SprayPAL: How capturing and replaying attack traffic can save your IDS/IPS

Dr. Patrick Engebretson | Mr. Kyle Cronin | Dr. Josh Pauli

Dakota State University | Madison, SD

1. Introduction

Testing Intrusion Detection Systems (IDS) to ensure the most malicious attacks are detected is a cornerstone of these systems, but there is no standardized method to execute these tests. Running live exploitations is not always a viable option – especially when the rule set isn't finalized, and clients are often nervous about the use of "hacker tools" on their networks. Furthermore, educators struggle to teach IDS concepts as a standalone principle without teaching attack methodologies at the same time. We are releasing two artifacts to help solve these problems. First we introduce PAL, a PCAP Attack Library full of individual pre-captured attack files that can be easily replayed for IDS testing and education. This library is completely preassembled, clean, and extendable to include further additions of attacks. Our initial library is created from the findings in the Common Attack Pattern Enumeration Classification (CAPEC) from the Department of Homeland Security. Second, we introduce SprayPAL, a software tool that we've developed to replay the PCAP attack library files. Users can send attacks to a specific target or broadcast to an entire subnet of machines. Additional features include the ability to select individual or multiple simultaneous attacks as well as provide layer 2 and 3 packet level manipulation. We conclude by presenting a methodology for capturing attacks and adding them to the public library.

2. Building a .pcap Attack Library (PAL)

The network architecture to build the initial PAL was very simple. This was done by design to ensure that only the traffic actually related to the attack was captured. Although it's somewhat trivial to remove packets originating from any source other than the "Attacker" and remove packets headed towards any destination other than the "Victim", this removal process is a non-factor in an isolated network as introduced in Figure 1.

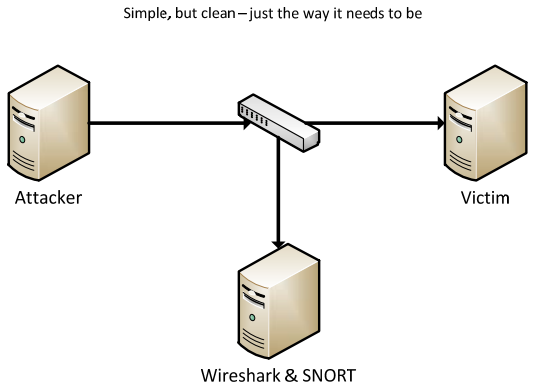

Figure 1. SprayPAL isolated network for .pcap file creation.

This could also be accomplished through the use of virtual machines. Using virtual machines reduces extraneous network traffic and makes the process of loading pre-configured "victims" simple. In this configuration the "Attack" also acts as the capture machine because Wireshark is running on the attacking machine.

All traffic sent from "Attacker" to "Victim" was also sent to the monitoring machine running Wirehsark and SNORT. This was done so that in case the "Victim" machine became unstable because of compromise the attack traffic would still be captured in Wireshark and SNORT rules monitored for triggering.

The process to build the .pcap Attack Library (PAL) is broken out into two separate phases; one before the attack and one after the attack is executed. The steps to build the attack are introduced in Figure 2.

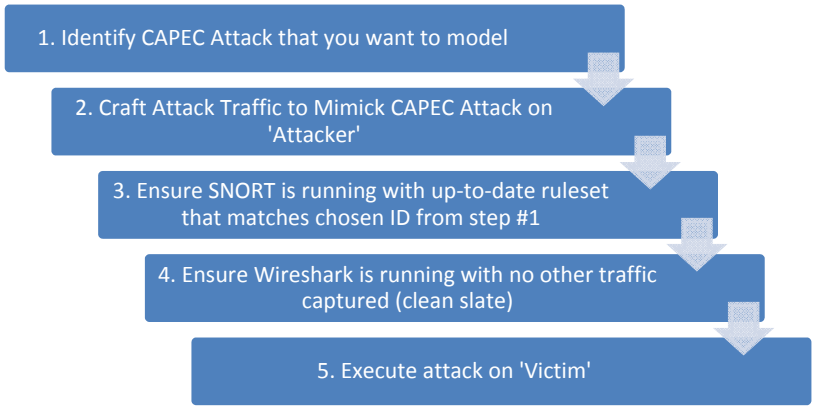

Figure 2. Steps to build attack traffic.

The key to a legitimate PAL is to catalogue the data in such a way that by referencing the CAPEC definition we can find corresponding PCAP files and Snort Intrusion Detection System (IDS) rules or any firewall or other packet filter ruleset. The steps to accurately capture and document each .pcap Attack file are introduced in Figure 3.

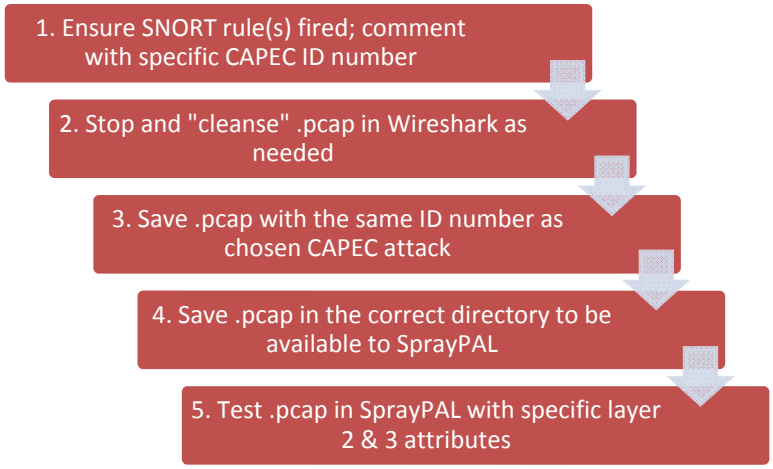

Figure 3. Steps to cleanse and document attack traffic.

By mapping real attack traffic captured in .pcap files to corresponding CAPEC definitions and Snort IDS rules, we are hoping that when instructors or penetration testers need to use certain attacks, they can identify a CAPEC definition for the attack that they want to perform. The result is a framework that saves both time and effort for instructors and system administrators wanting to teach defensive techniques (ruleset creation) or test their current configurations.

3. SprayPAL – a Smarter Replay Tool

SprayPAL's main difference over TCPReplay, and other packet replay tools, is that it allows easier manipulation of network traffic at either level 2 or level 3 in order to allow the traffic to be replayed to be refined further, thus allowing specific attacks to be delivered to a specific host or group of multiple hosts. In replaying the PCAP attack library files, users can send attacks to a specific target or broadcast to an entire subnet of machines. SprayPAL also includes the ability to select individual or multiple simultaneous attacks to stress your IDS/IPS further. For example, SprayPAL can deliver a TCP Syn Port Scan piggy-backed with a full TCP Connect Port Scan to test how your IDS system reacts. This, of course, is a simple example. SprayPAL currently includes 25 CAPEC attacks to choose from as introduced in the documentation.

4. Process to Grow PAL

We encourage the community to help grow our .pcap Attack Library by completing the steps outlined in section 2 above. The process is very simple and straight-forward beginning with a network infrastructure similar to Figure 1. This isolated network ensures only traffic from "Attacker" to "Victim" is captured in Wireshark, thus less cleansing of the .pcap files needs to be done.

"Attacker" software is at the discretion of the user. It is encouraged to use widely available tools so others can validate your .pcap files with the same toolset. Each attack must be mapped to an individual CAPEC Attack Pattern and be documented as such in the .pcap file. These attack .pcap files should have as much unnecessary traffic as possible removed. Once attacks are captured, use SprayPAL to manipulate layer 2 and 3 parameters during your replay (http://ia.dsu.edu/spraypal). SprayPAL will always include the most updated version of the PAL.

Traffic can be captured and .pcap files created in Wireshark (http://www.wireshark.org/) which also required WinPCAP as the packet capture and filtering engine (http://www.winpcap.org/). Attack traffic can be monitored and alerted on with SNORT (http://www.snort.org/).

5. Conclusions

The initial .pcap Attack Library (PAL) and the SprayPAL software tool can be downloaded at http://ia.dsu.edu/spraypal. Future additions to the PAL as .pcap files can be submitted to pat.engebretson@dsu.edu. All .pcap files will be individually tested and evaluated before inclusion into the PAL. Please ensure that your .pcap file is as "clean" as possible; it should only include traffic from the "Attacker" machine to the "Victim" machine and be tied back to one specific CAPEC Attack Pattern. Contact pat.engbretson@dsu.edu to join the mailing list to be informed of new releases of PAL and SprayPAL.