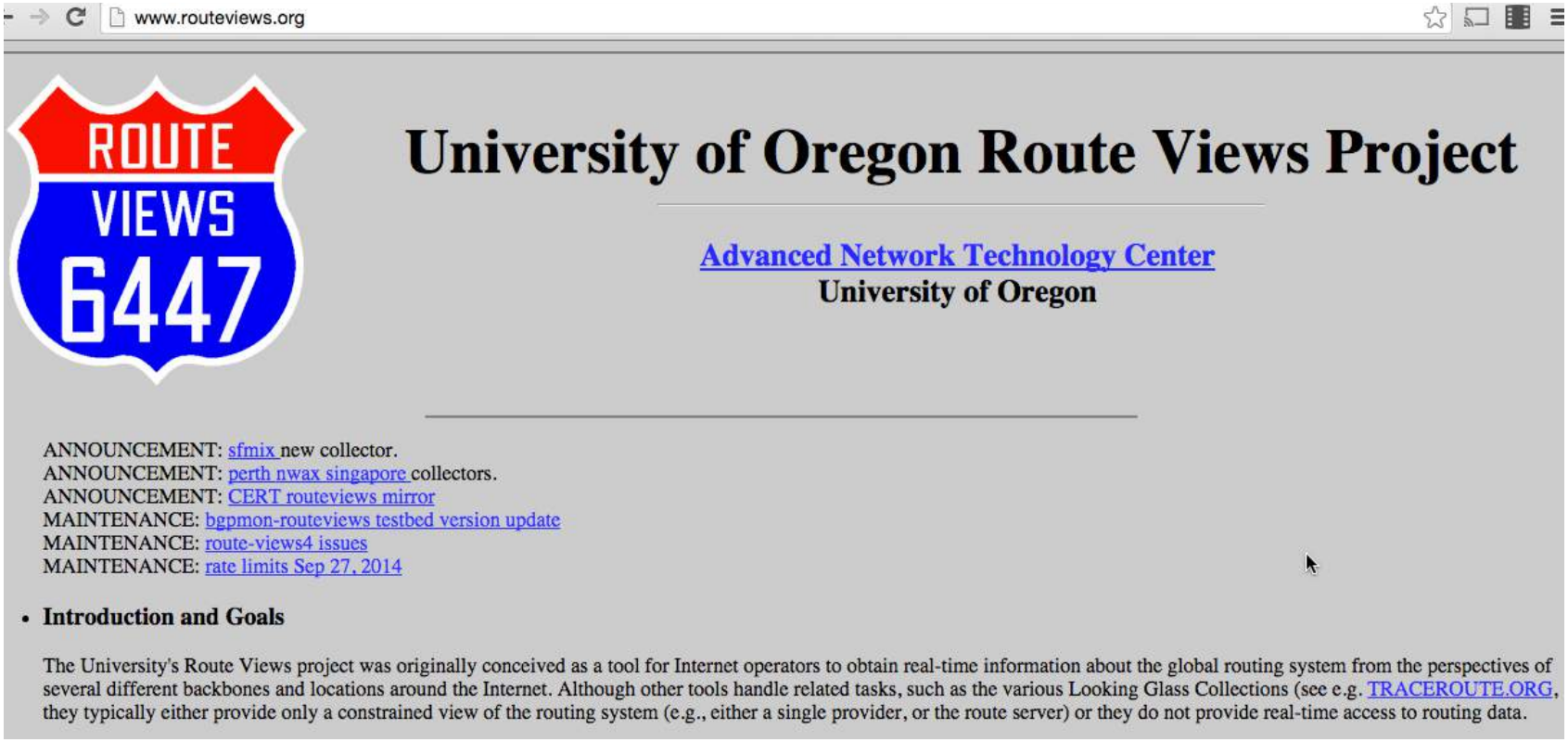
SNMP ENUMERATION: CONTROMISURE

- Disabilitare gli agenti SNMP sulle singole macchine
- Nel caso di agenti attivi:
  - configurare nomi di “community” difficili da indovinare
- Nella rete:
  - bloccare l’accesso alla porta 161 su tutto il perimetro della propria infrastruttura
- In generale:
  - impiegare la versione più recente del protocollo (SNMPv3)
    - disponibilità di meccanismi di crittografia e di autenticazione molto più avanzati

BGP ENUMERATION: TCP, PORTA 179

- Due passi:
  1. determinare il numero dell'Autonomous System (ASN) dell'organizzazione target
  2. eseguire una query sui router per identificare tutte le reti nelle quali il vettore di Autonomous System attraversati (AS path) termina con il numero di AS identificato nella fase precedente
- Impiego di servizi pubblicamente disponibili:
  - www.arin.net → query con keyword "ASN"
- Tecnica alternativa, a partire da un generico indirizzo IP dell'organizzazione target:
  1. query ad un router BGP 'pubblico'
  2. individuazione dell'ASN, identificato dal "last hop" nel vettore dei percorsi associato all'IP in questione
     - Route Views Project dell'Università dell'Oregon

ROUTE VIEWS PROJECT



IMPIEGO DI ROUTE VIEWS

```
MacBookPro-spromano:logs spromano$ telnet route-views.oregon-ix.net
Trying 128.223.51.103...
Connected to route-views.oregon-ix.net.
Escape character is '^]'.

**************************************************************************

                    Oregon Exchange BGP Route Viewer
          route-views.oregon-ix.net / route-views.routeviews.org

 route views data is archived on http://archive.routeviews.org

 This hardware is part of a grant by the NSF.
 Please contact help@routeviews.org if you have questions, or
 if you wish to contribute your view.

 This router has views of full routing tables from several ASes.
 The list of peers is located at http://www.routeviews.org/peers
 in route-views.oregon-ix.net.txt

 NOTE: The hardware was upgraded in August 2014.  If you are seeing
 the error message, "no default Kerberos realm", you may want to
 in Mac OS X add "default unset autologin" to your ~/.telnetrc

 To login, use the username "rviews".

 **************************************************************************


User Access Verification

Username: Kerberos: No default realm defined for Kerberos!
rviews
route-views>
```

```
route-views>show ip bgp 143.225.229.254
BGP routing table entry for 143.225.0.0/16, version 80899059
Paths: (36 available, best #29, table default)
  Not advertised to any peer
  Refresh Epoch 1
  3277 39710 9002 3356 137 137 137
    195.208.112.161 from 195.208.112.161 (194.85.4.4)
      Origin IGP, localpref 100, valid, external
      Community: 3277:39710 9002:9002 9002:64657
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  53364 3257 3356 137 137 137
    173.205.57.234 from 173.205.57.234 (10.10.10.252)
```

HURRICANE ELECTRIC
INTERNET SERVICES

Search

AS137 Consortium GARR

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers

```
as-block:       AS137 - AS137
descr:          RIPE NCC ASN block
remarks:        These AS Numbers are assigned to network operators in the RIPE
region.
mnt-by:         RIPE-NCC-HM-MNT
created:        2002-08-22T14:57:25Z
last-modified:  2014-02-24T13:15:12Z
source:         RIPE # Filtered

aut-num:        AS137
as-name:        ASGARR
descr:          Consortium GARR
org:            ORG-GIRA1-RIPE
import:         from AS20965 action pref=300; accept ANY
import:         from AS1299 action pref=100; accept ANY
import:         from AS3549 action pref=100; accept ANY
```

UNIX RPC ENUMERATION: PORTE 111 E 32771

- Servizio “portmapper”, implementato dal demone *rpcbind*
  - orchestra le richieste dei clienti e le porte da assegnare ai servizi in ascolto
  - l’equivalente del servizio “finger” (per l’enumerazione degli utenti), con riferimento ai servizi offerti da un nodo

IL TOOL RPCINFO

```
MacBookPro-spromano:logs spromano$ rpcinfo -p localhost
   program vers proto   port
    100000    2   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    4   udp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    4   tcp    111  portmapper
    100024    1   udp    752  status
    100024    1   tcp   1019  status
    100021    0   udp    621  nlockmgr
    100005    3   udp    853  mountd
    100005    1   tcp   1023  mountd
    100005    3   tcp   1023  mountd
    100011    1   udp    885  rquotad
    100011    2   udp    885  rquotad
    100011    1   tcp    997  rquotad
    100011    2   tcp    997  rquotad
```

IPSec/IKE ENUMERATION: UDP, PORTA 500

- IPSec:
  - il protocollo di livello tre con caratteristiche di sicurezza
- IKE:
  - Internet Key Exchange
    - il componente di IPSec che si fa carico di gestire la fase di negoziazione delle chiavi
    - fondamentale per “scoprire” la presenza di reti VPN (Virtual Private Networks) nell’organizzazione target
- L’enumeration, in questo caso, non è semplicemente basata sull’invio di pacchetti probe generici indirizzati alla porta 500
  - lo standard impone che pacchetti mal formattati siano ignorati dal servizio IPSec

IL TOOL "*IKE-SCAN*"

- Costruisce pacchetti compatibili con la specifica IPSec
- Una volta individuata una VPN, cerca di estrapolare informazioni utili sulla sua configurazione:
  - tipo di autenticazione (pre-shared keys vs certificati)
  - protocolli di crittografia adottati
  - modalità di funzionamento ("main mode" vs "aggressive mode")
- Possibile preludio alla fase di attacco, basata sull'impiego di tool quali *"psk-crack"*

IKE-SCAN IN AZIONE

```
# ./ike-scan 10.10.10.0/24
Starting ike-scan 1.9 with 256 hosts \
(http://www.nta-monitor.com/tools/ike-scan/)
10.10.10.1  Main Mode Handshake returned HDR=(CKY-R= 42c304f96fa8f857)
\
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 \
LifeType=Seconds LifeDuration(4)=0x00007080) VID= f4ed19e0cc114eb-
516faaac0ee37daf2807b4381f00000001
0000138d4925b9df0000000018000000
(Firewall-1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.087 seconds \
(11.47 hosts/sec).  1 returned handshake; 0 returned notify
```

IPSec/IKE ENUMERATION: CONTROMISURE

- Implementare politiche di filtraggio sugli indirizzi IP sorgente
  - soluzione utilizzabile in scenari suffiecentemente statici
    - reti VPN con partner commerciali, del tipo “site-to-site”
- Utilizzare quanto più possibile la modalità di funzionamento “Main Mode”
  - rispetto alla modalità “Aggressive”:
    - non consente di accedere ad informazioni sensibili, quali le chiavi condivise (pre-shared) ed i dati sul dispositivo
    - scambia dati con i peer in modo più sicuro
    - è meno soggetto ad attacchi di tipo Denial of Service (DoS)
- NB: la modalità “aggressive” diventa l’unica scelta nei casi in cui:
  - ci si debba necessariamente affidare all’autenticazione PSK (“pre-shared”)
  - si debbano creare collegamenti dinamici con client il cui indirizzo IP non sia noto a priori

DOMANDE?