Global Information Assurance Certification Paper

Does it come with Networking?

GIAC (GCIA) Gold Certification

Author: Tracy Brockman, tbrockma@verizon.net
Advisor: Rick Wanner
Accepted: February 17, 2017

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.

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

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

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.

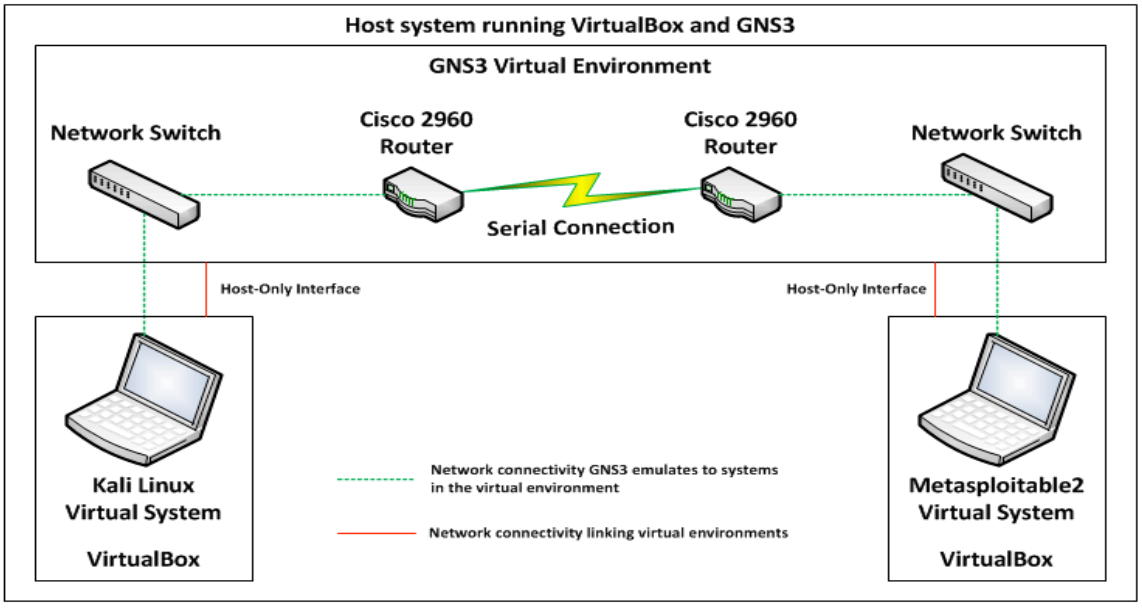


Figure 1: Scenario 1 Lab Setup

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.

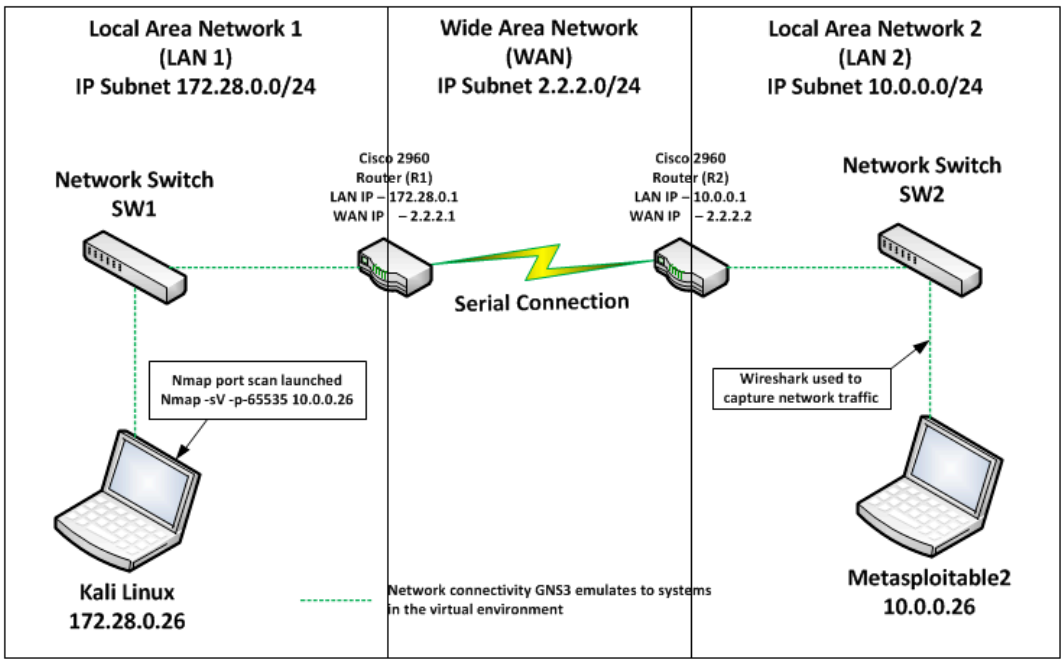


Figure 2: Scenario 1 Lab Configuration

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).

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
◢ Frame	100.0	133167	100.0	7506853	67 k	0	0	0
◢ Ethernet	100.0	133167	24.8	1864338	16 k	0	0	0
▷ Logical-Link Control	0.0	15	0.1	5565	49	0	0	0
◢ Internet Protocol Version 4	100.0	133121	35.5	2662420	23 k	0	0	0
▷ User Datagram Protocol	0.1	84	0.0	672	6	0	0	0
▷ Transmission Control Protocol	99.9	132999	39.5	2962919	26 k	132843	2946676	26 k
Internet Control Message Protocol	0.0	38	0.0	1280	11	38	1280	11
Data	0.0	53	0.0	3276	29	53	3276	29
Address Resolution Protocol	0.0	30	0.0	840	7	30	840	7

Figure 3: Protocol Hierarchy

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.

Ethernet · 4 | IPv4 · 4 | IPv6 | TCP · 66114 | UDP · 18

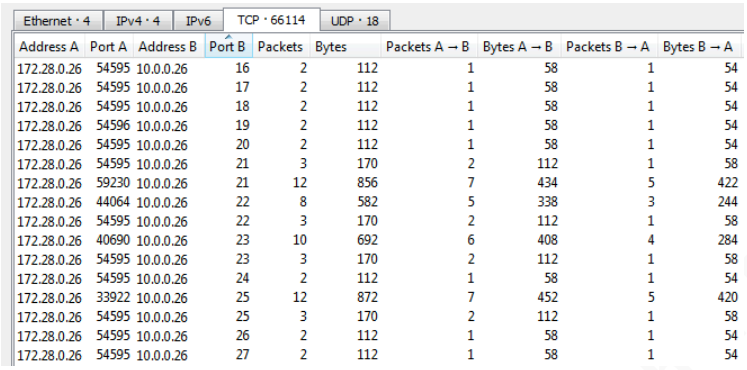
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
2.2.2.1	10.0.0.26	34	2380	34	2380	0	0	725.736590	161.6712	117	0
8.8.8.8	10.0.0.26	34	2844	0	0	34	2844	725.422614	161.9646	0	140
10.0.0.26	172.28.0.26	133,003	7485 k	66,437	3614 k	66,566	3871 k	8.711343	883.6769	32 k	35 k
10.0.0.26	10.0.0.255	50	9170	50	9170	0	0	65.684579	705.3720	104	0

Figure 4: Hosts

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.



Ethernet · 4 | IPv4 · 4 | IPv6 | TCP · 66114 | UDP · 18

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
172.28.0.26	54595	10.0.0.26	16	2	112	1	58	1	54
172.28.0.26	54595	10.0.0.26	17	2	112	1	58	1	54
172.28.0.26	54595	10.0.0.26	18	2	112	1	58	1	54
172.28.0.26	54596	10.0.0.26	19	2	112	1	58	1	54
172.28.0.26	54595	10.0.0.26	20	2	112	1	58	1	54
172.28.0.26	54595	10.0.0.26	21	3	170	2	112	1	58
172.28.0.26	59230	10.0.0.26	21	12	856	7	434	5	422
172.28.0.26	44064	10.0.0.26	22	8	582	5	338	3	244
172.28.0.26	54595	10.0.0.26	22	3	170	2	112	1	58
172.28.0.26	40690	10.0.0.26	23	10	692	6	408	4	284
172.28.0.26	54595	10.0.0.26	23	3	170	2	112	1	58
172.28.0.26	54595	10.0.0.26	24	2	112	1	58	1	54
172.28.0.26	33922	10.0.0.26	25	12	872	7	452	5	420
172.28.0.26	54595	10.0.0.26	25	3	170	2	112	1	58
172.28.0.26	54595	10.0.0.26	26	2	112	1	58	1	54
172.28.0.26	54595	10.0.0.26	27	2	112	1	58	1	54

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)

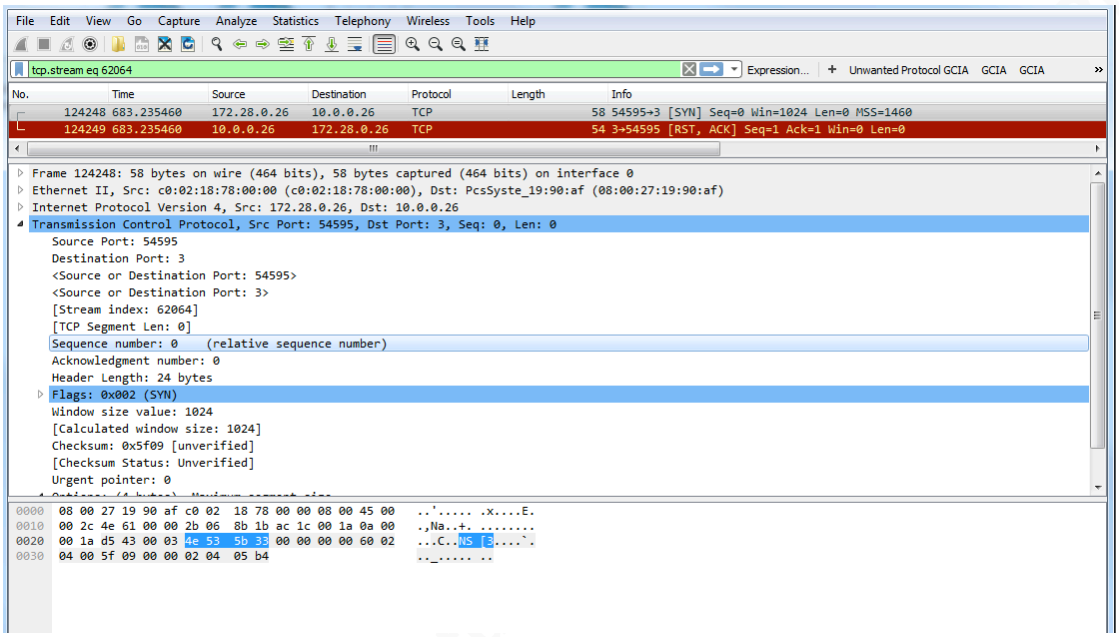


Figure 6: ISN

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:

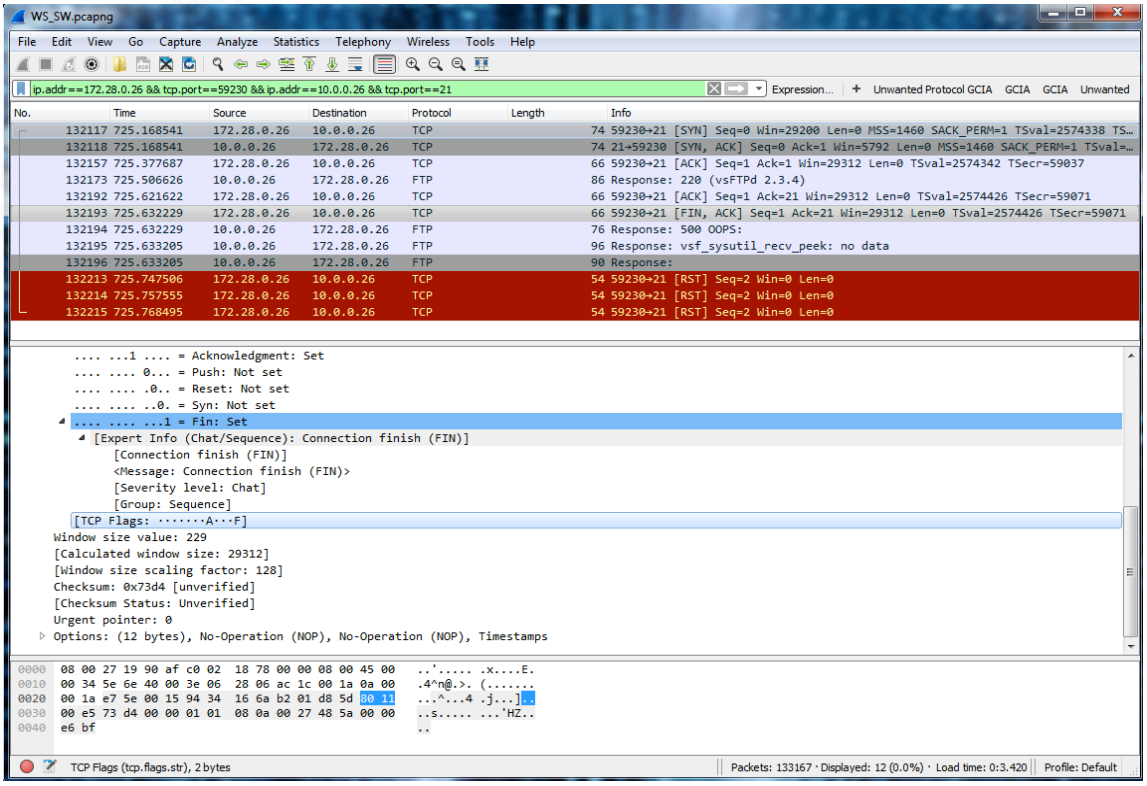


Figure 7: FTP Traffic

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.

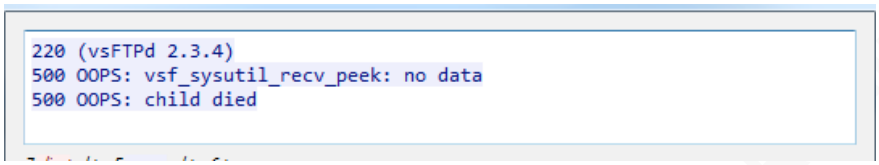


Figure 8: FTP Stream

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:

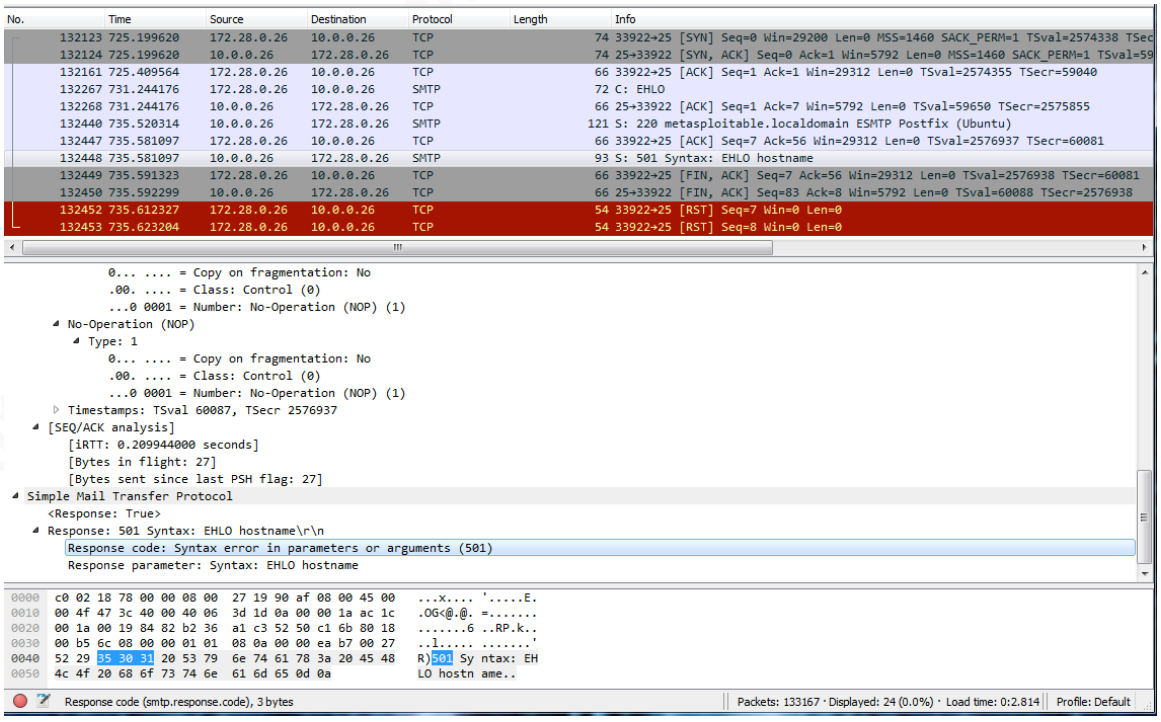


Figure 9: SMTP Traffic

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.

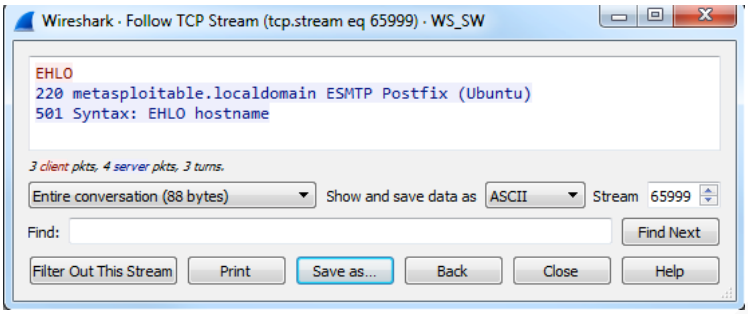


Figure 10: SMTP Stream

Kali then sent an EHLO \r\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 reviled 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 reviled 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

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.

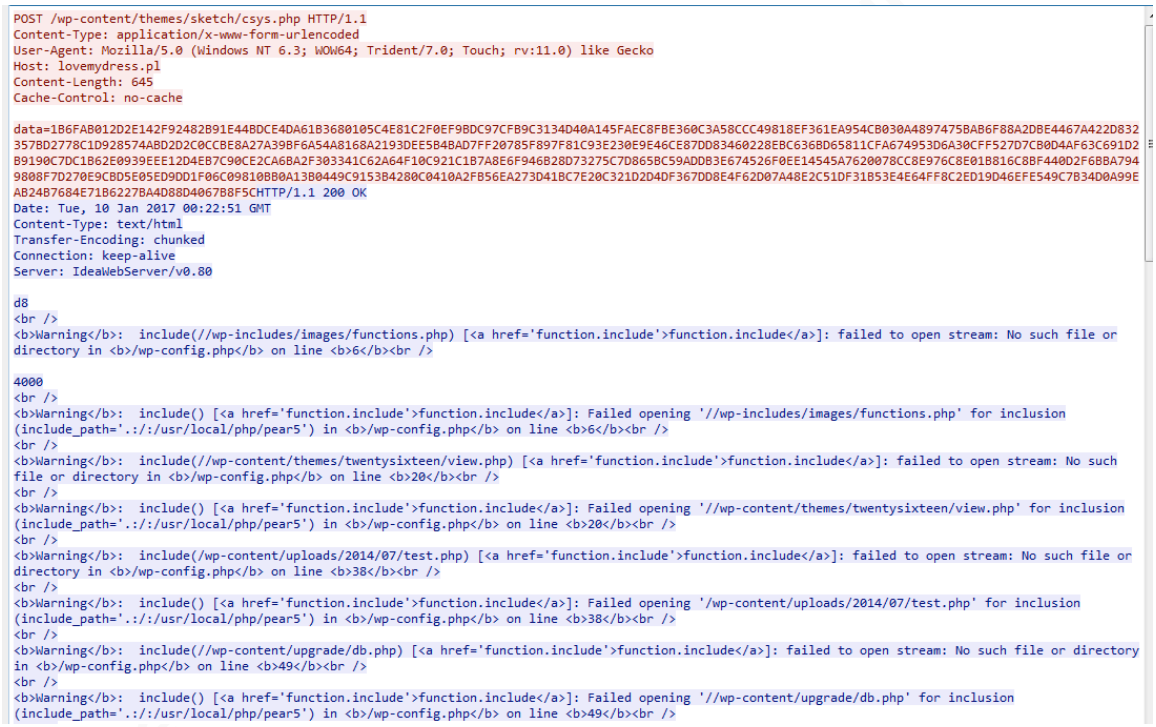
```
POST /jscripts/jsgaleria/csys.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: decorstal.pl
Content-Length: 645
Cache-Control: no-cache

data=1B6FAB012D2E142F92482B91E44BDCE4DA61B3680105C4E81C2F0EF9BDC97CFB9C3134D40A145FAEC8FBE360C3A58CCC49818EF361EA954CB030A4897475BAB6F88A
2DBE4467A422D832357BD2778C1D928574ABD2D2C0CCBE8A27A39BF6A54A8168A2193DEE5B4BAD7FF20785F897F81C93E230E9E46CE87DD83460228EBC636BD65811CFA67
4953D6A30CFF527D7CB0D4AF63C691D2B9190C7DC1B62E0939EEE12D4EB7C90CE2CA6BA2F303341C62A64F10C921C1B7A8E6F946B28D73275C7D865BC59ADDB3E674526F0
EE14545A7620078CC8E976C8E01B816C8BF440D2F6BBA7949808F7D270E9CBD5E05ED9DD1F06C09810BB0A13B0449C9153B4280C0410A2FB56EA273D41BC7E20C321D2D4D
F367DD8E4F62D07A48E2C51DF31B53E4E64FF8C2ED19D46EFE549C7B34D0A99EAB24B7684E71B6227BA4D88D4067B8F5CHTTP/1.1 404 Not Found
Content-Type: text/html
Content-Length: 495
Date: Tue, 10 Jan 2017 00:22:48 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
The requested URL /jscripts/jsgaleria/csys.php was not found on this server.
<HR>
<I>decorstal.pl</I>
</BODY></HTML>
```

Figure 11: decorstal.pl TCP Stream (188.116.16.64)

```
POST /modules/mod_stats/csys.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: iglesiaelrenacer.com
Content-Length: 645
Cache-Control: no-cache

data=1B6FAB012D2E142F92482B91E44BDCE4DA61B3680105C4E81C2F0EF9BDC97CFB9C3134D40A145FAEC8FBE360C3A58CCC49818EF361EA954CB030A4897475BAB6F88A
2DBE4467A422D832357BD2778C1D928574ABD2D2C0CCBE8A27A39BF6A54A8168A2193DEE5B4BAD7FF20785F897F81C93E230E9E46CE87DD83460228EBC636BD65811CFA67
4953D6A30CFF527D7CB0D4AF63C691D2B9190C7DC1B62E0939EEE12D4EB7C90CE2CA6BA2F303341C62A64F10C921C1B7A8E6F946B28D73275C7D865BC59ADDB3E674526F0
EE14545A7620078CC8E976C8E01B816C8BF440D2F6BBA7949808F7D270E9CBD5E05ED9DD1F06C09810BB0A13B0449C9153B4280C0410A2FB56EA273D41BC7E20C321D2D4D
F367DD8E4F62D07A48E2C51DF31B53E4E64FF8C2ED19D46EFE549C7B34D0A99EAB24B7684E71B6227BA4D88D4067B8F5CHTTP/1.1 404 Page not found
Date: Tue, 10 Jan 2017 00:22:49 GMT
Server: Apache/2.4.23
X-Powered-By: PHP/5.6.27
Cache-Control: no-cache
Pragma: no-cache
Set-Cookie: fa64bc26bd1c7448efdc072568342262=vaa3a4331fs7uqna4vvs77aqd7; path=/; HttpOnly
Set-Cookie: 1a95b95d1721c248720d8dd8db1b03ec=en-GB; path=/
Vary: Accept-Encoding,User-Agent
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

544b
<!DOCTYPE html>
<html lang="en-gb" dir="ltr">


<head>
            <meta name="viewport" content="width=device-width, initial-scale=1.0">
Packet 17937. 3 client pkts, 6 server pkts, 3 turns. Click to select.
```

Figure 12: iglesiaelrenacer.com TCP Stream (107.180.55.21)

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.



```
POST /wp-content/themes/sketch/csys.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: lovemydress.pl
Content-Length: 645
Cache-Control: no-cache

data=1B6FAB012D2E142F92482B91E44BDCE4DA61B3680105C4E81C2F0EF9BDC97CFB9C3134D40A145FAEC8FBE360C3A58CCC49818EF361EA954CB030A4897475BAB6F88A2DBE4467A422D832
357BD2778C1D928574ABD2D2C0CCBE8A27A39BF6A54A8168A2193DEE5B4BAD7FF20785F897F81C93E230E9E46CE87DD83460228EBC636BD65811CFA674953D6A30CFF527D7CB0D4AF63C691D2
B9190C7DC1B62E0939EEE12D4EB7C90CE2CA6BA2F303341C62A64F10C921C1B7A8E6F946B28D73275C7D865BC59ADDB3E674526F0EE14545A7620078CC8E976C8E01B816C8BF440D2F6BBA794
9808F7D270E9CBD5E05ED9DD1F06C09810BB0A13B0449C9153B4280C0410A2FB56EA273D41BC7E20C321D2D4DF367DD8E4F62D07A48E2C51DF31B53E4E64FF8C2ED19D46EFE549C7B34D0A99E
AB24B7684E71B6227BA4D88D4067B8F5CHTTP/1.1 200 OK
Date: Tue, 10 Jan 2017 00:22:51 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: IdeaWebServer/v0.80

d8
<br />
<b>Warning</b>:  include(//wp-includes/images/functions.php) [<a href='function.include'>function.include</a>]: failed to open stream: No such file or
directory in <b>/wp-config.php</b> on line <b>6</b><br />

4000
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.include</a>]: Failed opening '//wp-includes/images/functions.php' for inclusion
(include_path='.:/:/usr/local/php/pear5') in <b>/wp-config.php</b> on line <b>6</b><br />
<br />
<b>Warning</b>:  include(//wp-content/themes/twentysixteen/view.php) [<a href='function.include'>function.include</a>]: failed to open stream: No such
file or directory in <b>/wp-config.php</b> on line <b>20</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.include</a>]: Failed opening '//wp-content/themes/twentysixteen/view.php' for inclusion
(include_path='.:/:/usr/local/php/pear5') in <b>/wp-config.php</b> on line <b>20</b><br />
<br />
<b>Warning</b>:  include(/wp-content/uploads/2014/07/test.php) [<a href='function.include'>function.include</a>]: failed to open stream: No such file or
directory in <b>/wp-config.php</b> on line <b>38</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.include</a>]: Failed opening '/wp-content/uploads/2014/07/test.php' for inclusion
(include_path='.:/:/usr/local/php/pear5') in <b>/wp-config.php</b> on line <b>38</b><br />
<br />
<b>Warning</b>:  include(//wp-content/upgrade/db.php) [<a href='function.include'>function.include</a>]: failed to open stream: No such file or directory
in <b>/wp-config.php</b> on line <b>49</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.include</a>]: Failed opening '//wp-content/upgrade/db.php' for inclusion
(include_path='.:/:/usr/local/php/pear5') in <b>/wp-config.php</b> on line <b>49</b><br />
```

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.

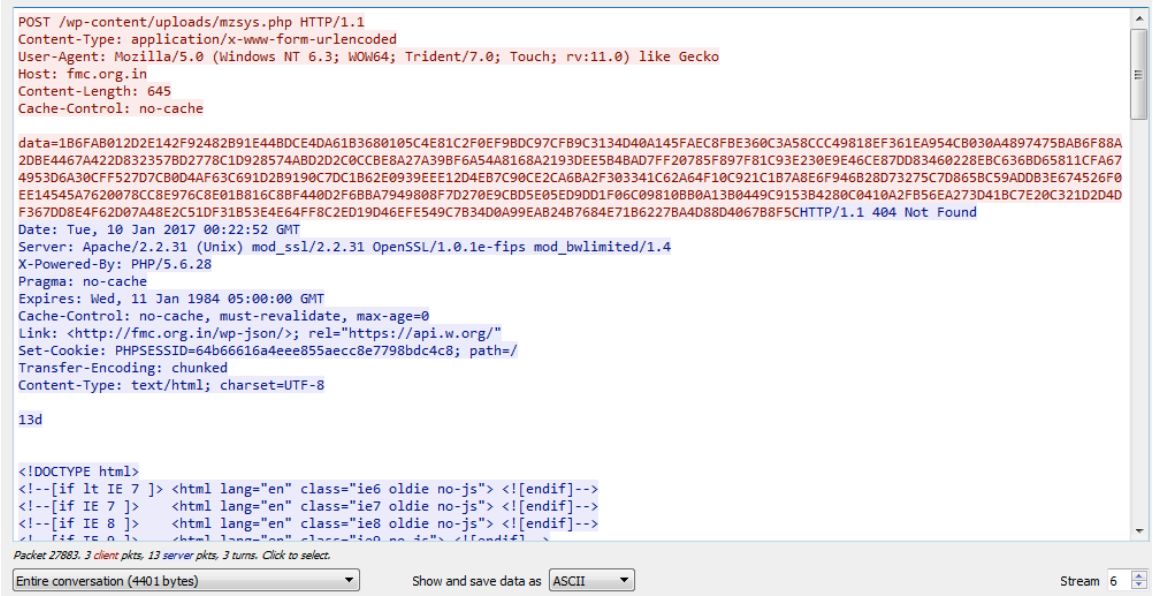


Figure 14: fmc.org.in TCP Stream (87.98.160.128)

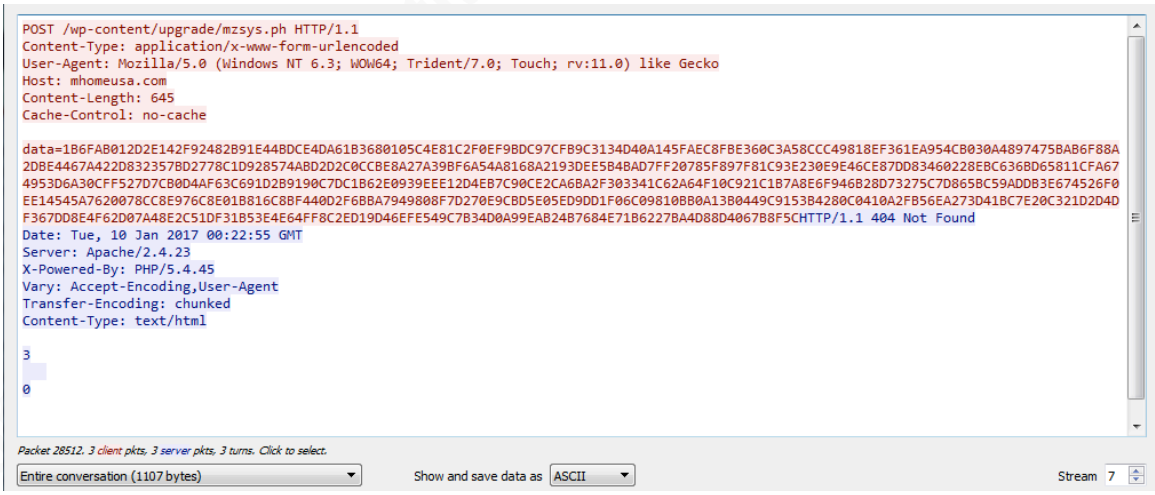


Figure 15: mhomeusa.com TCP Stream (23.229.187.167)

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=1B6FAB012D2E142F92482B91E44BDCE4DA61B3680105C4E81C2F0EF9BDC
97CFB9C3134D40A145FAEC8FBE360C3A58CCC49818EF361EA954CB030A489747

Tracy Brockman, tbrockma@verizon.net

5BAB6F88A2DBE4467A422D832357BD2778C1D928574ABD2D2C0CCBE8A27A39
BF6A54A8168A2193DEE5B4BAD7FF20785F897F81C93E230E9E46CE87DD834602
28EBC636BD65811CFA674953D6A30CFF527D7CB0D4AF63C691D2B9190C7DC1B
62E0939EEE12D4EB7C90CE2CA6BA2F303341C62A64F10C921C1B7A8E6F946B28
D73275C7D865BC59ADDB3E674526F0EE14545A7620078CC8E976C8E01B816C8B
F440D2F6BBA7949808F7D270E9CBD5E05ED9DD1F06C09810BB0A13B0449C9153
B4280C0410A2FB56EA273D41BC7E20C321D2D4DF367DD8E4F62D07A48E2C51D
F31B53E4E64FF8C2ED19D46EFE549C7B34D0A99EAB24B7684E71B6227BA4D88
D4067B8F5C

Second Data String:

data=FF982F7A97833388A40909A5E1EBAEE2C1AE4C6A15FBB8D18C8D6131F4D
CE8E28597D489FBC837502067C26DE0BE69BE9372A0FB0B531600E432AA63E546
F5879D6FDB74250A57D71C1D04507F7D423090FA91AA837B9A4C493E2C7D58BC
83CD1EC6232BF43A9A7D8A93F6B24A0C6AB97A666A0D9FCB54CE9D810174FC
049DF4E479FC8580943E26DF50E0FD1B714BFBA552184E15FB05D4D24CF4A642
AD6D0683FA9E52E286CFD84496C2B881E97CD67D56C045AADB3E3ECDD47BB1
FEF37D866C79B207F02C0B599A56CE211078E33ABF47669C770431D3516C35D97
0DEA5DBB0221710825267C57A4FCA7F39E26595D6645642A5B7AA2B588C8CEB1
57612B6A31ACC9F06CDAE54BCD4D9EBA2C5E2C015C26883BF495B8CA4FDDA
0CEBF85EEBD6C163D7FD186D41E0461ADE295EBBB83538D81A3A0B62FB297F7
B0656D51439

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.

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.

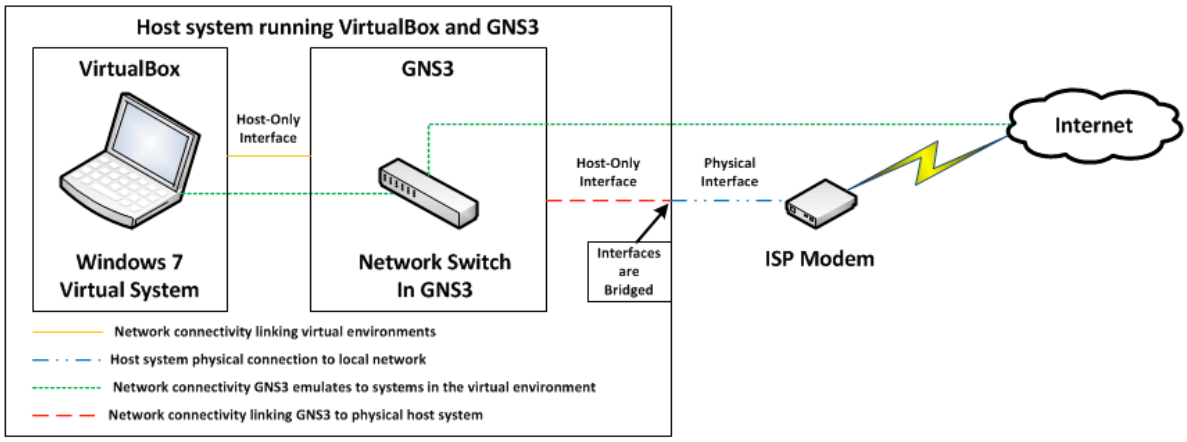


Figure 16: Scenario 2 Lab

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.

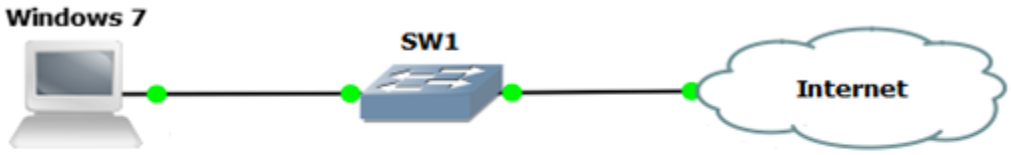


Figure 17: GNS3 View

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.

Ethernet · 1 | IPv4 · 12 | IPv6 | TCP · 17 | UDP · 14

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
8.8.4.4	192.168.137.3	28	3475	14	2361	14	1114	59.520128	512.0187	36	17
23.2.81.150	192.168.137.3	12	2800	6	2323	6	477	365.470841	29.3691	632	129
23.67.242.48	192.168.137.3	118,454	145 M	95,294	144 M	23,160	1284 k	59.627097	240.9388	4784 k	42 k
23.67.242.49	192.168.137.3	39	28 k	23	26 k	16	1809	62.475163	118.0969	1784	122
23.229.187.167	192.168.137.3	19	3512	8	1092	11	2420	107.062597	410.3223	21	47
65.52.108.154	192.168.137.3	24	7617	10	5976	14	1641	360.130067	66.0144	724	198
72.21.81.200	192.168.137.3	13	1775	6	1070	7	705	571.541775	15.0333	569	375
79.96.7.15	192.168.137.3	47	31 k	24	28 k	23	3072	100.171124	411.6097	551	59
87.98.160.128	192.168.137.3	38	9397	23	5829	15	3568	104.102275	412.9506	112	69
107.180.55.21	192.168.137.3	24	14 k	12	12 k	12	2585	101.092823	410.9633	240	50
134.170.58.222	192.168.137.3	159	132 k	91	99 k	68	33 k	65.318348	72.0055	11 k	3765
188.116.16.64	192.168.137.3	20	4246	10	1892	10	2354	99.652376	411.3755	36	45

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.

Ethernet · 1 | IPv4 · 12 | IPv6 | TCP · 17 | UDP · 14

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.137.3	49169	23.67.242.48	80	118,454	145 M	23,160	1284 k	95,294	144 M	59.627097	240.9388	42 k	4784 k
192.168.137.3	49170	23.67.242.49	80	39	28 k	16	1809	23	26 k	62.475163	118.0969	122	1784
192.168.137.3	49171	134.170.58.222	443	159	132 k	68	33 k	91	99 k	65.318348	72.0055	3765	11 k
192.168.137.3	49172	188.116.16.64	80	10	2123	5	1177	5	946	99.652376	0.4537	20 k	16 k
192.168.137.3	49173	79.96.7.15	80	20	14 k	9	1401	11	12 k	100.171124	0.8777	12 k	115 k
192.168.137.3	49174	107.180.55.21	80	11	7360	5	1184	6	6176	101.092823	0.4225	22 k	116 k
192.168.137.3	49175	87.98.160.128	80	19	6357	6	2124	13	4233	104.102275	2.9134	5832	11 k
192.168.137.3	49176	23.229.187.167	80	12	2003	7	1297	5	706	107.062597	403.8627	25	13
192.168.137.3	49177	65.52.108.154	80	7	766	5	539	2	227	360.130067	66.0144	65	27
192.168.137.3	49178	65.52.108.154	443	17	6851	9	1102	8	5749	362.744389	63.4000	139	725
192.168.137.3	49179	23.2.81.150	80	12	2800	6	477	6	2323	365.470841	29.3691	129	632
192.168.137.3	49181	188.116.16.64	80	10	2123	5	1177	5	946	510.619005	0.4089	23 k	18 k
192.168.137.3	49182	79.96.7.15	80	27	17 k	14	1671	13	15 k	510.926290	0.8546	15 k	146 k
192.168.137.3	49183	107.180.55.21	80	13	7577	7	1401	6	6176	511.778917	0.2772	40 k	178 k
192.168.137.3	49184	87.98.160.128	80	19	3040	9	1444	10	1596	514.303938	2.7490	4202	4644
192.168.137.3	49185	23.229.187.167	80	7	1509	4	1123	3	386	517.024696	0.3602	24 k	8572
192.168.137.3	49186	72.21.81.200	80	13	1775	7	705	6	1070	571.541775	15.0333	375	569

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.

```
# Hosts
#
# 14 entries.

188.116.16.64   decorstal.pl
23.67.242.49    a767.dspw65.akamai.net
23.67.242.48    a767.dspw65.akamai.net
65.55.50.189    www.update.microsoft.com.nsatc.net
23.229.187.167  mhomeusa.com
65.52.108.154   legacy.watson.data.microsoft.com.akadns.net
134.170.58.222  www.update.microsoft.com.nsatc.net
79.96.7.15      lovemydress.pl
23.67.242.72    a767.dspw65.akamai.net
87.98.160.128   fmc.org.in
23.2.81.150     e1863.dspb.akamaiedge.net
107.180.55.21   iglesiaelrenacer.com
23.67.242.65    a767.dspw65.akamai.net
72.21.81.200    cs9.wpc.v0cdn.net
```

Figure 20: Resolved Addresses

Tracy Brockman, tbrockma@verizon.net

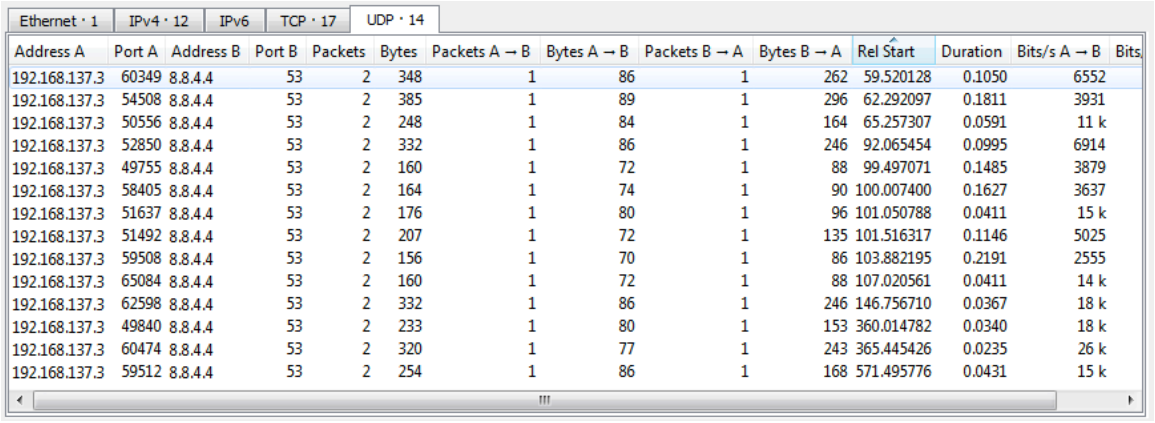
Wireshark resolved the IP addresses to the following sites by clicking on Analyze > Resolved Addresses. Several sites are registered to Microsoft and Akamai, including 23.67.242.48 [a767.dspw65.akami.net]. These sites normally deliver Windows and other application updates.

```
HEAD /v9/1/windowsupdate/redir/muv4wuredir.cab?1701100022 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Windows-Update-Agent
Host: download.windowsupdate.com

HTTP/1.1 200 OK
Content-Length: 23612
Content-Type: application/octet-stream
Last-Modified: Mon, 12 May 2014 21:56:34 GMT
Accept-Ranges: bytes
ETag: "6de593a2d6ecf1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 10 Jan 2017 00:22:08 GMT
Connection: keep-alive
X-CCC: US
X-CID: 2

GET /c/msdownload/update/others/2017/01/23883154_762caf2e31785f267fa47155b4c20f63e3233b80.cab HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Windows-Update-Agent
Host: download.windowsupdate.com
```

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.



Ethernet · 1 | IPv4 · 12 | IPv6 | TCP · 17 | UDP · 14

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits
192.168.137.3	60349	8.8.4.4	53	2	348	1	86	1	262	59.520128	0.1050	6552	
192.168.137.3	54508	8.8.4.4	53	2	385	1	89	1	296	62.292097	0.1811	3931	
192.168.137.3	50556	8.8.4.4	53	2	248	1	84	1	164	65.257307	0.0591	11 k	
192.168.137.3	52850	8.8.4.4	53	2	332	1	86	1	246	92.065454	0.0995	6914	
192.168.137.3	49755	8.8.4.4	53	2	160	1	72	1	88	99.497071	0.1485	3879	
192.168.137.3	58405	8.8.4.4	53	2	164	1	74	1	90	100.007400	0.1627	3637	
192.168.137.3	51637	8.8.4.4	53	2	176	1	80	1	96	101.050788	0.0411	15 k	
192.168.137.3	51492	8.8.4.4	53	2	207	1	72	1	135	101.516317	0.1146	5025	
192.168.137.3	59508	8.8.4.4	53	2	156	1	70	1	86	103.882195	0.2191	2555	
192.168.137.3	65084	8.8.4.4	53	2	160	1	72	1	88	107.020561	0.0411	14 k	
192.168.137.3	62598	8.8.4.4	53	2	332	1	86	1	246	146.756710	0.0367	18 k	
192.168.137.3	49840	8.8.4.4	53	2	233	1	80	1	153	360.014782	0.0340	18 k	
192.168.137.3	60474	8.8.4.4	53	2	320	1	77	1	243	365.445426	0.0235	26 k	
192.168.137.3	59512	8.8.4.4	53	2	254	1	86	1	168	571.495776	0.0431	15 k	

Figure 22: DNS Traffic

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).

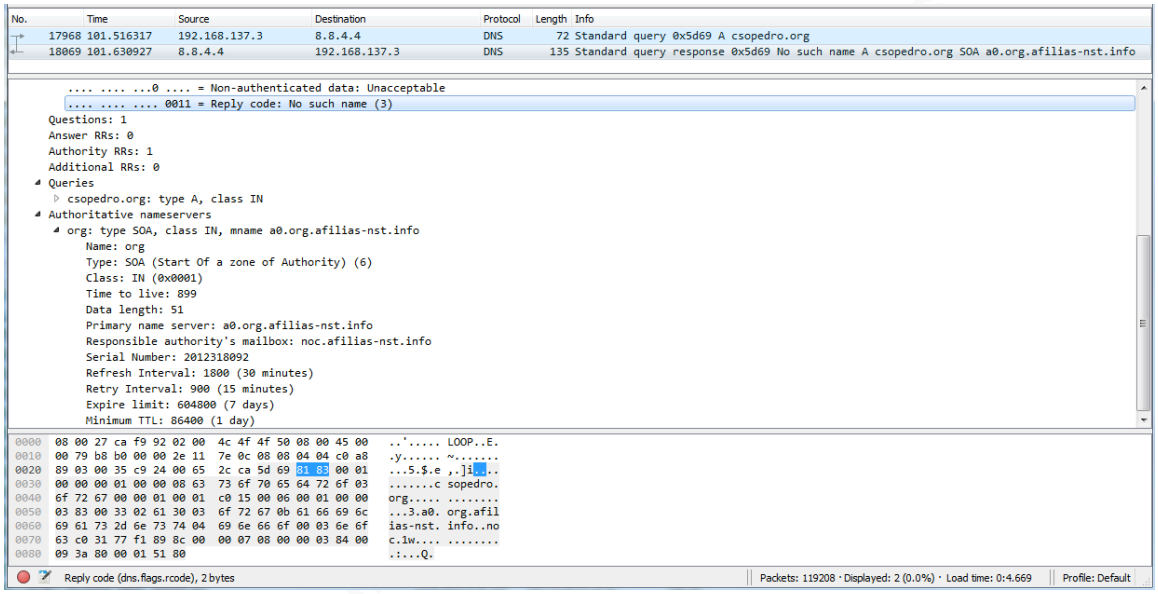


Figure 23: csopedro.org DNS query

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

Fogarty, S. (2015, March 2). *GNS3 Network Simulator Raises Its Game | Network Computing*. Retrieved from http://www.networkcomputing.com/networking/gns3-network-simulator-raises-its-game/1498033019

GNS3. (n.d.). GNS3 | The software that empowers network professionals. Retrieved January 10, 2017, from https://gns3.com/marketplace

Gregg, M. (2008). Hardware and Gear. In Build your own security lab: A field guide for network testing (p. 1). Indianapolis, IN: Wiley.

Hdmoore, & Egypt. (n.d.). *Metasploitable 2 Exploitability Guide* | Rapid7 Community and Blog. Retrieved January 7, 2017, from https://community.rapid7.com/docs/DOC-1875

ISACA. (2016). Cybersecurity Fundamentals Glossary. Retrieved from https://www.isaca.org/Knowledge-Center/Documents

Lyon, G. F. (2008). Preface. In Nmap network scanning: Official Nmap project guide to network discovery and security scanning (p. xxi). Sunnyvale, CA: Insecure.Com, LLC.

Offensive Security. (n.d.). Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. Retrieved January 10, 2017, from http://www.kali.org

Oracle. (n.d.). VirtualBox – Oracle VM VirtualBox. Retrieved January 7, 2017, from https://www.virtualbox.org/wiki/VirtualBox

Soni, A. (2014, March 31). *SANS Digital Forensics and Incident Response Blog | The Importance of Command and Control Analysis for Incident Response* | SANS Institute. Retrieved from https://digital-forensics.sans.org/blog/2014/03/31/the-

importance-of-command-and-control-analysis-for-incident-response - (Soni, 2014)

The SANS Institute. (2016). *Security 503: Intrusion Detection In-Depth* (Books 1-6)

Trend Micro. (n.d.) Ransomware - Definition - Trend Micro USA. Retrieved January 12, 2017, from https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Tracy Brockman, tbrockma@verizon.net