Unified Threat Management

Author: Bernard J. Christenson
Advisor: Dr. Jeffrey Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department

Abstract

Unified Threat Management (UTM) is an information security term that refers to a security appliance as a combination of hardware, software and networking technologies in which the primary function is to integrate increased security, visibility, and control over network security while also reducing complexity. UTM refers to a single security appliance, and within a UTM appliance, the typical features fall into the following three main subsets: firewall/intrusion prevention system (IPS)/virtual private network (VPN), secure Web gateway and messaging security. This paper approaches the OPNsense software platform, discusses the importance of network security, the market growth, OPNsense key features, and discuss how the IDS/IPS, Block SSL certificates and Traffic Shaping implementations complement security capabilities.

Introduction

Gartner indicates a UTM is a converged platform of point security products, particularly suited to small and midsize businesses [1]. Employing network security in for smaller networks can be challenging to manage and expensive for each specific security task in the infrastructure, as each aspect has to be maintained and continuously updated and individually to remain current with the latest forms of malware and cyber threats. OPNsense is free open source software platform firewall under the Open Source Initiative License. The project explains the key features: IDS/IPS, Traffic Shaper, Drop/Block SSL certificates fingerprinting properties and the advantages and benefits of this network security approach [3].

Background

Gartner indicates that 99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT Professionals at the time of the incident [1]. Therefore, by creating a single point of defense and providing a single console, most small to medium size business can deploy a UTM to act as the first line of defense to networks and offer a plethora of tools to mitigate the threats from Wide Area Networks and Local Area Networks [1] [2].

According to the International Data Corporation, it forecasted worldwide revenues for security-related hardware, software, and services reached $81.7 billion in 2017, an increase of 8.2% over 2016. IDC states, the trend for growth in the worldwide market driven by the UTM reaching $1.6 billion in 2Q of 2017 a year-over-year increase of 16.8% is the highest growth among all sub-markets [2].

Furthermore, by 2020 revenues will be nearly $105 billion the UTM market now represents more than 50% of worldwide revenues in the security appliance market as Firewall and UTM continue to be the most active areas of growth, as they add security features leveraging and addressing cloud protection [2].

Problem

Network security is a challenging problem that plays a significant role in drastically changing the business mindset searching for solutions that aim to simplify operations. A UTM such as OPNsense is an integrated security system software appliance that aims to provide cost-effective outcomes for small networks [2].

Methodology

The project discusses the Inline Stateful Inspection Firewall, ClamAV, Suricata IDS/IPS, SSL Blacklisting, and Traffic shaping features. The virtual appliance was installed and configured in the Oracle VM (Virtual Machine) VirtualBox Manager in Laptop1 within a Microsoft Windows 10 OS environment [Figure 1]. A safe virtual testing environment was set up using the VirtualBox Host-Only adapter for either the Host-to-VM testing with no Internet access or the Bridge LAN interface for Internet access. The Laptop2 hardware, also in a Windows 10 OS, is utilized for monitoring and capturing packets at the IDS/IPS interfaces using Wireshark port-mirroring the WAN/LAN port on the CISCO switch. The Clam Anti-Virus is an open source antivirus engine for detecting trojans, viruses, malware and other threats. Utilized the EICAR test sample for the IDS/IPS [Figure 4]. The Nmap scan in the implementation section was run initially with the Suricata IDS/IPS disabled and then enabled in the Windows 10 VM [3].

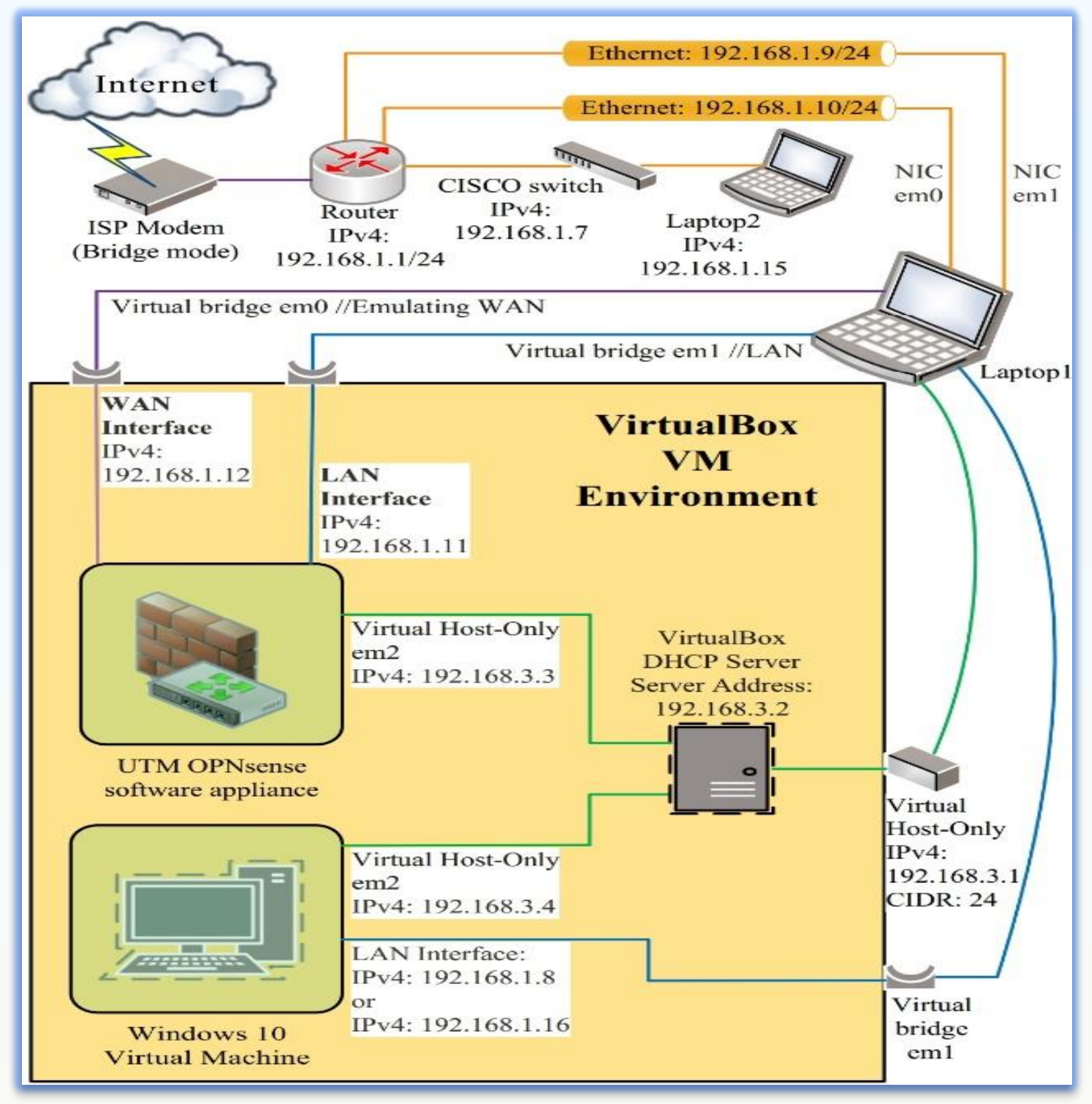

Ethernet: 192.168.1.9/24
Ethernet: 192.168.1.10/24
Internet
ISP Modem (Bridge mode)
Router IPv4: 192.168.1.1/24
CISCO switch IPv4: 192.168.1.7
Laptop2 IPv4: 192.168.1.15
NIC em0
NIC em1
Virtual bridge em0 //Emulating WAN
Virtual bridge em1 //LAN
Laptop1
WAN Interface IPv4: 192.168.1.12
LAN Interface IPv4: 192.168.1.11
VirtualBox VM Environment
UTM OPNsense software appliance
Virtual Host-Only em2 IPv4: 192.168.3.3
VirtualBox DHCP Server Server Address: 192.168.3.2
Virtual Host-Only em2 IPv4: 192.168.3.4
LAN Interface: IPv4: 192.168.1.8 or IPv4: 192.168.1.16
Windows 10 Virtual Machine
Virtual Host-Only IPv4: 192.168.3.1 CIDR: 24
Virtual bridge em1

Figure 1: Network Diagram of the testing environment

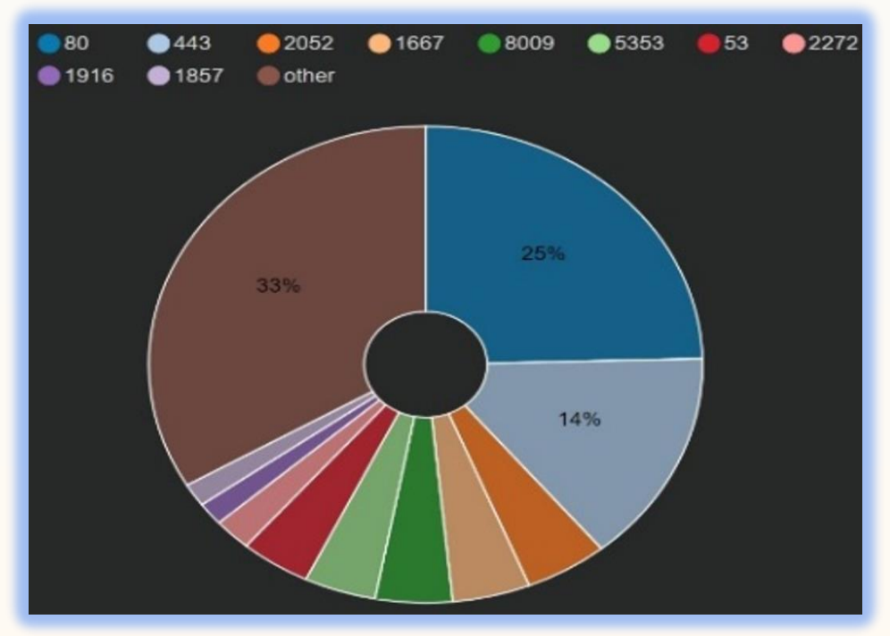
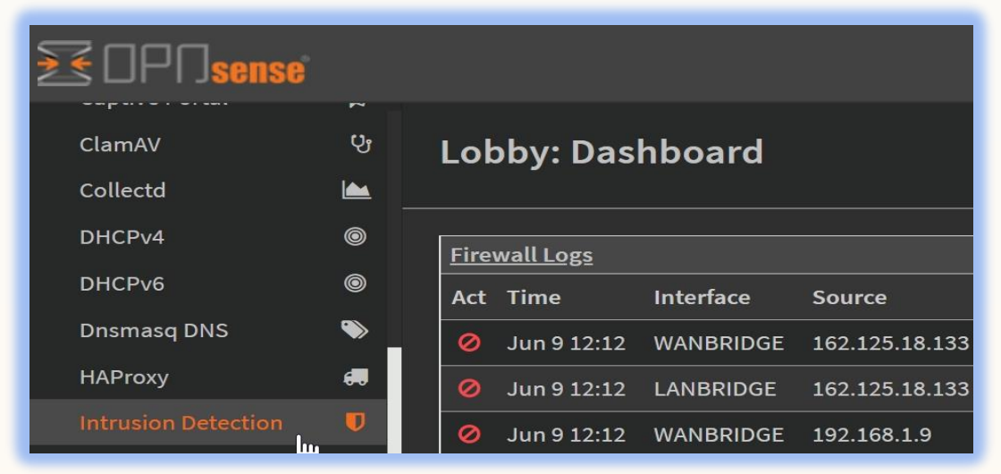
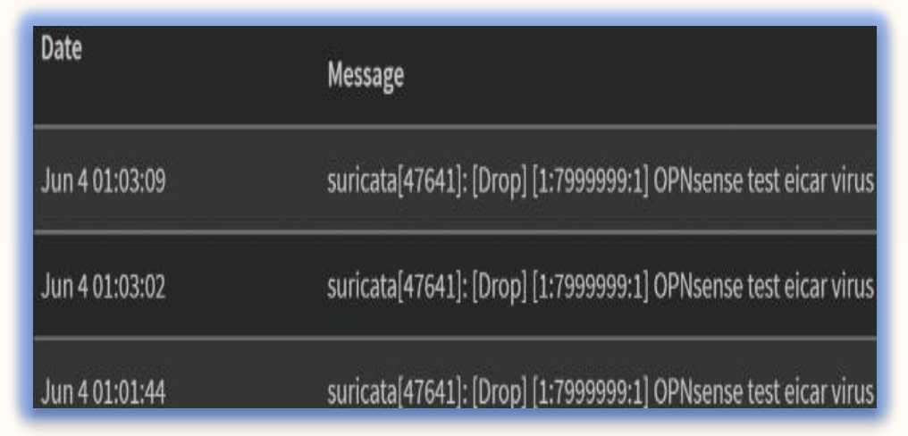


Figure 2: Firewall top source ports



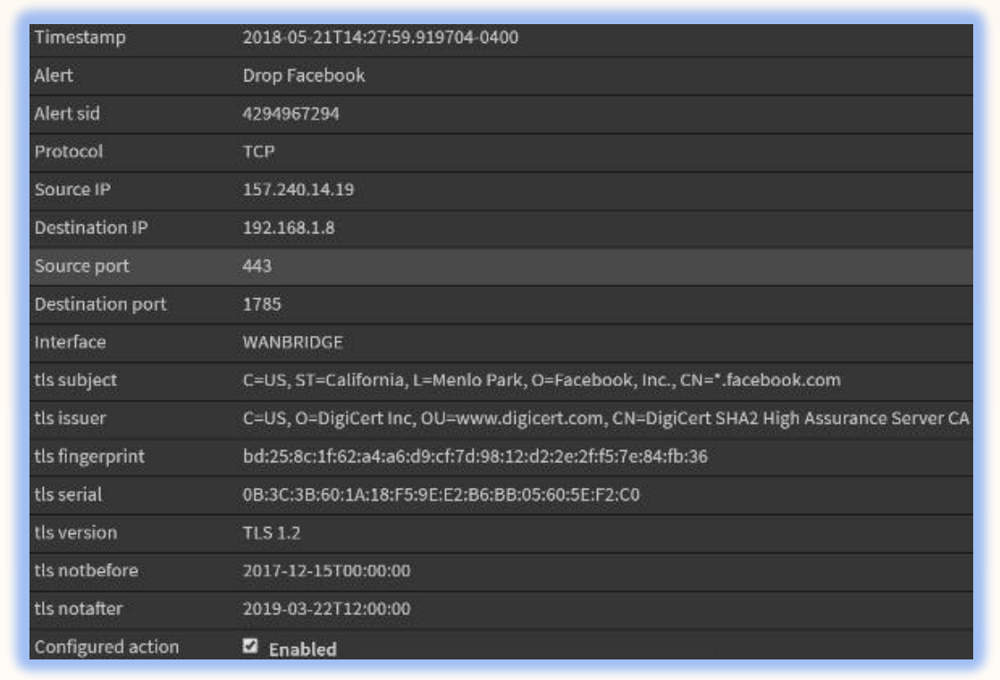
Act	Time	Interface	Source
⊘	Jun 9 12:12	WANBRIDGE	162.125.18.133
⊘	Jun 9 12:12	LANBRIDGE	162.125.18.133
⊘	Jun 9 12:12	WANBRIDGE	192.168.1.9

Figure 3: OPNsense Lobby: Dashboard



Date	Message
Jun 4 01:03:09	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus
Jun 4 01:03:02	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus
Jun 4 01:01:44	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus

Figure 4: IDS/IPS EICAR test virus detection alert



Timestamp	2018-05-21T14:27:59.919704-0400
Alert	Drop Facebook
Alert sid	4294967294
Protocol	TCP
Source IP	157.240.14.19
Destination IP	192.168.1.8
Source port	443
Destination port	1785
Interface	WANBRIDGE
tls subject	C=US, ST=California, L=Menlo Park, O=Facebook, Inc., CN=*.facebook.com
tls issuer	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
tls fingerprint	bd:25:8c:1f:62:a4:a6:d9:cf:7d:98:12:d2:2e:2f:f5:7e:84:fb:36
tls serial	0B:3C:3B:60:1A:18:F5:9E:E2:B6:BB:05:60:5E:F2:C0
tls version	TLS 1.2
tls notbefore	2017-12-15T00:00:00
tls notafter	2019-03-22T12:00:00
Configured action	☑ Enabled

Figure 5: IDS/IPS Block SSL Certificates alert

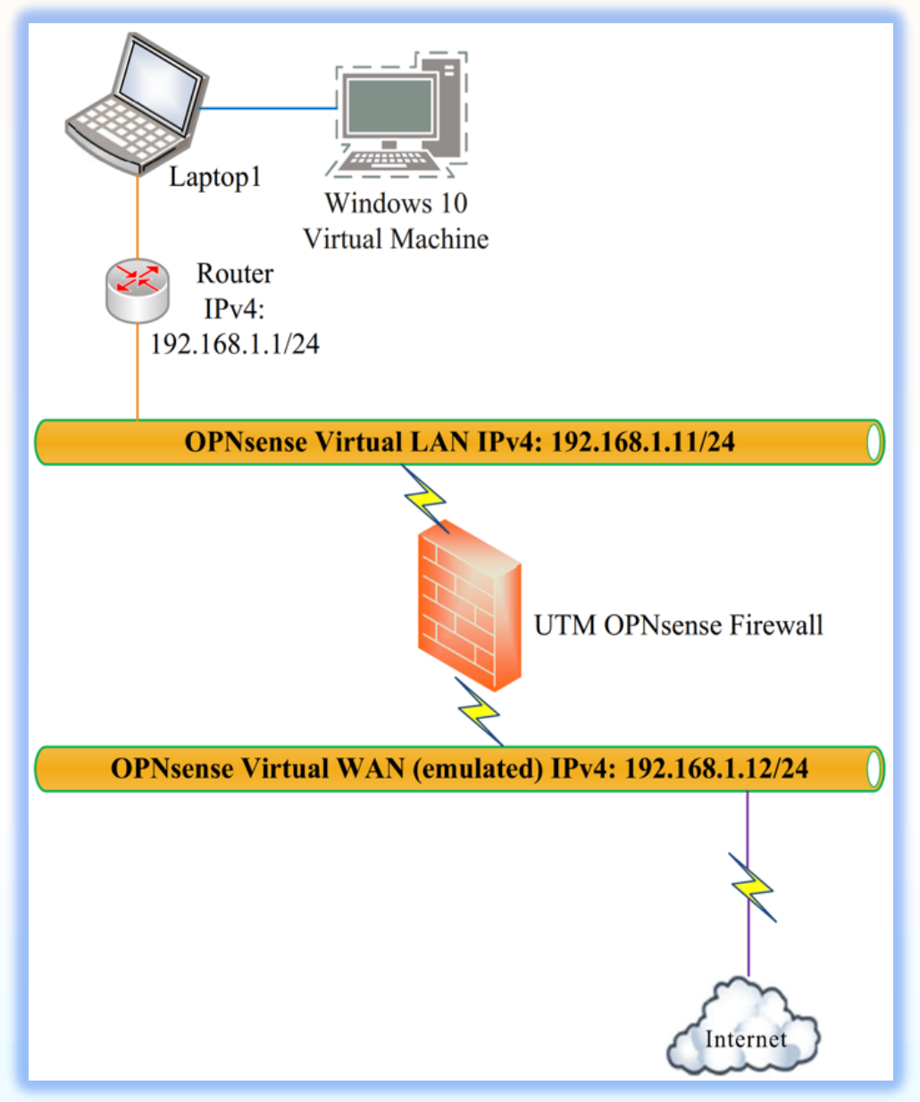

Laptop1
Windows 10 Virtual Machine
Router IPv4: 192.168.1.1/24
OPNsense Virtual LAN IPv4: 192.168.1.11/24
UTM OPNsense Firewall
OPNsense Virtual WAN (emulated) IPv4: 192.168.1.12/24
Internet

Figure 6: Traffic shaping Laptop1 Windows 10 VM

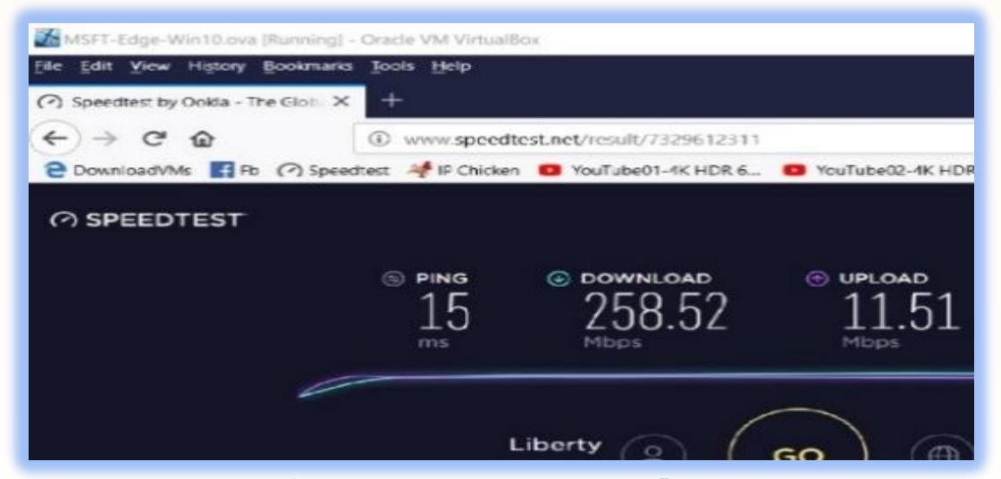

MSFT-Edge-Win10.ova [Running] - Oracle VM VirtualBox
File Edit View History Bookmarks Tools Help
Speedtest by Ookla - The Glob
www.speedtest.net/result/7329612311
DownloadVMs
Fb
Speedtest
IP Chicken
YouTube01-4K HDR 6...
YouTube02-4K HDR
SPEEDTEST
PING
15
ms
DOWNLOAD
258.52
Mbps
UPLOAD
11.51
Mbps
Liberty
GO

Figure 7: VM Speedtest without traffic shaping

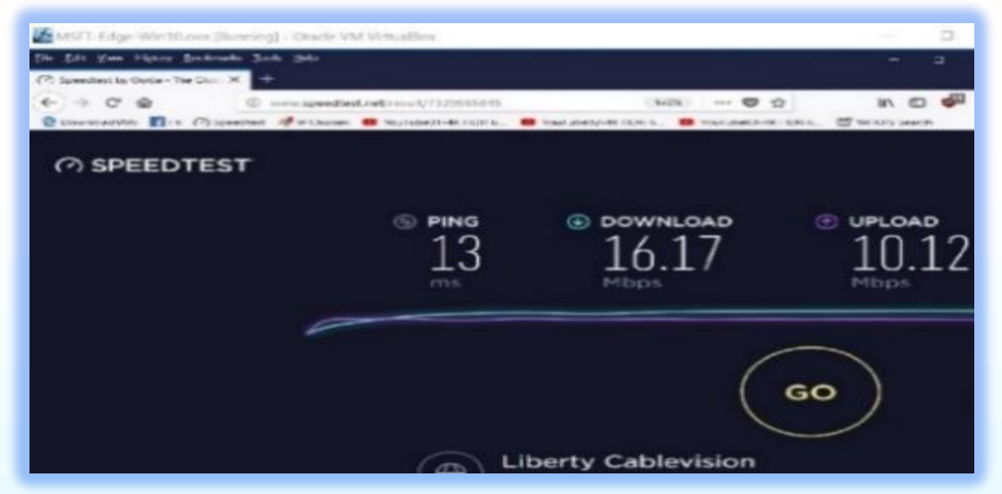
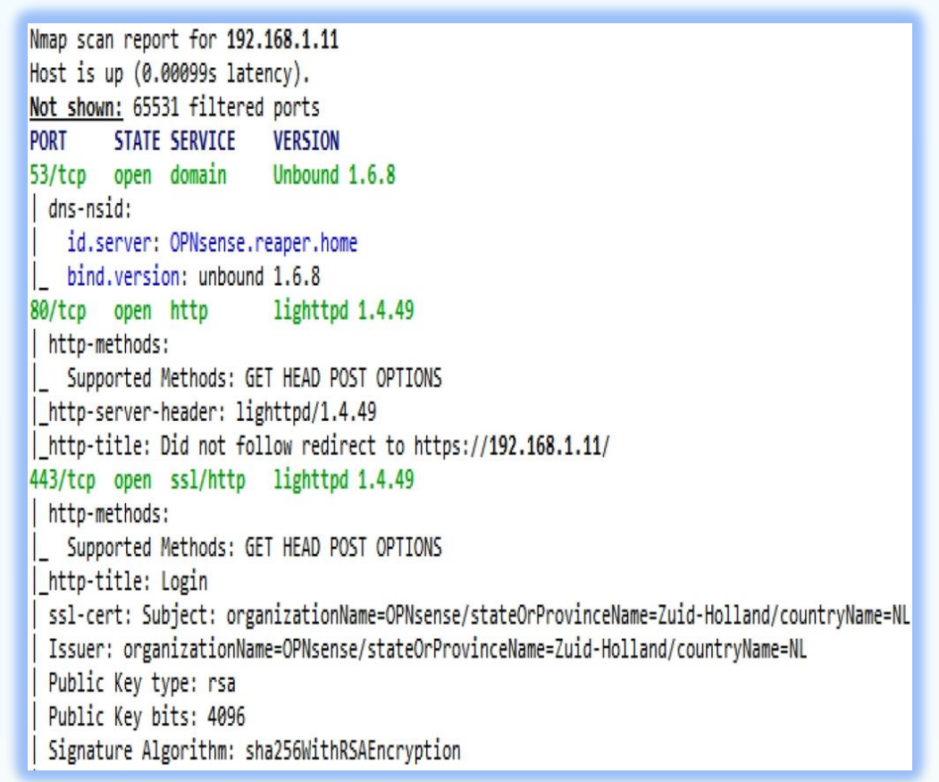


Figure 8: VM Speedtest with traffic shaping applied

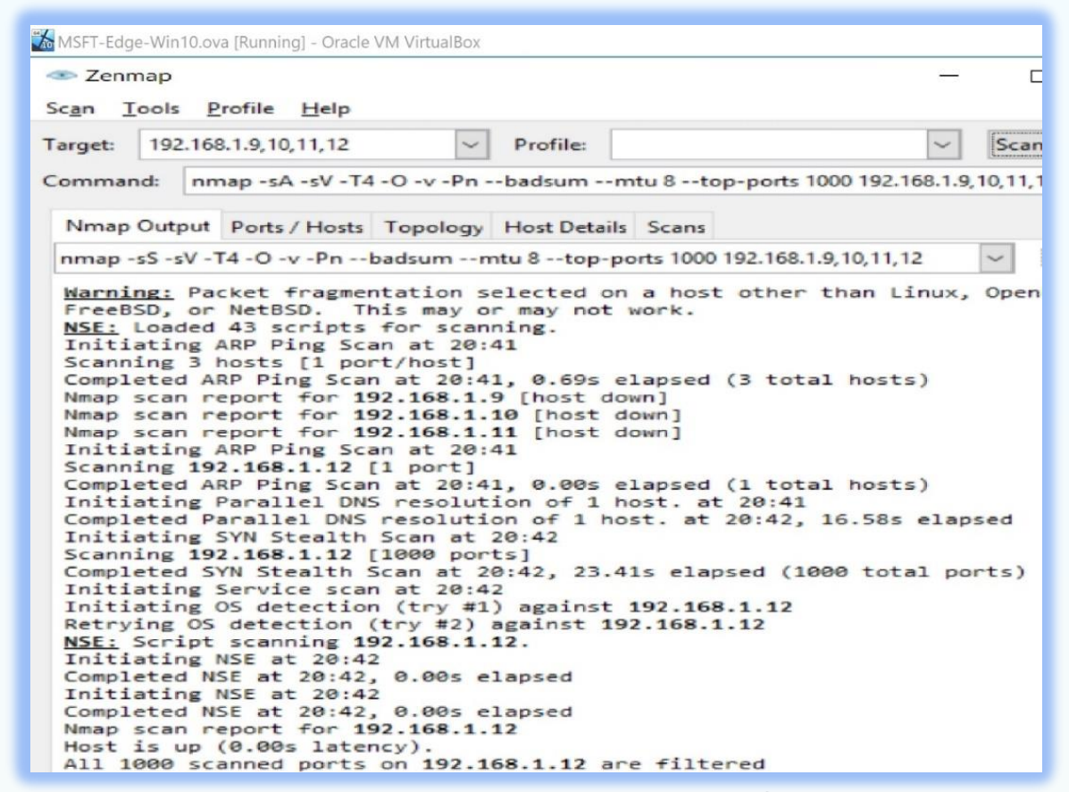
Implementation and Discussion

The implementation purpose is to demonstrate how the UTM reacts with Nmap, a free and open source (license) utility for network discovery and security auditing. IT Pros. use it for network inventory, monitoring host, service uptime and to test firewall defenses. Wireshark is an open-source network packet analyzer, that captures different protocols (OSI layers) and will display the packets as detailed as possible and helps to observe what's happening at a microscopic level. built-in 'Intense scan' and 'nmap -sS -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,12' commands demonstrate the versatility of testing an with these tools to research open/filtered ports and inbound/outbound communication. The pattern that starts to emerge is that to have effective results, Nmap should be used less aggressively and approach IDS/IPS more stealthily. The fragmented IP header output received fewer flags and in IDS/IPS vs. other tested Nmap command scan methods [3]-[5].



```
Nmap scan report for 192.168.1.11
Host is up (0.00099s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE    VERSION
53/tcp   open  domain     Unbound 1.6.8
| dns-nsid:
|   id.server: OPNsense.reaper.home
|_  bind.version: unbound 1.6.8
80/tcp   open  http       lighttpd 1.4.49
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd/1.4.49
|_http-title: Did not follow redirect to https://192.168.1.11/
443/tcp  open  ssl/http   lighttpd 1.4.49
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Login
| ssl-cert: Subject: organizationName=OPNsense/stateOrProvinceName=Zuid-Holland/countryName=NL
| Issuer: organizationName=OPNsense/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
```

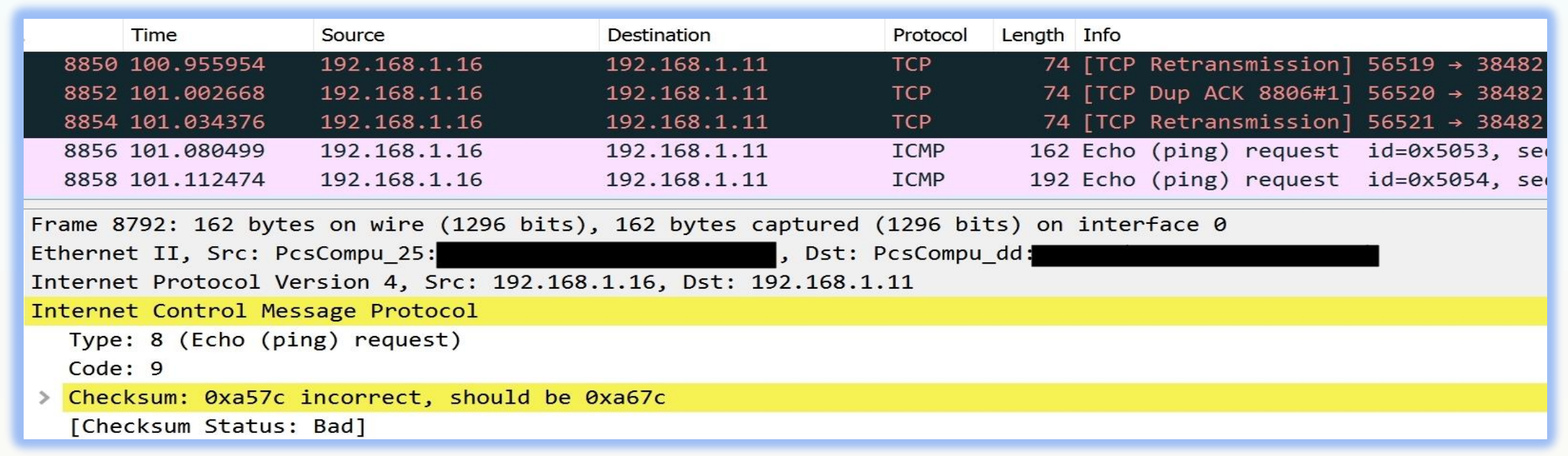
Figure 9: Nmap initial scan report



Target: 192.168.1.9,10,11,12
Command: nmap -sA -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,1

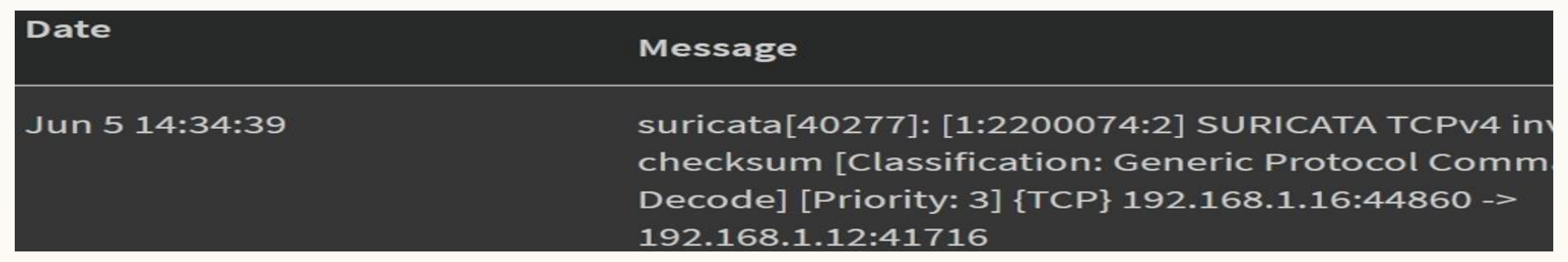
```
nmap -sS -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,12
Warning: Packet fragmentation selected on a host other than Linux, Open
FreeBSD, or NetBSD.  This may or may not work.
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 20:41
Scanning 3 hosts [1 port/host]
Completed ARP Ping Scan at 20:41, 0.69s elapsed (3 total hosts)
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Initiating ARP Ping Scan at 20:41
Scanning 192.168.1.12 [1 port]
Completed ARP Ping Scan at 20:41, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:41
Completed Parallel DNS resolution of 1 host. at 20:42, 16.58s elapsed
Initiating SYN Stealth Scan at 20:42
Scanning 192.168.1.12 [1000 ports]
Completed SYN Stealth Scan at 20:42, 23.41s elapsed (1000 total ports)
Initiating Service scan at 20:42
Initiating OS detection (try #1) against 192.168.1.12
Retrying OS detection (try #2) against 192.168.1.12
NSE: Script scanning 192.168.1.12.
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
Nmap scan report for 192.168.1.12
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.12 are filtered
```

Figure 10: Nmap TCP scan output for WAN/LAN



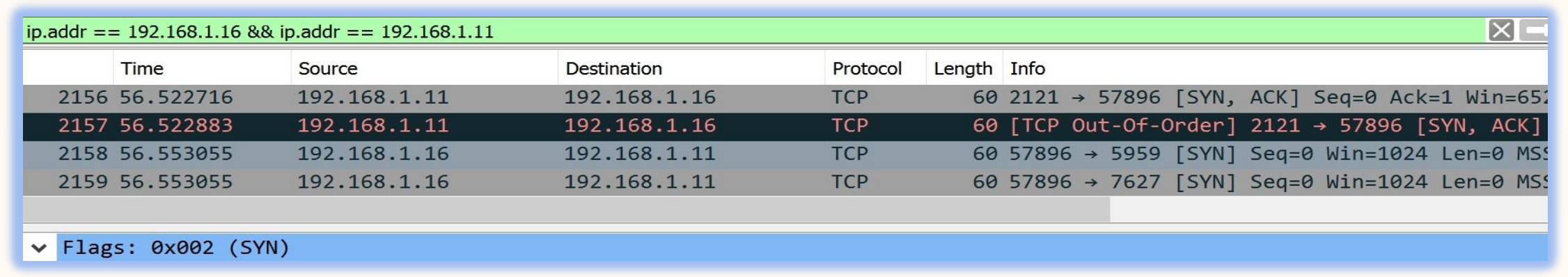
```
      Time         Source          Destination     Protocol Length Info
 8850 100.955954   192.168.1.16    192.168.1.11    TCP          74 [TCP Retransmission] 56519 → 38482
 8852 101.002668   192.168.1.16    192.168.1.11    TCP          74 [TCP Dup ACK 8806#1] 56520 → 38482
 8854 101.034376   192.168.1.16    192.168.1.11    TCP          74 [TCP Retransmission] 56521 → 38482
 8856 101.080499   192.168.1.16    192.168.1.11    ICMP        162 Echo (ping) request  id=0x5053, se
 8858 101.112474   192.168.1.16    192.168.1.11    ICMP        192 Echo (ping) request  id=0x5054, se

Frame 8792: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
Ethernet II, Src: PcsCompu_25:[redacted], Dst: PcsCompu_dd:[redacted]
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.11
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 9
>  Checksum: 0xa57c incorrect, should be 0xa67c
   [Checksum Status: Bad]
```

Figure 11: Wireshark output TCP and ICMP checksum incorrect alert



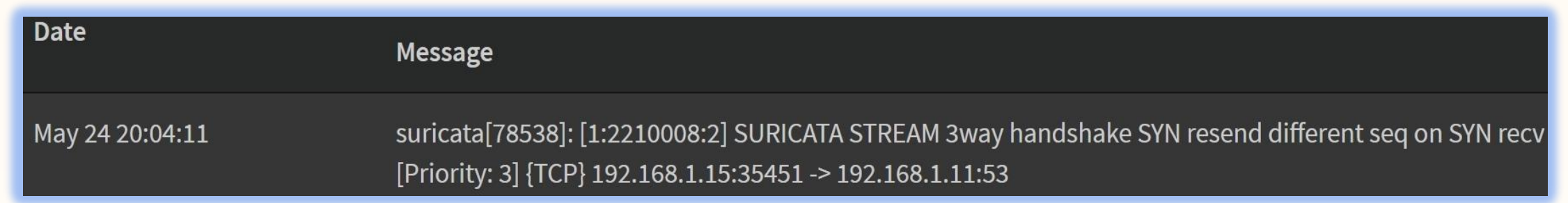
Date	Message
Jun 5 14:34:39	suricata[40277]: [1:2200074:2] SURICATA TCPv4 inv checksum [Classification: Generic Protocol Comm Decode] [Priority: 3] {TCP} 192.168.1.16:44860 -> 192.168.1.12:41716

Figure 12: IDS/IPS TCP invalid checksum alert



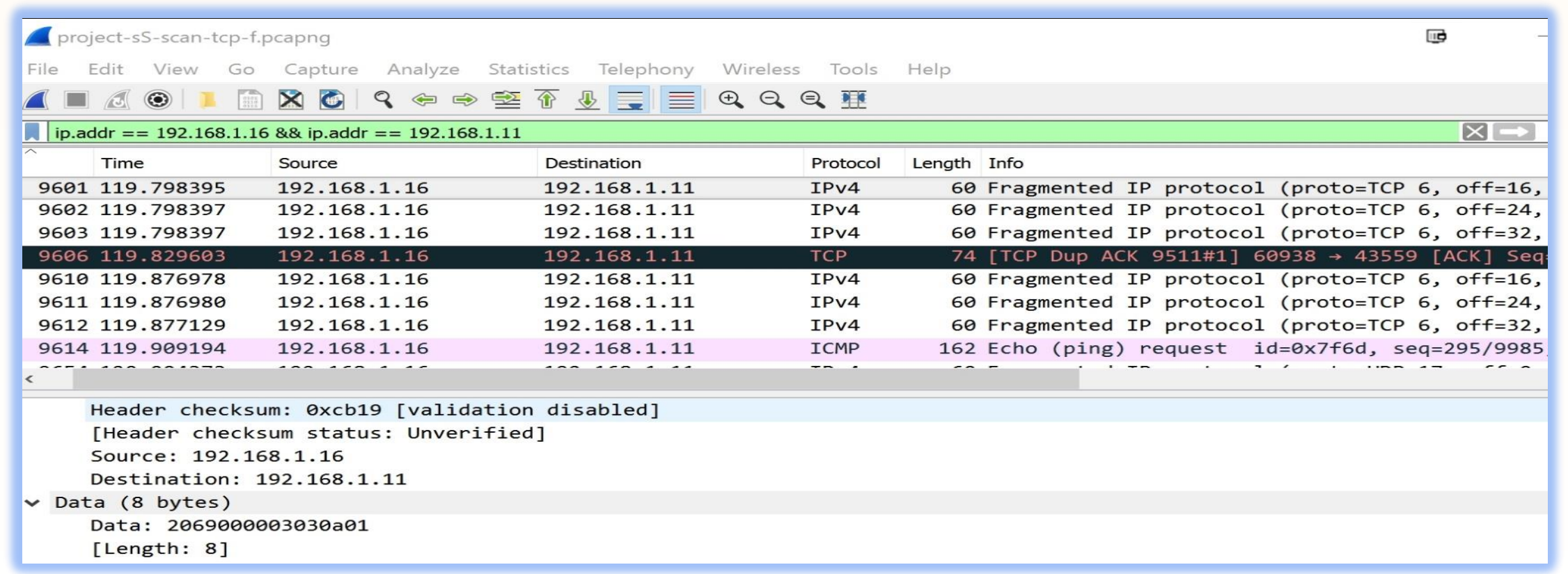
```
ip.addr == 192.168.1.16 && ip.addr == 192.168.1.11
      Time        Source          Destination     Protocol Length Info
 2156 56.522716   192.168.1.11    192.168.1.16    TCP          60 2121 → 57896 [SYN, ACK] Seq=0 Ack=1 Win=65
 2157 56.522883   192.168.1.11    192.168.1.16    TCP          60 [TCP Out-Of-Order] 2121 → 57896 [SYN, ACK]
 2158 56.553055   192.168.1.16    192.168.1.11    TCP          60 57896 → 5959 [SYN] Seq=0 Win=1024 Len=0 MS
 2159 56.553055   192.168.1.16    192.168.1.11    TCP          60 57896 → 7627 [SYN] Seq=0 Win=1024 Len=0 MS

v Flags: 0x002 (SYN)
```

Figure 13: IDS/IPS ICMPv4 unknown code at WAN IP's interface alert



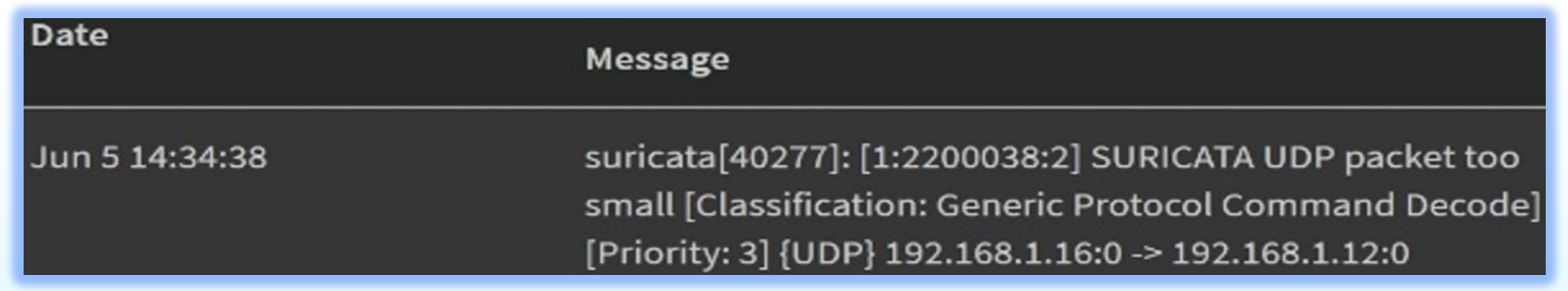
Date	Message
May 24 20:04:11	suricata[78538]: [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [Priority: 3] {TCP} 192.168.1.15:35451 -> 192.168.1.11:53

Figure 14: IDS/IPS-SYN stream request 3-way handshake detection



```
ip.addr == 192.168.1.16 && ip.addr == 192.168.1.11
      Time         Source          Destination     Protocol Length Info
 9601 119.798395   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=16,
 9602 119.798397   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=24,
 9603 119.798397   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=32,
 9606 119.829603   192.168.1.16    192.168.1.11    TCP          74 [TCP Dup ACK 9511#1] 60938 → 43559 [ACK] Seq
 9610 119.876978   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=16,
 9611 119.876980   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=24,
 9612 119.877129   192.168.1.16    192.168.1.11    IPv4         60 Fragmented IP protocol (proto=TCP 6, off=32,
 9614 119.909194   192.168.1.16    192.168.1.11    ICMP        162 Echo (ping) request  id=0x7f6d, seq=295/9985

     Header checksum: 0xcb19 [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.16
     Destination: 192.168.1.11
v  Data (8 bytes)
     Data: 2069000003030a01
     [Length: 8]
```

Figure 15: Wireshark output for Nmap fragmented IP header (MTU == 8)



Date	Message
Jun 5 14:34:38	suricata[40277]: [1:2200038:2] SURICATA UDP packet too small [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.1.16:0 -> 192.168.1.12:0

Figure 16: IDS/IPS-Alert for UDP Fragmented IP packets alert

Implementation and Discussion (continued)

For the Block SSL Certificates a network administrator could retrieve a SHA-1 fingerprint from a website. The signature configured with the appropriate settings will result in the IDS/IPS logging and drop/block the SHA-1 monitored thumbprint and providing a timestamp alert with WAN/LAN IP's, source/destination ports and certificate issuer for use with TLS [Figure 5]. The Traffic Shaping feature is useful for reserving dedicated bandwidth for real-time network traffic such as Voice over IP, sharing Internet traffic evenly using 'queues' to prioritize applications for various users. Purposes for traffic shaping are to provide time-sensitive real-time financial data network traffic throughput a priority over other non critical-data. Also, to limit the bandwidth of applications that consume a lot of network traffic when many users use the program [Figure 6]-[Figure 8] [3].

Conclusion

OPNsense provides a cost-effective way to identify and analyze challenging issues in network security for small and medium-sized businesses. A Free Open Source Software UTM doesn't consume too much footprint in the infrastructure. The benefits of implementing ClamAV, and IDS/IPS with Traffic Shaping help to provide multiple layers of security that are transparent to the end-user to configure and less complex. Furthermore, it provides a lower initial up-front cost as well as less management for appliances, lower software support costs and overhead expenses requirements to mitigate the incoming/outgoing network threats. Deploying A UTM in an environment to provide compliance Vulnerability, Business Impact Analysis, and Risk Assessments to support all future business continuity requirements.

Future Work

Area of future work could be combining features and enabling QoS (Quality of Service) in parallel with the Suricata IDS/IPS to improve network security. In addition, deploying the supported OPNsense Amazon Web Services cloud image for processing capabilities from a data center. Furthermore, future work testing with Nmap and Kali Linux Metasploit Framework, which is "a penetration testing platform that enables you to find, exploit, and validate vulnerabilities" [3]. These are the best approaches for IDS/IPS testing since they provide the tools, infrastructure, and content required to perform penetration tests and extensive security auditing [3]-[5].

Acknowledgements

I would like to acknowledge Dr. Jeffrey Duffany for his guidance and implementation best practices for this project.

References

[1]Gartner IT Glossary. Retrieved from https://www.gartner.com/it-glossary/unified-threat-management-utm//
[2] IDC. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS43066017
[3]OPNsense documentation. Retrieved from https://wiki.opnsense.org/index.html
[4]Nmap. Retrieved from https://nmap.org
[5]Wireshark. Retrieved from https://www.wireshark.org/