



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Virus infection: Sniffing the beast out

Alain Duminy

GIAC Security Essentials Certification Practical (GSEC)

April 2004

Practical Assignment Version 1.4b

© SANS Institute 2004, Author retains full rights.

Abstract

Year of the Virus, year of the worm... the terms are succeeding each other just to stress out one thing: the virus threat is now a daily challenge for all IT practitioners. A lot of security policies and protection systems are being put in place to handle the threat and decrease the risk of infection. But the chances remain for the infrastructure to be infected despite all these measures. The IT security practitioners and network managers should be ready to deal with the unknown and identify and track viruses that made it thru. This document describes how network sniffers and packet analyzers can be the weapon that will help you win the battle.

Introduction: the cost of connectivity.

If a few years ago, having to deploy a Local Area Network (LAN) in the enterprise was a serious endeavor that would involve the participation of specialized engineers and an expensive infrastructure investment, today, deploying a LAN is a much simpler task. All Personal Computers (PCs) come with an embedded network card fully configured, Windows server comes with the set of basic tools like DHCP server for IP address distribution and the cost of entry level switches and cabling have drastically dropped. Connecting this network to the Internet is not that difficult either with now a large offer of broadband Internet technologies available and affordable basic routers or "all in one" appliances.

With this incredible growth of LAN connected to the Internet, the amount of traffic over the Internet has drastically increased. An adverse effect of this growth is the increasing speed viruses propagate over the net. At the same time, with the information available right at hand, with more and easier virus building tools freely available for download over the net, with cheaper and wider access to computers and internet to the public, more and more "hacker-wanna-be's" can try their luck at building new viruses.

In short Virus fighting is now a daily priority issue for most corporate IT groups. With the increased number of attacks and their effect to business availability (mostly Denial of Service so far) in the past twelve to eighteen months, we have seen an increase in awareness of the issue and a global effort was done to protect the LANs from network infection.

It is safe to say that most large corporations have now taken the steps needed to protect their network from known viruses. LAN entry points (connection from the LAN to the Wide Area Network (WAN) or the Internet) are protected with in-line virus scanning, mail servers verify all incoming mails, filter out or quarantine some attachment types (like executable files, script files and some compressed/encrypted files that may contain viruses). Gateways (Simple Mail Transport Protocol (SMTP) gateways for example) are also protected with antivirus to avoid sending out infected mails. PCs, servers and other workstations are also individually protected from infection that may come thru removable storage media like diskettes, CDs, DVDs, smart drive and others.

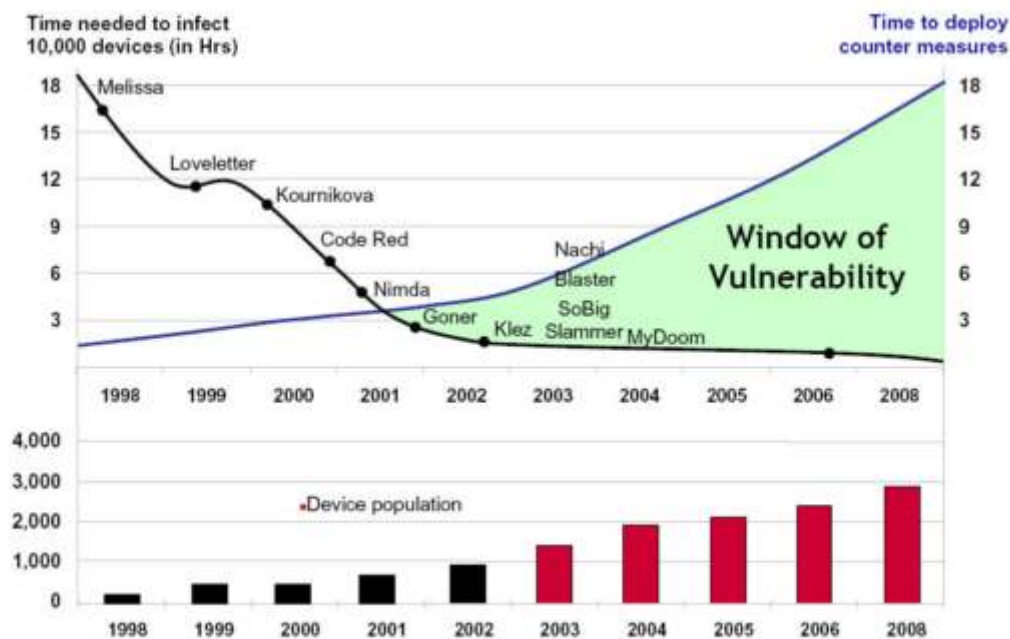
The next step taken by the large corporation was to ensure that the pattern files (files that described the way viruses look, also call the virus signature) of their

antivirus engines were up-to-date (that was definitely not the case before) to catch the latest variants of recently identified viruses.

We cannot win the race by just running.

With all this, one should feel safe against viruses. But a new paradigm rose. With smaller footprint (the footprint is the size of the virus), smarter ways of propagating and larger bandwidth available, viruses are now extremely fast to propagate. Time to deploy new security patches and updated virus patterns is also increasing due to the larger number of equipment attached to the LAN. At some point, viruses may already be attacking the network before the security systems are updated and ready. As shown in the graph below (kindly provided by the McAfee AVERT labs staff), the window of vulnerability of network is increasing exponentially.

The graph compares the time it takes for the latest viruses to infect 10,000 machines against the time it takes to deploy the equivalent counter measures. The time in between, highlighted in green, is the window of vulnerability during which the machines are not yet protected against the new threat. Anti-virus pattern is not yet available or fully deployed, security patching of vulnerabilities in operating systems and other applications is not yet tested and implemented, update of Intrusion Detection and Intrusion Prevention systems are not yet uploaded.



Source: McAfee AVERT Labs

Therefore, even with good security policy and careful implementation, the chances remain for the corporate LAN to be infected by a virus. The following part of the document describes the steps and tools to manually find, identify and isolate viruses that made it thru the security systems to the LAN.

First scenario: a misbehaving workstation.

Is one (or more) workstation having suspicious behavior or showing signs of having been compromised? The users report obvious changes in his desktop appearance, his browser behavior, or other suspicious signs. In that case, first thing to do is to go to that machine and verify that all the processes related to the anti-virus engine are loaded and running, check that the virus pattern file used is the latest one (confirm this thru checking the internet resources of the corresponding antivirus vendor if needed) and perform a full scan of the suspicious machine. Full scan means that you must include all file types, including compressed files, for all the local drives of the machine. Depending on the local security policies, the level of the suspicion and the business requirement, it might be good to already disconnect / isolate from the production LAN the target workstation. Verify that the operating system, the browser and other key application have been updated with the latest security patches and service packs. Most of the time, if the problem is virus related, the updated anti-virus would do the job, identify the virus and clean the machine. This was the easy way.

Second scenario: a misbehaving network.

It becomes more difficult when the signs of possible infections are not isolated on a single or a few workstations but when it comes as a more generic feeling like abnormal network traffic activity, sudden slow response time, new TCP or UDP port activity, sporadic non-unicast traffic increase, etc. You will note that to be able to spot these activities, once need to have a good knowledge of what the "normal" activity on the network is. It is good practice to keep records of network activity on a regular basis to build a reference, or base line, of what "normal" activity is. Depending on the IT infrastructure in place, basic information to start with are protocol distribution, bandwidth utilization of the main network links, CPU activity on switches and routers, main TCP and UDP ports used by legacy applications. A good practice is also to capture the traffic in the core of the LAN on a regular basis and go thru the packets to get used to read packet analyzer information and see what normal traffic in the LAN looks like. It will be easier to quickly spot suspicious traffic in the future. It is also important to keep on-hand an updated network configuration documentation to rapidly verify subnet ranges, default gateways and the like. Having a complete investigation "jump bag" is also good practice. The content of this jump bag would greatly depend on your IT infrastructure.

Lets walk thru a few real life examples.

Your users are complaining that the "network" is abnormally slow. Effectively, response time from the Internet or some internal application seems to be longer than usual. But after verifying, there has been no major infrastructure change nor known problem reported so far. Proceed then with a traffic capture using a sniffer in the core of the network (where most of the traffic pass-thru).

Setting-up a sniffer in your Network infrastructure in a nutshell

Packet sniffing is the action of capturing all or part of the network traffic on a particular link or network segment.

In a shared hub environment, all traffic within a subnet is broadcasted to all the ports of the hub (same broadcast domain). Therefore, any workstation in the network would receive 100% of the network traffic. The role of the network interface is to filter out from all this the traffic intended for that machine. But by setting the network card of this workstation to promiscuous mode, the whole traffic would be passed to the workstation. Then the use of a sniffer and packet analyzer software will help reorganize this traffic into network conversation. In a switch environment, only the traffic intended to the workstation(s) attached to a specific port will be forwarded to that port. Even in promiscuous mode, a machine would only see traffic intended for itself and broadcasts. In some high-end switches, it is possible to set up a span port and to replicate the traffic intended for many ports to this single port. A workstation attached to that port in promiscuous mode could then analyze the traffic with a sniffer software. Another solution is to install a physical tap on the network, best is on an uplink port of a switch, and analyze the traffic from the tap port with a sniffer and workstation in promiscuous mode. Different kinds of taps are available from Netoptics. See their web site for more information on taps:

<http://www.netoptics.com>

Note that using a network tap might be the best solution if your network is under heavy stress from a Denial of Service (DoS) attack. Under these circumstances, it might be impossible to access the switch and/or to setup a span port in that switch to sniff the traffic.

For the purpose of this document, all the packet capture and analysis were done using Sniffer Portable, a commercial solution from Network Associates. But there are a lot of other sniffer solutions on the market, with more or less additional features. Some are open source and free for download. See the box below for more information.

Incomplete IP addresses in some of the screenshots proposed are not mistakes from the software but post-editing of public addresses in order to keep the confidentiality of this document.

Sniffer software

There are a few sniffer softwares available. Here are the most commonly used:

Sniffer from Network Associates

Network Associates propose a whole suite of commercial sniffer products, from stand-alone in-line dedicated appliances to portable software solutions. Their offer can be found at

http://www.networkassociates.com/us/products/sniffer/mgmt_analysis/category.htm

All these are commercial products and there is no evaluation copy available.

TCPDump by the Network Research Group (NRG) of Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California
 TCPDump is a free packet sniffer software developed by the Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Berkeley. It works under Unix. Libpcap is the packet capture library that goes with it. The tools can be downloaded for free from <http://ee.lbl.gov/>

Ethereal

Ethereal is a packet sniffer analyzer available under windows and linux. It is open source software that can be downloaded from the Ethereal.com web site at the following URL: <http://www.ethereal.com/download.html>

SnoopAnalyzer Standard

Free packet sniffer and analyzer for Windows platforms. Can be downloaded at URL: http://www.snoopanalyzer.com/snoopanalyzer/standard_01.asp

After capturing the traffic in your core network (or any other area of the network where most of the traffic you want to observe is passing thru) for a few minutes, or until the buffer of your sniffer is full if the traffic is high, the first information to look at is the host table and the quantity of bytes in and out. Again, try to spot suspicious behavior.

Here is a screen shot taken from the host table after a capture in the core:

Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes
HTTP	28.81	2,102	2,039,372	4,131	1,390,443
Others		1,998	760,221	2,776	2,301,667
HTTP	28.82	1,385	1,087,610	2,356	366,734
Others		1,238	274,843	1,770	1,447,306
SNMP	172.23.4.14	539	109,368	540	101,473
Others		540	101,473	539	109,368
Others	7.104	661	858,300	351	33,932
HTTP	216.155.194.191	886	170,284	316	41,902
Others		142	9,088	282	401,380
Others	192.168.10.81	136	9,622	274	384,706
Others	172.23.241.31	410	478,317	232	51,356
HTTP	66.218.95.198	302	23,066	227	305,720
Others		200	171,700	205	172,366
HTTP	202.239.172.90	194	44,658	195	258,343
Others		200	47,114	190	245,616
Others	192.168.10.83	86	6,128	182	258,610
HTTP	147.208.133.111	672	817,314	143	9,230
Others		261	239,406	142	12,640
HTTP	172.23.181.20	146	9,344	141	83,586
Others		68	4,402	140	207,256
DNS	28.68	123	9,404	119	21,499
Others		110	52,528	108	6,912
Others	172.23.243.106	162	134,313	106	26,954
HTTPS	28.81	55	29,214	104	16,126
TCP135	172.23.9.6	0	0	100	6,600
Others		108	9,854	96	129,106
HTTP	63.240.53.161	236	36,104	85	32,391
Others		152	22,458	84	60,963
Others	172.23.168.130	123	148,960	83	11,794
SMTP	7.106	69	5,783	83	84,018
HTTP	64.235.234.14	120	13,074	78	90,426
Others		129	164,090	76	6,349
Others	172.23.10.85	120	141,574	76	5,860
HTTP	64.66.6.200	170	22,870	74	51,510
Others		92	13,948	71	101,457
DNS	172.23.237.90	68	7,626	71	4,860
Others		35	2,364	69	94,556
HTTP	203.177.3.42	90	5,784	69	79,204

The host and protocol table shows a node with outbound packets, but no inbound at all, on TCP port 135. This should immediately attract attention. Filtering out from the capture the conversations from this host on that TCP port might be interesting. Here is the result of the filter:

The screenshot shows a Wireshark packet capture with a list of 100 packets. All packets are SYN packets from source IP 172.23.9.6 to various destination IPs in the 172.24.23.0/24 subnet. The filter bar at the bottom shows the applied filter: `TCP D=172.24.23.0/24 && D=172.23.9.6 && D=172.23.9.6`. The packet list shows the following columns: No., Time, Source Address, Destination Address, Length, Protocol, and Info. The packets are all SYN packets with a length of 62 bytes.

No.	Time	Source Address	Destination Address	Length	Protocol	Info
17636	172.23.9.6	172.24.23.233	TCP	62	0.00.00.000	0.000.000
18271	172.23.9.6	172.24.23.234	TCP	62	0.00.00.002	0.002.740
18388	172.23.9.6	172.24.23.235	TCP	62	0.00.00.001	0.000.829
18302	172.23.9.6	172.24.23.236	TCP	62	0.00.00.004	0.002.732
18317	172.23.9.6	172.24.23.237	TCP	62	0.00.00.007	0.002.931
18339	172.23.9.6	172.24.23.238	TCP	62	0.00.00.010	0.002.910
18353	172.23.9.6	172.24.23.239	TCP	62	0.00.00.013	0.002.901
18392	172.23.9.6	172.24.23.240	TCP	62	0.00.00.016	0.002.938
18414	172.23.9.6	172.24.23.241	TCP	62	0.00.00.019	0.002.937
18444	172.23.9.6	172.24.23.242	TCP	62	0.00.00.022	0.002.936
18458	172.23.9.6	172.24.23.243	TCP	62	0.00.00.025	0.002.934
18475	172.23.9.6	172.24.23.244	TCP	62	0.00.00.028	0.002.936
18508	172.23.9.6	172.24.23.245	TCP	62	0.00.00.031	0.002.937
18539	172.23.9.6	172.24.23.246	TCP	62	0.00.00.034	0.002.936
18555	172.23.9.6	172.24.23.247	TCP	62	0.00.00.037	0.002.939
18586	172.23.9.6	172.24.23.248	TCP	62	0.00.00.040	0.002.925
18608	172.23.9.6	172.24.23.249	TCP	62	0.00.00.043	0.002.925
18604	172.23.9.6	172.24.23.250	TCP	62	0.00.00.046	0.002.924
18622	172.23.9.6	172.24.23.251	TCP	62	0.00.00.049	0.002.967
19063	172.23.9.6	172.24.23.252	TCP	62	0.00.00.052	0.002.967
19079	172.23.9.6	172.24.23.253	TCP	62	0.00.00.055	0.002.967
19096	172.23.9.6	172.24.23.254	TCP	62	0.00.00.058	0.002.967
19113	172.23.9.6	172.24.23.255	TCP	62	0.00.00.061	0.002.967
19122	172.23.9.6	172.24.23.256	TCP	62	0.00.00.064	0.002.967
19134	172.23.9.6	172.24.23.257	TCP	62	0.00.00.067	0.002.967
19173	172.23.9.6	172.24.23.258	TCP	62	0.00.00.070	0.002.967
19202	172.23.9.6	172.24.23.259	TCP	62	0.00.00.073	0.002.967
19212	172.23.9.6	172.24.23.260	TCP	62	0.00.00.076	0.002.967
19229	172.23.9.6	172.24.23.261	TCP	62	0.00.00.079	0.002.967
19263	172.23.9.6	172.24.23.262	TCP	62	0.00.00.082	0.002.967
19268	172.23.9.6	172.24.23.263	TCP	62	0.00.00.085	0.002.967
19274	172.23.9.6	172.24.23.264	TCP	62	0.00.00.088	0.002.967
19286	172.23.9.6	172.24.23.265	TCP	62	0.00.00.091	0.002.967
19295	172.23.9.6	172.24.23.266	TCP	62	0.00.00.094	0.002.967
19357	172.23.9.6	172.24.23.267	TCP	62	0.00.00.097	0.002.967
19478	172.23.9.6	172.24.23.268	TCP	62	0.00.00.100	0.002.967
19529	172.23.9.6	172.24.23.269	TCP	62	0.00.00.103	0.002.967
19573	172.23.9.6	172.24.23.270	TCP	62	0.00.00.106	0.002.967
19574	172.23.9.6	172.24.23.271	TCP	62	0.00.00.109	0.002.967
19595	172.23.9.6	172.24.23.272	TCP	62	0.00.00.112	0.002.967
19607	172.23.9.6	172.24.23.273	TCP	62	0.00.00.115	0.002.967
19625	172.23.9.6	172.24.23.274	TCP	62	0.00.00.118	0.002.967

Very interesting information can be seen from this screenshot. First thing to notice is the destination address. The host 172.23.9.6 is sending packets to every machine in a subnet, trying every single IP address in a very systematic way. They are all the same SYN packet of 62 bytes. Obviously this host is trying to initiate a connection on that TCP port testing one by one each IP address within a range of addresses. It might be a virus trying propagating itself. But as usual, the first thing to do is: do not panic! It could also be a game trying to find a partner player on the network or another application scanning the network for a server to connect to (like an Instant Messenger software for example). If your network documentation is up-to-date, you might be able to identify this machine on the network and check the running processes and perform an on-demand complete virus scanning. Under Windows, the command “netstat -ao” will list the open ports on that machine and their status, as well as the process ID associated to it.

Following is another example. The protocol distribution report showed a higher than usual ICMP traffic. The difference was large enough to raise the suspicion of the network administrator who required a capture of the traffic in the core network to verify the nature of this unusual ICMP activity. Below is a screenshot of the host table provided by the packet analyzer after capture:

Protocol	Address	In-Packets	In-Bytes	Out-Packets	Out-Bytes
ICMP	172.23.223.131	0	0	1,296	142,960
ICMP	172.23.209.199	0	0	1,298	141,680
HTTP	28.81	692	615,595	954	117,964
ICMP	172.23.205.47	0	0	1,272	139,920
ICMP	172.23.173.163	0	0	1,271	139,810
Others	7.104	544	62,768	963	1,156,812
ICMP	172.23.179.125	3	330	1,281	140,910
ICMP	172.23.159.27	0	0	822	90,420
ICMP	172.23.195.1	0	0	790	85,800
ICMP	172.23.4.75	0	0	831	91,410
ICMP	172.23.195.83	0	0	823	90,530
ICMP	172.23.223.22	0	0	583	64,130
ICMP	172.23.187.98	0	0	824	90,640
ICMP	172.23.145.252	0	0	822	90,420
ICMP	172.23.213.165	0	0	772	84,920
HTTP	28.62	263	227,248	611	70,826
Others	192.168.22.3	85	29,612	137	161,224
Others	172.23.8.5	39	25,578	27	3,734
HTTP	207.45.104.20	4	260	5	568
Others	28.81	786	127,955	948	732,617
DNS	28.68	101	8,756	162	26,241
Others	172.23.8.70	759	572,898	381	24,384
Others	172.23.8.13	273	356,562	158	33,480
DNS	172.23.4.98	2	491	2	170
DNS	172.23.8.100	6	1,405	9	779
DNS	172.23.179.160	2	469	2	120
Others	7.19	56	3,584	86	66,320
Others	172.23.187.22	0	0	1	64
Others	172.23.167.133	0	0	1	66
Others	172.23.207.152	57	29,744	36	7,414
Others	172.23.191.96	0	0	1	64

A few hosts can be identified sending ICMP packets but not receiving any. Drilling down to a single host ICMP conversation to analyze the details of this traffic, the report obtained from the packet sniffer analyzer looks like this:

The screenshot displays a network traffic capture with columns for No., Time, Source Address, Destination Address, Protocol, Length, and Info. The list shows numerous ICMP Echo requests. Below the list, a packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, and ICMP Echo. The raw packet data at the bottom shows a series of 'a' characters in the payload field.

Here again we can notice that the host machine is doing a systematic sweeping of a network range using ICMP echo. The ICMP packet is always the same 106 bytes long. At the bottom of the screen shot, the payload of the ICMP packets shows a succession of “a”. This is not the standard ICMP echo and this should raise your attention. In that particular case, later on, the scanning of the machine reported the presence of a version of Nachi virus. Indeed, a particular variant of Nachi is performing ping sweeping with a specially crafted ICMP Echo packet containing a padding of “a”. As the first capture shown that many machines were already infected and that the anti-virus pattern was not yet fully pushed to all the workstation (it came as a very heavy update as the anti-virus engine itself also needed to be replaced), we rapidly developed a sniffer filter to identify and capture only ICMP traffic that would show this particular payload. By moving the sniffer around the key areas of the network, we were able to prioritize the updating and cleaning of the infected machines and beat the virus to the finish. Note that Network Associates provides some specific filters dedicated to identify and report presence of the most popular virus and worms across the networks. These filters are available for download for free at the following URL:
http://www.networkassociates.com/us/security/resources/sv_home.htm#FILTERS

This last example is another capture done on the network after feedbacks were raised from users that the Internet access of the corporation was not as fast as it used to be. The packet sniffing was done on the segment just before the Internet router. Here is an interesting screenshot:

Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes
HTTP	28.81	2,234	1,832,36	3,990	617,826
	1.974	1,974	1,493,36	3,237	439,867
	28.82	1,533	291,635	2,243	1,957,773
	28.81	1,804	355,199	2,531	2,138,484
Others	7.104	1,130	1,284,24	644	83,422
	192.168.10.63	186	13,564	389	568,328
	192.168.10.81	158	13,024	370	511,816
	202.73.160.38	906	59,212	877	510,698
HTTP	216.195.194.191	1,345	271,060	460	63,268
	209.25.224.152	109	6,976	222	315,980
Others	172.23.163.146	119	19,019	165	10,878
HTTP	172.23.8.75	0	0	128	8,448
Others	192.168.10.83	109	12,986	154	137,004
	172.23.149.13	73	65,305	60	19,563
	216.109.119.227	72	4,609	67	100,242
HTTP	172.23.81.15	0	0	121	7,986
TCP445	172.23.12.130	0	0	140	9,240
Others	172.23.8.5	35	24,744	39	16,760
	172.23.163.36	80	101,401	44	4,787
HTTP	12.109.245.20	34	4,420	39	43,262
Others	192.168.24.2	189	13,506	132	22,343
	172.23.8.148	78	16,077	83	17,702
HTTP	172.23.16.17	0	0	48	3,168
	216.145.28.218	76	10,672	33	6,101
Others	172.23.8.70	135	54,962	135	8,640
	7.106	106	10,968	133	79,896
SMTP	172.23.8.106	252	212,944	180	17,051
Others	172.23.199.152	222	315,990	109	6,976
	7.104	62	8,128	36	38,291
HTTP	69.13.181.249	42	2,688	30	44,086
Others	172.23.195.228	54	40,918	41	11,674

Again we can notice some hosts having outgoing traffic without getting any reply (no inbound traffic). This is seen on both HTTP (TCP port 80) and TCP port 445. Drilling down the conversations from these hosts for these protocols, here is what the traffic analyzer is reporting for HTTP traffic (TCP port 80):

© SANS Institute

No.	Type	Source Address	Dest Address	Summary	Len	Rel. Time	Init. Time	Ack. Time
43	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
285	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1029	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1041	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1042	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1279	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1280	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1281	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1282	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1283	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1284	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1285	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1571	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1572	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1573	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1574	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1575	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1576	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1814	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1815	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1816	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1817	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
1818	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2045	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2046	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2087	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2088	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2229	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2230	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2454	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2457	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2458	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2459	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2737	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2738	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
2922	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3212	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3213	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3475	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3476	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3477	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3885	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3886	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
3887	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000
4193	TCP	172.23.8.75	172.23.8.75	172.23.8.75 → 172.23.8.75 [RST] Seq=172.23.8.75 Win=0 Len=0	62	0.00:00.000	0.00:00.000	0.00:00.000

This same host is apparently trying to initiate connection with a lot of different public IP addresses over port 80, so most probably those are public web sites. By itself it would not be too odd. But if you look at the timing information on the right hand of the screen shot, you will notice that in less than a second, there were 36 different tentative web site connections initiated by this host. This is now definitely suspicious.

Looking at the traffic generated on TCP port 445 from the other host, here is what can be seen:

No.	Source Address	Dest Address	Summary	Seq	Win	Len	Time
437	172.23.32.130	192.168.1.100	TCP	2111	0	0	0.000000
438	172.23.32.130	192.168.1.100	TCP	2112	0	0	0.000000
439	172.23.32.130	192.168.1.100	TCP	2113	0	0	0.000000
440	172.23.32.130	192.168.1.100	TCP	2114	0	0	0.000000
441	172.23.32.130	192.168.1.100	TCP	2115	0	0	0.000000
442	172.23.32.130	192.168.1.100	TCP	2116	0	0	0.000000
443	172.23.32.130	192.168.1.100	TCP	2117	0	0	0.000000
444	172.23.32.130	192.168.1.100	TCP	2118	0	0	0.000000
445	172.23.32.130	192.168.1.100	TCP	2119	0	0	0.000000
446	172.23.32.130	192.168.1.100	TCP	2120	0	0	0.000000
447	172.23.32.130	192.168.1.100	TCP	2121	0	0	0.000000
448	172.23.32.130	192.168.1.100	TCP	2122	0	0	0.000000
449	172.23.32.130	192.168.1.100	TCP	2123	0	0	0.000000
450	172.23.32.130	192.168.1.100	TCP	2124	0	0	0.000000
451	172.23.32.130	192.168.1.100	TCP	2125	0	0	0.000000
452	172.23.32.130	192.168.1.100	TCP	2126	0	0	0.000000
453	172.23.32.130	192.168.1.100	TCP	2127	0	0	0.000000
454	172.23.32.130	192.168.1.100	TCP	2128	0	0	0.000000
455	172.23.32.130	192.168.1.100	TCP	2129	0	0	0.000000
456	172.23.32.130	192.168.1.100	TCP	2130	0	0	0.000000
457	172.23.32.130	192.168.1.100	TCP	2131	0	0	0.000000
458	172.23.32.130	192.168.1.100	TCP	2132	0	0	0.000000
459	172.23.32.130	192.168.1.100	TCP	2133	0	0	0.000000
460	172.23.32.130	192.168.1.100	TCP	2134	0	0	0.000000
461	172.23.32.130	192.168.1.100	TCP	2135	0	0	0.000000
462	172.23.32.130	192.168.1.100	TCP	2136	0	0	0.000000
463	172.23.32.130	192.168.1.100	TCP	2137	0	0	0.000000
464	172.23.32.130	192.168.1.100	TCP	2138	0	0	0.000000
465	172.23.32.130	192.168.1.100	TCP	2139	0	0	0.000000
466	172.23.32.130	192.168.1.100	TCP	2140	0	0	0.000000
467	172.23.32.130	192.168.1.100	TCP	2141	0	0	0.000000
468	172.23.32.130	192.168.1.100	TCP	2142	0	0	0.000000
469	172.23.32.130	192.168.1.100	TCP	2143	0	0	0.000000
470	172.23.32.130	192.168.1.100	TCP	2144	0	0	0.000000
471	172.23.32.130	192.168.1.100	TCP	2145	0	0	0.000000
472	172.23.32.130	192.168.1.100	TCP	2146	0	0	0.000000
473	172.23.32.130	192.168.1.100	TCP	2147	0	0	0.000000
474	172.23.32.130	192.168.1.100	TCP	2148	0	0	0.000000
475	172.23.32.130	192.168.1.100	TCP	2149	0	0	0.000000
476	172.23.32.130	192.168.1.100	TCP	2150	0	0	0.000000
477	172.23.32.130	192.168.1.100	TCP	2151	0	0	0.000000
478	172.23.32.130	192.168.1.100	TCP	2152	0	0	0.000000
479	172.23.32.130	192.168.1.100	TCP	2153	0	0	0.000000
480	172.23.32.130	192.168.1.100	TCP	2154	0	0	0.000000
481	172.23.32.130	192.168.1.100	TCP	2155	0	0	0.000000
482	172.23.32.130	192.168.1.100	TCP	2156	0	0	0.000000
483	172.23.32.130	192.168.1.100	TCP	2157	0	0	0.000000
484	172.23.32.130	192.168.1.100	TCP	2158	0	0	0.000000
485	172.23.32.130	192.168.1.100	TCP	2159	0	0	0.000000
486	172.23.32.130	192.168.1.100	TCP	2160	0	0	0.000000
487	172.23.32.130	192.168.1.100	TCP	2161	0	0	0.000000
488	172.23.32.130	192.168.1.100	TCP	2162	0	0	0.000000
489	172.23.32.130	192.168.1.100	TCP	2163	0	0	0.000000
490	172.23.32.130	192.168.1.100	TCP	2164	0	0	0.000000
491	172.23.32.130	192.168.1.100	TCP	2165	0	0	0.000000
492	172.23.32.130	192.168.1.100	TCP	2166	0	0	0.000000
493	172.23.32.130	192.168.1.100	TCP	2167	0	0	0.000000
494	172.23.32.130	192.168.1.100	TCP	2168	0	0	0.000000
495	172.23.32.130	192.168.1.100	TCP	2169	0	0	0.000000
496	172.23.32.130	192.168.1.100	TCP	2170	0	0	0.000000
497	172.23.32.130	192.168.1.100	TCP	2171	0	0	0.000000
498	172.23.32.130	192.168.1.100	TCP	2172	0	0	0.000000
499	172.23.32.130	192.168.1.100	TCP	2173	0	0	0.000000
500	172.23.32.130	192.168.1.100	TCP	2174	0	0	0.000000

The same pattern can be noticed. In less than a second, the same host targets a large number of public IP addresses on TCP port 445. As this behavior seems to be seen originating from many hosts on the network, the efficiency of the Internet access infrastructure of the company is degrading under the beginning of DoS attack. It might be necessary to temporarily block TCP port 445 at the core level or to remotely disconnect the traffic generating machines before the whole Internet infrastructure collapse under the attack. Then do a manual virus cleaning and patching of the obviously infected hosts. Blocking TCP port 445 can be done by temporarily implementing inbound Access Control List on the core routers of the network infrastructure denying traffic for this port. Of course it is important to check first if any legitimate application are using this same TCP port. Hence, again the importance of keeping good documentation.

Another trail to find potentially infected machines is to sniff for ARP traffic and identify hosts that are initiating a lot of ARP requests in a very short period of time. Monitoring TCP and UDP port usage over the network is also good practice. The US Computer Emergency Team (US-CERT) publishes a list of most common ports used by viruses that can be found at the following URL: http://www.us-cert.gov/current/services_ports.html

If you are curious to know the application TCP and UDP port numbers for registered applications and assigned by the Internet Assigned Numbers Authority (IANA), you can check it at the following URL:

<http://www.iana.org/assignments/port-numbers>

Always be prepared:

When a possibly infected machine has been identified, and the local virus scanning has effectively reported the presence of a particular virus, it is good practice to go to the web site of the major anti-virus publishers or other security focused web sites and look for a description of the virus mechanism. It will help you build your knowledge of commonly used techniques by virus to propagate themselves or perform DoS attack for example. It will then be easier for you in the future to efficiently use your sniffer and packet analyzer to rapidly spot suspicious traffic.

Here are a few of these web sites:

Mc Afee AVERT labs at URL:

<http://www.networkassociates.com/us/security/home.asp>

The Symantec Security Response web site at URL:

<http://securityresponse.symantec.com/>

The Trend Micro Security Information web site at URL:

<http://www.trendmicro.com/vinfo/>

Computer Associates Virus Information Center at URL:

<http://www3.ca.com/threatinfo/virusinfo/>

Conclusion: the next step might be the trusted connection

It is more and more difficult for corporation to insure that all machines are fully virus protected on the network. What about mobile users that came from a long trip in developing countries where Internet access is scarce and exchange of documents is still done thru diskettes? These users were not able to update their anti virus pattern files for some time and may have been infected by a new virus. What about the contractors, the consultants and other partners that visited and needed to attach their laptops to your network? Do you have any control over the security measures they implement for their workstations? What about the young kid of your colleague that came over the weekend to see how fast Internet is at Dad's office and brought with him his school laptop? Vendors have acknowledged this risk and are now offering a way to control this. Called the "trusted connection" by Cisco, this is an effort from Cisco, Nortel and other network gear manufacturers and some large anti virus company to provide an end-to-end infrastructure that would validate a workstation against the company security policies before granting access to the network. In short, whenever a workstation is started or connected to the enterprise network, a client agent running on the workstation as a part of the anti virus package, will communicate first thru a dedicated protocol with a policy server. This server lists what should be present on this workstation for it to be trusted on the network. For example, a certain antivirus process should be running, with the latest pattern file available, a

VPN client software should be up and running, a certain OS should be installed with the latest vulnerability updates present, etc. If any of the condition were not met, the policy server would request the switch or router to isolate this workstation on a quarantine network thru ACL. This quarantine network is where the antivirus pattern and OS update servers are available. Until such time the workstation agent has not confirmed with the policy server that the workstation has been properly updated, the router would keep the machine off the corporate network. Visitor machines that cannot be identified by the policy server would the same way be kept on a guest-dedicated network where only limited resources would be available.

© SANS Institute 2004, Author retains full rights

List of references

Generic resources for Virus information:

Mc Afee AVERT labs; URL:

<http://www.networkassociates.com/us/security/home.asp>

The Symantec Security Response web site; URL:

<http://securityresponse.symantec.com/>

The Trend Micro Security Information web site; URL:

<http://www.trendmicro.com/vinfo/>

Computer Associates Virus Information Center; URL:

<http://www3.ca.com/threatinfo/virusinfo/>

The US Computer Emergency Team (US-CERT); ports used by viruses:

http://www.us-cert.gov/current/services_ports.html

Manufacturers and software publishers:

Netoptics, manufacturer of network taps; URL: <http://www.netoptics.com>

McAfee Network Associates Sniffer products; URL:

http://www.networkassociates.com/us/products/sniffer/mgmt_analysis/category.htm

Filters for Network Associates Sniffer, free download; URL:

http://www.networkassociates.com/us/security/resources/sv_home.htm - FILTERS

TCPDump and Libpcap from The Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California, URL: <http://ee.lbl.gov/>

Ethereal, packet sniffer analyzer, URL: <http://www.ethereal.com/download.html>

SnoopAnalyser Standard, URL:

http://www.snoopanalyzer.com/snoopanalyzer/standard_01.asp