2015

# At the Gates: Analysis of Malicious Activity Facing Residential IP Addresses

Alexander Hershey
*Grand Valley State University*

# *At the Gates*: Analysis of Malicious Activity Facing Residential IP Addresses

By
Alex Hershey
April 2015

# *At the Gates*: Analysis of Malicious Activity Facing Residential IP Addresses

By
Alex Hershey

A project submitted in partial fulfillment of the requirements for the degree of

Master of Science in

Computer Information Systems

At
Grand Valley State University

April 2015

Dr. Andrew Kalafut
**Professor**

April 2015
**Date**

# Table of Contents

## Abstract

The prevalence and permeation of technology in business has allowed for new and very creative ways to steal. With data breaches becoming more common (and more publicized), many people are aware of the threats that large companies face. However, the digital threats that a normal person faces are not as apparent. While many stories exist of people using technology to threaten or harass others, many are not necessarily aware of the threats these large scale data thieves pose to those who just simply own an always-on internet connection. This project was conceived as a way to see what threatens the common user. Using SecurityOnion, ESXI, and an unpatched operating system a simple network intrusion detection system was created to capture the reconnaissance traffic being sent to a residential IP address.

The usage of ESXI allows for fast deployment of new exploitable systems as well as easy packet capture with virtual switches. SecurityOnion was used due to its' ease of use and detailed tutorials. An unpatched, unregistered, and unprotected (no firewall or antivirus) copy of Windows XP was used as the honeypot. All unsolicited packets from unknown IP addresses were then analyzed for country of origin to gain statistics on where attackers are coming from (or rather where they wish to be seen coming from), as well as to see the most common ports that were being scanned for.


## Introduction

As per the 2014 Verizon Data breach report, there were 1,367 confirmed data breaches in 2013. This number is considered to be an underestimation of the true number of data breaches, as the report points out is based only on incidents companies were willing to discuss.

The 2015 Verizon Data Breach Report lists 2,122 data breaches for 2014. The reports both point to increasing sophistication for the attacks that were reported as well.

This leads to the main question that drove the project: With the availability of automated scanning tools, what does an IP address not listed on any DNS have to worry about from a malicious attacker? This lead to the next question: How does one track that potential activity? This project had two ways of trying to detect that activity. One strictly involved the use of a research honeypot (Windows XP) exposed to the web with no firewall or antivirus. This configuration did not rely on network monitoring to identify threats. Later, a NIDS was used to see what was attempting to interact with the honeypot.

## Background and Related Work

Honeypots refer to any host placed on a network to attract attention in order to distract attackers from truly valuable targets. Virtual Appliances such as Honeydrive offer a suite of preconfigured options for deploying honeypots with built in monitoring rapidly over a virtual environment. However, Windows XP was used as the honeypot due to XP's notoriety in attracting unwanted attention.

For the intrusion detection system, a network based intrusion detection system was used as opposed to a host based on my desire to modify the honeypot as little as possible. For that, I used the SecurityOnion Linux distribution which uses Snort in order to capture packets for later analysis.

## Project Requirements

The main requirement for this project was to be able to retrieve data from a potentially compromised operating system in order to analyze malware that had infected this system. The next objective was to provide a mechanism for redeploying a new honeypot as soon as the old host had become too corrupted (or if the malware was exhibiting more dangerous behavior such as pinging other systems to infect). These two project requirements could only be effectively met was with the use of virtual server. As the project progressed, a new requirement was added; all inbound network activity directed towards the honeypot was captured and logged in a human readable format. The addition of this element greatly increased the minimum hardware requirements as well.

## Implementation

While the above seems fairly straightforward, this was the end result of some trial and error. The project had three key phases for each of the methods used, which will be referred to as the “Non-IDS” and “IDS” attempt. These phases were divided as follows;

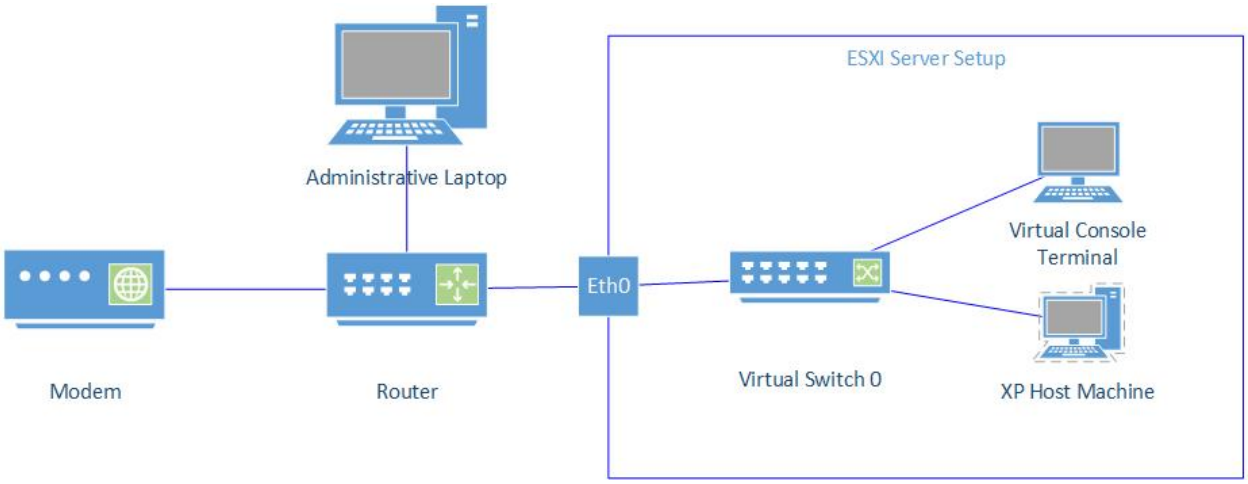
1. Hardware configuration;
2. Virtual server configuration; and
3. Results monitoring.

Hardware configuration referred to the setup of the hardware used to host the ESXI server, the installation of the ESXI software, as well as the configuration of the router. Virtual server

configuration involved the installation of the virtual appliances (Honeydrive), the honeypot, the NIDS, and the virtual switches within the ESXI host. The results monitoring involved;

- Periodic scans of the honeypot in the non-IDS attempt; and
- Periodic analysis of network data using Snorby and Elsa within the SecurityOnion OS for the IDS attempts.

**Non-IDS Attempt**




**Hardware Configuration**

The original project idea began as a way to try to analyze malware that attacked unprotected systems that were not actively accessing the internet. Based on the earlier design decisions, ESXI was installed on ProLiant DL365 G1 server. This allowed for the use of 20 GB of ram, 300GB HDD, dual 2.2GHZ Opteron processors, and up to 5 separate wired Ethernet connections to the router. As this was former datacenter equipment, the system required a HP Service Pack install unique to ESXI before the OS could be installed. ESXI was then successfully

installed on the server. The model of router used was an Asus RT-N66R. This model is equipped with a DMZ feature which forwards all incoming packets to a specific host machine.

## Virtual Server Configuration

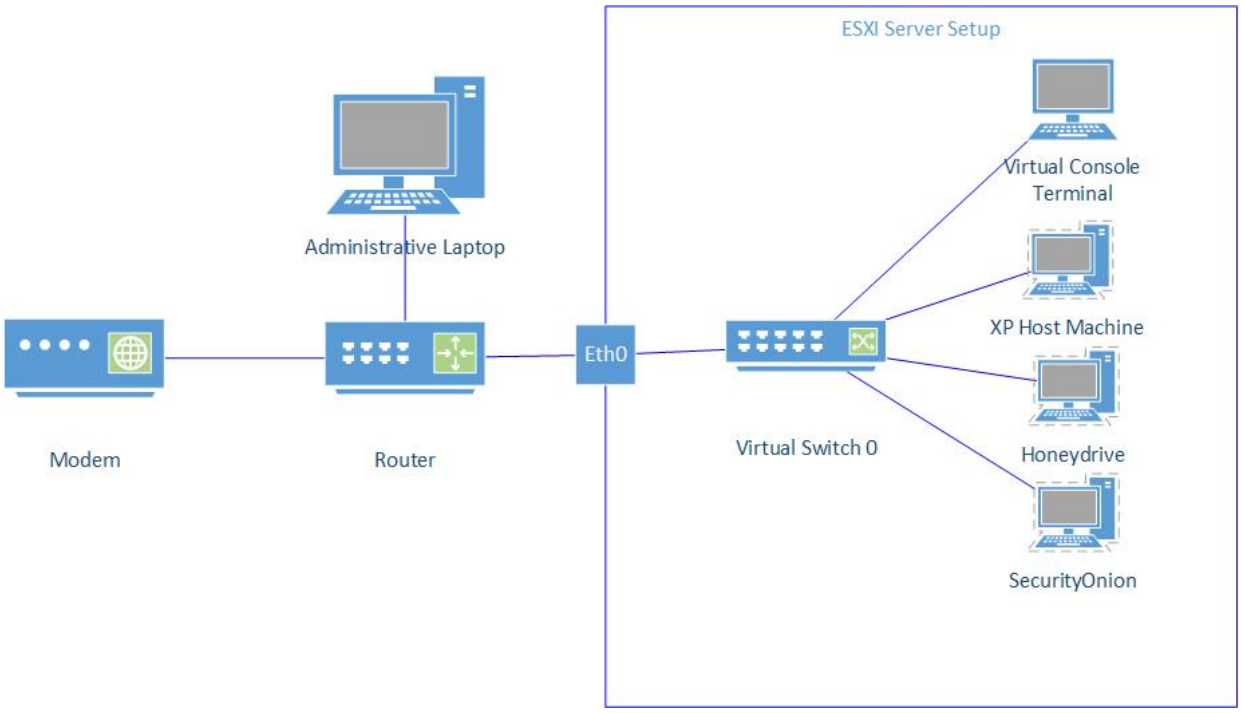
The configuration of the virtual server was fairly straightforward. After installing the VMWare vSphere Client on a management laptop the server was then remotely configured. It is important to note that the Administrative Laptop accessed the virtual server through The Windows honeypot was given 512mb of ram, 40GB of HDD space, and 1 2.2GHZ core dedicated to it to better emulate an old XP host. The host machine then had its' firewall deactivated, with additional ports specifically opened in the event Windows still blocked specific ports. These ports were TCP 135, 139, and 445 as well as UDP 135, 137, 138, and 445. A laptop equipped with NMap using a mobile data connection was then used to scan the network as an external entity and confirmed that these ports were accessible from the outside. All traffic was routed through a single virtual switch connected to a single Ethernet port.

## Results Monitoring

In order to assess what malware had infected the Windows machine, it was taken offline and scanned using an AVG Rescue CD. This allowed for scanning of the hard drive without modifying the honeypot, as well as allowing for scanning for malware that may hide itself from an on demand virus scanner. This was repeated 1 day, 3 days, and 7 days from original deployment date. No malware was found on any of the scans. It was at this point the scope of the project shifted. As it was very unlikely that no outside IP address ever attempted to access the honeypot, the project then sought to see what attempts had been made to access

the system. A network based intrusion detection system would allow for the capture of packets going to and from the system.

**First IDS Attempt**




**Hardware Configuration**

For the first IDS configuration, no changes were made to either the server or the router.

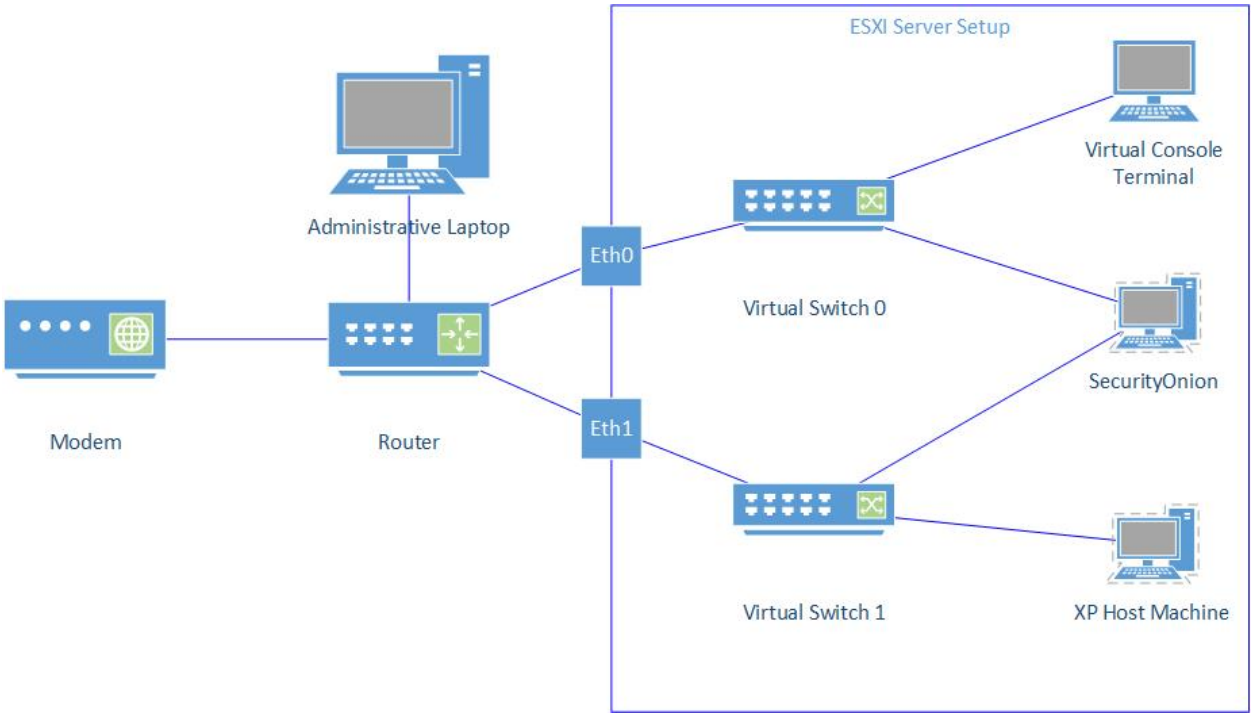
**Virtual Server Configuration**

Two new components were added to the virtual environment at the time. A Honeydrive virtual machine was deployed to the ESXI server as alternative to the Windows XP host in the event there was no network traffic to it. The Honeydrive was given one 2.2 GHZ core, 4GB of

RAM, and 80GB of HDD space. Secondly, a SecurityOnion virtual machine was deployed as well to act as the IDS for this environment. The SecurityOnion was given two 2.2 GHZ cores, 4GB's of RAM, and 80 GB of HDD space. After running through the Snort install scripts and instructions, it was set to monitor and utilize virtual switch 0. The virtual switch was then configured to promiscuous mode, which allowed for all attached hosts the activity on that virtual switch. That was the extent of changes made to the virtual server at that time.

At this point, NMap was launched from the Honeydrive against the XP host to test the IDS system. NMap was set to scan all ports from 1-65535. Both the SecurityOnion and Honeydrive instantly consumed 100% of the resources that were assigned to them. All activity was being monitored by Snort, but the resources demanded by both were not sufficiently covered by the system. Both units were then brought offline. Honeydrive was kept off, and all resources assigned to it were reassigned to the SecurityOnion. However, CPU usage never dipped below 97% for the SecurityOnion, even when NMap was not being used to scan the host machine. A more powerful server was going to be needed.

**Second IDS Attempt**




**Hardware Configuration**

The HP ProLiant DL365 was replaced with a HP xw8600 workstation. While this unit only had 16GB of RAM, it had dual quad-core 2.83GHz Intel Xeon processors. It also required no additional preparation to install ESXI. Two physical cables were connected to the router straight from the unit in order to try to isolate as much traffic from the IDS monitoring as possible. The router configuration remained unchanged.

**Virtual Server Configuration**

All virtual units were freshly reinstalled. The Windows host had the same resources dedicate to it, but the SecurityOnion was given 10GB of ram and six 2.83GHz cores. Two separate virtual switches were created and mapped to separate physical Ethernet ports. SecurityOnion was set to monitor virtual switch 1 (which was set to promiscuous mode instead

of switch 0) and utilize switch 0 for normal traffic. The virtual server console was also set to switch 0 so that the only traffic traversing switch 1 would be unsolicited outbound traffic. After a quick NMap scan to check the IDS configuration, the system was ready to be exposed to the outside world.

## Results Monitoring

The IDS started seeing unsolicited traffic within minutes of being exposed to the extranet. The logs were checked daily to view payload data and to see if the Windows host was sending any packets back. This continued for 19 days. The summary of the events follows.

## Results, Evaluations, and Reflections

On average, the IDS system registered a new event every 11.43 minutes. Here is a summary of some of the more interesting bits of information.

| Ten Most Popular Ports Scanned | Number of Occurrences (out of 2354 events) | Potential Use |
|---|---|---|
| 5060 | 525 | VOIP systems (Winsborrow, 2008) |
| 22 | 417 | SSH (Touch, 2015) |
| 1433 | 154 | Microsoft SQL Server |
| 3306 | 85 | MySQL Server |
| 53 | 83 | DNS Server |
| 80 | 59 | Web Host |
| 443 | 55 | SSL |
| 8080 | 50 | Web Host |
| 1900 | 47 | UPnP |
| 123 | 44 | NTP |

In 19 days, the home IDS system registered 2354 unique scans. However, there were definite patterns as to the source and interest of the scanners. While some were obvious (looking for websites) some were less obvious. The NTP port was something I did not expect, but on further research an exploit in some older systems allows for an NTP server to be used as an incredibly effective DDoS amplifier (Prince, 2014). As for the countries of origin for the attacks, there were few surprises there.

| Country | Percentage of Events |
|---|---|
| UNITED STATES | 17.96% |
| RUSSIAN FEDERATION | 10.50% |
| CHINA | 10.16% |
| POLAND | 6.62% |
| KOREA, REPUBLIC OF | 3.73% |
| FRANCE | 3.64% |
| INDIA | 3.46% |
| UKRAINE | 2.70% |
| JAPAN | 2.63% |
| BRAZIL | 2.27% |

There are some caveats about the country data, however. With Tor, it is nearly impossible to truly know where malicious traffic is coming from. That being said, there were IP addresses that scanned the network multiple times. The ten most commonly seen IP's are as follows:

| Source IP | Number of events |
|---|---|
| 218.77.79.43 | 142 |
| 61.160.224.129 | 99 |
| 61.240.144.66 | 98 |
| 61.240.144.64 | 86 |
| 61.240.144.65 | 85 |
| 61.240.144.67 | 78 |
| 43.255.191.165 | 67 |
| 43.255.191.168 | 64 |
| 61.160.224.130 | 63 |
| 212.83.171.94 | 52 |

Again, this is out of 2354 events. 35% of all events came from less than 3% of the IP addresses seen. This data points to scans being routine, systematic scans designed to explore the web looking for vulnerabilities. These repeat offenders also had very specific exploits they were looking for:

| Source IP | Port of Choice (Times scanned) |
|---|---|
| 218.77.79.43 | 443 (20) |
| 61.160.224.129 | 1521 (18) |
| 61.240.144.66 | 3306(7) |
| 61.240.144.64 | 5800, 50010, 1433 (4) |
| 61.240.144.65 | 3306 (7) |
| 61.240.144.67 | 1433 (6) |
| 43.255.191.165 | 22(67) |
| 43.255.191.168 | 22(64) |
| 61.160.224.130 | 32764, 11211, 8090 (9) |
| 212.83.171.94 | 5060(52) |

Each IP in the 61.240.144.6x group scanned the honeypot a minimum of 38 times, scanning the same port at most seven times. And the ports they were scanning for were fairly

telling as well. Oracle listener port 1512, VNC port 5800, MySQL port 3306, Microsoft SQL Server port 1433, and Hadoop data transfer port 50010 (Joe Touch, 2015) are more used by commercial enterprises than residential IP addresses. In fact, of the top ten most seen IP addresses, only 61.160.224.130 could be seen as attempting to exploit residential IP addresses through the use of port 32764. Port 32764 is a flaw in many routers which allows for remote exploitation (Horowitz, 2014). And while Tor may be skewing data terribly, here is where the most common IP addresses appear to be coming from:

| Source IP | Country of Origin |
|---|---|
| 218.77.79.43 | China |
| 61.160.224.129 | China |
| 61.240.144.66 | China |
| 61.240.144.64 | China |
| 61.240.144.65 | China |
| 61.240.144.67 | China |
| 43.255.191.165 | Hong Kong |
| 43.255.191.168 | Hong Kong |
| 61.160.224.130 | China |
| 212.83.171.94 | France |

## Conclusions and Future Work

While Tor makes it impossible to trace the true source of the traffic hitting the NIDS, the intent is clearly visible. The scans were expected, but not quite how I had anticipated them. The continued interest in VOIP was not expected, and as for the NTP exploit I had no idea that existed until I started researching for this project.

As for the future, I plan on going for a couple IS security certifications and furthering my knowledge experimenting with firewalls and switches. I am also being more vigilant in my home security and experimenting with more Linux builds. As the repeated scans showed me very clearly, IS security is more critical than ever before. It also showed me that there are differences in attack vectors based on the target. The XP host was running an install of SP2 with no firewall or anti-virus and was not infected in 19 days of exposure. If that isn't the most telling sign that PC's are infected because of what the user clicked on, I don't know what is.

# Bibliography


Burks, D. (2015, 2 05). SecurityOnion. Retrieved from http://sourceforge.net/projects/security-onion/files/12.04.5.1/

Horowitz, M. (2014, 1 27). *How and why to check port 32764 on your router*. Retrieved from Computerworld.com: http://www.computerworld.com/article/2475727/network-security/how-and-why-to-check-port-32764-on-your-router.html

ikoniaris. (2014, 7 26). HoneyDrive. Retrieved from http://sourceforge.net/projects/honeydrive/

Joe Touch, E. L. (2015, April 17). *Service Name and Transport Protocol Port Number Registry*. Retrieved from iana.org: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

Lakhani, A. (2013, 10 13). *Ultimate Guide to Installing Security Onion with Snort and Snorby*. Retrieved from drchaos.com: http://www.drchaos.com/ultimate-guide-to-installing-security-onion-with-snort-and-snorby/

Prince, M. (2014, February 13). *Technical Details Behind a 400Gbps NTP Amplification DDoS Attack*. Retrieved from CloudFlare: https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

Verizon. (2014). *2014 Data Breach Invesigations Report.* Retrieved from http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

Verizon. (2015). *2015 Data Breach Investigations Report.* Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Winsborrow, E. (2008, June 8). *Exploiting VoIP vulnerabilities to steal confidential data*. Retrieved from scmagazine.com: http://www.scmagazine.com/exploiting-voip-vulnerabilities-to-steal-confidential-data/article/111091/

WMware. (n.d.). ESXI. Retrieved from https://my.vmware.com/web/vmware/evalcenter?p=free-esxi6