GSEC

Practical Assignment

Version 1.4

Option 1 – Research on Topics in Information Security

Post-Scan Analysis – How to Identify SANS/FBI Top Twenty Vulnerabilities from Nmap Scan Results

Lin Han

September 11, 2002

Abstract

Vulnerability assessment is an effective way to help security managers identify potential risks in their organization infrastructure and act timely upon what is reported to protect their information assets. The purpose of this paper is to present a brief overview of vulnerability assessment, and explore the flexibility and raw-data-oriented feature of nmap, a network scan tool, as an option to determine whether a system is vulnerable to some of the SANS/FBI Top Twenty vulnerabilities from a port-scan perspective.

Introduction

With the advent of open systems, intranets, and the Internet, organizations' information assets are facing an increasing number of threats. In 2001, computer security incidents reported to the CERT Coordination Center are more than the total of the 13-year history [1]. Protecting information from exposure is getting more and more critical.

However, as hundreds of new vulnerabilities are being discovered annually and dozens of new patches are being released monthly [2], building a solid defense for an organization's information assets is a daunting task – security managers have to patch every hole in the environment, but attackers need to explore only one to get into the systems. Therefore, security managers must always be aware of security weaknesses within the organization infrastructure before potential attackers do – that is where vulnerability assessment fits.

Vulnerability Assessment

As defined in [3], "vulnerability assessment is the process of measuring and prioritizing potential security risks associated with network and host-based systems and devices to allow rational planning of technologies and activities that manage business risk."

Vulnerability assessment is widely recognized as a proactive approach to network security. It is performed to determine the actual security posture of a network environment, by actively probing targeted networks for their susceptibility to known (and potentially unknown) attacks. If some vulnerability is found, a well-defined corrective action plan can be carried out. Thereby necessary reparation may be made before an actual exploitative attack occurs [3][4].

Since an organization's networks may change frequently, vulnerability assessment should be performed on a regular basis. Frequent and well-managed vulnerability assessment offers early vulnerability detection, hence enabling rapid reparation to prevent intrusion and system compromise.

Vulnerability scanners are powerful tools to conduct vulnerability assessment [5]. They utilize a database of known vulnerabilities (sometimes called signatures) to probe a network or host to find problems. Vulnerability scanners can customize security policies, analyze vulnerabilities, and create reports to effectively communicate vulnerability discoveries and detailed corrective actions to all levels of an organization [6].

Hundreds of vulnerability scanners are available, in both freeware and commercial tools. They vary considerably according to their abilities and can be categorized into network scanner, host scanner, database scanner, online scanner, and wardialer [7][8].

Network scan presents a snapshot of the high-risk vulnerabilities to which security managers need to pay immediate attention. For example, assessment based on network scan might catch extremely critical vulnerabilities, such as misconfigured firewalls or vulnerable web servers in a DMZ, which could provide a step stone to attackers. Thus, a network scanner is the primary tool that should be employed in a vulnerability assessment process [6]. It performs quick and detailed analysis of an organization's network and system infrastructure from the perspective of an external or internal attacker.

There exist many network scanners [7][8], such as Nessus [9], SARA [10], and Whisker [11]. Among these tools, nmap [12] is a very popular one.

Nmap

Nmap (Network Mapper) is an open source utility for network exploration or security auditing. It was designed to rapidly perform port scan on large networks, as well as a single host. Nmap uses raw IP packets in a novel way to determine which hosts are up in the network, which services (ports) are offered, which operating systems are running, what type of packet filters/firewalls are in use, and so on [12]. Nmap can run on most types of operating systems, and both console and graphical versions are available. More attractive, nmap is a freeware.

Nmap is flexible. It suits different types of network scan – fast scan, stealth scan, and bypassing firewalls scan; provides a variety of features – decoyed packet, dynamic delay time calculation, and flexible target and port specification; and is capable of scanning diverse protocols – UDP, TCP, and ICMP.

Nmap supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles [13][14]:

- Vanilla TCP connect scan
- TCP SYN (half open) scan

- TCP FIN, Xmas, or NULL (stealth) scan
- TCP FTP proxy (bounce attack) scan
- Fragmentation (bypassing some packet filters) scan
- TCP reverse ident scan
- TCP ping scan
- TCP ACK and Window scan
- UDP ICMP port unreachable scan
- ICMP scan (ping-sweep)
- Direct (non portmapper) RPC scan
- Remote OS identification by TCP/IP fingerprinting

As many network security holes are dependent on the operating system version running on a targeted host, remote detection of machine architecture, OS version, and TCP/IP stack becomes the first priority for a network scanner.

Nmap can grab such information. It employs ping scan to detect hosts alive, many port-scan techniques to determine services provided, and TCP/IP fingerprinting to identify remote hosts' operating systems.

Twenty Most Critical Internet Security Vulnerabilities

Discovering all existing vulnerabilities in an organization infrastructure is a tedious task and requires huge amount of time and efforts. However, not all vulnerabilities apply equally to a specific infrastructure and not all vulnerabilities have the same severity or are as easy to exploit. Moreover, it turns out that most attackers are opportunistic – they exploit the limited number of vulnerabilities that are well known, counting on organizations not fixing the problems. This largely affects the probability for a certain vulnerability to be exploited. Consequently, security managers must be able to rank the severity of vulnerabilities to which their infrastructure is exposed, and identify the most critical ones in order to prioritize their efforts in fixing them [15].

To help alleviate the problem that security managers could not have corrected many of the flaws on their infrastructure simply because they did not know which vulnerabilities were most dangerous, the SANS/FBI Top Twenty vulnerability list was released on October 1, 2001, with the consensus of dozens of security experts from the most security-conscious federal agencies, the leading security software vendors and consulting firms, the top university-based security programs, the CERT Coordination Center and the SANS Institute. This list describes the vulnerabilities that were exploited by the majority of successful attacks on computer systems via the Internet, as well as all necessary information to correct the vulnerabilities.

The SANS/FBI Top Twenty list is a living document, updated when more critical threats and more current or convenient methods are identified. The list can be segmented into three categories – general vulnerabilities that affect all systems, vulnerabilities to Windows systems, and vulnerabilities to Unix systems [16].

1. *Top Vulnerabilities That Affect All Systems*

- Default installs of operating systems and applications
- Accounts with no passwords or weak passwords
- Non-existent or incomplete backups
- Large number of open ports
- Not filtering packets for correct incoming and outgoing addresses
- Non-existent or incomplete logging
- Vulnerable CGI programs

2. *Top Vulnerabilities to Windows Systems*

- Unicode vulnerability (web server folder traversal)
- ISAPI extension buffer overflows
- IIS RDS exploit (Microsoft Remote Data Services)
- NETBIOS - unprotected Windows networking shares
- Information leakage via null session connections
- Weak hashing in SAM (LM hash)

3. *Top Vulnerabilities To Unix Systems*

- Buffer overflows in RPC services
- Sendmail vulnerabilities
- Bind weaknesses
- R commands
- LPD (remote print protocol daemon)
- Sadmind and mountd
- Default SNMP strings

Thousands of organizations use the above list to prioritize their efforts so that they could patch the most dangerous holes first.

Identifying Top Twenty Vulnerabilities from Nmap Scan Results

Several commercial vulnerability scanners may be used to scan for SANS/FBI Top Twenty vulnerabilities [16]. Besides, there are some freeware available as well, among which SARA is a famous automated scanning tool, designed specifically to discover and report on the status of vulnerabilities on the SANS/FBI Top Twenty list. It runs on most Unix operating systems, capable of scanning a wide range of network servers and devices.

Due to the nature of nmap and the multiple advanced techniques it supports, it is possible to detect Top Twenty vulnerabilities using nmap scan. This brings several advantages:

- Nmap is raw-data-oriented. It provides security mangers with the flexibility of conducting various analysis – by specific open ports, by certain operating systems, by service profiles (common services), and so on.
- Since namp can produce machine parseable or human readable output files, it is possible to convert the output file (.gnmap) into a Comma Separate Value (.csv) file, and further into a database. This will make it

easy to compare two consecutive scans so as to check whether any improvements have been made since last scan.

- Nmap is a general-purpose network scanner. It was not designed specifically to identify Top Twenty vulnerabilities. Thus, when a new vulnerability relating to some services comes out, it is possible to verify whether any system is vulnerable only by searching in the database.
- The analysis of nmap scan results can show a main direction for further vulnerability assessments which need to be conducted in a high-risk environment.

In the following, we will explore the use of nmap as an option to identify some of the “challenging” Top Twenty vulnerabilities from a port-scan perspective.

a. Default installs of operating systems and applications

Default installations of an operating system nearly always include extraneous services and corresponding open ports. These services are operating system dependent. For example, we can find out potential default installation of Unix operating system or a Unix box whose hardening measures are not conducted enough, by looking in nmap scan results for the system with Unix OS fingerprint and ports 7 (echo), 19 (chargen), 37 (time), and 79 (finger) open. More investigation should be done if such systems are found.

b. Large number of open ports

The more ports that are open, the higher risk a system presents since attackers can break into the system via these open ports and exploit vulnerabilities associated with the corresponding services.

Nmap is a perfect port scanner. It can discover whether a system in a network is up and to which ports the system is listening.

By sorting namp scan results according to the number of opened SANS common vulnerable ports (see Appendix 1) and nmap referred open ports (see Appendix 2), security managers can rate the risk of their organization networks, as shown in Figure 1. Further vulnerability assessment is necessary in the identified high-risk areas.

c. Not filtering packets for correct incoming and outgoing addresses

Nmap has options to send decoyed packets or spoofed packets [17]. Security managers can use this feature to test the packet filtering functionality of their external firewalls or routers.

d. Vulnerable CGI programs, Unicode vulnerability (web server folder traversal), ISAPI extension buffer overflows, and IIS RDS exploit (Microsoft Remote Data Services)

Nmap is unable to catch these vulnerabilities directly, but it does show a direction for further investigation, e.g., Whisker scan, by providing a list of IP addresses. The list is easy to build – simply seeking in nmap scan results for the systems with port 80 (http) open and the following OS fingerprints.

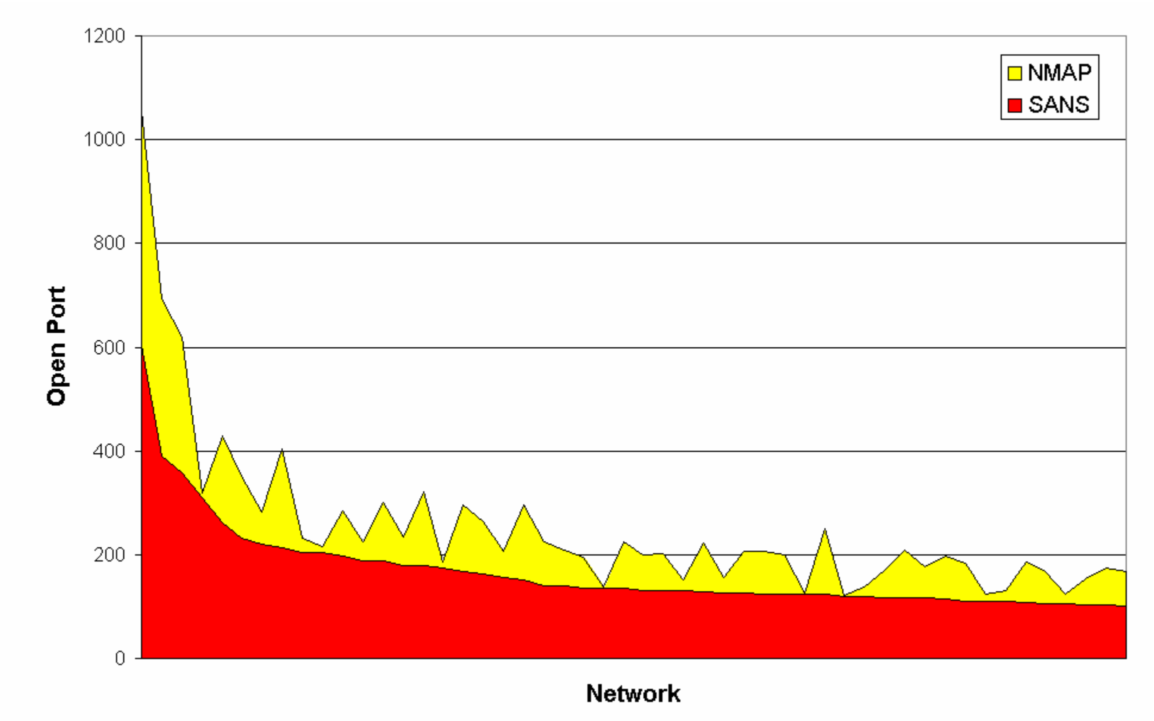

Figure 1. Risk Map

- ○ All possible operating systems (for CGI program vulnerability);
- ○ Windows NT or Windows 2000 (for the other three vulnerabilities).

Taking this list as the input, Whisker can determine whether the systems are really vulnerable – among the entries with the pattern “200 Ok:” in the output file, if the following shows up, the corresponding system presents certain vulnerability.

- ○ “GET /cgi-bin/” or “HEAD /cgi-bin/”, and some sample programs under the cgi-bin directory – vulnerable CGI programs;
- ○ “GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir” or “GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir” – unicode vulnerability;
- ○ “GET /whisker.idq” – ISAPI extension buffer overflows;
- ○ “HEAD /msadc/msadcs.dll” – IIS RDS exploit.

e. NETBIOS - unprotected Windows networking shares

As above, nmap can provide an IP address list for further investigation other than detecting NETBIOS vulnerability directly. The list can be constructed by searching in nmap scan results for the systems with the OS fingerprint of Windows NT or Windows 2000 and having ports 139 (netbios-ssn) or 445 (microsoft-ds) open. The addresses can be used by the NAT (NetBIOS Auditing Tool) [18] utility to discover the unprotected Windows networking shares.

```
NAT.EXE 1.2.3.4 -u userlist.txt -p passwdlist.txt -o 1.2.3.4.txt
```

where

1.2.3.4 represents an IP address;
userlist.txt lists all the possible accounts; and
passwdlist.txt lists all the possible passwords.

If a system has unprotected Windows networking shares, the following entry exists in *1.2.3.4.txt*.

“*WARNING: Able to access share:*”

f. Information leakage via null session connections

An nmap-generated IP address list – IP addresses of the systems with the OS fingerprints of Windows NT or Windows 2000 and having ports 135 (epmap), 136, (profile), 137 (netbios-ns), 138 (netbios-dgm), 139 (netbios-ssn) or 445 (microsoft-ds) open, can be used to verify the existence of null session connections by a master batch file which calls another batch file (*net_use_scan.bat*) repeatedly:

```
call net_use_scan.bat 1.2.3.4

call net_use_scan.bat 5.6.7.8

……
```

where 1.2.3.4 or 5.6.7.8 represents an IP address.

The batch file *net_use_scan.bat* is composed of three commands:

```
net use  \\%1\ipc$  /user:“” “” >> net_use_scan.log

net use |grep %1 >> net_use_scan.log

net use \\%1 /delete >> net_use_scan.log
```

All systems with null session connections can be determined through analyzing the log file *net_use_scan.log*

```
grep “OK” net_use_scan.log
```

g. Buffer overflows in RPC services

Rpc.ttdbserverd, rpc.cmsd, and rpc.statd are the three RPC services that are most commonly exploited through buffer overflow attacks which are successful because the RPC programs do not do proper error checking.

By searching in nmap scan results for the Unix boxes with ports 111 (sunrpc) or 2049 (nfs) open and at the same time with at least one of the ports from 32770 to 32789 (RPC loopback ports) open, potentially vulnerable systems can be found. These systems need to be further examined to see whether the latest patches have been installed.

h. Sendmail vulnerabilities

If any Unix or Linux boxes with port 25 (smtp) open are found in nmap scan results, it probably means these systems have the Sendmail vulnerability. Then it is necessary to check whether Sendmail has been upgraded or patched correctly.

i. Bind weaknesses

Nmap scan results can be used to find whether there are some systems in an infrastructure having BIND weaknesses – just looking for the Unix or Linux boxes with port 53 (domain) open. If so, DNS servers must be verified whether they are updated to the latest version and patch level.

j. R commands

Remote login (rlogin), remote shell (rsh), and remote copy (rcp) are the three commonly used r commands. If Unix or Linux boxes with the ports 513 (login), 514 (shell), or 544 (kshell) open are found in nmap scan result, these systems have to be further examined for the file */etc/hosts.equiv* or *~/.rhosts* so as to determine whether they are vulnerable to r commands.

k. LPD (remote print protocol daemon)

Any discovered Sun or Linux boxes with port 515 (printer) open present the potential to this vulnerability. Further verification on the version number needs to be done.

l. Sadmind and mountd

This is a special case of buffer overflows in RPC services. If Unix boxes with port 111 (sunrpc) open and either of the following cases happening, then the systems are possibly vulnerable. Patch level needs to be checked.

- Ports 2049 (nfs) and 1023 (mountd) [19] are open;
- Port 32773 (rpc.sadmind) [20] is open.

m. Default SNMP Strings

Nmap cannot detect the default SNMP strings, but lists all IP addresses of the network-connected devices which are running SNMP (TCP/UDP ports 161, 162, 199, 391, 1993, or TCP port 705 [21]). However, according to my experience, this is not reliable. Solarwinds network management tools [22] are good at catching this vulnerability.

The following table summarizes this section.

Vulnerability	OS	Possible Port(s)	Nmap
Default installs of operating systems and applications	Unix*	7, 19, 37, 79*	D
Large number of open ports	All	1 - 65535	D

* This is only an example.

Not filtering packets for correct incoming and outgoing addresses	All	**	D
Vulnerable CGI programs	All	80	P
Unicode vulnerability	Windows NT, windows 2000	80	P
ISAPI extension buffer overflows	Windows NT, windows 2000	80	P
IIS RDS exploit	Windows NT, windows 2000	80	P
NETBIOS - unprotected Windows networking shares	Windows NT, windows 2000	139, 445	P
Information leakage via null session connections	Windows NT, windows 2000	135, 136, 137, 138, 139, 445	P
Buffer overflows in RPC services	Unix	111, 2049, 32770 - 32789	D
Sendmail vulnerabilities	Unix, Linux	25	D
Bind weaknesses	Unix, Linux	53	D
R commands	Unix, Linux	513, 514, 544	D
LPD	Solaris, Linux	515	D
Sadmind and mountd	Unix	111, 1023, 2049, 32773	D
Default SNMP strings	Unix, network devices	161, 162, 199, 391, 705, 1993	P

D – show the vulnerability
P – provide a pointer

Conclusions

Vulnerability assessment is an effective way of detecting vulnerabilities, hence taking corrective actions before actual attacks occur. As a network scanner, nmap helps discover active hosts, open services, and running operating systems. From a post-scan perspective, nmap can assist in assessing the SANS/FBI Top Twenty vulnerabilities presented in an organization's infrastructure. Even though this method is not as accurate as some other specifically designed tools, especially for Windows systems, it does provide a main direction for the further vulnerability assessment in an identified high-risk environment. Furthermore,

** The specified ports depend on which packet filtering functionality to be tested.

nmap offers easy-process raw data, as well as possibility to catch new coming vulnerability.

Acknowledgement

I would like to take the opportunity to thank Alexander Lopyrev for his help and contribution in nmap data gathering and post-scan analysis. Special thanks go to Yuxiao Zhao for his great comments on this paper.

References

[1] Redsiren. “RedSiren Security Vulnerability Assessment.” URL: http://www.atomictangerine.com/pdf/Consulting/ProfessionalServices_IVACVA.pdf (August 30, 2002).

[2] Forristal, Jeff and Shipley, Greg. “Vulnerability Assessment Scanners.” Network Computing. January 8, 2001. URL: http://www.networkcomputing.com/1201/1201f1b1.html (August 30, 2002).

[3] Citadel Security Software, Inc. “Network Vulnerability Assessment and Remediation.” White Paper. URL: http://www.citadel.com/Downloads/whitepaperherculesfinal.pdf (August 30, 2002).

[4] Qualys, Inc. “Managed Vulnerability Assessment: A Proactive Approach to Network Security.” Technical White Paper. URL: http://www.qualys.com/whitepapers/wp_mva.pdf (August 30, 2002).

[5] SANS Institute. “Security Essentials.” SANS Online Training. URL: http://www.sans.org/onlinetraining/track1.php (August 31, 2002).

[6] Internet Security Systems. “Network and Host-Based Vulnerability Assessment.” White Paper. URL: http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nva.pdf (August 31, 2002).

[7] Talisker. “Vulnerability Scanners Overview.” URL: http://www.networkintrusion.co.uk/scanners.htm (August 31, 2002).

[8] Lopyrev, Alexander. “Distributed Scan Model for Enterprise-Wide Network Vulnerability Assessment.” November 27, 2001. URL: http://rr.sans.org/audit/scan_model.php (August 20, 2002).

[9] Nessus. August 26, 2002. URL: http://www.nessus.org (September 1, 2002).

[10] Advanced Research Corporation. “Security Auditor's Research Assistant.” August 15, 2002. URL: http://www-arc.com/sara (September 1, 2002).

[11] Rain Forest Puppy. “Whisker Information, Scripts, and Updates.” May 5, 2002. URL: http://www.wiretrip.net/rfp/p/doc.asp/i2/d21.htm (September 1, 2002).

[12] Insecure. “Introduction.” August 10, 2002. URL: http://www.insecure.org/nmap (August 31, 2002).

[13] Fyodor. “The Art of Port Scanning.” September 6, 1997. URL: http://www.insecure.org/nmap/nmap_doc.html (August 31, 2002).

[14] Talisker. “Network Vulnerability Scanners.” August 23, 2000. URL: http://www.networkintrusion.co.uk/N_scan.htm (August 31, 2002).

[15] Harnist, Eric. “Intelligent Vulnerability Scanner.” January 20, 2002. URL: http://www.giac.org/practical/Eric_Harnist_GSEC.doc (September 1, 2002).

[16] SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated).” Version 2.504. May 2, 2002. URL: http://www.sans.org/top20.htm (August 31, 2002).

[17] Insecure. “Nmap Network Security Scanner Man Page.” URL: http://www.insecure.org/nmap/nmap_manpage.html (September 2, 2002).

[18] FLNI (Front Liberateur National d'Internet). URL: http://www.flni.org/flni/english/down.htm (September 8, 2002).

[19] Lucas, Michael. “Understanding NFS.” February 14, 2002. URL: http://www.onlamp.com/pub/a/bsd/2002/02/14/Big_Scary_Daemons.html (September 3, 2002).

[20] Internet Security Systems. “Rpc.sadmind.” URL: http://www.iss.net/security_center/advice/Services/SunRPC/rpc.sadmind/default.htm (September 3, 2002).

[21] CERT Coordination Center. “CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).” August 28, 2002. URL: http://www.cert.org/advisories/CA-2002-03.html (September 5, 2002).

[22] SolarWinds.Net, Inc. “Network Management & Discovery Tools.” URL: http://solarwinds.net/Toolsets.htm (September 4, 2002).

Appendix 1

SANS common vulnerable ports [16] are listed as follows.

TCP ports:

1-20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 109, 110, 111, 119, 123, 135, 137, 138, 139, 143, 161, 162, 179, 389, 443, 445, 512, 513, 514, 515, 1080, 2049, 4045, 6000-6255, 8000, 8080, 8888

UDP ports:

1-20, 37, 53, 69, 111, 123, 135, 137, 138, 161, 162, 389, 445, 514, 2049, 4045

Appendix 2

The following lists of open ports are distributed with nmap.

TCP ports (1150):

1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 29, 31, 33, 35,
37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58,
59, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80,
81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101,
102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117,
118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133,
134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149,
150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165,
166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181,
182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197,
198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213,
214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 242, 243, 244, 245, 246, 247,
248, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 280, 281, 282, 308, 309,
310, 311, 312, 313, 314, 315, 316, 317, 321, 344, 345, 346, 347, 348, 349, 350,
351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366,
367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382,
383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398,
399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414,
415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430,
431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446,
447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462,
463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478,
479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494,
495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510,
511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526,
527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542,
543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558,
559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574,
575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590,
591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 606, 607, 608, 609, 610, 611,
628, 631, 634, 636, 660, 666, 637, 691, 704, 706, 709, 729, 730, 731, 740, 741,
742, 744, 747, 748, 749, 750, 751, 752, 753, 754, 758, 759, 760, 761, 762, 763,
764, 765, 767, 769, 770, 771, 772, 773, 774, 775, 776, 780, 781, 782, 783, 786,
799, 800, 801, 871, 873, 888, 989, 901, 950, 953, 975, 990, 992, 993, 994, 995,
996, 997, 998, 999, 1000, 1008, 1024, 1025, 1026, 1027, 1029, 1030, 1031,
1032, 1033, 1050, 1058, 1059, 1067, 1068, 1080, 1083, 1084, 1103, 1109, 1110,
1112, 1127, 1139, 1155, 1178, 1212, 1222, 1234, 1241, 1248, 1346, 1347, 1348,
1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361,
1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374,
1375, 1376, 1377, 1378, 1379, 1380, 1381, 1383, 1384, 1385, 1386, 1387, 1388,
1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401,
1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414,
1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427,
1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440,
1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453,
1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466,

1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1600, 1650, 1651, 1652, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1680, 1720, 1723, 1827, 1900, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032, 2033, 2034, 2035, 2038, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2064, 2053, 2065, 2067, 2105, 2106, 2108, 2111, 2112, 2120, 2201, 2232, 2241, 2301, 2307, 2401, 2430, 2431, 2432, 2433, 2500, 2501, 2564, 2600, 2601, 2602, 2603, 2604, 2605, 2627, 2638, 2766, 2784, 2998, 3000, 3001, 3005, 3006, 3049, 3052, 3064, 3086, 3128, 3141, 3264, 3268, 3269, 3306, 3333, 3372, 3389, 3421, 3455, 3456, 3457, 3462, 3900, 3984, 3985, 3986, 3999, 4000, 4008, 4045, 4132, 4133, 4144, 4321, 4333, 4343, 4444, 4480, 4500, 4557, 4559, 4672, 4987, 4998, 5000, 5001, 5002, 5010, 5011, 5050, 5145, 5190, 5191, 5192, 5193, 5232, 5236, 5300, 5301, 5302, 5303, 5304, 5305, 5308, 5400, 5405, 5432, 5510, 5520, 5530, 5540, 5550, 5555, 5631, 5632, 5680, 5713, 5714, 5715, 5716, 5717, 5800, 5801, 5802, 5803, 5900, 5901, 5902, 5903, 5977, 5978, 5979, 5997, 5998, 5999, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6008, 6009, 6050, 6101, 6103, 6105, 6106, 6110, 6111, 6112, 6141, 6142, 6143, 6144, 6145, 6146, 6147, 6148, 6346, 6547, 6548, 6502, 6558, 6588, 6666, 6667, 6668, 6969, 6699, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7007, 7008, 7009, 7010, 7070, 7100, 7200, 7201, 7326, 7597, 8007, 8009, 8080, 8081, 8082, 8888, 8892, 9090, 9100, 9111, 9152, 9535, 9876, 9991, 9992, 10000, 10005, 10082, 10083, 11371, 12000, 12345, 12346, 13701, 13702, 13705, 13706, 13708, 13709, 13710, 13711, 13712, 13713, 13714, 13715, 13716, 13717, 13718, 13720, 13721, 13722, 13782, 13783, 16959, 17007, 18000, 20005, 22273, 22289, 22305, 22321, 22370, 26208, 27374, 27665, 31337, 32770, 32771, 32772, 32773, 32774, 32775, 32776, 32777, 32778, 32779, 32780, 32786, 32787, 43188, 44442, 44443, 47557, 49400, 54320, 61439, 61440, 61441, 65301

UDP ports (997):

1, 2, 3, 5, 7, 9, 11, 13, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 29, 31, 33, 35, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199,

200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215,
216, 217, 218, 219, 220, 221, 222, 223, 242, 243, 244, 245, 246, 247, 248, 256,
257, 258, 259, 260, 261, 262, 263, 264, 280, 281, 282, 308, 309, 310, 311, 312,
313, 314, 315, 316, 317, 321, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353,
354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369,
370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385,
386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401,
402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417,
418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433,
434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449,
450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465,
466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481,
482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497,
498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513,
514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529,
530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545,
546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561,
562, 563, 564, 565, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578,
579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594,
595, 596, 597, 598, 599, 600, 606, 607, 608, 609, 610, 611, 634, 635, 640, 650,
660, 666, 637, 704, 709, 729, 730, 731, 737, 740, 741, 742, 744, 747, 748, 749,
750, 751, 752, 753, 758, 759, 760, 761, 762, 763, 764, 765, 767, 769, 770, 771,
772, 773, 774, 775, 776, 780, 781, 782, 783, 786, 800, 801, 888, 996, 997, 998,
999, 1000, 1008, 1012, 1025, 1028, 1030, 1031, 1032, 1058, 1059, 1067, 1068,
1080, 1083, 1084, 1110, 1155, 1167, 1212, 1222, 1248, 1346, 1347, 1348, 1349,
1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362,
1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375,
1376, 1377, 1378, 1379, 1380, 1381, 1383, 1384, 1385, 1386, 1387, 1388, 1389,
1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402,
1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415,
1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428,
1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441,
1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454,
1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467,
1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480,
1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493,
1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506,
1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519,
1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532,
1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545,
1546, 1547, 1548, 1549, 1550, 1551, 1552, 1600, 1645, 1646, 1650, 1651, 1652,
1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1701,
1812, 1813, 1900, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995,
1996, 1997, 1998, 1999, 2000, 2001, 2002, 2004, 2005, 2006, 2007, 2008, 2009,
2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022,
2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032, 2033, 2034, 2035, 2038, 2040,

2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2065, 2067, 2103, 2104, 2105, 2106, 2108, 2201, 2232, 2241, 2307, 2401, 2430, 2431, 2432, 2433, 2500, 2501, 2627, 2784, 3049, 3130, 3141, 3264, 3333, 3421, 3455, 3456, 3457, 3900, 3984, 3985, 3986, 3996, 3997, 3998, 4000, 4008, 4045, 4132, 4133, 4321, 4343, 4444, 4500, 4672, 5000, 5001, 5002, 5010, 5011, 5050, 5145, 5190, 5191, 5192, 5193, 5236, 5300, 5301, 5302, 5303, 5304, 5305, 5308, 5500, 5540, 5555, 5632, 5713, 5714, 5715, 5716, 5717, 6110, 6111, 6141, 6142, 6143, 6144, 6145, 6146, 6147, 6148, 6549, 6502, 6558, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7007, 7008, 7009, 7010, 7100, 7200, 7201, 7648, 7649, 7650, 7651, 9535, 9876, 10080, 17007, 17185, 18000, 22370, 26000, 26900, 27015, 27444, 27500, 27910, 27960, 28910, 31335, 31337, 32770, 32771, 32772, 32773, 32774, 32775, 32776, 32777, 32778, 32779, 32780, 32786, 32787, 39213, 45000, 47557, 54321