Passive Mapping:

An Offensive Use of IDS

By Coretez Giovanni

Intrusion Detection Systems (IDS) are used to help defend domains by sitting on network choke points and recording all inbound and outbound packet traffic. These well-positioned tools have always been thought of as a defense weapon against cyber crime. But a tool has no say in how it is used.

Passive mapping is a technique of listening to a choke point in the network and using the data to map a network. IDS naturally can perform this function. Passive mapping differs from active mapping where the software sends packets out and listens to the response to determine a network layout. NMAP is an active mapping piece of software. The Air Force was looking into passive mapping techniques some time ago but nothing seemed to happen with it.

What are the advantages of passive mapping over that of active mapping that someone would spend research money on it? There are three discriminators between active and passive techniques: low uptime discovery, unusual port discovery and loss of illumination.

Low Uptime Discovery

Passive mapping is quite useful in finding and analyzing systems that might only be on for a matter of seconds while they transmit and receive data. If the system talks past the choke point then passive mapping will find it. This has strengths over an active mapping system where it discovers only systems that happen to be on during that time period. Therefore, passive mapping discovery is related to information sent, while active mapping discovery is related to uptime.

Discovery of Services

Scanning a network for all possible ports can take some time. And scanning reduces the network bandwidth while making its presence known. Passive mapping can be used for services discovery, especially those hard to find services that hide in the upper port numbers or only talk after being triggered.

There has been much in the press over the years about security companies using the default ports to find tools like TFN and BO2K. As Dr. Mudge might say, “Snake Oil”. One can easily change the default ports in the code, change procedure names and pad the file. These techniques will help avert being detected by cheap scans and low grade system checkers. If one intends to find backdoors into the network, then the use of passive mapping is essential.

One example of service finding is in TCP. In a TCP handshake there is an initial SYN-ACK package by the receiver. Simply searching the TCPDUMP for SYN-ACK connections will get a list of active listening ports. If TCP is used for a high port backdoor, then the SYN-ACK from a port greater than 1024 (might want to take out ports like 8080 if user defined services are allowed) is a good clue that there is a TCP service on the box.

By using the SYN-ACK, and not high-low schema, you bypass the problem of low initiating source (especially in high port Trojans). And the SYN-ACK search helps reduce redundant data sets.

Reduction of Illumination

One of the side effects of passive mapping is that it is invisible to the users on the network. Anti-Sniff (www.l0pht.com) demonstrates a capability of finding sniffers, but compared to active mapping techniques the illumination is negligible. However, the moving of the results across the network however will still cause illumination in a distributed sniffer configuration.

Corollaries

Reverse Mapping Occurs

So what, what about the offensive use of passive mapping? Well, passive mapping not only maps your network, but it slowly maps the network that your users are going to. This means that a large distributed network of filters could collect "good" maps of networks. Not only will it record normal traffic results, but if there are other scanners and mappers running on the network by those nasty users, you get their maps too.

Examples

"… a government official for the first time publicly acknowledged the existence of the Internet control project, called the System of Operative and Investigative Procedures or SORM-2, its Russian acronym."

- SERGEI SHARGORODSKY, Associated Press, February 21, 2000

SORM-2 could be used to map networks inside and outside Russia. The shear size of data from 350 service providers produces a low illumination mapping capability that is worth being envious of having.

It is not always possible to place sniffers on some one else's turf. Packets flow, unless programmed otherwise, through the quickest route. By increasing speed and bandwidth of their countries, German and French organizations can map other countries in the EU and also in the US by creating quicker routes through their countries. It may be worth some good intelligence money spent to see where high speed fiber is being placed and who is spending the money.

Conclusion

With the demonstration of distributed denial of service attacks, many people are asking what is next. One logical step would be to actually use these collections of compromised systems in other than denial of service techniques. These techniques are however easier to implement and have a larger scale of use by organized financed groups.

Thanks to Johnny "Mind Thief" Anonymous for pointing out the great example of the Russian IDS constellation as a premo example using this technique.

A side note: I was talking with Simple Nomad during lunch. We were sharing ideas when he brought up passive mapping. I showed him this paper and some other material I had handy, but I wanted to make a note here so others know that Simple Nomad has also been working on the same lines and wanted to ensure that he receives equal credit in this technique.

Derrick Jamison made the passive mapping filter quicker with the following tcpdump filter:

tcpdump –q –n 'tcp[13] = 18'*From the line above it should be noted that this technique is not theory, but it works. We have tested it and find it has many uses.*