Global Information Assurance Certification Paper

Virus infection:
Sniffing the beast out

Alain Duminy

GIAC Security Essentials Certification Practical (GSEC)
April 2004
Practical Assignment Version 1.4b

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.

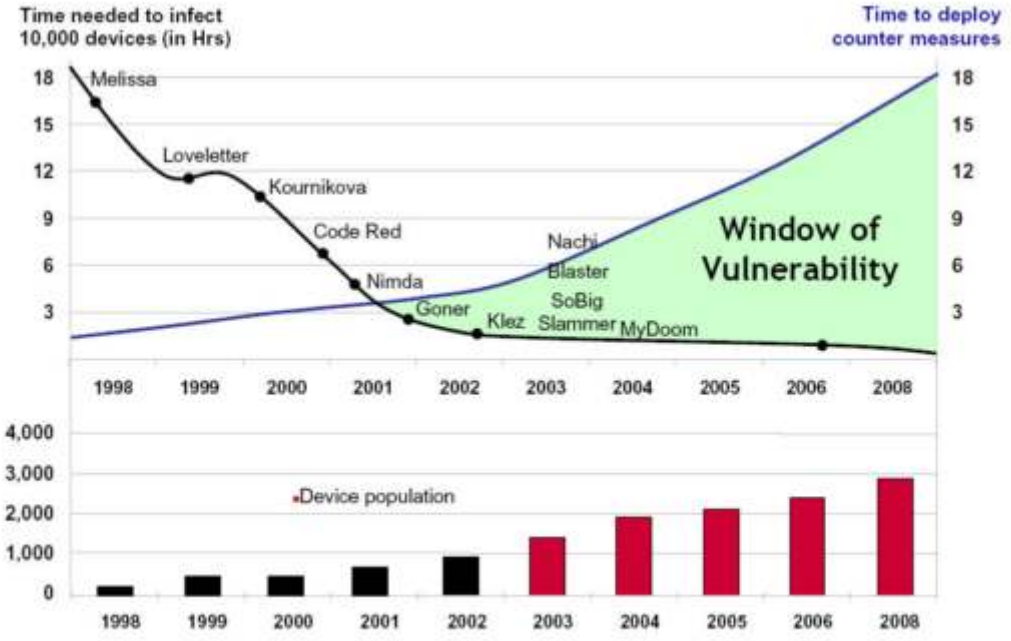
Introduction: the cost of connectivity.
If a few years ago, having to deploy a Local Area Network (LAN) in the enterprise was a serious endeavor that would involve the participation of specialized engineers and an expensive infrastructure investment, today, deploying a LAN is a much simpler task. All 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, once 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 compare 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

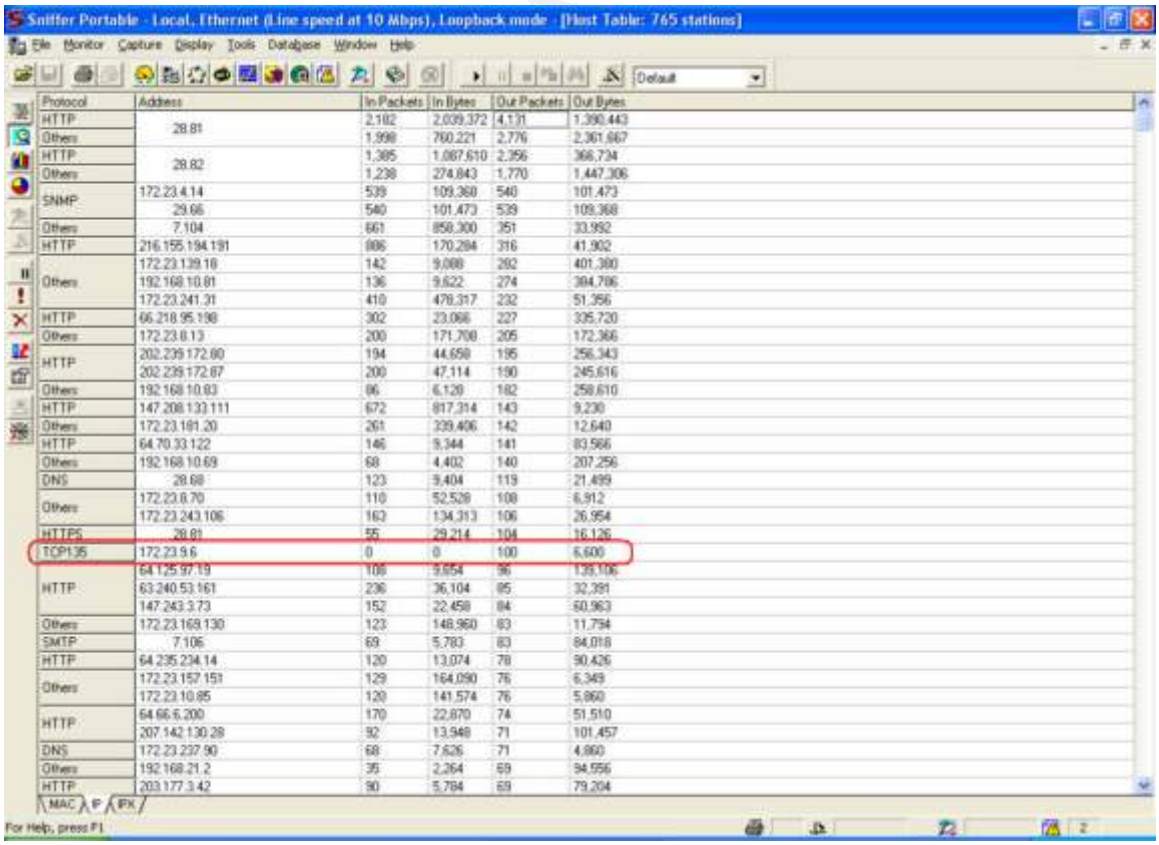
All these are commercial products and there is no evaluation copy available.

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/

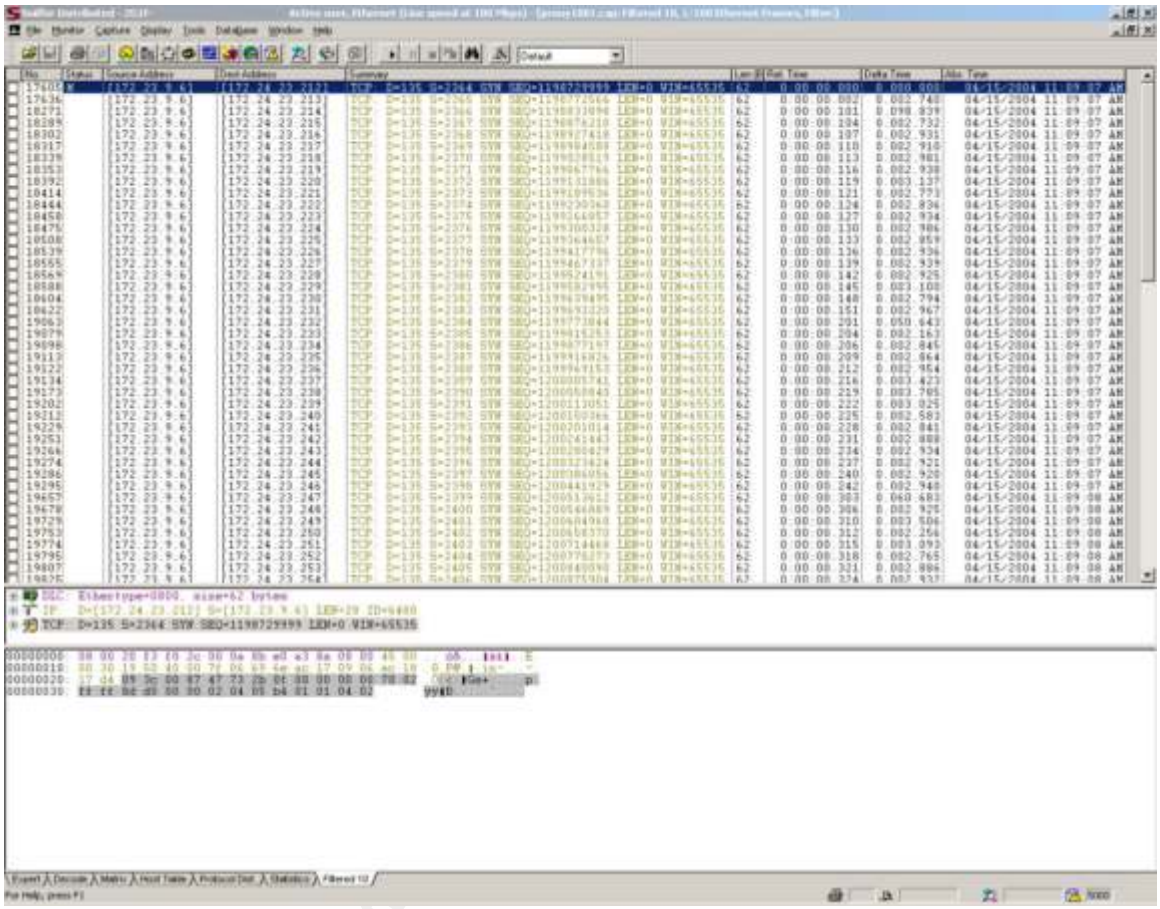
Ethereal
Ethereal is a packet sniffer analyzer available under windows and linux. It is open source software that can be downloaded from the Ethereal.com web site at the following URL: http://www.ethereal.com/download.html

SnoopAnalyser 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:

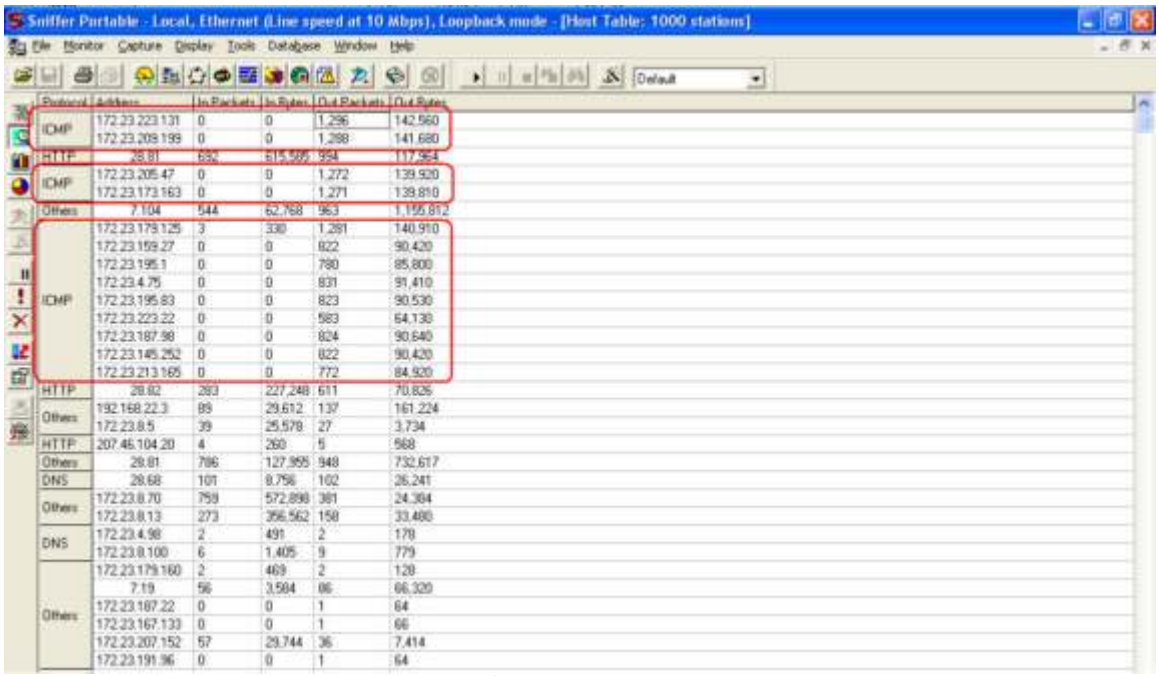


The host and protocol table shows a node with outbound packets, but no inbound at all, on TCP port 135. This should immediately attract attention. Filtering out from the capture the conversations from this host on that TCP port might be interesting. Here is the result of the filter:



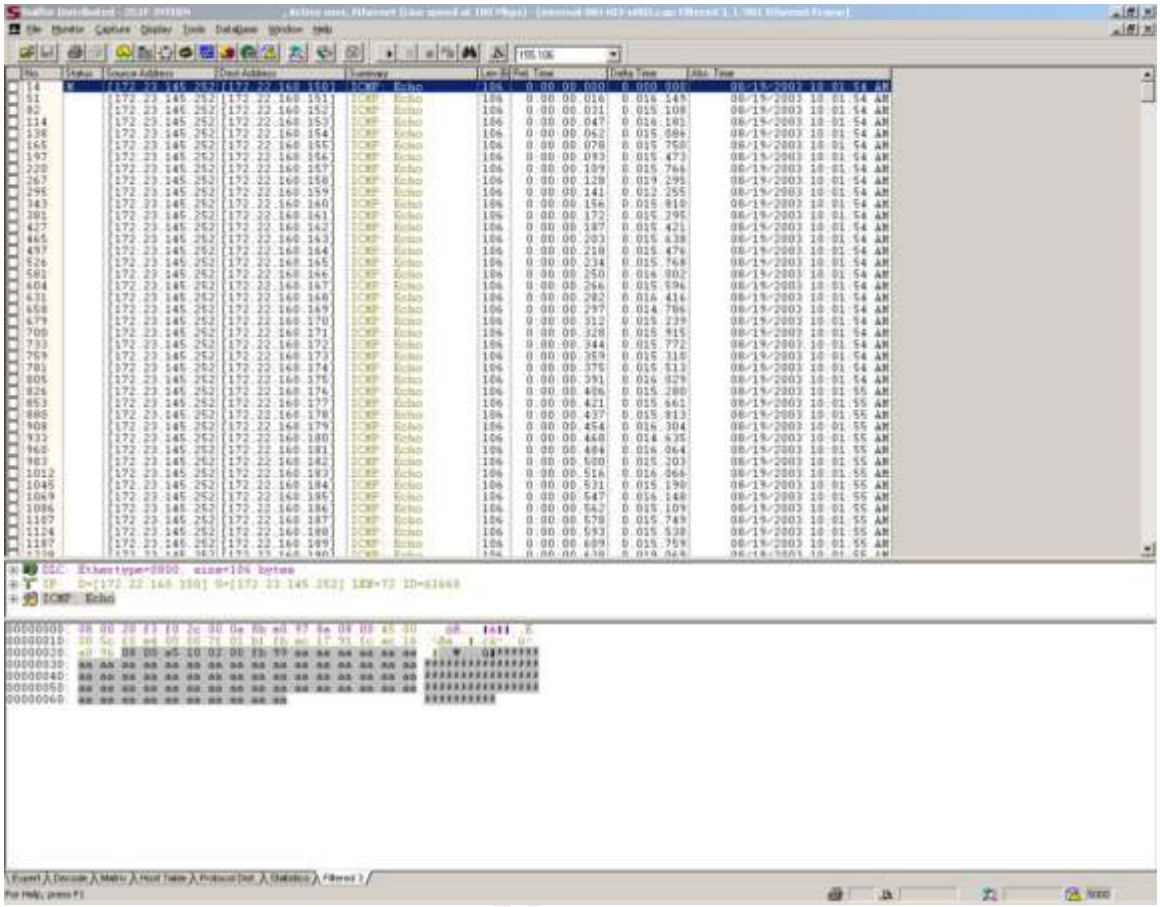
Very interesting information can be seen from this screenshot. First thing to notice is the destination address. The host 172.23.9.6 is sending packets to every machine in a subnet, trying every single IP address in a very systematic way. They are all the same SYN packet of 62 bytes. Obviously this host 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:



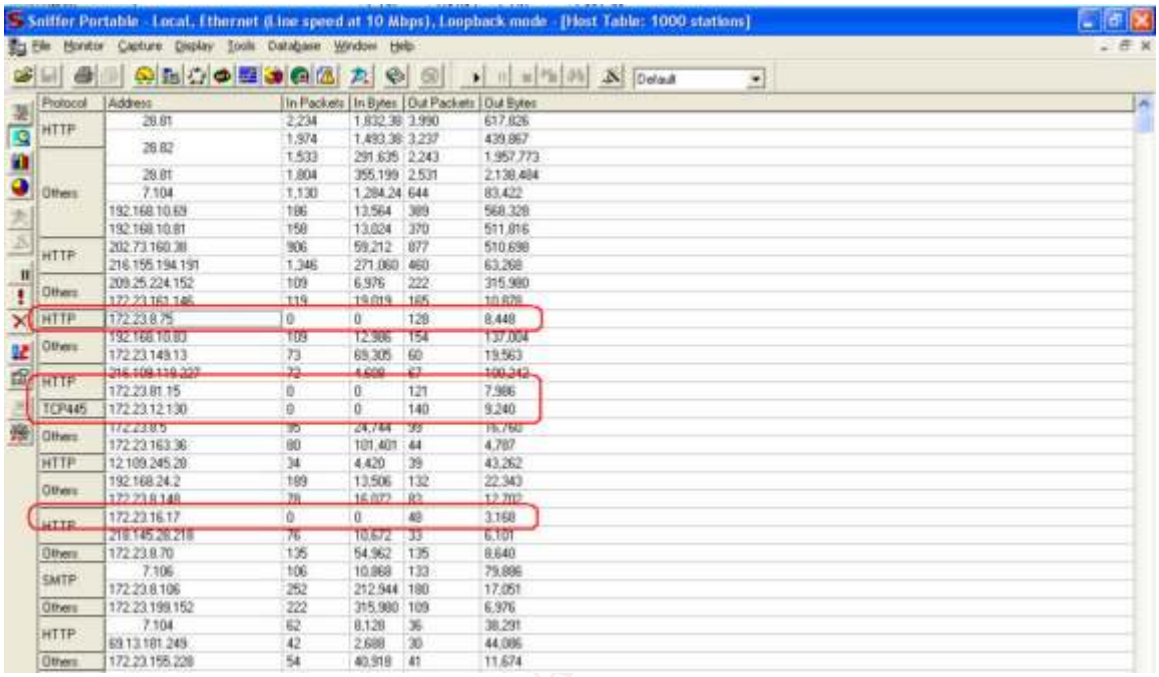
Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes
ICMP	172.23.223.131	0	0	1,296	142,560
	172.23.209.199	0	0	1,288	141,680
HTTP	28.81	692	615,585	954	117,964
ICMP	172.23.205.47	0	0	1,272	139,920
	172.23.173.163	0	0	1,271	139,810
Others	7.104	544	62,768	963	1,155,812
ICMP	172.23.179.125	3	330	1,281	140,910
	172.23.159.27	0	0	822	90,420
	172.23.195.1	0	0	780	85,800
	172.23.4.75	0	0	831	91,410
	172.23.195.83	0	0	823	90,530
	172.23.223.22	0	0	583	64,130
	172.23.187.98	0	0	824	90,640
	172.23.145.252	0	0	822	90,420
	172.23.213.165	0	0	772	84,920
HTTP	28.82	283	227,248	611	70,826
Others	192.168.22.3	89	29,612	137	161,224
	172.23.8.5	39	25,578	27	3,734
HTTP	207.46.104.20	4	260	5	568
Others	28.81	786	127,955	948	732,617
DNS	28.68	101	8,756	102	26,241
Others	172.23.8.70	759	572,898	381	24,384
	172.23.8.13	273	356,562	158	33,460
DNS	172.23.4.98	2	491	2	178
	172.23.8.100	6	1,405	9	779
Others	172.23.179.160	2	469	2	128
	7.19	56	3,584	86	66,320
	172.23.167.22	0	0	1	64
	172.23.167.133	0	0	1	66
	172.23.207.152	57	29,744	36	7,414
	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:

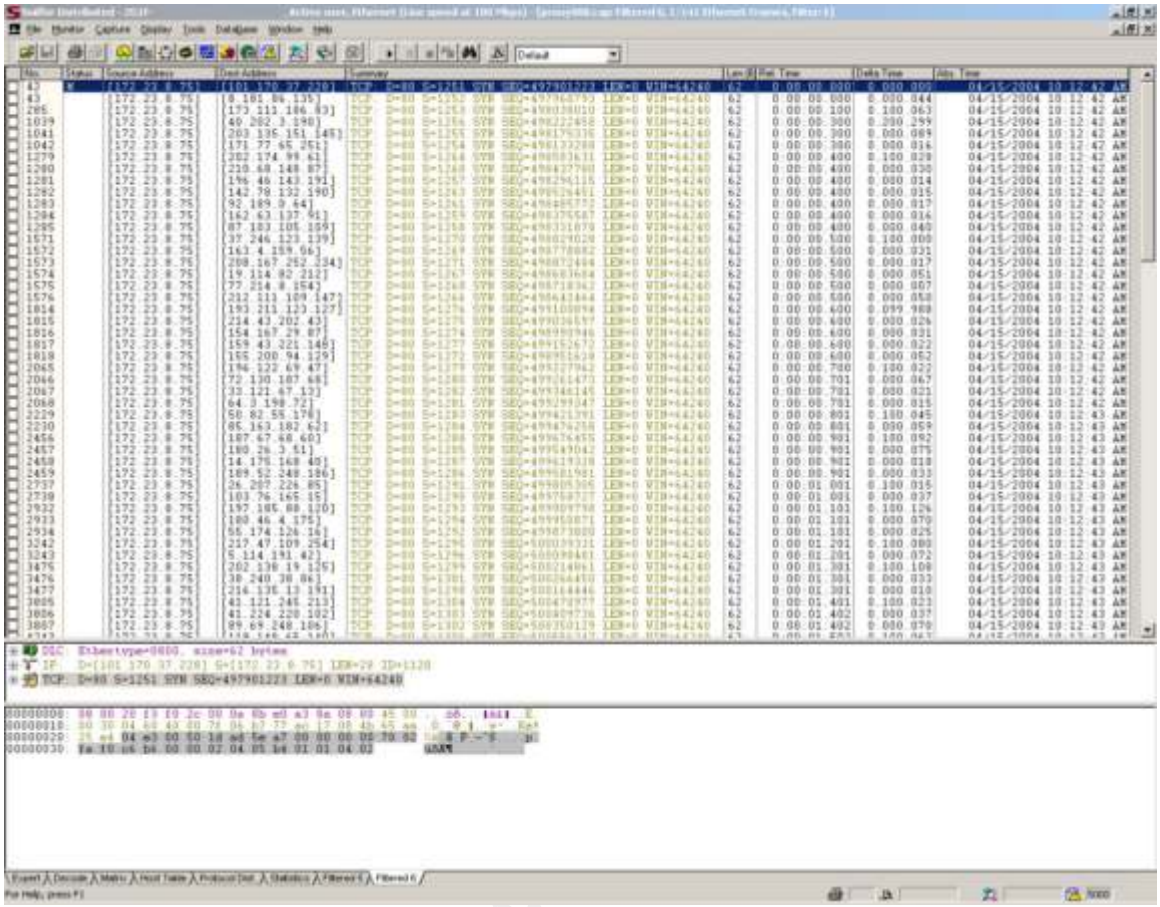


Here again we can notice that the host machine is doing a systematic sweeping of a network range using ICMP echo. The ICMP packet is always the same 106 bytes long. At the bottom of the screen shot, the payload of the ICMP packets shows a succession of “à”. This is not the standard ICMP echo and this 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 “à”. 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:

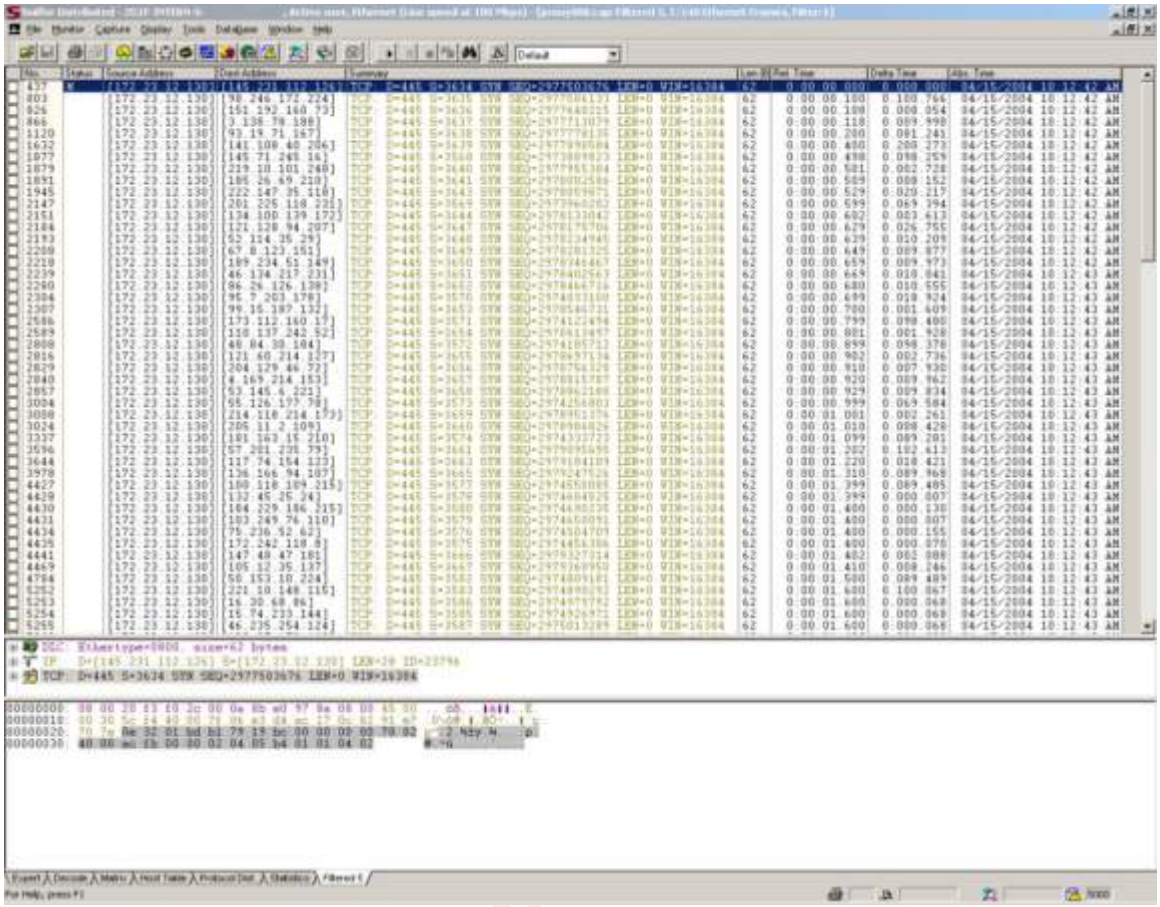


Again we can notice some hosts having outgoing traffic without getting any reply (no inbound traffic). This is seen on both HTTP (TCP port 80) and TCP port 445. Drilling down the conversations from these hosts for these protocols, here is what the traffic analyzer is reporting for HTTP traffic (TCP port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



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:



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 were 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 were only limited resources would be available.

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

McAffee 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