murf Explained

Creation Date.................The Twenty Third of Febuary, 1999 (23/2/99) Author Name...................Lethal Intelligence Extasy™
Author Contact Information....lie@macman.net / None / None Organization..................ParadoxeD Ltd. - paradoxed@usa.net / None Base Font.....................Geneva (9 pt size / Plain style)>
Tab Index.....................4
Content Length................10k
Platform Distributions........MacOS
Contributions Accepted........Yes
Copyright.....................ParadoxeD Ltd.

Included Files................"papasmurf.c"
Included Documentation........None
Included External Resources..."Top10_Broadcast_Servers.txt"

Related Files................."papasmurf.c"
Related Documentation.........None
Related External Resources....None

Official Archived Locations...Happle Hotline Server", "Paradoxed Ltd. Hotline Server
Official Release Bodies.......Happle Magazine

One of The Most Deadly Internet Warfare Utilities Ever Concieved... Smurf

Smurf attacks can range in strength from a PPP 56k connection to the wicked power of an oc3 backbone and greater. Needless to say this tool of mass internet destruction is feared by all walks of life within the world of networking. I will first discuss in short the history of how it completes it's deadly task.

Many individuals have heard of the now famous "Ping Of Death", or "POD". By pinging an entity with massive amounts of icmp or udp packets, one can seriously lag or even kill a connection. The general rule of pinging for an attacker is simple. A faster connection to ping with means more lag or a better chance of killing the target connection. However, because most businesses utlize T-1 and faster connection speeds it is extremely difficult and rare for a malacious user to cause serious harm. Because these high-speed connections are costly and require certain elements not found in most homes or apartment buildings (You must, for instance, live within 5 miles of a phone company building in most cases), most people with harmful intentions cannot easily obtain them. This has prevented many massive attacks on major networks. The rules have changed in recent years, however. With the birth of the broadcast server came the inevitable exploitation of such services. The ability of any internet citizen to smash huge network connections to cyber-rubble. Smurf works on a simple principle with horrifying results in an extremely short amount of time. The inner workings of smurf will be discussed now as we delve farther into this godlike war machine of chaos.

Without amplification (explained later in this section) smurf is a simple but effective ICMP spoofing program. One can send an ICMP packet to any destination with a customized source address. In effect, you are pinging a server and fooling it into thinking somone else origionated the ping. This of course would prompt a response packet (pong) from the server which would make it's way to the

spoofed source address of the origional packet. I call the local pizza parlor and ask for an extra large pepporoni pizza, give them the address of my economics teacher and hang up the phone (and now he's stuck with the bill, or extra bandwidth). Earlier in this section I mentioned amplification, and here is where we discuss how smurf can be modified into a powerhouse of deadly packets. An individual who intended to smurf a victim could ping a very fast host and be content. However, this will only cause that host to ping your enemy with as many packets as you are sending. In other words, the pizza parlor is only going to send as many pizzas as I order to my enemy and I can be confident that they will all arrive on time because of this particular parlor's good reputation. But what if I wanted to order a thousand pizzas at once, have them all sent to my victim in one delivery and repeat THAT process with about the same reliability? It can be done, and I will tell you how.

Earlier in this article I briefly mentioned broadcast servers. These special servers are run on many networks (more than one might think). What is a broadcast server, you ask? It's a server which relays packets it recieves to all the hosts on it's network. What does this mean? It means if you find a network with 1000 hosts and a broadcast server, you can ping the broadcast server with 1 packet and recieve 1001 packets back (from 1001 different ip addresses). This would be like calling up your favorite telemarketer and having them order thousands of pizzas from every parlor in the city and sending them to the same house all at the same time (my economics teacher). Fire up your favorite ping program and beat a broadcast server as fast and hard as you possibly can, you'll find yourself with a dial tone in a flash. It should be clear just how smurf operates at this point. Because smurf can "lie" about it's ping origin, you can tell the broadcast server that your victim is beating on it with icmp (or udp) packets, which will cause all 1001 hosts to pong your victim into the ground with responses of the specified calibur.

Broadcast servers are, in recent years, becoming rare. I have seen but two in my lifetime that reply with more than 1000 hosts. Scanning for broadcast servers is not a difficult task. Set up an ICMP packet logging application (such as ICMP Logger) and ping the ip address which you believe may be a broadcast server. Count the number of replies you recieve and if it ranges above 9 you have a suitable smurf amplifier. Repeat this process as necassary to test all suspected networks. It should be noted that broadcast servers are almost always going to end with .0 or .255. In addressing terms, this means that if you suspect 194.23.124.66 to be a host on a network utilizing a broadcast server, you should ping 194.23.124.0 and 194.23.124.255, counting the number of replies you recieve.

So, what should you do exactly when you have smurf compiled and you've got some broadcast servers? Put all of your broadcast servers into a text file separated by carriage returns. Save the file in the same directory as your smurf application. When smurfing, it's best to keep the packet size under 1000 bytes. This is vital if you plan to use the same broadcast servers over time to achieve the same result. By slamming a broadcast server with packets that are too large you will be showing the administrators of that network that there is a serious problem. Extremley large packets are usually noticed and recorded for further inspection. If a problem is suspected the chances are good that a security consultant or other knowledgable computer genious will look into the issue and discover that the network which you are using to amplify your smurf attacks is being used for just that. Once this information is passed along to the administrator, you can bet your hard earned dollar that network will not serve as an amplifier for very long. To stay on the safe side I recommend 1000 bytes maximum per packet. Smurf is smart enough to utlize your entire list of broadcast servers, hitting each with the same statistics. This will ease the load and make things less conspicuous for your attack while it's in progress and after the event has taken place.

So, how can somone trace you down if you are smurfing them? Well it's very tough, but possible. If you shoot your mouth off before, during or after you smurf a victim it's more than likley he or she will report you to your internet service provider and ask them to verify their logs. If this is the case, you may face criminal prosecution for Denial Of Service (DoS). If they even suspect you as the perpetrator they might contact your ISP as afore mentioned, so it's best to be silent about your hatred for people if you plan to attack them.

To conclude, i'd just like to say that smurfing is for the most part a BAD idea. People get busted for smurfing all the time, and they pay for their foolishness dearly. If you strongly dislike an individual, ignore them. This is by far the most mature solution to an otherwise time wasting problem. After all, is it REALLY worth wasting your precious time to deal with somone who doesn't know their ass from a hole in the ground? Honestly, what difference will it make? None, accept that you will be risking your

ass in fines if you are caught. Yes, you'll kill their connection, but it will only aggrivate matters to a more extreme level than before. I hope you all learned something in this article, and I hope I can release more articles in the future. Thanks to everybody who helped me out, you're a great crowd.

Lethal Intelligence Extasy™

- End Of Document (EOD) -