

Passive Mapping:

The Importance of Stimuli

By Coretez Giovanni

This is a short paper written to clarify the significant differences of passive and active mapping, and how this difference impacts attacking a network. Since writing a first concept paper, I was surprised to see how quickly the community created passive tools. The [Siphon](#) project by [bind](#) & [aempirei](#) is an excellent example of the progress and made myself feel better that I just was not writing to myself. Stopping at passive OS detection however would miss the mark of the power of passive techniques. The idea of fingerprinting the OS is a natural extension of the mimicking the active mapping concepts, but the differences between the two techniques (passive and active) allows for different strategies in the offensive realm.

The objective of scanning, from the offensive view, is not to determine what ports are open, or even what applications are running, but really to determine what vulnerabilities exist. This extension of mapping is derived from the use of NMAP in practice for NMAP is the discovery engine of well-known vulnerability scanners like Nessus and Vetescan.

Review of Active Mapping

To review, active scanning refers to gathering network understanding in order to exploit by *initiating action* into the network. The attacker controls the initiation, but has no knowledge of the network¹. Therefore, active mapping tools

¹ This is due to the nature of the tool. It is designed to scan IP routing networks and

are aimed at standards and default configurations as a basis of knowledge. In general, certain port responses indicate the high probability that a particular application is bound to that port. For example, a response on port 23 usually means that the system has a telnet server running on it. Furthermore, due to the nature of active mapping producing detectable activity on the network, active mapping attempts avoidance by creating network anomalies that if successful is not recorded.

Unfortunately for an attacker, detectors use these anomalies for correlation and response once a scanner signature is known. Finally, active mapping can be complete in its brute force means of checking address space unlike passive mapping.

Review of Passive Mapping

In turn, passive mapping is incomplete in the mapping of a network. The probability of completeness in scanning is extremely low, and gains in network understanding do not increase significantly in ratio to time².

Stimulus

The key to understanding *information gathering* is to understand the relationship between *stimulus and reaction*. In mapping system attributes, vulnerability being one, attributes are discovered not by their acceptance of a packet, but by its reaction. The sending packet that induces the target system to reveal information is a Stimulus. So, in active mapping the stimulus is controlled while in passive mapping it occurs with user use of the system. Active mapping, due to lack of knowledge, generates stimulus based on knowledge of standards and default configurations. In passive mapping, the stimulus is based not

therefore examines a network based on default values for IP applications, routing protocols, and system interpretation.

² The characteristics of passive mapping are described in further detail in the first paper, "[Passive Mapping: an Offensive use of IDS.](#)"

out of standards and configurations as much as it is out of users' knowledge of the system. That knowledge is what an attacker is attempting to learn in order to exploit its weaknesses.

Stimulus Relationship with the User

One of the largest advantages of passive mapping has to do with the stimuli user generates. The set of user generated stimulus, especially at the application layer, cannot be sent via active mappers. One example is the Stimulus-Reaction packets that occur during and after identification and authentication (I&A)³ phase of a connection. Only when I&A is implemented in the default mode or there is predefined guessing is this possible for active scanners.

Passive mappers can operate at the application layer. Sniffers are a great example of passive information gathering at the application layer. The user ID and password combination occurs at this layer. Passive collection can give an intruder information that will be useful even after the initial access account by given the aggressor the knowledge of other applications that can be exploited that cannot be seen from the network view. These internal applications (non-service oriented programs) can prepare the attacker for vulnerabilities accessible to limited access user accounts.

Network Noise

If you are familiar with analyzing network traffic you will not be surprised at the amount of packets that generated from network management. Network noise occurs from both properly implemented and misconfigured services. The later are often constantly looking for non-existing counterparts. One hacker friendly protocol is SNMP version 1. SNMP sends status and configuration data for all to share. And finally, there are data movers like mail, anti-virus updates, audit files and back-up files

³ I&A is something a person "has in possession", "is (as in biometrics)", "knows" or "is in location".

shooting across the network. Passive mapping can show weaknesses in software versions, misconfigurations and alternative entry points. When remote administration is used the collection of log information can be gained that demonstrates what warnings the administrator is use to and can show weaknesses in systems that are not running properly.

User's Noise and Knowledge

Users demonstrate to the aggressor the use of mounts, telnet, ssh and ftp services to name a few. I&A tokens and schemas can be stolen using passive collection. Though application and system information can be gained through banner scanning, application protocol analysis can also retrieve this information passively when a banner is not used. For example, Firewall-1 logs when services like DNS appear on non-standard ports. Some administrators try to hide ports (and systems) by placing services in the chargen and echo ports since vulnerability scanner don't really look for services that can be exploited there (unless you are interested in denial of service). There is an assumption that when scanning a network there is a direct relationship between a specific port number and an application. Telnet is on port 23. SMTP is on port 25. SSH is on port 22. But sometimes network savvy administrators place applications on a port that scanners ignore to investigate like the echo port (port 7).

Client Weakness

What of determining client weakness? Passive mapping OS fingerprinting gains data, but it does not help in compromising the system if no service listening is determined on the system. Sometimes you get lucky and find an X configuration. X services actual reverse the client-server relationship and can add vulnerability to the user. Tools like BO2K and Netbus are well designed to take advantage of bad user habits and yield better results going after client systems. Direct attacks against client stations do not work unless the client has a

service (and therefore is no longer just a client). When passive collecting data, log reduction can be enhanced through reducing client data that is useless in compromise.

Using IDS design

This all might sound wonderful but unsupported. Actually, passive mapping to determine weaknesses in a system is quite capable using defensive tools. IDS analyst refer to passive discovery of vulnerabilities as, "Tuning the network."

Intrusion detection tools use four significant techniques to find intrusions:

- String (or pattern matching)
- Packet header analysis
- Context Pattern recognition: Use of n-code
- Threshold Alarming

These tools use the same basic structure:

- sniffer
- constructor
- analyzer
- responder

Offensive passive techniques can grow quickly by using the defensive IDS designs except applying offensive reactions to the response.

Direction of Passive Techniques

Passive mapping can do tricks that are similar to active mapping (like OS detection), but it has a different stimulus and therefore will be better at some mapping concepts than others. When defending a network passive techniques are not just used for intrusion detection, but also in discovering unreported services and new systems to validate against the security posture. Offensively, passive detection can be tied to vulnerability discovery. For example, a worm design can be constructed that does not actively scan to grow, but passively.

For example, tying TCP Hunt to attempt to replicate onto a new system by noticing the "#" string of a root user. After checking to ensure its not already there, the replicating worm then install itself and continue the expansion process. This is an old vulnerability just a different propulsion mechanism.

Passive mapping is a safe way to determine the target network's defensive systems by detecting noisy security tools. Again for example, the determination of port 2998 that screams to the attacker that this is an ISS Real Secure system without needing to scan processes and ports.

Also, passive mapping can be used to profile a network to determine acceptable use of protocols that will allow exploit communication to mimic the technique (avoiding threshold alarming).

Conclusion

To summarize the main points, "Passive Mapping" is just another technique in the attacker's toolbox. It affords maximum stealth. It gains both network and user knowledge. And it can be highly automated replacing its counterpart software component (active mapping) in avoiding IDS systems. But passive mapping is not equal to active mapping. It uses a different Stimulus. It is not as complete and not controlled in its gathering. To understand the benefits of attacking methods consider its defensive design as "Intrusion Detection Software". It uses the same analysis techniques and passive mapping can have automated triggers but with offensive responses. In conclusion, passive mapping is a unique step in offensive techniques.

The information contained in this paper is for education purposes only. This paper is the property of Endeavor Systems, Inc., and is not to be replicated for commercial advertisement or gain without the written permission of Endeavor Systems, Inc.
© 2000 Endeavor Systems, Inc.