Global Information Assurance Certification Paper

The Inside-Out Firewall Vulnerability

Richard Hammer – hammer@lanl.gov

My subnet is located behind 2 firewalls so I don't worry about a lot of the dangers that Network Administrators directly exposed to the internet worry about. The institutional firewall limits incoming connections and our firewall limits them even more as well as most outgoing ports. My policy has been to not open a port in either direction unless there is a very good programmatic reason. Scanning my network for known vulnerabilities and password sniffing from the outside is almost impossible. In the past I had pondered the concept of hackers having our clients connecting out to sites, but dismissed it as unlikely. I was actually feeling pretty safe until the PrettyPark Trojan/Worm visited a month ago. In this paper I will walk you through my PrettyPark experience and discuss the possibility of hackers targeting your systems from the inside of your firewall.

PrettyPark

A full description of PrettyPark can be found at the following sites:

http://www.symantec.com/avcenter/venc/data/prettypark.worm.html
&
http://vil.nai.com/vil/wm98500.asp

This was the first time that we had a known instance where one of our machines was infected with a Trojan that actually tried to make connections out of our firewalls. We were fortunate to have tcp port 6667 (out bound) closed at our firewall. I played around with the infected machine and actually opened our outgoing firewall port 6667 for about 1 minute and was able to capture the infected machine connecting to IRC sites. Listed below is a screen capture from SessionWall3 showing a successful connection:

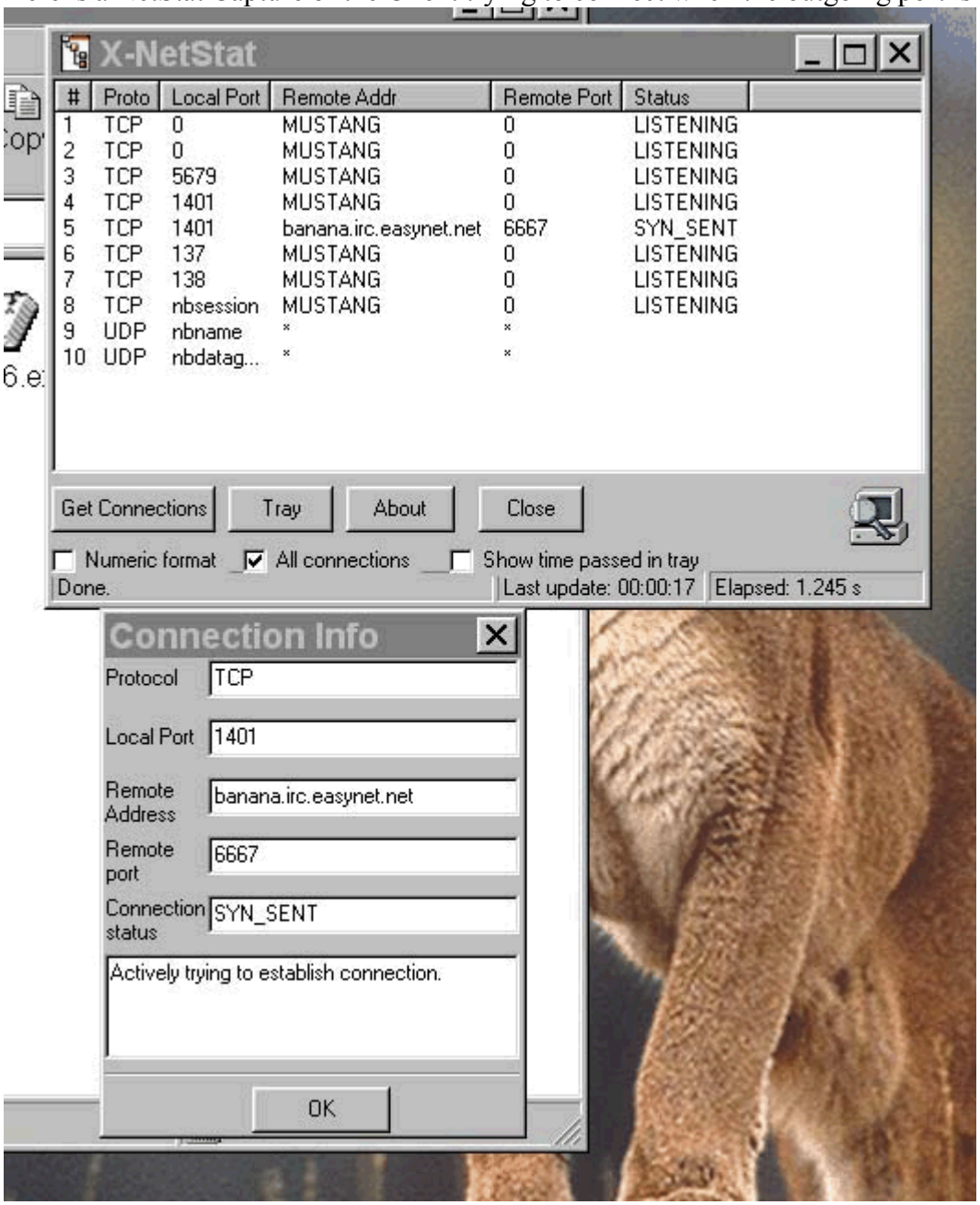
```
Client IP = 172.16.164.60
Server IP = 207.152.95.10
Client physical address = 00:A0:24:D5:B2:4F
Server physical address = 00:A4:C0:91:D2:9C
Client port = 4155
Server port = 6667 TCP
```

Client -> Server
NICK Fzi`Vb|
USER zl|e[c_oPWq eehg_VW :cMGNpnXT

You can get an evaluation copy of SessionWall3 at the following site:

http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/

Here is a NetStat Capture of the Client trying to connect when the outgoing port is closed.



In a little over a minute the infected machine connected to 3 of the 8 known IRC sites that

PrettyPark makes connections to. Here is a listing from my firewall showing one of the connections:

Mar 30 16:34:56 2000 f_rgeneric_tcppproxy a_server t_nettraffic p_major
pid: 1878 ruid: 2115 euid: 2115 pgid: 200 fid: 2000001 cmd: 'tcpgsp'
domain: RGnx edomain: RGnx srcip: 172.16.164.60 srcport: 4155 srcregion: NIS6A
dstip: 207.152.95.10 dstport: 6667 dstregion: BLUE-YELLOW protocol: 6
service_name: Internet Relay Chat acl_id: outgoing rules:SERVICE:0 result: 1
encrypted: 0 netsessid: 38e3e4a000066129

Mar 30 16:34:56 2000 f_rgeneric_tcppproxy a_server t_nettraffic p_major
pid: 1878 ruid: 2115 euid: 2115 pgid: 200 fid: 2000001 cmd: 'tcpgsp'
domain: RGnx edomain: RGnx srcip: 172.16.164.60 srcport: 4155 srcregion: NIS6A
dstip: 207.152.95.10 dstport: 6667 dstregion: BLUE-YELLOW protocol: 6
bytes_client_written: 0 bytes_server_written: 51
service_name: Internet Relay Chat reason: closing connection
netsessid: 38e3e4a000066129

According to Norton and McAfee, PrettyPark will send info to these sites to stay connected and will retrieve any commands received from the IRC channel. I did not allow this machine to stay connected long enough to get some sniffer output of someone sending commands to our infected machine. I noticed that PrettyPark cycles through the 8 sites quit rapidly. When one fails to connect it tries the next site almost immediately.

The user of the infected machine was pretty good about updating his virus definition files. He was using McAfee Viruscan with 2/23/2000 dat files. The time stamp on FILES32.VXD was 3/1/2000 and this version of the virus definition files did not detect PrettyPark. A week later I installed Computer Associate's SessionWall3 Intrusion/Virus detection program. SessionWall3 is a pretty good, easy to use program for scanning your network. SessionWall actually caught two other cases of PrettyPark entering our network. One evening I cleared the SessionWall scanner and noticed IRC connect attempts to a site that rang a bell in my brain (banana.irc.easynet.net:6667). I was lucky that I had cleaned a system infected with PrettyPark and one of the sites was named banana something.

Even if you can get your users to update their virus protection your machines are vulnerable to this type of attack until the dat files include the Trojan signature. Mass distributed worms like PrettyPark will always be relatively easy to detect and clean. Writers of this type of Trojan will not have our machines connect to machines that can be traced to them. Only opening outgoing ports that are required for business will stop most of these mass distributed Trojans.

Scary Stuff

Selective targeting of my subnet is the vulnerability that I worry about the most right now. PrettyPark tells us a lot about how to do these things:

1) Deliver the code to the target.
2) Execute the code
3) Create outgoing connection to hacker's machine.
4) Get the information
5) Trash/disable the infected system and cover tracks.

I have been thinking about selective targeting for some time now and have discussed it recently with a fellow colleague. It seems far fetched but I found a paper on the internet, "Placing Backdoors Through Firewalls" by van Hauser / [THC] - The Hacker's Choice, that gives instruction, lists dangers, and supplies scripts to do exactly what I listed above.

I can think of two low tech ways to deliver and execute the code. One would be to have an insider install the code, another would be to use e-mail and let the double click syndrome install the code. My experience tells me that the average user will double click on anything that looks funny, interesting, business related, or comes from someone they know. I would guess that the double click syndrome is the most popular way to execute malicious code. Making the outgoing connection look legitimate is important, van Hauser offers several suggestions, tunnel from Phrack 52, ssh, netcat , ack-telnet, and http (example script supplied). Once the code is executed getting data from a targeted machine looks easy. With a legitimate looking connection there is a real good chance that this kind of attack will not even be noticed. Virus protection will not work unless the hacker uses a known piece of malicious code and since the traffic will look legitimate so our network scanners won't detect it. The smart hacker will then get the info and start covering his/her tracks. Deleting the malicious code and corrupting a couple system files will look like just another system failure.

Possible Solutions

1) Closing unneeded outgoing ports. Better have strong support before you do this, because users will start to whine when they can't chat with their aol buddies during work hours.

Sites with Good port lists:
http://home2.freegates.be/bchicken/index2.html
http://www.dark-e.com/lowfi.html
http://www.sans.org/y2k/ports.htm

2) Use Personal firewall programs, port scanners and port blockers. I use one of these at home and it works pretty well. Host based protection should be able to stop and detect these types of attacks. Getting users to accept and understand these types of solutions will be difficult since most double clickers can barely update their virus dat files.

Personal Port Scanners, Blockers and Firewalls:
http://www.agnitum.com/products/jammer/jtour1.phtml
http://home2.freegates.be/bchicken/index2.html
http://net-security.org/various/download/
http://davidovv2.homestead.com/freetoolsservices.html
http://www.zonelabs.com/
http://grc.com/su-firewalls.htm
http://www.symantec.com/sabu/nis/

3) Scan and delete known Viruses/Trojans/Worms at your gateway. Do not allow them to get to the double clickers of the world! I use SessionWall3 and it works pretty well for me.
http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/

4) Train users NOT to DOUBLE CLICK on attachments that are not business related.

Clearly critical data should not be stored on networks that have liberal outgoing connection policies and no personal protection.

Resources

You can find van Hauser's Paper at:
http://www.anticode.com/cgi-bin/showdsc.anticode?cat=backdoors-and-rootkits.html

Much thanks to Richard Kandarian – He was the first person that I ever heard actually talk about selective targeting! He has other Solutions that I will not go into here!

Good Sites for information on Trojans:
http://anti-trojan.virtualave.net/page6.html
http://home2.freegates.be/bchicken/index2.html
http://www.commodon.com/threat/threat-all.htm
http://www.dark-e.com/lowfi.html

Last Updated: February 24th, 2018

Upcoming Training

SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
Mentor Session - AW SEC401	Melbourne, FL	Mar 01, 2018 - May 10, 2018	Mentor
SANS London March 2018	London, United Kingdom	Mar 05, 2018 - Mar 10, 2018	Live Event
Mentor Session - SEC401	Vancouver, BC	Mar 06, 2018 - May 15, 2018	Mentor
Mentor Session - SEC401	Grand Rapids, MI	Mar 09, 2018 - Apr 13, 2018	Mentor
SANS San Francisco Spring 2018	San Francisco, CA	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Paris March 2018	Paris, France	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Secure Osaka 2018	Osaka, Japan	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Munich March 2018	Munich, Germany	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TX	Mar 19, 2018 - Mar 24, 2018	Live Event
Mentor Session - SEC401	Studio City, CA	Mar 20, 2018 - May 01, 2018	Mentor
Mentor Session - AW SEC401	Mayfield Village, OH	Mar 21, 2018 - May 23, 2018	Mentor
SANS Boston Spring 2018	Boston, MA	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS 2018 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 03, 2018 - Apr 08, 2018	vLive
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201804,	Apr 09, 2018 - May 16, 2018	vLive
Community SANS Charleston SEC401	Charleston, SC	Apr 09, 2018 - Apr 14, 2018	Community SANS
Community SANS St. Louis SEC401	St Louis, MO	Apr 16, 2018 - Apr 21, 2018	Community SANS
SANS London April 2018	London, United Kingdom	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, Switzerland	Apr 16, 2018 - Apr 21, 2018	Live Event
Mentor Session - AW SEC401	Memphis, TN	Apr 17, 2018 - May 17, 2018	Mentor
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
Baltimore Spring 2018 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Apr 23, 2018 - Apr 28, 2018	vLive
SANS Riyadh April 2018	Riyadh, Saudi Arabia	Apr 28, 2018 - May 03, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, IL	May 01, 2018 - May 08, 2018	Live Event
Community SANS Houston SEC401	Houston, TX	May 07, 2018 - May 12, 2018	Community SANS
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event