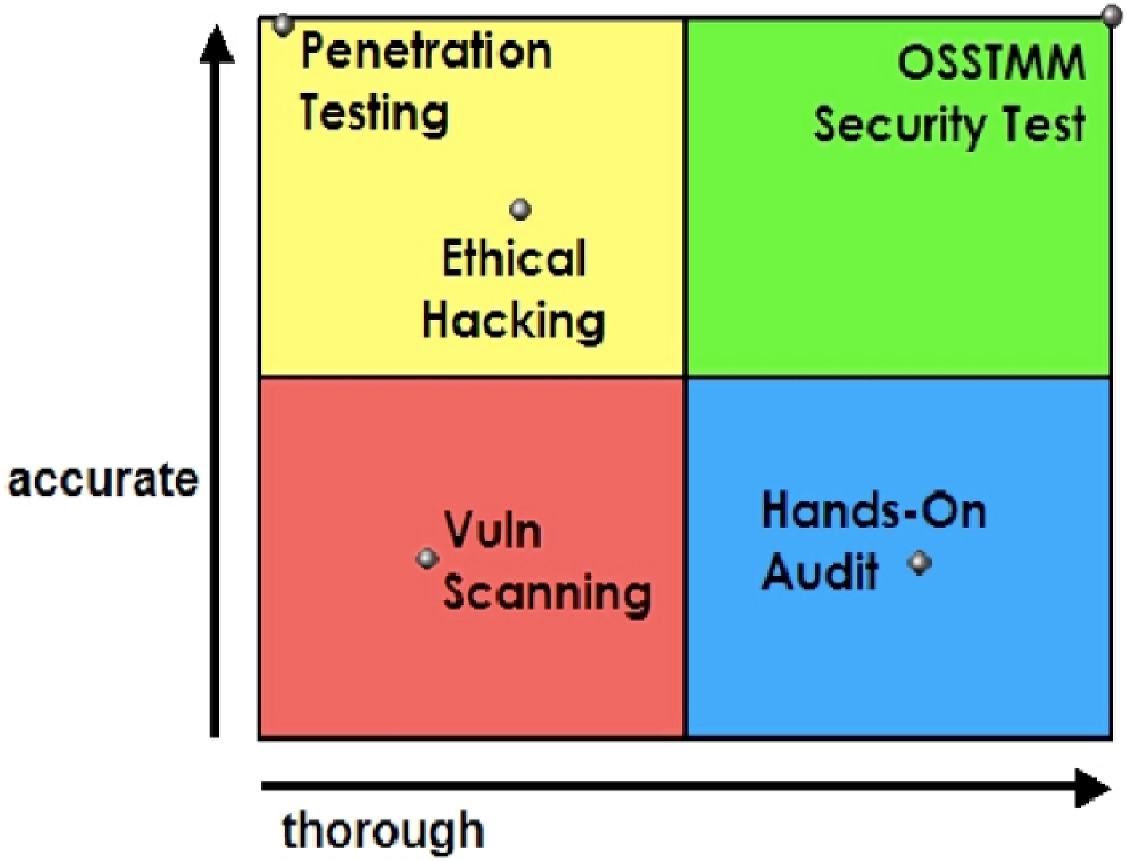
تست امنیت شبکه
(Network Security Testing)

دلیل تست امنیت

- آگاهی از وضعیت حال حاضر امنیت
- ارزیابی میزان توانایی مقابله در مقابل نفوذ
- طرح ریزی برای پشتیبانی

محدوده



Penetration Testing

Ethical Hacking

OSSTMM Security Test

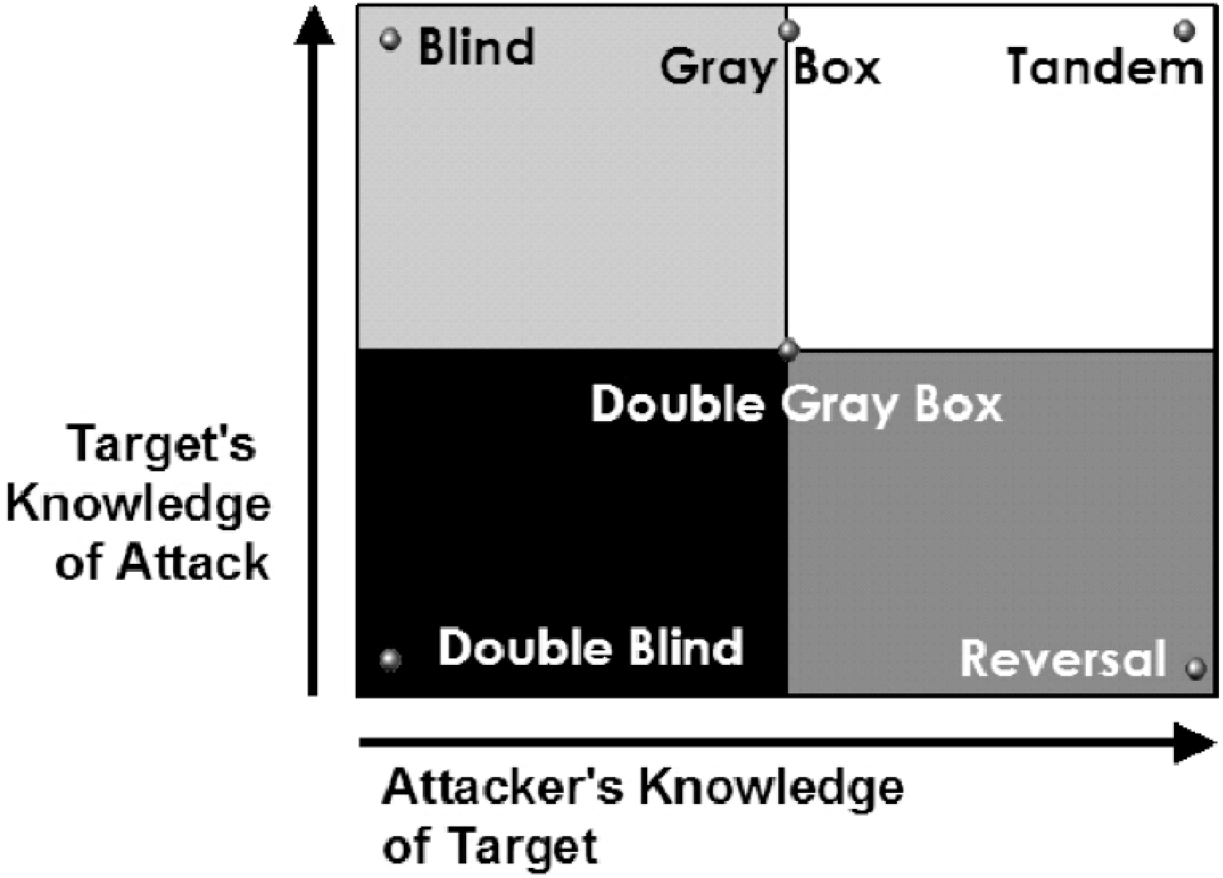
Vuln Scanning

Hands-On Audit

accurate

thorough

انواع تست امنیت



تکنیک های شبکه ای

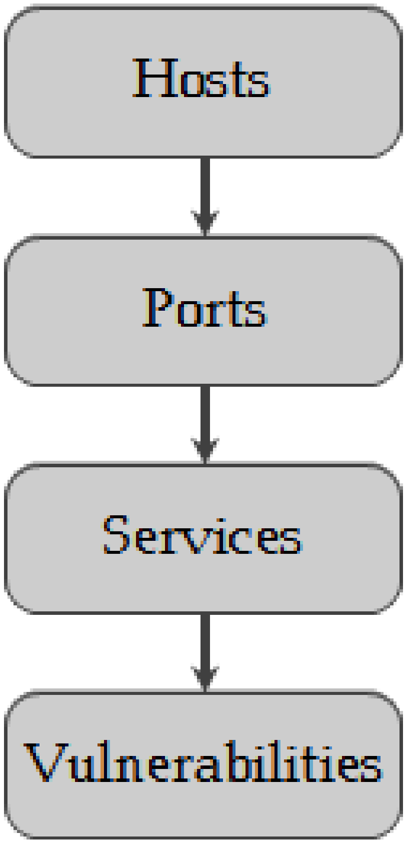
- دیده وری (Scouting) و شناسایی شبکه
- انگشت نگاری (Fingerprinting) سیستم عامل
- اسکن کردن آسیب پذیری ها
- تحلیل ترافیک شبکه

Network Scouting

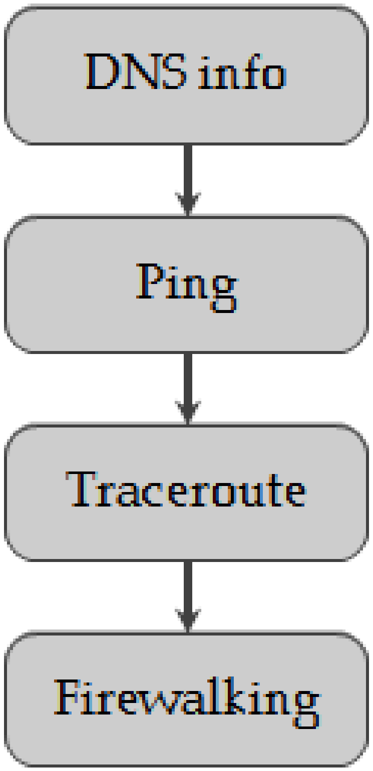
دیده وری شبکه

- دیده وری شبکه اولین قدم است.
- برای حمله اول باید خوب هدف را شناخت.
- ابزارهای استاندارد لینوکس/یونیکس
- Nmap (Network Mapper)

فرایند دیده وری



بازنمایی توپولوژی



Whois

- Domain Name: STANFORD.EDU

- Registrant:
- Stanford University
- The Board of Trustees of the Leland Stanford Junior University
- 241 Panama Street, Pine Hall, Room 115
- Stanford, CA 94305-4122
- UNITED STATES

Whois

- Administrative Contact:

- Domain Admin
- Stanford University
- 241 Panama Street Pine Hall, Room 115
- Stanford, CA 94305-4122
- UNITED STATES
- (650) 723-4328
- sunet-admin@stanford.edu

Whois

- Name Servers:

– ARGUS.STANFORD.EDU	171.64.7.115
– AVALLONE.STANFORD.EDU	171.64.7.88
– ATALANTE.STANFORD.EDU	171.64.7.61
– AERATHEA.STANFORD.EDU	152.3.104.250

Digging DNS Records

```
•   Dig stanford.edu
•   ;; ANSWER SECTION:
•   stanford.edu.             3600      IN      A       171.67.216.3
•   stanford.edu.             3600      IN      A       171.67.216.4
•   stanford.edu.             3600      IN      A       171.67.216.7
•   stanford.edu.             3600      IN      A       171.67.216.8
•   stanford.edu.             3600      IN      A       171.67.216.9

•   ;; AUTHORITY SECTION:
•   stanford.edu.             172800    IN      NS      Avallone.stanford.edu.
•   stanford.edu.             172800    IN      NS      Argus.stanford.edu.
•   stanford.edu.             172800    IN      NS      Atalante.stanford.edu.
•   stanford.edu.             172800    IN      NS      Aerathea.stanford.edu.

•   ;; ADDITIONAL SECTION:
•   Argus.stanford.edu.       3600      IN      A       171.64.7.115
•   Avallone.stanford.edu.    3600      IN      A       171.64.7.88
•   Atalante.stanford.edu.    3600      IN      A       171.64.7.61
•   Aerathea.stanford.edu.    3600      IN      A       152.3.104.250
```

Port Scanning

- پیدا کردن پورت های باز

```
•  Starting Nmap 4.85BETA3 ( http://nmap.org ) at 2009-05-11 16:37
•  PDT
•  Interesting ports on localhost (127.0.0.1):
•  Not shown: 996 closed ports
•  PORT       STATE    SERVICE
•  22/tcp     open     ssh
•  80/tcp     open     http
•  631/tcp    open     ipp
•  9050/tcp   open     tor-socks
```

Ping

- استاندارد: استفاده از ICMP
- استفاده از TCP (مثلاً پورت ۸۰)
- ARP Ping (در شبکه محلی)

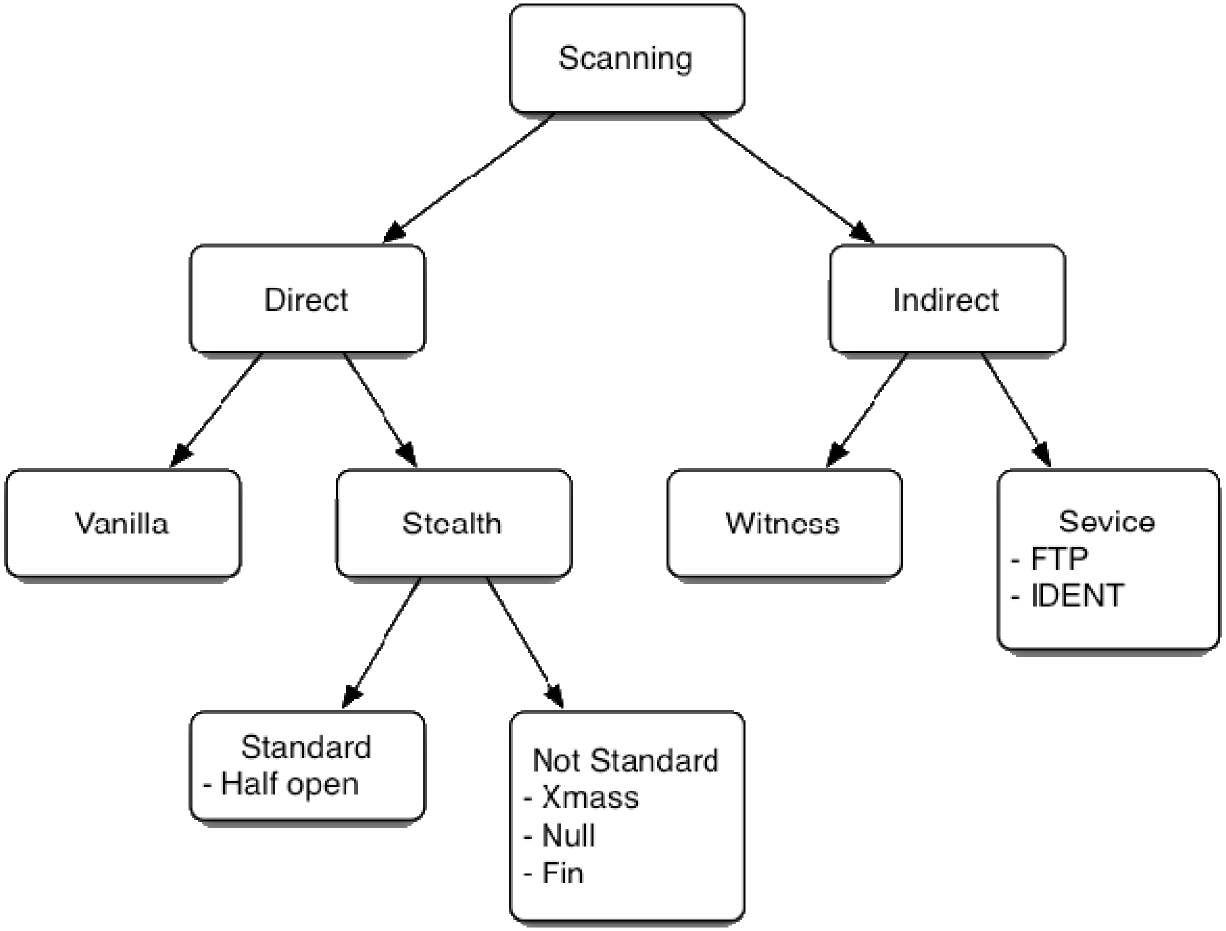
```
•   box:~# arping 192.168.0.1
•   ARPING 192.168.0.1
•   60 bytes from 00:21:91:f8:48:3a (192.168.0.1): index=0 time=6.410 msec
•   60 bytes from 00:21:91:f8:48:3a (192.168.0.1): index=1 time=3.351 msec
•   60 bytes from 00:21:91:f8:48:3a (192.168.0.1): index=2 time=2.839 msec
•   60 bytes from 00:21:91:f8:48:3a (192.168.0.1): index=3 time=7.165 msec
```

پیدا کردن روترها

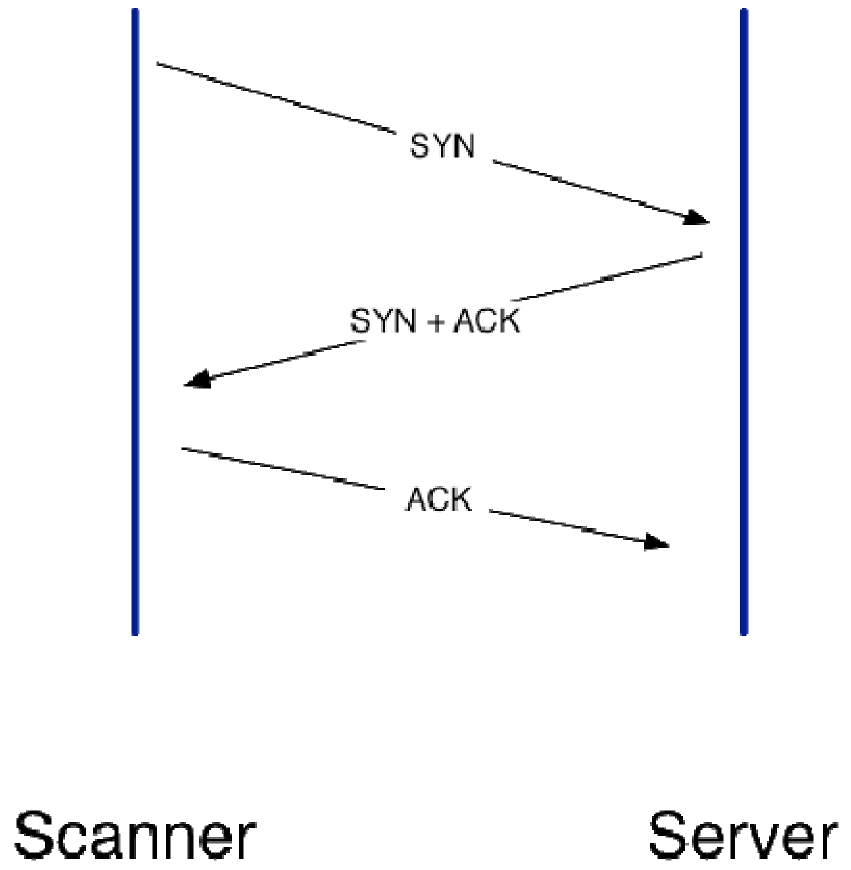
- traceroute

```
•    traceroute to www.l.google.com (74.125.19.147), 64 hops max, 40 byte packets
•     1  171.66.32.1  1.329 ms  0.820 ms  0.893 ms
•     2  171.64.1.17  1.205 ms  0.884 ms  1.045 ms
•     3  171.64.1.129  1.910 ms  3.633 ms  1.835 ms
•     4  137.164.50.33  1.962 ms  2.540 ms  3.192 ms
•     5  137.164.46.203  4.371 ms  4.424 ms  3.677 ms
•     6  137.164.46.205  2.564 ms  3.099 ms  3.170 ms
•     7  137.164.131.237  2.594 ms  3.804 ms  2.433 ms
•     8  137.164.130.94  2.789 ms  2.695 ms  2.715 ms
•     9  216.239.49.250  3.878 ms  5.500 ms  5.405 ms
•    10  209.85.251.94  7.837 ms  4.840 ms  12.804 ms
•    11  74.125.19.147  3.637 ms  4.196 ms  6.283 ms
```

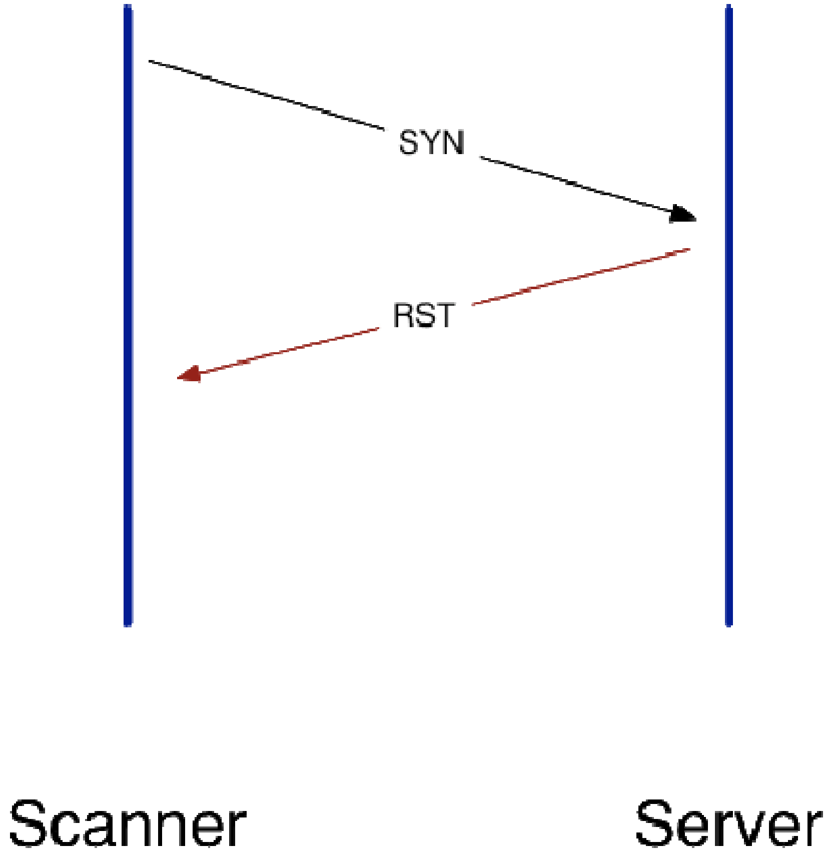
انواع اسکن


Scanning
Direct
Indirect
Vanilla
Stealth
Witness
Sevice
- FTP
- IDENT
Standard
- Half open
Not Standard
- Xmass
- Null
- Fin

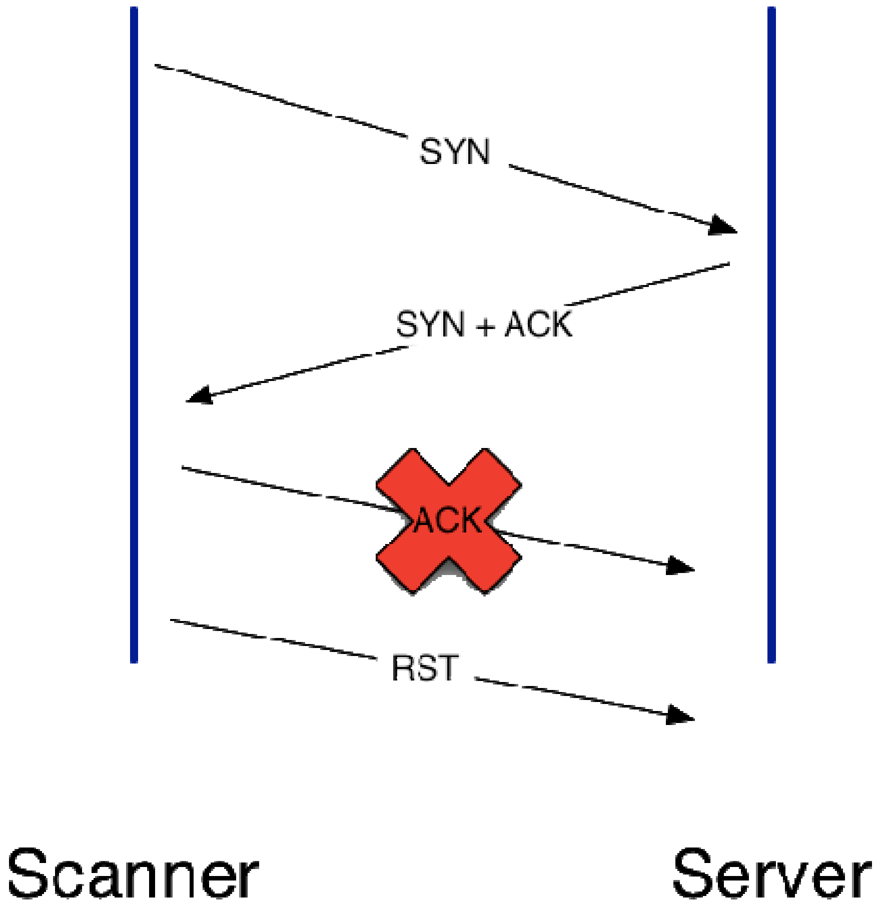
Vanilla Scan 1



Vanilla Scan 2



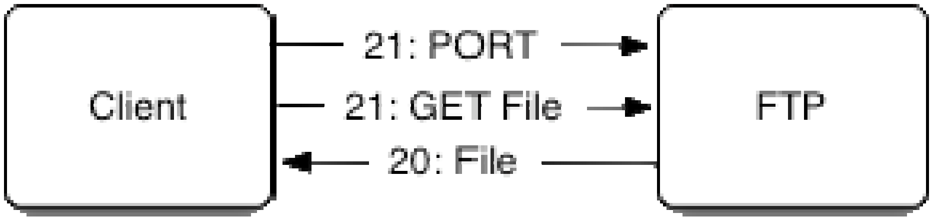
Half-Open Scan



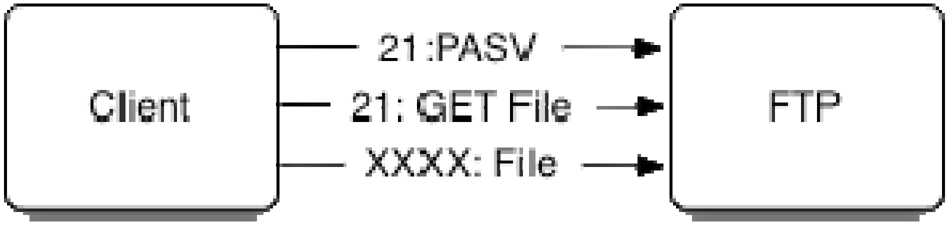
اسکن های غیر استاندارد

- اسکن Null
- اسکن Xmas
- اسکن Fin
- اسکن Maimon
- اسکن Ack

FTP

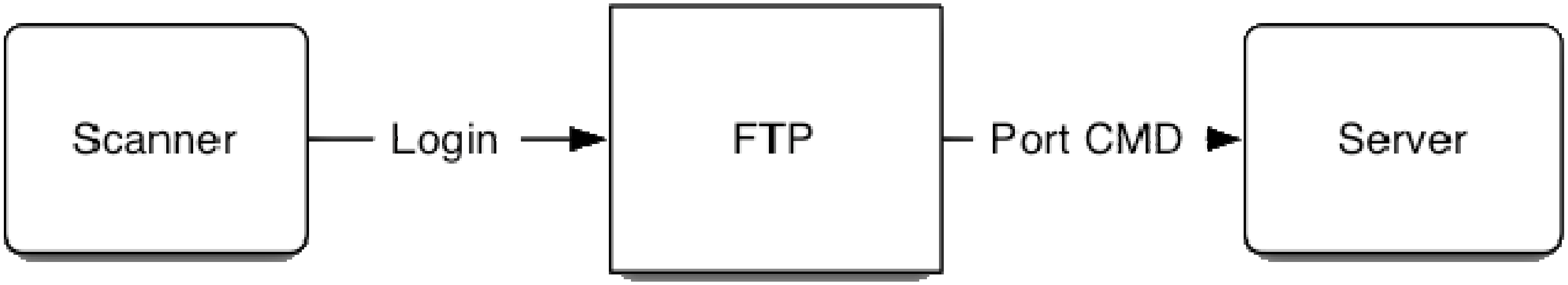


Active



Passive

Bounce Scan

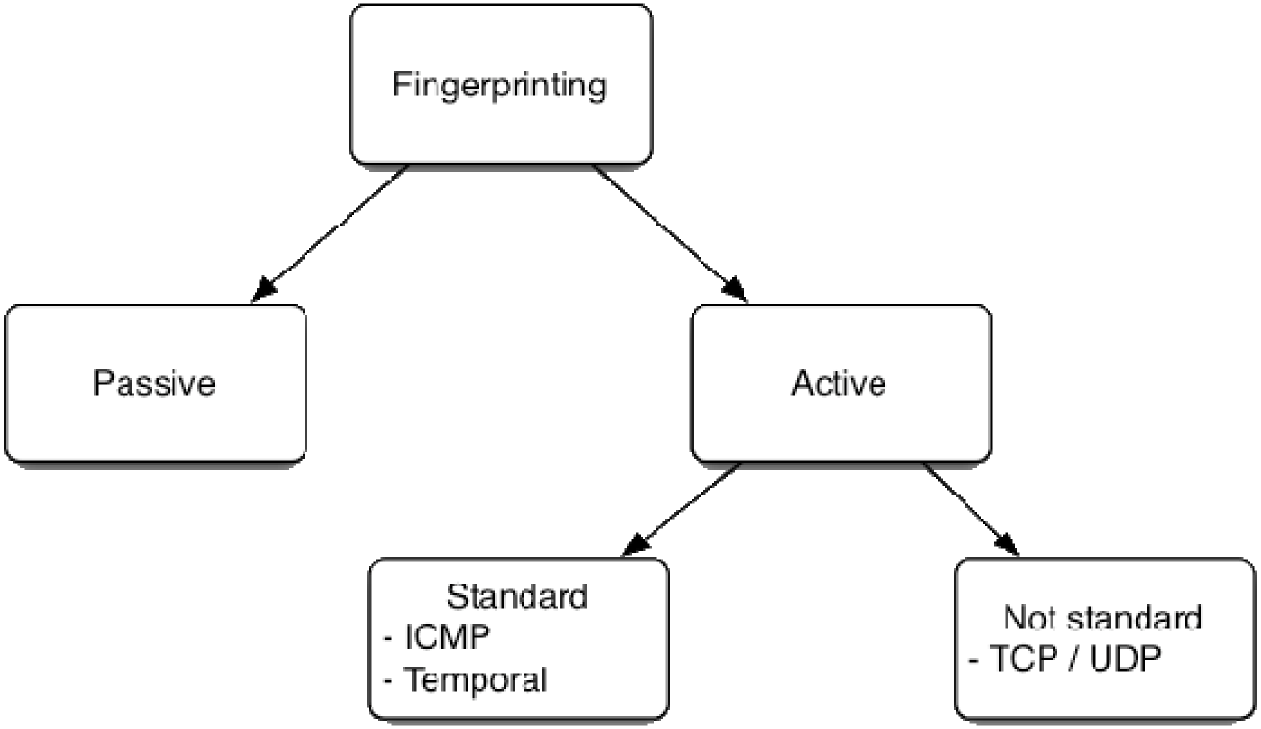


شناسایی سرویس

```
•  Interesting ports on whispermoon (213.215.31.18):
•  Not shown: 989 closed ports
•  PORT      STATE      SERVICE       VERSION
•  21/tcp    open       ftp           (Generally vsftp or WU-FTPD)
•  22/tcp    open       ssh           OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
•  25/tcp    open       smtp          Postfix smtpd
•  80/tcp    open       http          Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.5 with
   Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
•  135/tcp   filtered   msrpc
•  139/tcp   filtered   netbios-ssn
•  443/tcp   open       ssl/http      Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.5 with
   Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
•  445/tcp   filtered   microsoft-ds
•  993/tcp   open       ssl/imap      Dovecot imapd (SASL enabled)
•  995/tcp   open       ssl/pop3
```

Fingerprinting

انواع انگشت نگاری



Fingerprinting

Passive

Active

Standard
- ICMP
- Temporal

Not standard
- TCP / UDP

ایده اصلی

- در RFC جزییات پیاده سازی مشخص نشده است.
- هر برنامه نویس به صورت سلیقه ای بعضی از پارامترها طبق میل خود تعیین می کند.
- تفاوت های ظریفی در پشته شبکه وجود دارد.

Passive Fingerprinting

- بررسی بسته هایی که درون شبکه در حال عبور هستند.
- انواع انگشت نگاری منفعل:
  - ماشین هایی که به ما متصل می شوند (SYN)
  - ماشین هایی که ما به آن ها متصل می شویم (SYN+ACK)
  - ماشین هایی که نمی توانیم به آن ها متصل شویم (RST)
  - ماشین هایی که ارتباطات آن ها توسط ما قابل دیدن است.

POF

- Format : wwww:ttt:mmm:D:W:S:N:I:OS Description
  - wwww - window size
  - ttt - time to live
  - mmm - maximum segment size
  - D - don't fragment flag (0=unset, 1=set)
  - W - window scaling (-1=not present, other=value)
  - S - sackOK flag (0=unset, 1=set)
  - N - nop flag (0=unset, 1=set)
  - I - packet size (-1 = irrevelant)

خروجی POF

- <Wed Feb 27 18:26:58 2008> 213.215.x.x:45291 - Linux 2.6 (newer, 2) (up: 1421 hrs) -> 208.83.x.x:2703 (distance 0, link: ethernet/modem)
- <Wed Feb 27 18:27:02 2008> 212.24.x.x:62994 - FreeBSD 5.3-5.4 (up: 4556 hrs) -> 213.215.x.x:80 (distance 9, link: ethernet/modem)
- <Wed Feb 27 18:27:16 2008> 90.2.x.x:1322 - Windows 2000 SP4, XP SP1+ -> 213.215.x.x:80 (distance 9, link: pppoe (DSL))

نوع لینک

- بررسی MTU
  - Maximum Transmission Unit –
  - DSL ،1462 –
  - Ericsson HIS ،1656 –

Active Fingerprinting

1. ECN notification
2. window scale (10), NOP, MSS (1460), timestamp (TSval: 0xFFFFFFFF; TSecr: 0), SACK permitted. The window field is 1.
3. MSS (1400), window scale (0), SACK permitted, timestamp (TSval: 0xFFFFFFFF; TSecr: 0), EOL. The window field is 63.
4. Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), NOP, NOP, window scale (5), NOP, MSS (640). The window field is 4.
5. SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), window scale (10), EOL. The window field is 4.
6. MSS (536), SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0), window scale (10), EOL. The window field is 16.
7. MSS (265), SACK permitted, Timestamp (TSval: 0xFFFFFFFF; TSecr: 0). The window field is 512.

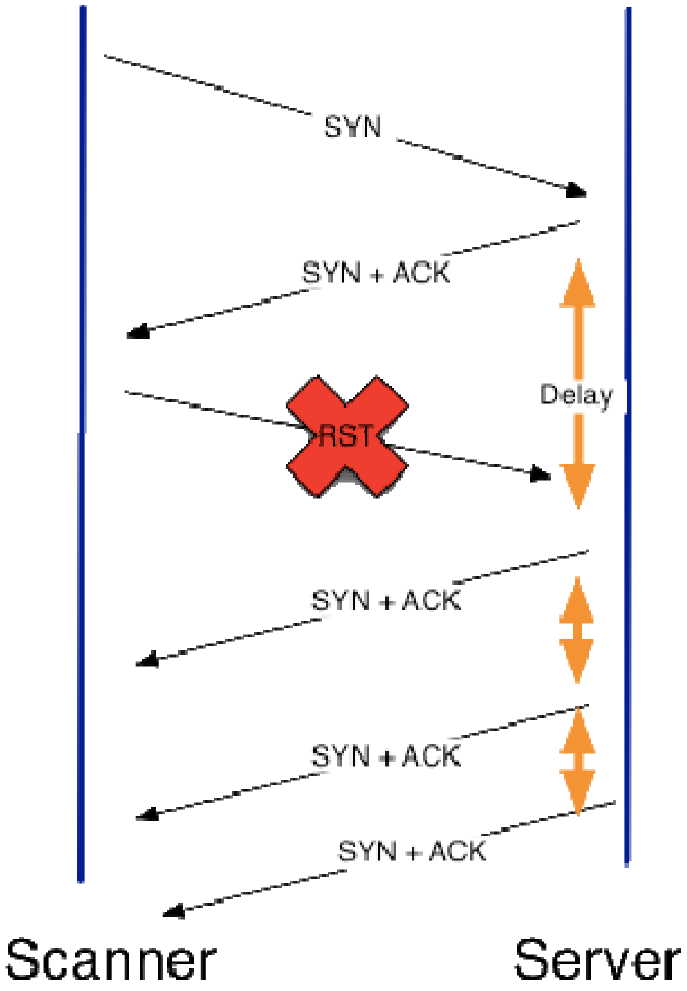
Nmap (4.11)

- **nmap -v -O 192.168.0.1**
- Interesting ports on 192.168.0.1:
- Not shown: 1678 closed ports
- PORT   STATE SERVICE
- 80/tcp   open http
- 4444/tcp open krb524
- MAC Address: 00:21:91:F8:48:3A (Unknown)
- No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).

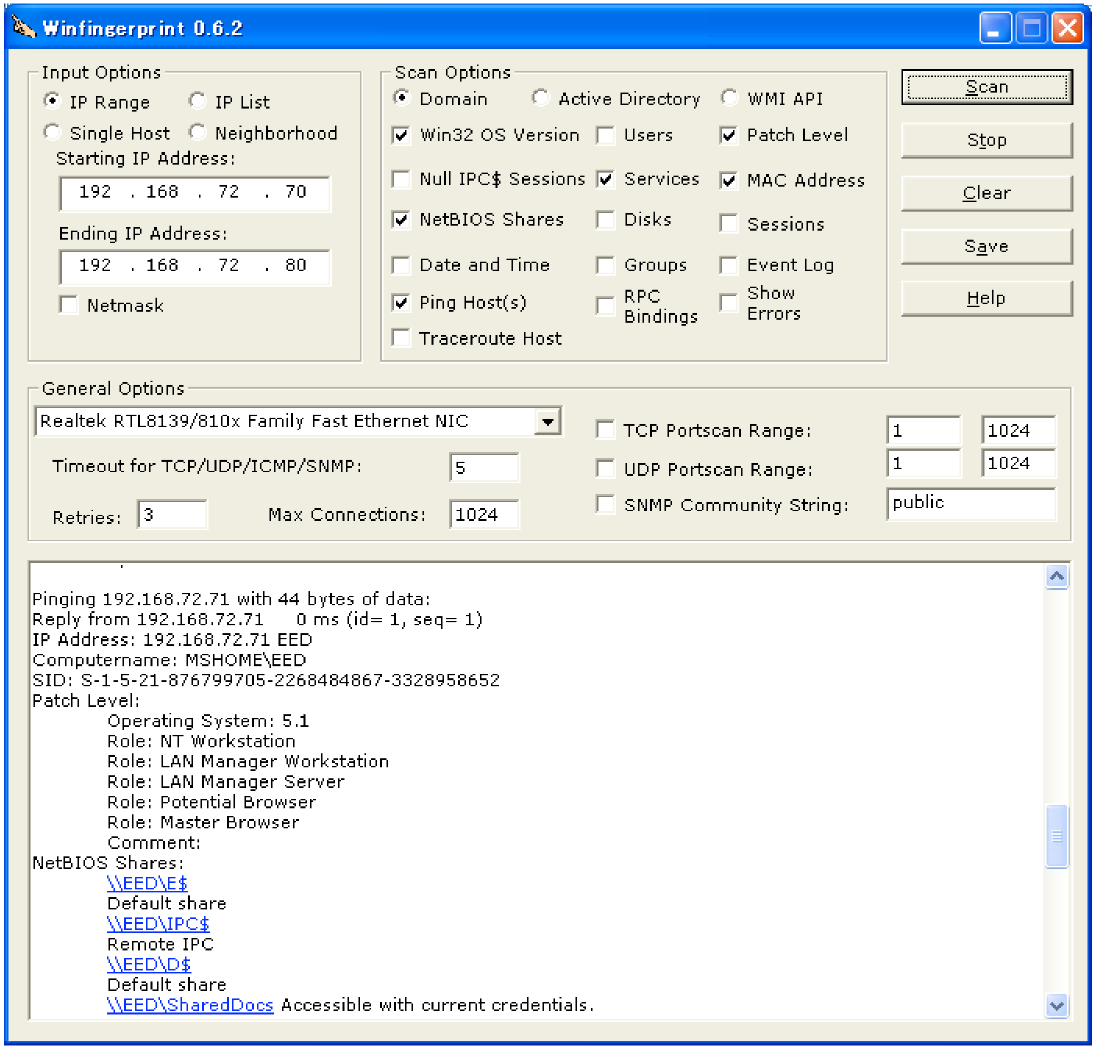
Nmap (4.8x)

- **nmap -O -v 192.168.0.1**
- PORT   STATE SERVICE
- 80/tcp   open http
- 4444/tcp open krb524
- 8099/tcp open unknown
- MAC Address: 00:21:91:F8:48:3A (D-Link)
- Device type: print server|router
- Running: D-Link embedded
- OS details: D-Link DPR-1260 print server, or DGL-4300 or DIR-655 router
- Network Distance: 1 hop
- TCP Sequence Prediction: Difficulty=174 (Good luck!)
- IP ID Sequence Generation: Incremental

Temporal Fingerprinting



Winfingerprint



Input Options

● IP Range ○ IP List
○ Single Host ○ Neighborhood

Starting IP Address: 192 . 168 . 72 . 70

Ending IP Address: 192 . 168 . 72 . 80

□ Netmask

Scan Options

● Domain ○ Active Directory ○ WMI API

☑ Win32 OS Version □ Users ☑ Patch Level
□ Null IPC$ Sessions ☑ Services ☑ MAC Address
☑ NetBIOS Shares □ Disks □ Sessions
□ Date and Time □ Groups □ Event Log
☑ Ping Host(s) □ RPC Bindings □ Show Errors
□ Traceroute Host

General Options

Realtek RTL8139/810x Family Fast Ethernet NIC

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3 Max Connections: 1024

□ TCP Portscan Range: 1 1024
□ UDP Portscan Range: 1 1024
□ SNMP Community String: public

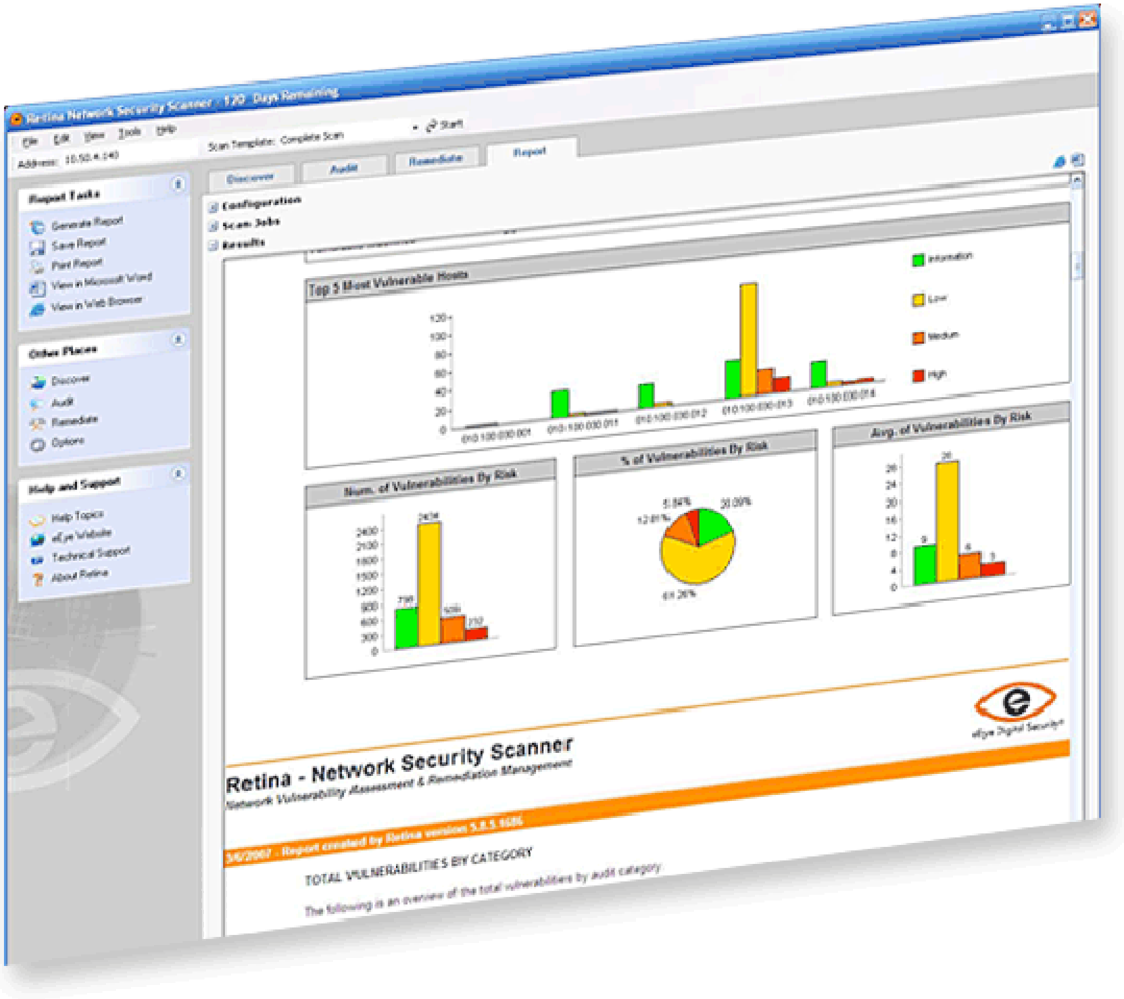
```
Pinging 192.168.72.71 with 44 bytes of data:
Reply from 192.168.72.71     0 ms (id= 1, seq= 1)
IP Address: 192.168.72.71 EED
Computername: MSHOME\EED
SID: S-1-5-21-876799705-2268484867-3328958652
Patch Level:
         Operating System: 5.1
         Role: NT Workstation
         Role: LAN Manager Workstation
         Role: LAN Manager Server
         Role: Potential Browser
         Role: Master Browser
         Comment:
NetBIOS Shares:
         \\EED\E$
         Default share
         \\EED\IPC$
         Remote IPC
         \\EED\D$
         Default share
         \\EED\SharedDocs Accessible with current credentials.
```

Vulnerability Scanner

اسکن کردن آسیب پذیری ها

- ابزاری که مجموعه ای از آسیب پذیری ها را دارد و تعیین می کند که چه هاست هایی دارای چه آسیب پذیری هایی هستند.
- انواع روش های اسکن آسیب پذیری:
  - محلی
  - از راه دور
  - ترکیب این دو

Retina



Retina - Network Security Scanner

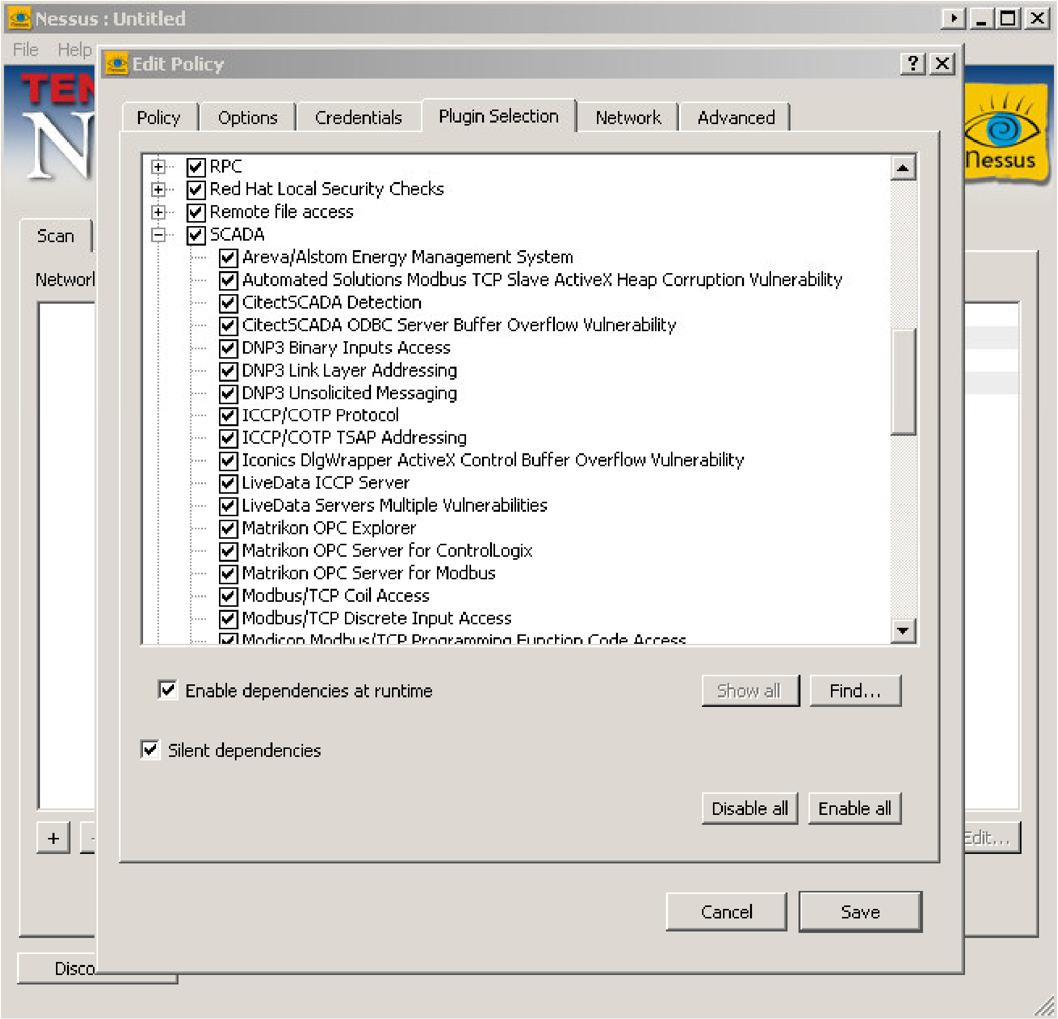
Network Vulnerability Assessment & Remediation Management

3/6/2007 - Report created by Retina version 5.8.5.1686

TOTAL VULNERABILITIES BY CATEGORY

The following is an overview of the total vulnerabilities by audit category

Nessus

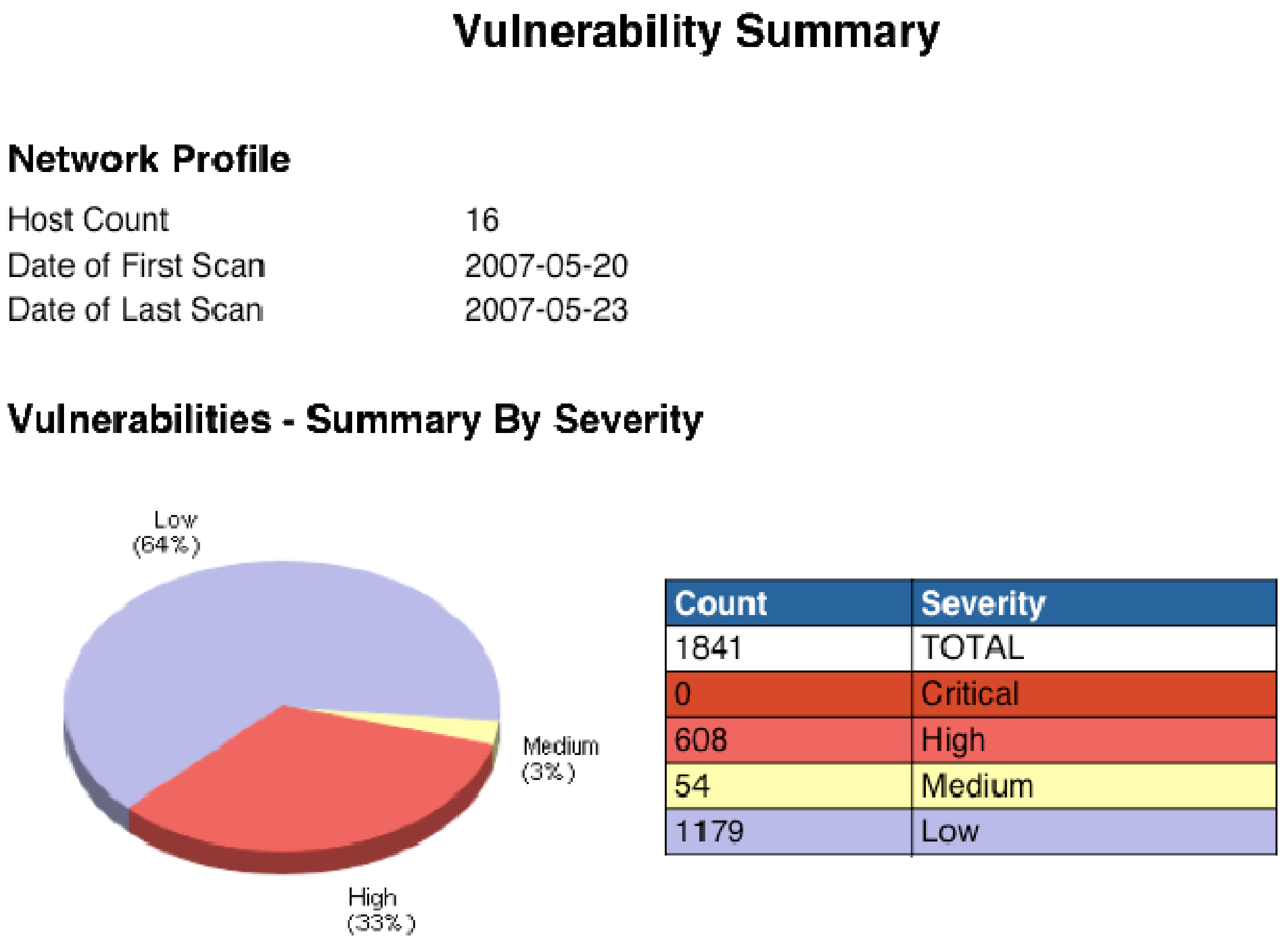


- ☑ RPC
- ☑ Red Hat Local Security Checks
- ☑ Remote file access
- ☑ SCADA
  - ☑ Areva/Alstom Energy Management System
  - ☑ Automated Solutions Modbus TCP Slave ActiveX Heap Corruption Vulnerability
  - ☑ CitectSCADA Detection
  - ☑ CitectSCADA ODBC Server Buffer Overflow Vulnerability
  - ☑ DNP3 Binary Inputs Access
  - ☑ DNP3 Link Layer Addressing
  - ☑ DNP3 Unsolicited Messaging
  - ☑ ICCP/COTP Protocol
  - ☑ ICCP/COTP TSAP Addressing
  - ☑ Iconics DlgWrapper ActiveX Control Buffer Overflow Vulnerability
  - ☑ LiveData ICCP Server
  - ☑ LiveData Servers Multiple Vulnerabilities
  - ☑ Matrikon OPC Explorer
  - ☑ Matrikon OPC Server for ControlLogix
  - ☑ Matrikon OPC Server for Modbus
  - ☑ Modbus/TCP Coil Access
  - ☑ Modbus/TCP Discrete Input Access
  - ☑ Modicon Modbus/TCP Programming Function Code Access

☑ Enable dependencies at runtime

☑ Silent dependencies

گزارش Nessus



Vulnerability Summary

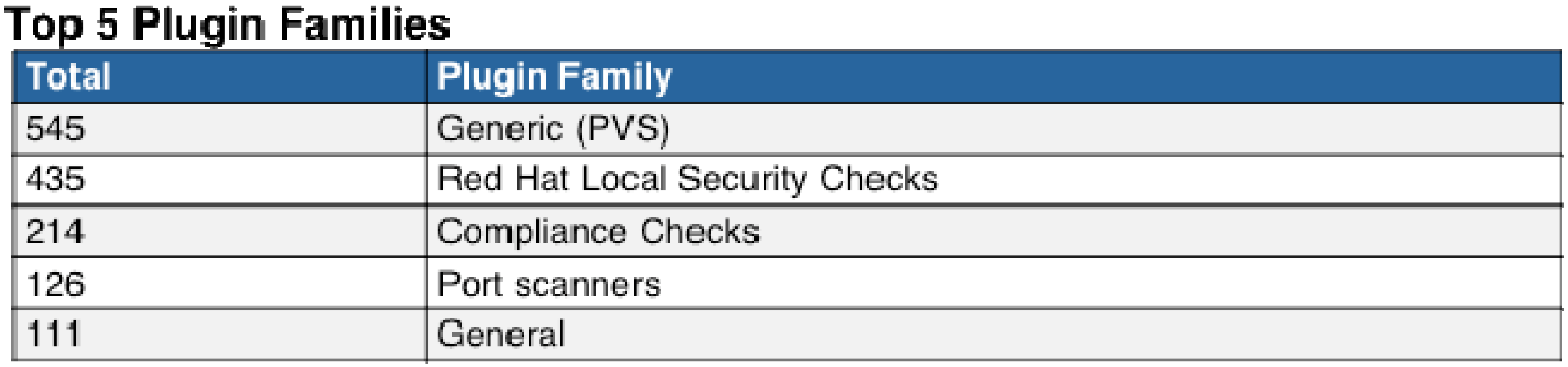
Network Profile

Host Count	16
Date of First Scan	2007-05-20
Date of Last Scan	2007-05-23

Vulnerabilities - Summary By Severity

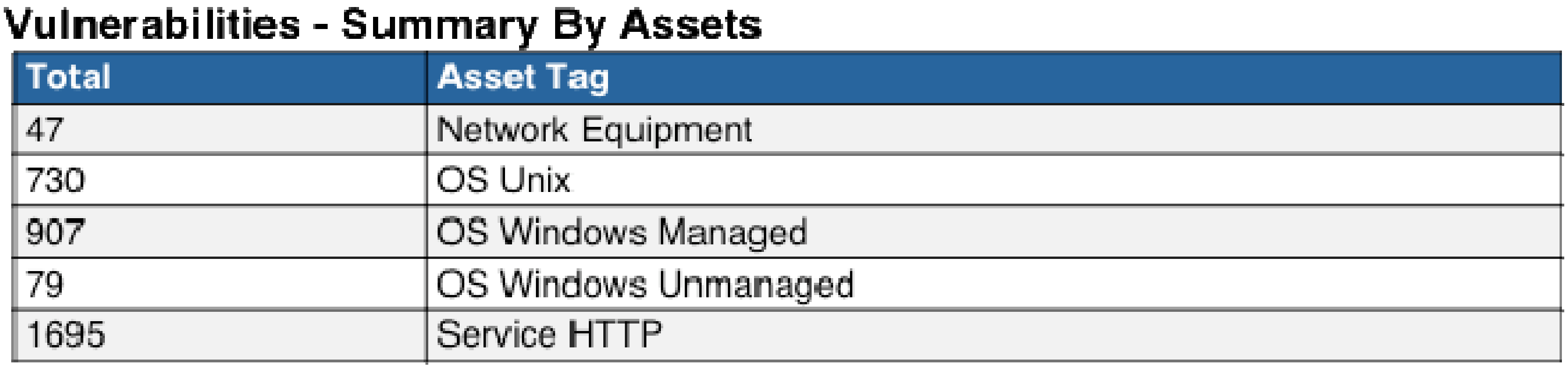
Count	Severity
1841	TOTAL
0	Critical
608	High
54	Medium
1179	Low

گزارش Nessus



Top 5 Plugin Families

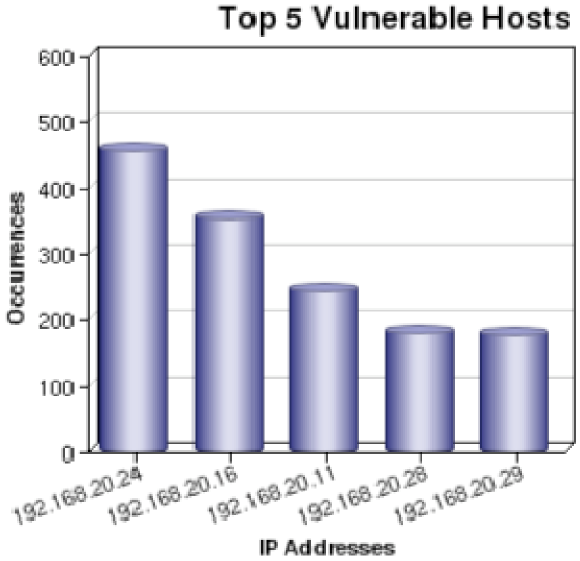
Total	Plugin Family
545	Generic (PVS)
435	Red Hat Local Security Checks
214	Compliance Checks
126	Port scanners
111	General

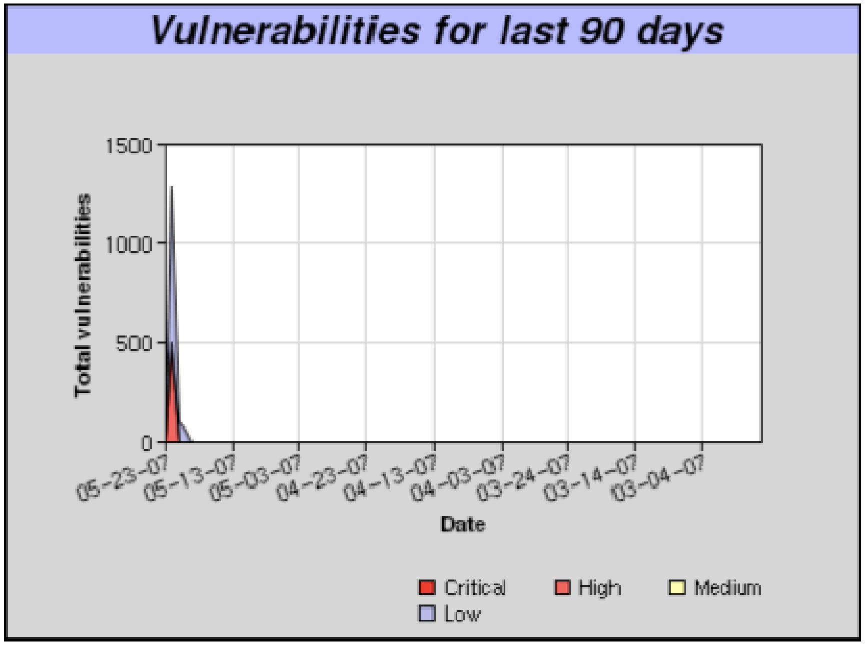


Vulnerabilities - Summary By Assets

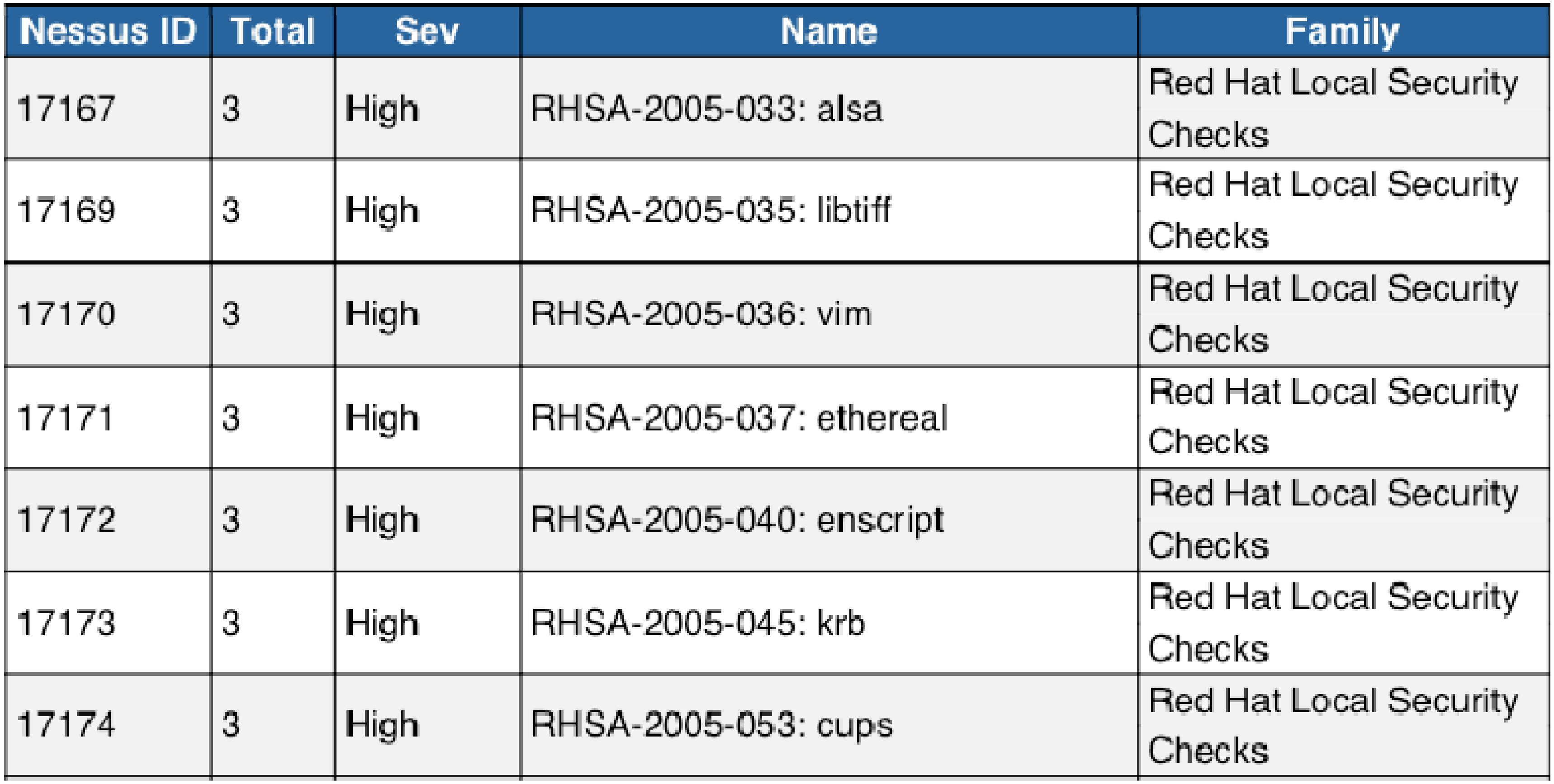
Total	Asset Tag
47	Network Equipment
730	OS Unix
907	OS Windows Managed
79	OS Windows Unmanaged
1695	Service HTTP

گزارش Nessus



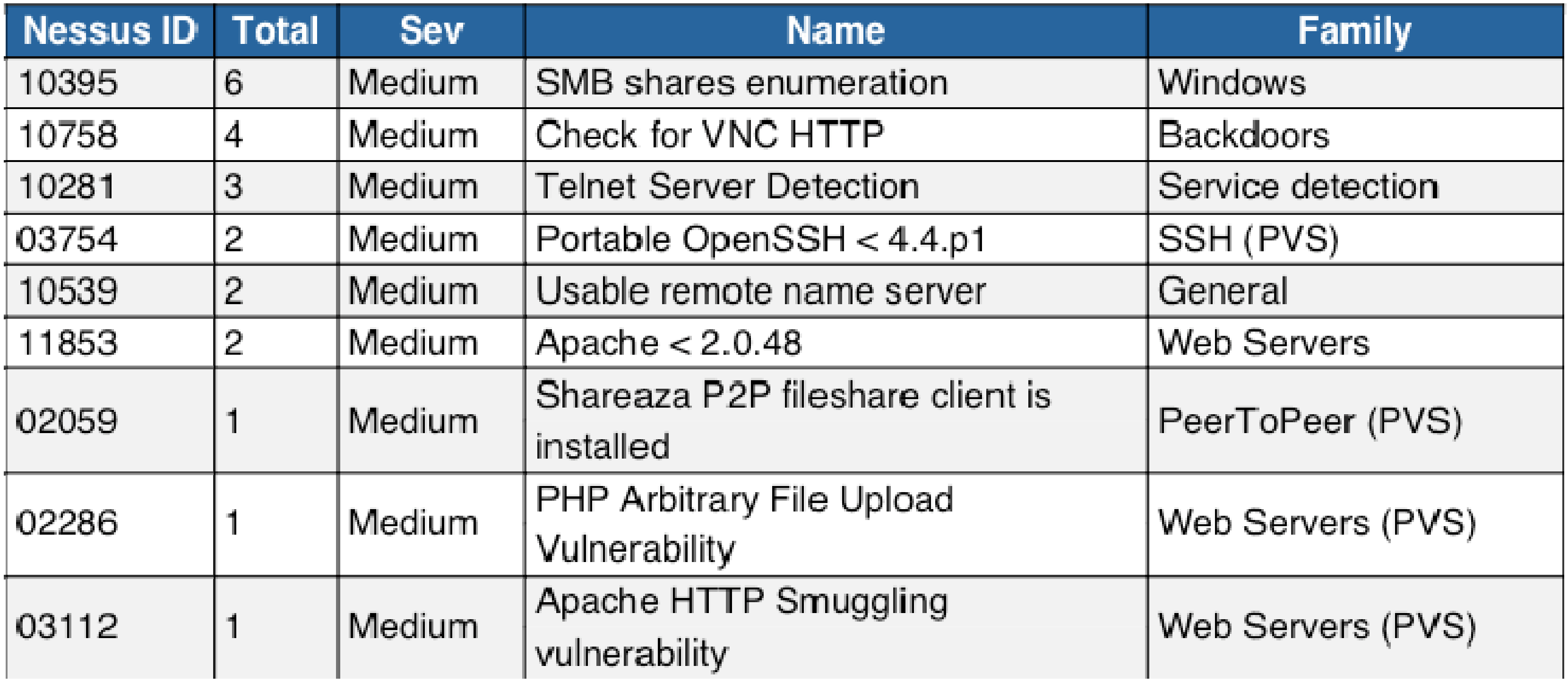


گزارش Nessus



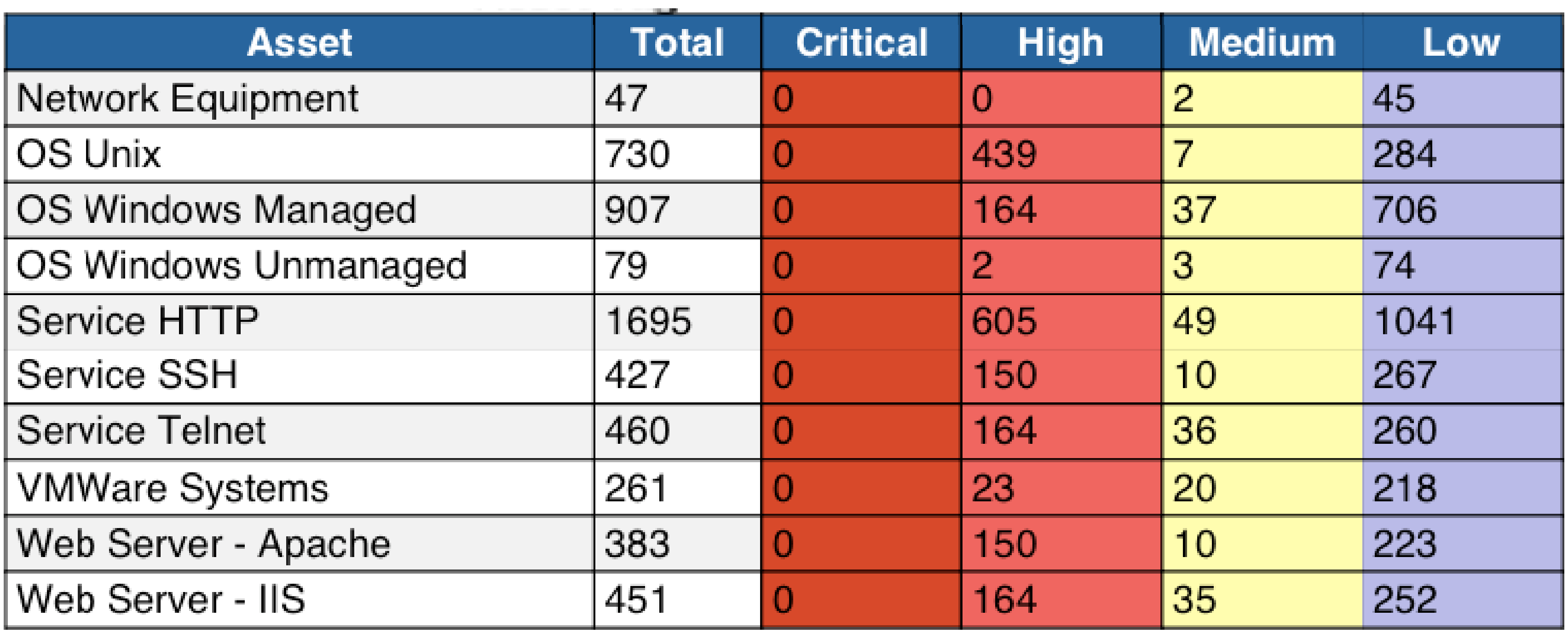
Nessus ID	Total	Sev	Name	Family
17167	3	High	RHSA-2005-033: alsa	Red Hat Local Security Checks
17169	3	High	RHSA-2005-035: libtiff	Red Hat Local Security Checks
17170	3	High	RHSA-2005-036: vim	Red Hat Local Security Checks
17171	3	High	RHSA-2005-037: ethereal	Red Hat Local Security Checks
17172	3	High	RHSA-2005-040: enscript	Red Hat Local Security Checks
17173	3	High	RHSA-2005-045: krb	Red Hat Local Security Checks
17174	3	High	RHSA-2005-053: cups	Red Hat Local Security Checks

گزارش Nessus



Nessus ID	Total	Sev	Name	Family
10395	6	Medium	SMB shares enumeration	Windows
10758	4	Medium	Check for VNC HTTP	Backdoors
10281	3	Medium	Telnet Server Detection	Service detection
03754	2	Medium	Portable OpenSSH < 4.4.p1	SSH (PVS)
10539	2	Medium	Usable remote name server	General
11853	2	Medium	Apache < 2.0.48	Web Servers
02059	1	Medium	Shareaza P2P fileshare client is installed	PeerToPeer (PVS)
02286	1	Medium	PHP Arbitrary File Upload Vulnerability	Web Servers (PVS)
03112	1	Medium	Apache HTTP Smuggling vulnerability	Web Servers (PVS)

گزارش Nessus



Asset	Total	Critical	High	Medium	Low
Network Equipment	47	0	0	2	45
OS Unix	730	0	439	7	284
OS Windows Managed	907	0	164	37	706
OS Windows Unmanaged	79	0	2	3	74
Service HTTP	1695	0	605	49	1041
Service SSH	427	0	150	10	267
Service Telnet	460	0	164	36	260
VMWare Systems	261	0	23	20	218
Web Server - Apache	383	0	150	10	223
Web Server - IIS	451	0	164	35	252

تحلیل ترافیک شبکه

- 17:31:16.301217 IP (tos 0x0, ttl 42, id 24244, offset 0, flags [none], proto: TCP (6), length: 44) 192.168.0.194.52232 > 192.168.0.1.80: S, cksum 0x6485 (correct), 3647930309:3647930309(0) win 3072 <mss 1460>

- 17:31:16.301667 IP (tos 0x0, ttl 57, id 37298, offset 0, flags [none], proto: TCP (6), length: 44) 192.168.0.194.52232 > 192.168.0.1.81: S, cksum 0x6884 (correct), 3647930309:3647930309(0) win 2048 <mss 1460>

- 17:31:16.301987 IP (tos 0x0, ttl 64, id 48783, offset 0, flags [none], proto: TCP (6), length: 44) 192.168.0.1.80 > 192.168.0.194.52232: S, cksum 0xc685 (correct), 2609643106:2609643106(0) ack 3647930310 win 4096 <mss 1460>

- 17:31:16.417655 IP (tos 0x0, ttl 64, id 48786, offset 0, flags [none], proto: TCP (6), length: 44) 192.168.0.1.80 > 192.168.0.194.52425: S, cksum 0x8030 (correct), 2610399074:2610399074(0) ack 1654600479 win 4096 <mss 1460>

- 17:31:16.417679 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: TCP (6), length: 40) 192.168.0.194.52425 > 192.168.0.1.80: R, cksum 0xcaf4 (correct), 1654600479:1654600479(0) win 0

- 17:31:17.021331 IP (tos 0x0, ttl 61, id 4162, offset 0, flags [none], proto: UDP (17), length: 328) 192.168.0.194.52300 > 192.168.0.1.39695: UDP, length 300
- 17:31:16.993102 IP (tos 0x4, ttl 58, id 43133, offset 0, flags [none], proto: ICMP (1), length: 178) 192.168.0.194 > 192.168.0.1: ICMP echo request, id 34388, seq 296, length 158

- 17:31:17.217108 IP (tos 0x0, ttl 41, id 17642, offset 0, flags [none], proto: TCP (6), length: 60) 192.168.0.194.52444 > 192.168.0.1.79: FP, cksum 0x5191 (correct), 1654600478:1654600478(0) win 65535 urg 0 <wscale 15,nop,mss 265,timestamp 4294967295 0,sackOK>

- 01:25:08.063167 192.168.1.40.http > 192.168.1.40.http: S [bad tcp cksum a8e4!] 3868:3868(0) win 2048 (ttl 255, id 3868, len 40

```
23:57:12.623167 192.168.1.2.40 > 192.168.1.3.netbios-ssn: S [tcp sum ok] 740990201:740990201(0) win 16384 <mss 1460,nop,nop,sackOK>
                (DF) (ttl 128, id 39059, len 48)

23:57:12.623167 192.168.1.3.netbios-ssn > 192.168.1.2.40: S [tcp sum ok] 3674022113:3674022113(0) ack 740990202 win 5840
                <mss 1460,nop,nop,sackOK> (DF) (ttl 64, id 0, len 48)

23:57:12.623167 192.168.1.2.40 > 192.168.1.3.netbios-ssn: . [tcp sum ok] 1:1(0) ack 1 win 17520 (DF) (ttl 128, id 39060, len 40)

23:57:12.623167 192.168.1.2.40 > 192.168.1.3.netbios-ssn: P 1:256(255) ack 1 win 17520 urg 255
>>> NBT Packet
flags=0x42
NBT - Unknown packet type
Type=0x424F4F4F
Data: (251 bytes)
[000] 4F 4F 4F 4F 4F 4F 4F 4F  4F 4F 4F 4F 4D 00 20 00  OOOOOOOO OOOOM. .
[010] 39 00 35 00 00 00 FF FF  C0 F8 12 00 99 2A 41 00  9.5..... .....*A.
[020] 10 F9 12 00 28 F9 00 00  00 00 11 00 00 00 70 6F  ....(... ......po
[030] 72 74 20 34 30 00 00 00  00 00 19 00 00 00 00 00  rt 40... ........
[040] 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
[050] 00 00 19 00 00 00 F0 84  15 08 90 A9 15 08 08 A9  ........ ........
[060] 15 08 00 00 00 00 00 00  00 00 11 00 00 00 5F 59  ........ ......_Y
[070] 23 40 10 B4 01 40 00 00  00 00 11 00 00 00 30 98  #@...@.. ......0.
[080] 15 08 C8 C8 15 08 00 00  00 00 21 00 00 00 2F 6C  ........ ..!.../l
[090] 69 62 2F 6C 69 62 6E 73  73 5F 6E 69 73 70 6C 75  ib/libns s_nisplu
[0A0] 73 2E 73 6F 2E 32 00 00  00 00 19 04 00 00 8B 50  s.so.2.. .......P
[0B0] 60 91 F0 78 47 9B 70 2C  D7 9B 70 91 BC 9C F0 48  `..xG.p, ..p....H
[0C0] C0 9D 70 FE 89 9E F0 2A  A0 9F F0 A5 60 A0 F0 0C  ..p....* ....`...
[0D0] 80 A1 F0 12 2E A2 F0 4C  7A A3 F0 81 35 A4 70 23  .......L z...5.p#
[0E0] 5E A5 F0 35 25 A6 F0 9B  27 A7 70 26 58 A8 F0 7D  ^..5%... '.p&X..}
[0F0] 07 A9 70 34 EE A9 F0 5F  E7 AA F0                 ..p4..._ ...

 (DF) (ttl 128, id 39061, len 295)

23:57:12.623167 192.168.1.3.netbios-ssn > 192.168.1.2.40: . [tcp sum ok] 1:1(0) ack 256 win 5840 (DF) (ttl 64, id 1714, len 40)
23:57:12.633167 192.168.1.3.netbios-ssn > 192.168.1.2.40: R [tcp sum ok] 1:1(0) ack 256 win 5840 (DF) (ttl 64, id 1715, len 40)
```