Abstract

Analyzing packet captures is one of the many tasks a security professional performs. Most analysis is usually on a packet capture (pcap) file, on a standalone system, utilizing a program like tcpdump or Wireshark. While this method is effective at analyzing and identifying an event, it is only a single view of what is happening and often leaves the analyst to theorize what is happening. Having a full network environment to validate a theory would be ideal. However, most organizations do not permit testing on the production network and creating a physical lab environment that emulates the production network can be expensive. By leveraging GNS3, an analyst can create customizable network lab environments for testing. GNS3 is an open source program that allows for the creation of portable and customizable emulated network environments. The goal is to demonstrate how security professionals can create lab environments that allow them to generate attacks and analyze the network packet captures in an isolated network environment.
1. Introduction

Most lab environments are standalone and lack network connectivity, which can limit the analysis of events. Marcus Ranum defined network forensics as "the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents." (as cited in SANS, 2016 Book 503.5 p.108) While a standalone lab allows an analyst to analyze network events, they lack the ability to capture and record events as they happen. This limitation only gives an analyst a snapshot view of what was happening. A fully functioning lab should be an essential component in every security professional's toolbox.

The principal hurdle preventing the building of labs with networking capabilities is the financial cost of purchasing and maintaining duplicate hardware and. Then there are the resources needed to maintain the lab since most networks are dynamically changing, this can make it difficult to keep labs up to date. Open source tools provide an economical solution allowing for the creation of a lab environment that includes network functionality.

By leveraging Graphical Network Simulator-3 (GNS3) to emulate a network that integrates with other virtual and physical devices a security professional can have a holistic view of an attack while overcoming the financial and resource hurdles in maintaining a lab. This paper demonstrates creating custom labs, generating attacks, and then analyzing network packet captures with a couple of different scenarios.

2. GNS3

The goal is to have a lab with networking that is customizable and inexpensive that provides "... a controlled environment in which unexpected events are nonexistent or at least minimized. Also, having a lab provides a consequence-free setting in which damage that might result from experimentation is localized). (Gregg, 2008, p. 2) GNS3 is an open source network simulation software that can be used to design, build and test networks in a virtual lab environment without the need for physical network equipment.

Tracy Brockman, tbrockma@verizon.net
GNS3 has several features that make a versatile tool for use in labs. Some of those features are:

- It can be combined with a variety of virtual and physical devices, operating systems, and applications allowing for use in several environments. This feature allows the user to create customizable labs for whatever the situation requires.
- It is capable of using the same operating system builds that the physical equipment does, which enables the use of production configurations in the lab.
- Several different companies are developing appliances and applications to run in or with GNS3. (GNS3, n.d.)

There are some limitations to note as well:

- Brand name equipment like Cisco or Juniper, do not permit public distribution of the network operating system. A paid support contract with the vendor will be required to deploy the network operating system for lab usage.
- Newer or larger network equipment may not be available nor supported within the GNS3 application.
- For larger and more complex networks, the host system may require additional resources.

Despite these limitations, GNS3 can provide the networking component that gives a security professional a holistic view of an attack that a standalone environment cannot provide. It provides a contained, customizable, and inexpensive environment that allows users to execute attacks or use for other scenarios while capturing and recording them. The analyst can use this information to discover additional details about an attack or other incidents.

2.1. Capabilities and Use Cases

GNS3 was “…built on top of Dynamips” (Fogarty, 2015) and was originally used by the creator to study for his CCNP certification (GNS3, n.d.) and is now used by other network professionals “as a means of testing, learning, and preparing for certifications exams.” (Fogarty, 2015) Similar to networking professionals a security professional can use GNS3 to study for security certification exams. Leveraging GNS3 to study for

Tracy Brockman, tbrockma@verizon.net
various security exams provides the student with self-contained labs to perform or replay an attack, perform malware analysis, or other hands-on skills need to study for the exam. GNS3 has several other security uses that a professional can leverage in their day-to-day activities, some of these are:

GNS3’s ability to simulate networks makes it an ideal environment for performing network forensics or training in an isolated environment. GNS3 has Wireshark integrated with it giving an analyst the ability to perform simultaneous packet “[c]apture[s] on any link between any nodes” (GNS3, n.d.). Wireshark can capture the traffic and perform the analysis part of the network forensics process. Additionally, being able to perform captures on multiple links simultaneously can provide additional views of the traffic that may not be visible in the live environment. This additional information could be used for improving network architecture designs. An analyst could use the information to identifying ideal placement of network taps, intrusion detection sensors (IDS), or intrusion prevention sensors (IPS) or by testing rules and configurations.

During an incident investigation, an incident handler can leverage GNS3 to recreate the environment in a self-contained lab and replay the event to see if any additional information can be acquired. The information obtained by replaying the event could be used to identify the need for further containment, eradication, or lessons learned. Additionally, incident responders can use GNS3 as part of their training program and utilize it to orchestrate tabletop exercises.

Simulating networks using GNS3, by emulating live equipment in a self-contained environment, or integrating with physical and virtual systems allows for a variety of uses. In addition, as companies continue to develop appliances and applications to integrate with the product, so do the capabilities and uses. The following scenarios demonstrate a couple of the security uses and capabilities of GNS3.

3. First Scenario

The first scenario is a demonstration that will analyze the results of an active reconnaissance scan. These scans probe systems for open ports and service to find

Tracy Brockman, tbrockma@verizon.net
potential weaknesses. The information collected during these scans could be used to perform a more advanced attack in the future.

### 3.1. Lab Setup

The components utilized in the lab to test this scenario are:

A Kali Linux image containing nmap is used to demonstrate what an attacker could use when performing an active reconnaissance scan against an environment. Kali is a Linux distribution with many preinstalled security tools useful for penetration testing. (Offensive Security, n.d.) "Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing." (Lyon, 2008, p. xxi)

A system running Metasploitable2, "The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities." (Hdmoore & Egypt, n.d.)

Both Kali Linux and Metasploitable2 are virtual systems running in VirtualBox. "VirtualBox is a general-purpose full virtualizer for x86 hardware, targeted at server, desktop, and embedded use." (Oracle, n.d.)

GNS3 virtual environment, running Wireshark. Wireshark is a network protocol analyzer used to capture data packets passing across a network. Wireshark decodes and provides an analysis of the traffic while, displaying the various fields of the packet frame.

---

**Figure 1: Scenario 1 Lab Setup**

---

Tracy Brockman, tbrockma@verizon.net
The GNS3 simulator is used to emulate two networks connected to a Wide Area Network (WAN). To accomplish this two virtual Cisco 2960 routers communicating via a serial interface is used. Connected to each router will be a network switch that connects to the two virtual systems, which connect to GNS3 via VirtualBox's virtual host-only interfaces. The two separate networks will represent the attacker's network running Kali Linux and the target host running Metasploitable2. Wireshark is used to capture the network traffic flowing across the lab environment.

A port enumeration scan is launched from Kali Linux using nmap against Metasploitable2 using the following command: `nmap -sV -p-65535 10.0.0.26` to demonstrate an active reconnaissance scan. A port is "[a] process or application-specific software element serving as a communication endpoint for the Transport Layer IP protocols (UDP and TCP)." (ISACA, 2016) A port enumeration scan is "[t]he act of probing a system to identify open ports" (ISACA, 2016) while trying to identify what services may be listening on the open port. The network traffic during the scan is captured between the network switch (SW2) and Metasploitable2 utilizing Wireshark.
3.2. Dissecting Packets

After performing the scan and capturing the network traffic, the next step is to perform an analysis on the packet capture files using Wireshark. The first thing reviewed is what protocols are being used. A protocol is "[t]he rules by which a network operates and controls the flow and priority of transmissions." (ISACA, 2016) To examine the protocols go to Statistics > Protocol Hierarchy. As expected, the primary protocols observed are IPv4 with nearly all being Transmission Control Protocol (TCP).

![Figure 3: Protocol Hierarchy](image)

Next, for what hosts are a part of the conversations, click on Statistics > Endpoints from the toolbar. The results show that four IP addresses were observed.

![Figure 4: Hosts](image)

The IP addresses of the Kali Linux system and the Metasploit system have the highest byte count and packets, with the outliers being 10.0.0.255 and 8.8.8.8. Since the target network subnet is 10.0.0.0 /24, it can be determined that 10.0.0.255 is the broadcast IP address for this subnet and 8.8.8.8 is one of Google's Domain Name Servers (DNS). Normally broadcast and DNS traffic are filtered from captures as known traffic.

Since most of the traffic identified earlier was TCP, clicking on the TCP tab permits the review of the TCP conversation statistics. These statistics can assist in identifying which hosts were communicating on what port, the byte count of the traffic...
and the direction the traffic was flowing.

Figure 5: TCP Conversations

Figure 5 shows 66114 different conversations primarily between 10.0.0.26 and 172.28.0.26 each occurring on a different TCP port. Normal communication between two hosts can vary from two to a dozen ports, pending on the length of time of a conversation and what protocols the systems are using. Sorting column ‘Port B’ reveals the port numbers are incrementing by one, starting with port 1 through 65535.

Another observation, a majority of the conversations between 10.0.0.26 and 172.28.0.26 are just two packets of 112 bytes. Traffic between two hosts is normally at least six packets the first three are the TCP three-way handshake used to establish a connection (Syn, Syn-Ack, Ack) and the final three for a graceful termination (Fin, Fin-Ack, Ack). Also observed are larger byte counts on some of the well-known ports. Well-known ports are those from 0 and 1023. These traffic patterns are expected during a port enumeration scan.

3.3. Deeper Analysis

Next, a more in-depth look at the traffic packets associated with the conversations was reviewed. To review the packet associated with a conversation, select one of the conversation and click the Follow Stream button. After reviewing a few of these packets, it was observed that all the initial SYN packets had an initial sequence number of zero, "The first TCP sequence number selected by each side in the exchange is known as the Initial Sequence Number (ISN). It should be a random number." (SANS, 2016)
Next reviewed, were a couple of the conversations with larger byte counts, port 21, normally associated with File Transfer Protocol (FTP) and port 25, Simple Mail Transfer Protocol (SMTP) were selected.

Examining port 21 FTP:

Figure 7: FTP Traffic

Tracy Brockman, tbrockma@verizon.net
It is observed the Kali system establishing a successful connection to the target host on port 21 FTP. The Kali system then sends two packets to the host the first packet is an ACK with a sequence number one, followed immediately with a FIN.

![Figure 8: FTP Stream](image)

The target host responds with an error as shown in Figure 8 and terminates the connection. Although it appears no files or data was transferred, the host did disclose information about the system and version of FTP running. This information can be helpful for future attacks.

Examining port 25 SMTP:

![Figure 9: SMTP Traffic](image)

Again, Kali successfully established a connection to the host on port 25, usually SMTP. Kali then sends the host two packets the first packet is an ACK to sequence number seven followed immediately with a FIN, ACK to the same sequence number.

Tracy Brockman, tbrockma@verizon.net
Kali then sent an EHLO \n command to the host, the host responded with the fully qualified domain name (FQDN) of the system, and Extended SMTP (ESMTP) is running. The target host responds with a 501 error as shown in Figures 9 & 10 and terminates the connection. This information can be helpful for future attacks.

3.4. Summary

This scenario demonstrated what an active reconnaissance scan might look like coming into a network by leveraging GNS3 to emulate that network. It allowed for the execution, capture, and analysis of an attack in an isolated environment. The information collected during this scenario could be used as a training exercise or to make recommendations to existing configurations to prevent these types of scans in the future.

4. Second Scenario

The second scenario demonstrates how a GNS3 lab environment might be used in an incident response investigation. The first part analyzes the network traffic captured leaving a Windows 7 system that is infected with malware and observed communicating with several command and control servers (C&C). C&C servers are "…typically used to execute arbitrary commands on a victim system, report the status of a compromise to an attacker, or exfiltrate information." (Soni, 2014) The second part recreates the incident in an isolated lab to see if the initial investigation missed anything or any additional information can be learned about the malware.

4.1. Initial Analysis

A Windows system was infected with ransomware malware. Correlating several syslog files to the time of the reported infection the Windows system could be seen
communicating to the following IP addresses on TCP port 80, Hypertext Transfer Protocol (HTTP):

- 188.116.16.64
- 79.96.7.15
- 107.180.55.21
- 87.98.160.128
- 23.229.187.167

To identify if the IP addresses were associated with the ransomware, the IP addresses were researched using sites www.robtex.com and www.rbls.org. The following information was identified about each site:

188.116.16.64: More than one hundred host names are associated with this IP address. The DNS packets revealed the host name the malware was going to as decrostal.pl. The IP address and hostname are registered in Poland. The site was not flagged as unsafe nor was it on any Registered Block Lists (RBL).

107.180.55.21: More than one hundred host names are associated with this IP address. The DNS packets revealed the host name the malware was going to as iglesiaelrenacer.com. The IP address and hostname are registered to GoDaddy in the US. By visiting the site, it was identified as a site in Canada. This site was not flagged as unsafe but was listed by one RBL for spam.

79.96.5.15: Only one host name was associated with this IP address, lovemydress.pl, this matched what was found in the DNS packet. The IP address and site are registered with a cloud hosting service in Poland. This site was not flagged as unsafe but was listed by one RBL for spam.

87.98.160.128: More than one hundred host names are associated with this IP address. The DNS packets revealed the host name the malware was going to as fmc.org.in. The IP address belongs to a hosting service in France this website is registered to an organization in India. The site was not flagged as unsafe nor was it on any RBL's.

23.229.187.167: More than eighty host names are associated with this IP address. The DNS packets revealed the hostname the malware was going to as mhomeusa.com. The IP address and hostname are registered to GoDaddy in the US. The site was no

Tracy Brockman, tbrockma@verizon.net
Does it come with Networking? longer active after visiting the site. This site was not flagged as unsafe but was listed by one RBL for spam.

Next, the packet captures are analyzed to gather additional information about the event.

4.2. Analyzing the Packets

Analyzing the packet capture, the malware connected twice to each site and tried executing a PHP script. The following TCP streams for IP address 188.116.16.64 (Figure: 12), and 107.180.55.21 (Figure: 13) shows the script the malware tried to launch, csys.php, but the file was not found on either server.

Figure 11: decorstal.pl TCP Stream (188.116.16.64)

Figure 12: iglesiaelrenacer.com TCP Stream (107.180.55.21)

Tracy Brockman, tbrockma@verizon.net
The next TCP stream reviewed was IP address 79.96.5.15 (Figure: 14). Similar to the two previous mentioned sites, it connected to this site twice, this time it was able to find the csys.php script. There was not enough information in packet capture to determine what the purpose of this script was.

Figure 13: lovemydress.pl TCP Stream (79.96.5.15)

Similar to the previous sites, it connected to the following two sites twice, this time it tried to launch a different PHP script. The following TCP streams for IP address 87.98.160.128 (Figure: 16), and 23.229.187.167 (Figure: 17) shows the script the malware tried to launch, mzsys.php, again the file was not found on either server.

Tracy Brockman, tbrockma@verizon.net
Tracy Brockman, tbrockma@verizon.net

Does it come with Networking?

Researching the script file names on Trendmicro.com, this site indicated that csys.php and mzsys.php is associated with the Tesla variant of ransomware.

Lastly, in addition to the Windows system connecting to the above websites twice, there was another similarity identified. The first time the Windows system connected to each website, it had an identical data string in the HTTP packet. A different identical data string was observed in the HTTP packet during the second connection to each website.

**First Data String:**

data=1B6FAB012D2E142F92482B91E44BDCE4DA61B3680105C4E81C2F0EF9BDC97CFB9C3134D40A145FAEC8FBE360C3A58CCC49818EF361EA954CB030A489747
Next, to see if any additional information could be obtained about the malware, the malware was launched in an isolated lab.

### 4.3. Replaying Attack

After interviewing the employee whose system was infected, the file containing the malware executable was identified. The malware file was placed and executed in an isolated lab to see if any additional information about the malware was missed during the initial investigation. Reasons for missing information could be a packet capture filter filtered the traffic, traffic was identified as known good traffic, or an alert was misidentified as a false positive by the security information and event management (SEIM) system. To ensure accuracy in identifying what the malware was doing an isolated lab environment was setup.

#### 4.3.1. Lab Setup

The components utilized in the lab to test this scenario are:

A Windows 7 image will run in VirtualBox. To make sure the malware runs unobstructed the anti-virus and firewall are disabled on the Windows system.

Tracy Brockman, tbrockma@verizon.net
A GNS3 emulated network, running Wireshark.

A bridge network interface between a VirtualBox host-only interface and a host system’s network interface connected to the Internet.

**Figure 16: Scenario 2 Lab**

The Windows 7 image connects to GNS3 via a VirtualBox host-only interface. GNS3 connects to the Internet via the VirtualBox host-only interface that is bridged to the host system’s network interface.

**Figure 17: GNS3 View**

The GNS3 environment emulates the Windows 7 system (IP address 192.168.137.3) connected to a network switch and the switch connected to the Internet. This lab setup allowed the malware to communicate with the C&C servers on the Internet without infecting any other systems. The network traffic during the scan is captured between the network switch (SW1) and the Windows system utilizing Wireshark.

### 4.3.2. Second Review

After launching the malware and letting the system become encrypted, the packet captures are analyzed. First was to examining what IP addresses were observed.

Tracy Brockman, tbrockma@verizon.net
Does it come with Networking?

Figure 18: Hosts 2

The results show that fourteen IP addresses were observed after launching the malware. The five previously identified IP addresses plus nine additional addresses.

Figure 19: TCP Traffic 2

Another observation was the large amounts of TCP traffic incoming from an external IP address 23.67.242.48 to the Windows system.

Figure 20: Resolved Addresses

Tracy Brockman, tbrockma@verizon.net
Wireshark resolved the IP addresses to the following sites by clicking on Analyze > Resolved Addresses. Several sites are registered to Microsoft and Akamai, including 23.67.242.48 [a767.dspw65.akami.net]. These sites normally deliver Windows and other application updates.

Figure 21: Windows Download

After, further review of the traffic between the two hosts was identified as Microsoft updates. During the initial review, no downloads were observed between the websites and the Windows system, so it is assumed the malware initiated a Microsoft update because it needed an update to complete the encryption process.

Next, reviewing the UDP traffic, there were a series communications on port 53, DNS between the Windows system and a Google DNS server 8.8.4.4. The Windows update and DNS traffic were filtered from the initial captures because this traffic is considered normal traffic.

Figure 22: DNS Traffic

Tracy Brockman, tbrockma@verizon.net
After reviewing the traffic, it was indeed a series of DNS queries. There appeared to be one more site the malware attempted to communicate with, csopedro.org, but the DNS query was unable to return an address for this site (Figure 23).

![Figure 23: csopedro.org DNS query](image)

Since the site is no longer available, it can only be assumed this was another site that had hosted a PHP script.

To see if the PHP scripts contained any additional information the PHP files were extracted from the packet capture. To extract an object from a capture click on File > Extract Object > and select the object type. After reviewing, the extracted files only contained the same data strings shown in the initial review. It can only be assumed that the data strings captured could have been the public encryption key used to encrypt the files. The public key is one part of an asymmetric key exchange the other part is a private key. The public key is used to encrypt the data, and the private key is needed to decrypt the data. Ransomware uses asymmetric key encryption method when encrypting the files on a machine. (Trend Micro, n.d.)

Finally, after reviewing all five sites and the information extracted from the packet captures, the following assumptions are made:

- The malware is becoming less effective with the PHP file only being found on one site the remaining owners remediated the compromise on their site.

Tracy Brockman, tbrockma@verizon.net
• Four of the websites appeared to be legitimate sites, while the remaining website was no longer active. Because the sites appeared to be legitimate it could indicate that the owners of the websites were unaware their sites were compromised and being used as part of a malware attack.
• Based on the first two assumptions, none of the sites was the actual attacker.

4.4. Summary
This scenario demonstrated while analyzing a pcap file in a standalone lab can provide information on a security attack it only gives a snapshot view of what may be happening. A more holistic view was observed by replaying the attack in the isolated lab, and additional information was obtained. In this case, it was determined no other attack or data exfiltration occur during the event.

5. Conclusion
This paper demonstrated by having a lab environment that utilizes GNS3, a security professional can have a complete view of an attack or other incidents. GNS3 provides a customizable and inexpensive solution for establishing a controlled environment for testing theories, performing network forensics, testing new configurations, or for training. GNS3 is a versatile tool that enhances any security professional's arsenal of tools.

Tracy Brockman, tbrockma@verizon.net
References


Tracy Brockman, tbrockma@verizon.net
importance-of-command-and-control-analysis-for-incident-response - (Soni, 2014)


### Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS vLive - SEC503: Intrusion Detection In-Depth</td>
<td>SEC503 - 202008,</td>
<td>Aug 10, 2020 - Sep 16, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Essentials Live Online 2020</td>
<td>Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020 - Live Online</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Network Security 2020 - Live Online</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS October Singapore 2020 - Live Online</td>
<td>Singapore, Singapore</td>
<td>Oct 12, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London October 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Oct 12, 2020 - Oct 17, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020 - Live Online</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020</td>
<td>London, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London November 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020 - Live Online</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defense Initiative 2020 - Live Online</td>
<td>Washington, DC</td>
<td>Dec 14, 2020 - Dec 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>