North Star Software Developers

Company Training Manual



D3D4A D4 A69 B6 **B**6 06B7 4A697 6A21

North Star Software Developers

Company Training Manual

Prepared by: Brett Logan Strategic Security Consulting Group

EXECUTIVE SUMMARY	5
0.1 MITIGATION AND INCIDENT RESPONSE ASSESSMENT	<i>6</i>
0.2 Purpose of This Manual	7
SECTION ONE: TRAFFIC ANALYSIS	8
21.1 PACKET CAPTURING	9
1.2 FILTERING THROUGH CAPTURED PACKETS	
1.2 Alert Response Procedures	
SECTION TWO: FIREWALLS	18
2.1 FIREWALL FUNDAMENTALS	
SECTION THREE: INTRUSION DETECTION AND PREVENTION	24
3.1 SIGNIFICANCE OF INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)	
3.2 IDPS TOOLS AND METHODOLOGY	
SECTION FOUR: VULNERABILITY ASSESSMENT	29
4.1: NMAP SCANNING AND DETECTING	
4.2 DETECTING NETWORK ATTACKS USING WIRESHARK	
SECTION FIVE: NETWORK SCANNING AND ASSESSMENT	37
5.1 Network Scanning	
5.2 NETWORK ASSESSMENT USING WIRESHARK	41
5.3 VIEWING NETWORK TOPOLOGIES	
SECTION SIX: AUDITING AND LOG COLLECTION	43
LOOPBACK TRAFFIC	
CREATING/SAVING LOGS	
TOOLS OVERVIEW	49
SECTION EIGHT: REFERENCES	51

Executive Summary and Purpose

Executive Summary

North Star Software Developers operates out of Los Angeles, California, creating widely utilized software solutions. Having many customers, the security of customer data such as credit card numbers is of prime importance. Recently, a network server was compromised, potentially exposing this customer data and harming the reputation of NSSD. This breach revealed a vulnerability in detecting whether the attack vector was internal or external, and showcases the need for updated security policy and enhanced employee training.

Strategic Security Consulting Group has developed this manual to train NSSD IT personnel how to better protect the network to prevent future breaches from being successful. The manual will cover traffic analysis, firewalls, intrusion detection, vulnerability assessment, network assessment, and auditing/log collection.

Using Wireshark, IT personnel at NSSD will have the ability to better understand, and thus defend the network. Network defense is of prime importance in any organization, with the rate of cyber-attacks and data breaches constantly increasing. Some of the methods and strategies included are the ability to scan the network in search of vulnerabilities such as open ports, and also the ability to detect an adversarial network scan, indicating an attacker is probing the network. The combined information in all six of the following sections will create more able IT personnel, thus strengthening the overall security posture at NSSD.

0.1 Mitigation and Incident Response Assessment

A key part of training NSSD employees in the proper use of tools such as Wireshark is the increase in overall security this offers. The ability to monitor and understand the network creates faster detection and results in improved incident response: "there are many cases in which organizations did not know they had been hacked for months, and these situations could easily have been avoided. Proper security-oriented monitoring will alert the relevant people when any threat is encountered, allowing for immediate action to be taken" (Guim 2021). Portions of this manual such as firewall configuration and intrusion detection help mitigate security risks by preventing network breaches and alerting to attempted access and other suspicious activity. In the event of a successful breach, pre-determined incident response methods and strategies can help minimize damages and overall effects. An example of incident response plans from this manual is the collection and analysis of logs as covered in section six, which can reveal details of attack methods and allow personnel to address security vulnerabilities.

0.2 Purpose of This Manual

North Star Software Developers (NSSD) operates in a competitive environment where network security is of prime importance. Without proper protocols and precautions, NSSD is more vulnerable to threats such as hacking and data breaches, both of which can affect customers, employees, and stakeholders alike. Successful breaches can potentially cripple operations and open NSSD up to legal battles. Rapidly developing industry regulations make the protection of customer data a legal and ethical responsibility, and maintaining optimal network security policy helps meet these obligations.

To meet NSSD's strategic security goals of protecting the software development process and code, and sensitive client information from internal and external breaches, IT personnel must fully understand how to utilize various network security tools. This manual will explain these tools, and how to test, describe, and recommend them in various situations. By having this information and the ability to apply it appropriately, IT personnel will be able to mitigate the risk of any future breaches, as well as possible effects of a successful breach. The overall value of the policy changes stems from the directed knowledge imparted and how this affects the company. Knowledge is power, and preparedness is key; the purpose of this manual is to impart IT personnel with an understanding of available tools and how to wield them in defense of the NSSD network, resulting in a protected company that can focus on optimal operations and continued profitability.

Section One: Traffic Analysis

1.1 Packet Capturing

For IT personnel to best defend the NSSD network from attack, traffic analysis is conducted to establish baselines and identify anomalies: "traffic analysis is the process by which messages are intercepted and examined for the purpose of performance, security, and general network operation" (Hassan 2017). These messages, or packets, are the flow of information between two hosts on the network, and analyzing them in detail can provide valuable information pertaining to protocol used, IP addresses, MAC addresses, and much more. Doing so increases security by finding malicious or suspicious traffic. NSSD uses Wireshark to capture these packets for analysis, and IT personnel should be familiar with its application and use. Reference the following screenshot to become familiar with the Wireshark interface:



- Press green start button (A) to begin capture
- Press red stop button (B) to stop capture
- All captured packets can be found in the packet list (D)
- Filter for specific protocol by entering specification in filter window (C) and then pressing apply filter button (G)

- Further details of a selected packet header can be found in window (E)

1.2 Filtering through captured packets

When capturing packets via Wireshark, the amount of data collected can be staggering. Fortunately, "wireshark allows the user to quickly filter all that data, so you only see the parts you're interested in, like a certain IP source or destination. You can even compare values, search for strings, hide unnecessary protocols and so on" (Profitap 2018). This can help IT personnel to identify the source of anomalous traffic and how it is interacting with the NSSD network.

The following commands can be used in the filter window to isolate commonly used protocols while searching for specific packet captures:

- *ipv6* for ipv6 traffic
- *ip and !ipv6* for ipv4 traffic
- ip.addr == 224.0.0.0/8 for multicast traffic
- ip.addr == 172.16.200.255 for broadcast traffic
- *icmp* for icmp traffic
- *arp* for arp trtaffic
- *tcp* for tcp traffic
- *udp* for udp traffic
- *ftp* for ftp traffic
- *smtp* for smtp traffic
- *dns* for dns traffic
- tcp.port = = 17 for qotd traffic
- telnet for telnet traffic
- tcp.port = = 19 for CHARGEN traffic
- tcp.port = 13 for DAYTIME traffic
- tcp.port = = 7 for ECHO traffic
- *ssh* for secure shell traffic

- *rdp* for remote desktop traffic
- *smb* for server message block traffic
- *nbns* for NetBIOS Name Service traffic
- *http* for Hypertext Transfer Protocol traffic

Example A:

You are an IT personnel tasked with viewing NSSD's current wireless networks and

connected devices in search of anything abnormal. Using Wireshark, you perform a packet

capture as instructed above, and then find a router using SSID of OPENWIFI. To

accomplish this, use the filter pane and apply the filter: wlan.addr = =

00:1C:10:B5:55:DC, resulting in a snapshot of all wireless traffic involving the Sisco

Linksys router with the SSID of OPENWIFI.

Your output should look something like this:

Situatedi File Edit View Go Capture Analyze Stat © ● ▲ ▲ ▲ △ Parter Analyze Stat Filter: Wan.addr == 00:10:10:85:55:00 No. Time Source 1 0.000000 Cisco-ti_b5:55:d 4 0.224757 Apple_ba:bb:3b 9 0.553466 Apple_ba:bb:3b 9 0.553466 Apple_ba:bb:3b 12 0.570362 13 0.570367 Apple_ba:bb:3b 17 0.977461 Apple_c0:e9:9e (21 1.011776 192.168.2.101 22 1.725557 Apple_c0:e9:9e (wifitest-01.cap Wireshark stics Telephony Jools Internals Help stics Telephony Jools Internals Help stics Telephony Jools Internals Help stics Telephony Telephony Stransford Stransford Destination Protocol Length Broadcast 802.11 12 Chicsco-ti_b5:55:dc 802.11 12 Chicsco-ti_b5:55:dc 802.11 11 TA) Cisco-ti_b5:55:dc 802.11 11 Taylesco-ti_b5:55:dc 802.11 11 Taylesco-ti_b5:55:dc 802.11 11 Taylesco-ti_b5:55:dc 802.11 11 Taylesco-ti_b5:55:dc 802.11 11	captures 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)] Image: I
File Edit Yiew Go Capture Analyze Stati Image: State Image: State <th>wifitest-01.cap Wireshark stics Telephony Iools Internals Help stics Telephony Iools Internals Help stics Telephony Iools Internals Help statistion Protocol Length Q Q Destination Protocol Length Z Q R Cisco-Li_b5:55:dc 802.11 22 Z Z Z Z Z Z Z R Z Z Q</th> <th>1.12.6 (v1.12.6-0-geelfce6 from master-1.12)] - Image: Second frame, SN=2976, FN=0, Flags=, BI=100, SSID=0PENWIFI 6 Request-to-send, Flags= 0 Name query NB WPAD=000-4 4 Null function (No data), SN=1260, FN=0, Flags=T 6 Request-to-send, Flags= 7 Request-to-send, Flags= 8 Request-to-send, Flags= 9 Regrest-to-send, Flags= 9 Regrest-to-send, Flags= 9 Regrest-to-send, Flags=</th>	wifitest-01.cap Wireshark stics Telephony Iools Internals Help stics Telephony Iools Internals Help stics Telephony Iools Internals Help statistion Protocol Length Q Q Destination Protocol Length Z Q R Cisco-Li_b5:55:dc 802.11 22 Z Z Z Z Z Z Z R Z Z Q	1.12.6 (v1.12.6-0-geelfce6 from master-1.12)] - Image: Second frame, SN=2976, FN=0, Flags=, BI=100, SSID=0PENWIFI 6 Request-to-send, Flags= 0 Name query NB WPAD=000-4 4 Null function (No data), SN=1260, FN=0, Flags=T 6 Request-to-send, Flags= 7 Request-to-send, Flags= 8 Request-to-send, Flags= 9 Regrest-to-send, Flags= 9 Regrest-to-send, Flags= 9 Regrest-to-send, Flags=
Elle Edit Yiew Go Capture Analyze Stati Image: State of the state	tics Telephony Iools Internals Help → → → → → → → ↓ □ □ □ ○ ○ ○ ○ Destination Protocol Expression Clear A Destination Protocol 192.168.2.255 NBNS 11 192.168.2.255 NBNS 11 Cisco-Li_b5:55:dc (802.11 1 cisco-Li_b5:55:dc (802.11 1 192.168.2.255 NBNS 11	I I I I I I I I I I I I I I I I I I I
Image: Constraint of the state of	•• •• •	Image: Solution Image: Sol
Filter: wlan.addr == 00:1C:10:85:55:0C No. Time Source 1 0.000000 C1sco-t1_b5:55:d 4 0.224757 Apple_c0:e9:9e (6 0.295424 192.168.2.101 7 0.553466 Apple_ba:bb:3b 9 0.553466 Apple_ba:bb:3b 10.570370 C1sco-t1_b5:55:d 12 0.570374 Apple_ba:bb:3b 13 0.570874 Apple_ba:bb:3b 17 0.977461 Apple_c.c0:e9:9e (19 0.977461 Apple_c.c0:e9:9e (21 1.011776 192.168.2.101 22 1.725557 Apple_c.c0:e9:9e (v Expression Clear Destination Protocol Length 2 Broadcast 802.11 22 Appression Clear A 202.11 21 192.168.2.255 NBNS 11 11 21 Cisco-Li_b5:55:dc 6802.11 1 1 TA) Cisco-Li_b5:55:dc 802.11 1 1 192.168.2.255 NBNS 11 1	pply Save Info 9 Beacon frame, SN=2976, FN=0, Flags=, BI=100, SSID=OPENWIFI 6 Request-to-send, Flags= 0 Name query NB WPAD=00- 4 wull function (No data), SN=1260, FN=0, Flags=T 6 Request-to-send, Flags= 0 Clear-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags=
No. Time Source Cisco-Li_b5:55:d 4 0.224757 Apple_c0:e9:9e (6 0.295424 192.168.2.101 7 0.553466 Apple_ba:bb:3b 9 0.553466 Apple_ba:bb:3b 10 0.570370 Cisco-Li_b5:55:d 13 0.570874 Apple_ba:bb:3b 17 0.977461 Apple_ba:bb:3b 17 0.977461 Apple_c0:e9:9e (21 1.011776 192.168.2.101 22 1.725557 Apple_c0:e9:9e (Destination Protocol Length 22 802.11 22 32 325.55 802.11 11 192.168.2.255 NBNS 11 11 192.168.2.255 NBNS 11 12 (raco-Li_b5:55:dc 802.11 1 1 1: (Apple_ba:bb:3b (rA) 802.11 1 1 1: (apple_ba:bb:3b (rA) 802.11 1 1 1: (acco-Li_b5:55:dc (802.11 1 1 1: (acco-Li_b5:55:dc (802.11) 1 1	Info 9 Beacon frame, SN=2976, FN=0, Flags=, BI=100, SSID=OPENWIFI 9 Request-to-send, Flags= 0 Name query NB WPAD=00> 4 Null function (No data), SN=1260, FN=0, Flags=T 6 Request-to-send, Flags= 0 Clear-to-send, Flags= 6 Request-to-send, Flags= 7 Request-to-send, Flags= 7 Request-to-send, Flags= 8 Request-to-send, Flags= 9 Request-to-send, Flags=
24 1.725557 Apple_c0:e9:9e (25 1.728117 Apple c0:e9:9e (FA)Cisco-Li_b5:55:dc (802.11 1 rA)cisco-Li_b5:55:dc (802.11 1 rA)cisco-Li_b5:55:dc (802.11 1 rA)cisco-Li_b5:55:dc (802.11 1	D Name query NB WPAD-00> 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Request-to-send, Flags= 6 Reduest-to-send. Flags=
B Frame 4: 16 bytes on wire (128 b ■ IEEE 802.11 Request-to-send, Fla Type/subtype: Request-to-send ■ Frame Control Field: 0xb400 00 = Version: 0 01 = Type: Control fr 1011 = Subtype: 11 ■ Flags: 0x00 .000 0000 1001 0110 = Duration Receiver address: Cisco-L.b5:	<pre>its), 16 bytes captured (128 bits) gs: (0x001b) ame (1) : 150 microseconds 55:dc (00:1c:10:b5:55:dc)</pre>	Image: Second secon
Transmitter address: Annle c0: 0000 04 00 96 00 00 1c 10 55 55	P9:9P (60:FR:1d:r0:P9:9P) dc 60 F8 1d c0 e9 9P U	CO0.312

Example B: While searching through wireshark packets, you need to locate more information by

following the TCP stream of a capture. The steps to do so are:

- Perform Packet Capture
- Filter according to specific search purposes
- Highlight packet of interest from the list of captured packets
- *Right-click* on the packet
- Select follow TCP stream

This will open a new window with more detailed information, helping to identify things pertinent to security such as the addition of new groups/users. In this screenshot, note the addition of a new group (golden state warriors) and user (Stephen):



CYBERLEET TRAINING MANUAL

		Default col	umns in a	packet c	apture output		W	lireshark	Capturing	Modes			1	Miscellane	ous	
Name of the loop from the list from the list from the list be protone along the list be protone al		No. Frame number f	rom the beginni	ing of the pi	icket capture	Promiscuous m	ode Sets int	terface to cap	ture all packet	ts on a networ	k segment to	which it is	Slice	Operator [] -	Range of values	
	Sour	Time Seconds from t	he first frame	Put The or	Ethernet address		associat	ted to	tenfaca ta can	tues all teaff	is it can pas	alua	Membership	Operator () - In	1	
	Destinati	ion (dst) Destination ad	dress		CONTRACT MANY CAS	Monitor mod	e (Unix/Li	inux only)	cervace to cap	the art train	it it tan ret	erve		CTRL+E - Start/	Stop Capturing	
Light leng at the frame indeg of t		Protocol Protocol used	in the Ethernet	t frame, IP p	wacket, or TCP segment					Contract F	Alter Com					
Logical OperatorsLogical OperatorsNote that a decision of the outline solution		Length Length of the	frame in bytes							Lapture F	ilter Syn	tax				
			Logical (Operators	5	Syntax	protocol	direction	nosts	value	Logical	operator		tco dat 202 16	ns 14 30 1	
Index of M error IIUpper A Upper AAll the conditions should and the ME of the ME of ME of A 	Operator	Descript	Lon		Example	example.	.cep			Disnlay F	ilton Sun	tax		ttp ort averat		
mem inter <	and or 88	Logical A	AND		All the conditions should match					Companison	LICET Syn	COA				
To PTo PT	on on 11	Insical		Either	all on one of the condition should match	Syntax	protocol	String 1	String 2	Operator	value	logic	cal operator	Exp	ressions	
<form> Indicate Indicate</form>			***.			Example	http	dest	ip	**	192.168.1	.1	and	te	p port	
Not or 1 Inter or 2 Inter				exclusive	alternation - Only one of the two conditions				Kevboard S	hortcuts	- main di	isplav wir	ndow			
Notional problem Notional problem </td <td>xor or an</td> <td>Logical)</td> <td>KOR</td> <td></td> <td>should match not both</td> <td>Accelerator</td> <td></td> <td>Descrip</td> <td>tion</td> <td>A</td> <td>celerator</td> <td></td> <td>D</td> <td>escription</td> <td></td>	xor or an	Logical)	KOR		should match not both	Accelerator		Descrip	tion	A	celerator		D	escription		
Interval (a) [-1]Automa (b) the space of the sp							House between	screen element	a a from t							
This regardly working wor	not or !	NOT (Negat.	ion)		Not equal to	Tab or Shift+Tab	toolbars to ti	he packet lis	to the packet	A	It+-> or	Move to the n	ext packet in t	he selection his	tory.	
Hitering packets (bisplay Filters) → Note the next packet or detail iter. → In the packet detail, geen the solution to the next packet or detail iter. → In the packet detail, geen the solution to the next packet or detail iter. → In the packet detail, geen the solution to the next packet or detail iter. → In the packet detail, geen the solution to the next packet or detail iter. → In the packet detail, geen the solution to the next packet or detail iter. A fitte next. Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2" Colspan="2" Colspan="2" <t< td=""><td>[n] []</td><td>Substring op</td><td>erator</td><td></td><td>Filter a specific word or text</td><td></td><td>detail.</td><td></td><td></td><td>Op</td><td>otion+→</td><td></td><td></td><td></td><td></td></t<>	[n] []	Substring op	erator		Filter a specific word or text		detail.			Op	otion+→					
Nerve is the probability of the pr		Filterin	ng packets	(Display	/ Filters)	1	Nous to the su	est eachet on	data11 item				datail ones	the selected tree		
in g or r Index	Operator	Der	scription		Example	÷	Hove to the h	ext packet or	octars reen.		1.0	in the packet	becars, opens	the selected tre	e iten.	
No control International part of part o	eq or ==		Equal		ip.dest == 192.168.1.1	Ť	Move to the p	revious packet	or detail ite	n. s	hift+→	In the packet	detail, opens	the selected tre	e item and all c	
Note of is Out is and is and is about it abs: abs: 1 abs: 2 a							Move to the m	ext packet, e	en if the pack	et list						
if e or >Greater thanGreater thanframe.in >10crist ^ n or 10crist ^ n or 10crist ^ n or 10crist ^ n or 10crist ^ n or 10or 10 </td <td>ne or 1=</td> <td>N</td> <td>ot Equal</td> <td></td> <td>1p.dest != 192.168.1.1</td> <td>Ctrl+ ↓ or F8</td> <td>isn't focused</td> <td></td> <td></td> <td></td> <td>trl+></td> <td>In the packet</td> <td>detail, opens</td> <td>all tree items.</td> <td></td>	ne or 1=	N	ot Equal		1p.dest != 192.168.1.1	Ctrl+ ↓ or F8	isn't focused				trl+>	In the packet	detail, opens	all tree items.		
It or c Liss than fram. lnn (100) It or list in the list	gt or >	Gre	ater than		frame.len > 10	Ctrl+ 1 or F7	Move to the p	revious packer	, even if the	packet	Ctrl+ In the packet		detail, closes	all tree itens.		
it is the set base fault frame.ins + 18 Ctrl, (ro, un were). Backagee: It the space fault, space is the	lt or <	L	ess than		frame.len <10		Move to the m	ext packet of	the conversation	00						
the state of latethe state of latethe problem picture of the convertable of	ge or >=	Greater	than or Equal		frame.len >= 10	Ctrl+.	(TCP, UDP or	IP).		B	ackspace	In the packet	detail, jumps	to the parent no	de.	
(10°, up 0° str); (10°, up 0° str); (10°, up 0° str); <th col<="" td=""><td>le or <=</td><td>Less t</td><td>han or Equal</td><td></td><td>frame.lenc=10</td><td>Ctrl+.</td><td>Move to the p</td><td>revious packet</td><td>of the conver</td><td>sation Retu</td><td>rn or Enter</td><td>In the packet</td><td>detail, togele</td><td>s the selected t</td><td>ree item.</td></th>	<td>le or <=</td> <td>Less t</td> <td>han or Equal</td> <td></td> <td>frame.lenc=10</td> <td>Ctrl+.</td> <td>Move to the p</td> <td>revious packet</td> <td>of the conver</td> <td>sation Retu</td> <td>rn or Enter</td> <td>In the packet</td> <td>detail, togele</td> <td>s the selected t</td> <td>ree item.</td>	le or <=	Less t	han or Equal		frame.lenc=10	Ctrl+.	Move to the p	revious packet	of the conver	sation Retu	rn or Enter	In the packet	detail, togele	s the selected t	ree item.
Copier filter bis/ly liter Filter optiets daring capture his Packets for a capture display Protocols - Values Copier filter bis/ly liter Filter optiets is Packets for a capture display Protocols - Values Usage Filter optiets is Packets for a capture display Filter optiets is Packets for a capture display Usage Filter optiets is Packets is Packets for a capture display Usage Filter optiets is Packets is Packets is Packets daring capture is Packets is Packets is Packets daring capture display Filter optiets is Packets is Packets daring capture is Packets is Packets daring capture is Packets daring capture is Packets daring capture is Packets daring capture filter by packets daring capture filter by packets daring capture packet is Packets daring capture is Packets daring capture filter by packets daring capture is Packet daring capture is Packet daring capture data filter by packet daring capture is Packets daring capture data filter by packet daring capture is Packets daring capture data filter by packet data filter by packet data filter by darins and packet daring capture data filter by darins and filter is Packet daring capture data filter by darins and filter filter capture data filter daring filter daring filter darin			Filter	Types			(TCP, UDP or	1P).								
Binary HiterWhere Accels from a capture displaythere, fddi, jp, arp, rarp, decret, lat, sca, noprc, nopol, top and udpLongon Elletting commanderUsageUsageFilter systaxNine State Filter by IPState rystaxState rystaxFilter by Barinadio IPUsageFilter systaxFilter by Barinadio IPUsageFilter systaxFilter by Darinadio IPState rystaxFilter by Darinadio IPState rystaxFilter SystamFilter SystamFilter by Darinadio IPUsageFilter SystamFilter	Carr	ture filter	TALLET	iypes	ilter packets during capture					Protocol	s - Value	25				
Common Filter system Sage Sage <th< td=""><td>Dis</td><td>play Filter</td><td></td><td>Hide</td><td>Packets from a capture display</td><td></td><td></td><td>ether, fdd</td><td>i, ip, arp, m</td><td>rarp, decnet</td><td>, lat, sca,</td><td>mopre, mopd</td><td>1, tcp and u</td><td>dp</td><td></td></th<>	Dis	play Filter		Hide	Packets from a capture display			ether, fdd	i, ip, arp, m	rarp, decnet	, lat, sca,	mopre, mopd	1, tcp and u	dp		
Lotange Filter systax Usage Filter systax Niter Systam Filter systax Filter Systax<						amon filteni										
Note that we determ to be able to be		Hereit				ommon Filteri	ig commanu	5								
All restart Filter by Destination DP IDeader = 10.16.90.1 Filter by Out Integration DP Filter by Destination DP IDeader = 10.16.90.1 Filter by Use state Filter by Use state Filter by Use state Filter by Destination DP IDeader = 10.16.90.1 IDeader = 10.16.90.1 Filter by Use state Filter by Use state Filter by Dringe IDeader = 10.16.90.1 IDeader = 10.16.90.10 INTEGRATING Beacher Silter IDEADER = 10.16.90.10 Filter by Marine DU Daddres IDeader = 10.16.90.10 IDEADER = 10.16.90.10 INTEGRATING Beacher Silter IDEADER = 10.16.90.10 Filter by Marine DU Daddres IDEADER = 10.16.90.10 INTEGRATING Beacher Silter IDEADER = 10.16.90.10 IDEADER = 10.16.90.10 Filter by Marine DU Daddres IDEADER = 10.16.90.10 IDEADER = 10.16.90.10 INTEGRATING Beacher Silter IDEADER = 10.16.90.10 Filter by defrastion poet IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 Filter by defrastion poet IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 Filter by defrastion poet IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 Filter by defrastion poet IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10 IDE.0.90.10	111 mm	Usage			Filter Syntax			C11ter	ge				Filter s	yntax		
Filter by for example Intervent of the system of the sy	Filte	shark Filter by IP			ip.addr == 10.10.50.1			Filter but	ine stamp			ferma ti	me >= "lune !	nost name	-00"	
Hitter by Dringer Ip.ader >> 10.18.9.1. Ip	Eil	tar by Source TP			in sec == 10.10.50.1			Carter by	And a camp			TI BOC. LA	tco flags	un 1	.00	
Filter by Multiple Tps Ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100 Wireshark Bracon Filter Image: State of the state state state state capture state of the state capture	Fi	Iter by IP range		ir	addr >= 10.10.50.1 and in.addr <= 10.10.	50.100		Filter S	YN flag			tcp.flags	syn == 1 and	tcp.flags.ack	0	
Filter out P address (1(p.addr = 10.10.50.1) Mitreshawk braadest filter eth.dst = nf.rf.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff.ff	Filt	er by Multiple Ips		i	.addr == 10.10.50.1 and ip.addr == 10.10.	50.100		lireshark Be	acon Filter			wl	an.fc.type su	btype = 0x08		
Filter sport Explore sport spor	Filt	ter out IP address			!(ip.addr == 10.10.50.1)		Wi	reshark broa	dcast filter			eth	.dst == ff:f	f:ff:ff:ff:ff		
Filter by port = 25 Host mare filter \rightarrow top, discontance \rightarrow to		Filter subnet			ip.addr == 10.10.50.1/24		Wi	reshark mult	icast filter				(eth.dst[8] & 1)		
Mate address filter — by detribution point for the state of the part of of the		Filter by port			tcp.port == 25			Host name	filter				ip.host =	hostname		
Filter by ip address and pert ip, addr = 18, 18, 50, 1 and Tcp, port = 25 EXT Flag filter Text Flag filter text filter text filter UBL: Colspan="4">text: Stand reg, port = 25 KBT Flag filter text: Stand reg, port = 25 UBL: Colspan="4">UBL: Colspan="4">text: Stand reg, port = 25 UBL: Colspan="4">Text: Stand reg, port = 25 Colspan= Text: Stand reg, port = 25 Stand Stand reg, port = 25 <td>Filter</td> <td>by destination port</td> <td></td> <td></td> <td>tcp.dstport == 23</td> <td></td> <td></td> <td>MAC addres</td> <td>is filter</td> <td></td> <td></td> <td>eth</td> <td>.addr == 00:7</td> <td>0:f4:23:18:c4</td> <td></td>	Filter	by destination port			tcp.dstport == 23			MAC addres	is filter			eth	.addr == 00:7	0:f4:23:18:c4		
Object to the set of the the set	Filter b	by ip address and po	rt		ip.addr == 10.10.50.1 and Tcp.port ==	25		RST flag	filter				tcp.flags.n	eset == 1		
Nonline Teem Memu Itee Description Toolbar Icen Toolbar Icen Memu Itee Memu Itee Description 4 Start Capture - Start Uses the same packet capturing options as the previous session, or uses defaults if no options were set - Go Forward Go - Go Forward Sump forward in the packet capture session 4 Stop Capture - Start Uses the same packet capture quitor eagure Em Go to Packet Go - Go roward Sump forward in the packet capture 4 Stop Capture - Stop Stops currently active capture Em Go to Packet Go - Go to Packet Go - Go roward Jump to first packet of the eagure 6 Options Capture - Aptions Opens "file open" dialog box Em Go to Te List Packet Go - Isst Packet Jump to Jast packet of the eagure 6 Options File - Open Opens "file open" dialog box to loid a capture for viewing Em Calorize View - Auto Scroll in Live Capture Auto scroll packet list during Live Capture Calorize View - Auto Scroll in Live Capture Calorize the packet list during Live Capture Calorize View - Auto Scroll in Cal						Main toolha	r items									
Name	olbar Icon	Toolbac Item	Menu	Iten	Description	Huin coorde	Toolbar Icor	Too	bar Item	Men	. Ttem			escription		
Aligned Start Capture - Start Session, or uses defaults if no options were set Image: Capture - Start Start Capture - Start Start Start Capture - Restart Restarts active capture session Image: Capture - Start Start capture - Start Start capture session Image: Capture - Start Start capture - Start Capture - Start Restarts active capture session Image: Capture - Start Start capture - Start Start capture session Image: Capture - Start -		1001001 1000			Uses the same packet capturing options a	s the previous	1001001 1001		iou. Item					eser aperon		
Image: Stop Capture - Stop Stops Stops Stops Capture - Stop Stops Stop		Start	Capture -	→ Start	session, or uses defaults if no optio	ns were set	-	Go	Forward	$Go \rightarrow G$	io Forward		Jump forward	in the packet	history	
Image: Capture - Stop Capture - Stop Stops currently active capture Capture - Stop Stops currently active capture Image: Capture - Stop Capture - Asstart Restarts active capture session Image: Capture - Stop So - Go to Packet So - Go to Packet <td>-</td> <td>12200</td> <td>1210/2110/0</td> <td>1122303</td> <td></td> <td></td> <td>4604</td> <td>12015</td> <td>100000</td> <td>0.2010.020</td> <td>0.0200005</td> <td></td> <td>120.00</td> <td></td> <td>2</td>	-	12200	1210/2110/0	1122303			4604	12015	100000	0.2010.020	0.0200005		120.00		2	
Image: Section Control Content Control Control Control Control Control Control Contro		Stop	Capture -	→ Stop	Stops currently active captu	re	100	Go t	o Packet	Go → Go	to Packet		Go to	specific packe	rt.	
Maximum Capture - maximum Maximum Capture - for the capture session			A		Berner Statistics and and		-		dana Baabaa	· · · · · ·						
Image: Constraint of Constr	42.	Restart	Capture →	Restart	Restarts active capture sess.	100		60 10	Inst Packet	00 → F1	rst Packet	10	ip to first p	acket of the c	apture file	
Open File open Opens "file open" dialog box to load a capture for viswing Acto Scroll in Live Capture Acto Scroll packet list during Image: Imag	0	Options	Canture -+	Ontions	Opens "Capture Options" dialog	box		Go To	Last Packet	$60 \rightarrow 10$	ast Packet	30	no to last o	cket of the ca	nture file	
Open File → Open Opens Opens <th< td=""><td>C</td><td>operonant</td><td>captore</td><td>operonym</td><td>opens capture options dialog</td><td>. DOA</td><td>-</td><td>00 10</td><td>LUST FOCKEL</td><td>00 - 1</td><td>ant rather</td><td></td><td>op to rast p</td><td>reset of the ci</td><td>ipture rise</td></th<>	C	operonant	captore	operonym	opens capture options dialog	. DOA	-	00 10	LUST FOCKEL	00 - 1	ant rather		op to rast p	reset of the ci	ipture rise	
Viewing Capture Capture Live Capture Save As File - Save As Save current capture file Image: Capture View - Colorize Colorize the packet list Close File - Close Close current capture file Image: Capture View - Zoon In Zoon into the packet data (increase) Reload View - Reload Reloads current capture file Image: Capture file Image: Capture file Image: Capture file		Open	File →	Open	Opens "File open" dialog box to load a	capture for	100	Auto Sc	roll in Live	View → Au	to Scroll i	n Auto	scroll pack	t list during	live capture	
Image: Save As File - Save As Save current capture file Image: Colorize View - Colorize Colorize the packet list Image: Colorize File - Close File - Close Close current capture file Image: Colorize View - Zoon In Zoon into the packet data (increase) Image: Colorize View - Reload Reloads current capture file Image: Colorize View - Zoon Out Zoon out of the packet data (increase)	_				viewing		1.00	0	apture	Live	Capture					
Close File → Close Close current capture file Zoom In Zoom In Zoom into the packet data (increased) Close Neload View → Reload Reloads current capture file Q Zoom Out View → Zoom Out Zoom out of the packet data (decreased)		Save As	File → Sa	ave As	Save current capture file			0	olorize	View -	Colorize		Colorize the	packet list	(or not)	
Reload File → Close Close current capture file Q Zoom In View → Zoom In Zoom into the packet data (increation) Image: Second Contemport View → Reload Reloads current capture file Q Zoom Out View → Zoom Out Zoom out of the packet data (decreation)																
Reload View -> Reload Reloads current capture file Zoom Out View -> Zoom Out Zoom Out Zoom Out Zoom Out Down out of the packet data (decree)	×	Close	File \rightarrow	Close	Close current capture file		O.	z	oom In	View -	+ Zoom In	Zoom int	to the packet	data (increas	e the font si	
C Relaad View> Relaad Relaads current capture file C Zoom Out View -> Zoom Out Zoom Out Zoom out of the packet data (decree,	-															
	0	Reload	$\texttt{View} \rightarrow$	Reload	Reloads current capture fil	e	e,	Z	oom Out	View →	Zoom Out	Zoom out	of the packe	t data (decrea	se the font s:	
	0		1.117 1.117			10.020	0			0.000			201			
G Find Packet Edit → Find Packet Find packet based on different criteria C Normal Size View → Normal Size Set zoon level back to	4	Find Packet	Edit -+ Fina	d Packet	Find packet based on different c	riteria	2	Nor	mal 51ze	View -> 1	Normal Size		Set zoom	level back to	100%	
	-	Pr		a Barah	And have been an and second have	-	11				- 1 C-1					

(Keary 2020)

1.2 Alert Response Procedures

As part of an increased network security focus, NSSD has engaged in the use of an intrusion detection system (IDS) to monitor the network: "IDS are automated systems that monitor and analyze network traffic and generate "alerts" in response to activity that either match known patterns of malicious activities or is unusual. In some cases, alerts trigger further automated processes such as recording the suspect activity and/or scanning the computer(s) involved for signs of compromise" (Berkeley 2021).

To effectively respond to detected events, IT personnel are to utilize wireshark in investigating the potential threat. The following procedures are to be followed in the event of an IDS alert:

- IDS sends alert that anomalous traffic has been detected

- IT personnel immediately perform packet capture via wireshark

- In accordance with alert type, IT personnel will filter wireshark capture (for example, if IDS detects unusual http traffic, personnel shall filter packet capture by http)

- Once suspicious/unusual activity is located, a report should be generated and submitted to management for immediate review.

Significance of Alert Response

The appropriate response to security alerts could mean the difference between stopping a data breach or malware infestation before it is successful. Network monitoring establishes an activity baseline, and the IDS will help to identify any deviations from this baseline. It is up to IT personnel to then isolate and investigate the security threat. Wireshark is NSSD's tool of choice for these investigations, and proper utilization will help the department quickly understand what threat is faced and where.

The response to these threats is as important and their identification. Following procedures results in a much quicker event reaction and has the potential to stop or reduce the severity of an attack.

Section Two: Firewalls

2.1 Firewall Fundamentals

One of the key components of NSSD's network security is the deployment of firewalls. A firewall monitors both incoming and outgoing traffic, and can be configured to block or allow traffic based on predetermined security rules. Another benefit of firewalls is that they can be used to create detailed reports and logs, both of which can help the IT department in troubleshooting issues, as well as maintaining regulatory compliance.

Among the firewall tools that NSSD uses is the Windows Firewall, a host-based firewall that provides protection for computers on our network. This type of firewall is especially helpful in preventing the spread of malicious software via network traffic, such as trojan horse attacks and worms. Due to the widespread use and applicability of Windows Firewall, IT personnel should familiarize themselves with enabling the firewall, rule creation, and how to block/allow/filter traffic.

Example B: Blocking HTTP and Allowing HTTPS traffic using Windows Firewall

First, you will access the Windows Firewall as outlined above in steps 1, 2, 3, and 4 of example A. This time, however, you will click on **Allow a program or feature through windows firewall (1)**



Next, ensure that **secure world wide web services (HTTPS)** (2) is *allowed* by clicking the box next to it and both private/public networks. Ensure the World Wide Web Service (HTTP) (3) is *blocked* by making sure it is *not selected*. Click OK to save these changes and you have successfully blocked HTTP traffic and allowed HTTPS traffic on this computer.

Allow programs to communicate through Windows Firewall			
To add, change, or remove allowed programs and ports, click Change set	tings.		
What are the risks of allowing a program to communicate?	💝 Cha	nge settings	
Allowed programs and features:			
Name	Home/Work (Private)	Public 🔺	
Routing and Remote Access			
⊠sampleflag-999818.exe			
Secure Socket Tunneling Protocol			
Secure World Wide Web Services (HTTPS) 2			
☑Simple Mail Transfer Protocol (SMTP)			
SNMP Trap			
⊠Telnet	V	¥.	
Telnet server Remote Administration			
□Windows Firewall Remote Management			
□Windows Management Instrumentation (WMI)			
□Windows Remote Management			
Windows Security Configuration Wizard			
World Wide Web Services (HTTP) 3	V		
	ОК	Cancel	

Especially with the increase in successful cyber-attacks across a wide swathe of businesses and industries, NSSD seeks to improve our network security through the concept of network segmentation: "network segmentation is the act of dividing a computer network into smaller physical or logical components. Two devices on the same network segment can then talk directly to each other. For communication to happen between segments, the traffic must flow through a router or firewall. This passage allows for traffic to be inspected and security policies to be applied" (NAS 2021). The creation of multiple subnets within a network makes it much more difficult for an attacker to access the network in its entirety, because firewalls between the segments are able to block traffic. As IT personnel, it is essential for you to understand the steps required for segmenting networks, which can be accomplished via Windows Firewall by configuring profiles: Domaine, Private, and Public. Each profile will protect connections according to their network location type, thus grouping different areas of the network into like location types will effectively segment it.

Example C: Windows Firewall Network Locations Public vs. Private Recall the previous example's allowed programs list. To navigate back, open the firewall and click on **allowed programs and features**. Here you will find the columns are sorted by network location and contain two profiles: public and private. By checking the appropriate boxes, for example, you may allow only HTTP traffic on private profiles and only HTTPS on public profiles.

Allow programs to communicate throug	h Windows Firewall			
To add, change, or remove allowed programs a	and ports, click Change settings.			
What are the risks of allowing a program to co	mmunicate?	😽 Cha	nge settings	
Allowed programs and features:			\frown	7
Name	(Home/Work (Private)	Public +	É l
☑1-flag5-567891				
BranchCache - Content Retrieval (Uses H	TTP)			
□BranchCache - Hosted Cache Client (Uses	HTTPS)			
□BranchCache - Hosted Cache Server (Use	s HTTPS)			
□BranchCache - Peer Discovery (Uses WSD))			
COM+ Network Access				
□COM+ Remote Administration				
☑ COM+ Server Replication	🥚 😑 📄 — Edited ~			
☑ Core Networking	¶ → Helvetica ≎ Reg		•	
☑DFS Management	▼ ► ► ►		V	
Distributed Transaction Coordinator	0 1 2			
☑ File and Printer Sharing	Brett Logan		•	
⊠flag2-222889.exe	0010 0, 2021		2	
☑ FTP Server			¥ _	
		Details	Remove	
		Allow anothe	r program	_
ving the same settings to a	Il hosts within a	segment of	vour n	etwork
ying the same settings to a		segment of	your n	CIWOIN
esult in only those hosts all	lowing (or blocki	ng) a partici	ular pr	ogram.
		OK	Cancel	

Guidelines for Implementation of Methods for Detecting Attacks

Many attacks can be identified by anomalous traffic on the network. One common tactic that attackers can use against companies is distributed denial of service, or DDoS. This method involves overwhelming a network with large amounts of requests, causing systems and services to shut down. IT personnel are encouraged to identify the potential for this type of occurrence by monitoring unusual firewall activity such as numerous failed access attempts. Firewall logs keep a record of all activity, and IT Personnel are able to set up logging in Windows Firewall by undertaking the following:

-Open Windows Firewall with Advanced Security. Right-Click on Windows Firewall with Advanced Security and go to Properties.



-Recalling the previously mentioned profiles, for this example choose private

-Click Private Profile > Logging > Customize

Firewall state: Off Inbound connections: Block (default) Outbound connections: Allow (default)	ault) 💌
Inbound connections: Block (default) Outbound connections: Allow (default)	iault) 💌
Outbound connections: Allow (default)	ault) 💌
Protected network connections: Custo	Customize
Settings	
Specify settings that control Windows Firewall behavior.	Customize
Logging	
Specify logging settings for Custo	Customize
troubleshooting.	$\overline{}$

-Under log dropped packets, switch to YES

-copy the default path for the log file. ($\$systemroot\$\system32\LogFiles\Firewall\pfirewall.log$) and then Press OK

ustomize Logging	Settings for th	ne Private Pr	ofile	
Name:	6\system32\LogF	Files\Firewall\p1	firewall.log	Browse
Size limit (KB):	4,096	÷.		
Log dropped packets	:	Yes		•
Log successful conne	ections:	No (d	efault)	•
Note: If you are confi that the Windows Fire containing the log file	guring the log file ewall service acc	e name on Gro ount has write	up Policy ob permission:	oject, ensure s to the folder
Default path for the lo %systemroot%\syste	og file is m32\logfiles\firev	vall\pfirewall.loc	>	
Learn more about log	iging			
			ОК	Cancel

-Open File Explorer and Browse to where the Windows Firewall log is stored, you will see a pfirewall.log Copy this to your desktop to create a shortcut to the logs.

Creating a shortcut such as this makes reviewing and analyzing firewall logs easier, and IT Personnel are encouraged to familiarize yourselves with types of traffic and what typical logs look like. While this is just one method for detecting attacks using firewalls, it can be highly effective.

Section Three: Intrusion Detection and Prevention

3.1 Significance of Intrusion Detection and Prevention Systems (IDPS)

IDPS is a core piece of NSSD's overall cybersecurity posture. Our intrusion detection system allows the ability to monitor and analyze network traffic to uncover potential security incidents, violations, or threats, while the intrusion prevention system acts to stop those detected threats. Our IDPS relies on anomaly-based methods to detect attacks, for example "a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours. The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly" (NIST 2021). This why all IT personnel must understand how to navigate and utilize our chosen intrusion detection system, Snort.

3.2 IDPS Tools and Methodology A. Snort: Snort is a program that allows capture and analysis of traffic, helping to identify anomalies such as unwanted incoming or outgoing traffic. For IT personnel to effectively use snort, you must first use a sniffer to record traffic, and then send the captured traffic to a file to be analyzed. *note: a sniffer should operate in promiscuous mode to see all network traffic. At NSSD this is accomplished by connecting the sniffer to the Switched Port Analyzer (SPAN) port. B. Linux distribution Kali 2: this is the sniffer used to capture traffic and send it to a file for analysis using snort. The Linux/UNIX utility *tcpdump* is used by IT personnel to capture network traffic. To view available switches for *tcpdump*, you can use the command: root@kali2:~# tcpdump --help --help vers 1.0.1k 8 2015 Jan 2015 aAbdDefhHIJKlLnN0pqRStuUvxX#] [-C file size] [-E algo:secret -B size seconds tstamptype] [-M secret --number] interface in|out|inout] --time-stamp-precision precision -s snaplen 1 V file 1 /ersion [-y datalinktype] [-z command filecount expression] To run tcpdump on the network interface (eth0 for example) is connected to, use the command: root@kali2:~# tcpdump -i eth0 ali2: # tcpdump -i eth0 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode To stop capturing traffic via the sniffer, press: Ctrl + CTo capture traffic and send it to a file for analysis, use command: root@kali2:~# tcpdump -i eth0 -nnntt -s 0 -w capnet1.cap -C 100

And finally, to better understand the above syntax, please refer to the following table:



Example: Detect an attack using Snort to analyze network traffic log files. In this example the NSSD network is under attack by a hacker using brute force tactics in an attempt to gain administrator account access.

Step 1: Use the following command to view a newly created alert.ids file: root@kali2:~# ls

Step 2: Use the following command to analyze the file: root@kali2:~# leafpad alert.ids

Step 3: Be on the lookout for clusters of alerts grouped close together, an indicator of attack. In this example the numerous repeated bad logins timed closely together are indicative of the brute force attack software trying various passwords in quick succession.



C. Whitelisting and Blacklisting

Two methods of managing network access are whitelisting and blacklisting. NSSD's IDPS utilizes these lists in an effort to prevent malicious activity and only allow access for approved users and programs. Whitelists are a list of benign entities that are allowed access, while on the opposite end of the spectrum blacklists are a list of entities that are blocked. These entities might include hosts, applications, usernames, specific ports, and file names/extensions. All NSSD IT personnel should be familiar and up to date with these lists, which can change frequently depending on updated threats and new users.

As you attempt to identify network traffic that may need to be whitelisted or blacklisted, it is helpful to create custom rules to alert for certain occurrences such as file name, account name, or output from an executed file. You can do so by editing the local.rules file in Snort.

Example: Editing The local.rule File in Snort to Detect Particular Types of <u>Traffic</u>

Step 1: Open the local rules file by entering the following command: root@kali2:~# leafpad /etc/snort/rules/local.rules

Step 2: Edit the rule (as shown circled in red) to alert for the type of traffic needed



Step 3: Be sure to save the edit by clicking **File** \rightarrow **Save**

File	Edit	Search	Options	Help
Ne	ew		Ct	rl+N
Op	Open Ctrl+			
Sa	ve		C	trl+S
Sa	ive As		Shift+C	trl+S
Pr	int Pr	eview	Shift+C	trl+P
Pr	int		C	trl+P
Qu	uit		Ct	rl+Q

Congratulations, you have now successfully edited a rule to look for certain types of traffic on the NSSD network. As you can see, the combination of sniffers, log analysis, and custom rule editing enables IT Personnel to exercise greater control and utilization of our intrusion detection and prevention systems, thus keeping our network safe.

Section Four: Vulnerability Assessment

Vulnerability scans are an important part of NSSD's network defense because they provide feedback on the health and security of the network, helping identify abnormal behaviors and vulnerable devices.

Using Wireshark, IT employees may discover malicious activity of an attacker based on the output after certain filters are applied. These outputs are a result of a potential attacker running various scans in an attempt to breach our network, typically by finding open ports. As part of a vulnerability assessment, IT personnel may also use the same nmap scanning methods that a would-be attacker does. This gives critical insight into network vulnerabilities that security teams can then mitigate.

4.1: NMAP Scanning and Detecting

The following chart shows the scan technique, the command used to run the scan, and the Wireshark filter which will reveal resulting traffic to indicate the scan has taken place. The <target> section of the command is replaced with the desired IP address.

Technique Used	Wireshark Filter	Command
TCP SYN	tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size<=1024	nmap -sS <target></target>
TCP connect ()	tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size>1024	nmap -sT <target></target>
TCP Null	tcp.flags==0	nmap -sN <target></target>
TCP FIN	tcp.flags==0x001	nmap -sF <target></target>
TCP Xmass	tcp.flags.fin==1 && tcp.flags.push==1 && tcp.flags.urg==1	nmap -sX <target></target>

UDP port	icmp.type==3 and icmp.code==3	nmap -sU <target></target>
		(Infosec 2021)
Summary of scan tech	nnique and purpose:	

TCP SYN scan: detection of numerous packets in a short time indicates an attacker may be running SYN scans, SYN port sweeps, or SYN floods.

TCP connect () scan: identical to SYN scan, but with a larger window size revealing TCP connection which indicates an attacker may be conducting port scans or sweeps.

TCP Null: An attacker might send packets without flags set in an attempt to discover open ports.

TCP FIN: An attacker might also set only the FIN flag in attempt to bypass firewalls and discover open ports.

TCP Xmass: Another way an attacker may seek to discover open ports is by sending packets with FIN, PUSH, and URG flags set.

UDP Port scan: A high number of ICMP packets showing port/destination unreachable may indicate the attacker is running UDP port scans.

It is helpful to think like a would-be attacker might, trying various methods to poke and prod the network in search of any openings or weak points. Following are examples using nmap to conduct network vulnerability tests.

To start, one might seek to identify any live hosts in the network, which can be accomplished via ping scan. For example, to identify all live hosts with a network ID of 10.1.1.* you would use the command: root@Kali-Attacker:~# nmap -sP 10.1.1.*



To initiate a ping scan while simultaneously spoofing the source MAC address, use command **nmap** –**v** –**sP** –**spoof-mac 0 10.1.1.***

Host is up (0.00020s latency). Nmap done: 256 IP addresses (2 hosts up) s	canned in 14.26 seconds
<pre>Groot@Kali-Attacker:~# nmap -v -sP -spoof-m</pre>	ac 0 10.1.1.*
Starting Nmap 6.47 (http://nmap.org) at Spoofing MAC address CE:2E:D5:9A:37:42 (No	2021-06-19 20:00 EDT
Initiating Ping Scan at 20:00	
Scanning 256 hosts [4 ports/host]	
Ping Scan Timing: About 15.28% done; ETC:	20:04 (0:02:52 remaining)
Ping Scan Timing: About 29.93% done; ETC:	20:04 (0:02:23 remaining)
Ping Scan Timing: About 59,13% done: ETC:	20:04 (0:01:24 remaining)
Ping Scan Timing: About 73.78% done; ETC:	20:04 (0:00:54 remaining)
Completed Ping Scan at 20:04, 206.22s elap	sed (256 total hosts)
Nmap scan report for 10.1.1.0 [host down]	
Nmap scan report for 10.1.1.1 [host down]	e Edited ~
Nmap scan report for 10.1.1.2 [host down]	
Nmap scan report for 10.1.1.4 [host down]	1 Melverica C Reg
Nmap scan report for 10.1.1.5 [host down]	
Nmap scan report for 10.1.1.6 [host down]	Brett Logan
Nmap scan report for 10.1.1.7 [host down]	June 18, 2021
Nmap scan report for 10.1.1.8 [host down]	
Nmap scan report for 10.1.1.9 [host down]	e, the more you are attre to near.



In the following image, the *nmap -sT 192.168.1.6* command is used to scan the network for vulnerable systems (note this command is a TCP connect () scan as indicated in the chart above). The output indicates that TCP ports 22, 25, 80, and 514 are all open.



NMAP may even be used to discover what operating system and device is in use by

making approximate guesses until the correct one is discovered using command:

nmap -O --osscan-guess 192.168.1.50



These types of scans can be detected in Wireshark based upon certain traffic patterns they create.

Example A: Detecting SYN scans using Wireshark

Step 1: After opening Wireshark and running capture, enter filter as shown in chart above

Step 2: Click *Apply*

Step 3: Correct filter syntax will appear with a green background. In this instance we are

filtering out packets with Syn flag not set, ACK flag not set, and window size <= 1024

bytes

Step 4: The scan shows a high amount of SYN packets, indicating an attacker may be

running nmap -sS <target> to run SYN scans in the network.



4.2 Detecting Network Attacks Using Wireshark

Just as various port scans can be detected using Wireshark filters, so too can potential network attacks. IT personnel are instructed to use the following filters in Wireshark to reveal corresponding attacks

Technique	Wireshark Filter	Command/Tool
ARP poisoning	arp.duplicate-address-detected or arp.duplicate-address-frame	arpspoof, ettercap
ICMP flood	icmp and data.len > 48	fping, hping

Unexplained packet loss		
	tcp.analysis.lost_segment or tcp.analysis.retransmission	Not Applicable
mary of scan technique	and purpose:	(Infosec 2021)
Poisoning : Also know	n as ARP spoofing, this allows an atta	acker to initiate a man-in-
niddle attack. Using thi	is filter will reveal if a single IP addre	ss is being claimed by
than one MAC address	s, a likely indicator of such attack.	
IP flood : By filtering fo	r large data size, IT personnel can det	ect oversized ICMP
tets indicative of an attac	cker attempting a denial-of-service att	ack.
AN hoping : This filter c	an reveal packets tagged with multiple	e VLAN tags, indicating
ttacker's attempt at bypa	assing network access controls.	
Example B: Dete	ecting Denial-of-Service Attack Us	ing Wireshark
p 1: After opening Wires	hark and running capture, enter filter	as shown in chart above
p 2: Click <i>Apply</i>		
ep 3: Again, if the syntax	is correct, filter background should ap	ppear green. With this
er you are filtering for pa	ckets with larger than 48 bytes of data	1.

Step 4: The protocol section of Wireshark reveals a large number of ICMP packets, a good indication that an attacker is flooding the network intentionally to perform a denial-of-service attack.



As you can see, there are many uses of NMAP in vulnerability assessment, as well as corresponding Wireshark filters to detect such activity if it is malicious rather than being performed for assessment purposes.

Using these tools helps identify and rectify any weaknesses or misconfigurations in the NSSD network.

Section Five: Network Scanning and Assessment

Network scanning is an essential piece of NSSD's overall cybersecurity program. Scans can help IT personnel protect the network from attack by identifying weaknesses or vulnerabilities. Often an attacker will initiate a scan themselves to surveil the network before attack, and the identification of such scans can help analysists understand the method and route of attack. Scan results can offer details such as

-IP Addresses

-Open Ports

-Operating System

-Vulnerabilities

5.1 Network Scanning

Using the filter in Wireshark allows detection of malicious activity based upon certain atypical traffic which reveals that a scan has taken place. The following scan types and their corresponding Wireshark filters are a valuable tool:

Ping Sweep

This type of scan reveals which IP addresses are active on the network. To detect the presence of such scans using Wireshark, the following filters are used:

Detecting an icmp ping sweep

icmp.type==8

icmp.type==0

Detecting a TCP ping sweep

tcp.dstport==7

Detecting a UDP ping sweep

rt==7				
ed increase ir	ı packets as	revealed by	y these filters	may indicate a
	capnet1.cap [W	/ireshark 1.12.6 (Git R	ev Unknown from unknown] •••
File Edit View Go C	apture Analyze Statist	tics Telephony Tools	Internals Help	
• • 🖌 🗖 🧷	n 🗋 🗶 ၈ ۹	. + + -2 ∓ ±	.	🗄 📓 🔛 🔛 📰 🚺
Filter: icmp.type==8	>	- Exp	ression Clear Apply Save	
No. Time	Source	Destination	Protocol Length 1	nfo
169 62.398121	216.1.1.200	10.0.0.1	ICMP 60 I	Echo (ping) request id=Ox
170 62.398147	216.1.1.200	10.0.0.2	ICMP 60 I	Echo (ping) request id=Ox
1/1 62.398155	216.1.1.200	10.0.0.3	TCMP 60 1	cho (ping) request id=0x
173 62.398207	216.1.1.200	10.0.0.5	TCMP 60	-cho (ping) request id=0x
174 62.398211	216.1.1.200	10.0.0.6	ICMP 60	Echo (ping) request id=0x
176 62.398249	216.1.1.200	10.0.0.7	ICMP 60	Echo (ping) request id=Ox
177 62.398252	216.1.1.200	10.0.0.8	ICMP 60 I	Echo (ping) request id=Ox
178 62.398252	216.1.1.200	10.0.0.9	ICMP 60 1	Echo (ping) request id=Ox
179 62.398302	216.1.1.200	10.0.0.10	ICMP 60 I	Echo (ping) request id=0x
181 62,398423	216.1.1.1	216.1.1.200	ICMP 70	Redirect (Redi
100 03.398380	216.1.1.200	10.0.0.13		(-i)
Frame 169: 60 byte	s on wire (480 bits)	, 60 bytes captured	(480 bits)	
• Ethernet II, Src:	Vmware_02:25:46 (00:	:50:56:02:25:46), Ds	t: Vmware_02:2e:9a (00:	50:56:02:2e:9a)
Internet Protocol	Version 4, Src: 216.	1.1.200 (216.1.1.20	o), Dst: 10.0.0.1 (10.0	.0.1)
 Internet Control M 	lessage Protocol			- Edited ~
0000 00 50 56 02 20	94 00 50 56 02 25	46.09.00.45.00 P	DV&E E	Helvetica C Reg
0010 00 1c 7d 25 00	00 30 01 29 f2 d8	01 01 c8 0a 00	%0.)	
0020 00 01 08 00 58	26 9f d9 00 00 00	00 00 00 00 00	X&	Brett Logan
	00 00 00 00 00 00			June 23, 2021
🔵 💅 File: "capnet 1.cap" :	242 kB 00:07:01 Pa	ckets: 2875 · Displayed: 59.	(20.6%) · Load time: 0:00.012	Profile: Default

ARP Sweep

When filtering by ARP in Wireshark, personnel can look for an ARP sweep which indicates an attacker has sent an ARP broadcast for every IP in a subnet, hoping for a response which would indicate which IP addresses are active. The signature of this scan type is the use of "ff:ff:ff:ff:ff:ff:ff for the destination MAC which is used for broadcast.



Stealth Scan/TCP Half Open

Used to detect which ports are open or closed, an attacker can initiate a TCP connection by sending a SYN packet to the targeted port. Open ports will respond with SYN+ACK and closed ports will respond with RST of RST+ACK. When the attacker discovers an open port, they will respond with RST to avoid making an actual TCP connection. In Wireshark, the signs of this type of scanning include numerous TCP sessions with less than 4 packet communications, and/or many RST packets.

TCP Full Connect Scan

Unlike a stealth scan, this method results in the attacker responding to the TCP+ACK with ACK to establish a TCP connection and then terminate it. The following Wireshark filters can be utilized to find SYN, SYN+ACK,RST, and RST+ACK packets:

tcp.flags==0x002 tcp.flags==0x012 tcp.flags==0x004

tcp.flags==0x014

	capnet1.cap [Wireshark 1.1]	2.6 (Git Rev Unknown from unknown)]	000
File Edit View Go Capture A	nalyze Statistics Telephony Tools	Internals Help	
© 🖲 🛋 🖉 🛅 🗋	* o く + + ふ <u>*</u> Ŧ	🗐 😨 e e e e 🗹 🎬 🕅 🕵	5 2
Filter: arp	- Exp	ession Clear Apply Save	
No. Time Source	Destination	Protocol Length Info	
21 97.35307 Vimare_ 22 9.448521 Vimare_ 25 10.363392 Vimare_ 26 10.363392 Vimare_ 21 2.797100 Vimare_ 31 12.797137 Vimare_ 34 12.797137 Vimare_ 36 3.452094 Vimare_ 37 13.452094 Vimare_	22/20190 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:98 Broadcast 22:20:99 Broadcast	APP 60 who has 128.0.1 APP 60 who has 128.0.3 APP 60 who has 128.0.3	4.1297 Tell 216.1.1.1 4.1297 Tell 216.1.1.1 4.1297 Tell 216.1.1.1 0.607 Tell 216.1.1.1 1.077 Tell 216.1.1.1 2.537 Tell 216.1.1.1 4.1297 Tell 216.1.1.1 1.077 Tell 216.1.1.1 2.537 Tell 216.1.1.1
41 14.481701 Vmware_ 42 14.481725 Vmware_	02:2e:9a Broadcast 02:2e:9a Broadcast 02:2e:9a Broadcast	ARP 60 Who has 193.0.14 ARP 60 Who has 128.9.0. ARP 60 Who has 128.63.2	4.1297 Tell 216.1.1.1 .1077 Tell 216.1.1.1 2.537 Tell 216.1.1.1
 Frame 21: 60 bytes on wire Ethernet II, Src: Vmware_0 Address Resolution Protoco 	(480 bits), 60 bytes captured 2:2e:9a (00:50:56:02:2e:9a), Dst l (request)	480 bits) Broadcast (ff:ff:ff:ff:ff:ff)	Edited ~
0000 ff f	0 56 02 2e 9a 08 06 00 01 0 56 02 2e 9a d8 01 01 01 0 0e 81 00 00 00 00 00 00 0 00 00 00 00	P V	F F F F 0 1 2 Brett Logan June 23, 2021

TCP Null Scan

Here the attacker sends a TCP packet with no flags to look for an RST response from closed ports. To look for this type of scan in Wireshark use filter:

tcp.flags==0x000

UDP Scan

A high number of packets with ICMP type 3 Code 3 can indicate an attacker sending UDP packets to a port to discover whether it is open or closed (this response indicates to the

attacker that the port is closed). To search for this type of scanning, use Wireshark filter:

icmp.type==3

icmp.code==3



Example: In this image IT Personnel can discover unwanted outgoing traffic, indicating a malicious actor has breached the network.

Stream Co	ntent				1					
[b.7a [B (3D Copyright	U.t\$.23= ,.3"m s.nxnsl". .~xz t (c) 2006 M	1]iw.j .M= icrosoft	TP:V. S.CQ .tCzX(F	Thicrosoft W	LDM.d.#C d.sn j.A' Windows rights r	[Version 6 reserved.	6.0.60	001]	(S#;	- 0
C:\Users	Administrat	or\Deskt	op>dir							
Volume 1 Volume 1	in drive C h Serial Numbe	as no lat r is 2891	bel. 1-8AEB							1 1 2 2
Director	ry of C:\Use	rs\Admini	istrator	Desktop						
11/21/20 11/21/20 11/21/20 10/01/20	16 11:51 AM 16 11:51 AM 16 11:51 AM 16 10:41 AM	<dir: <dir:< td=""><td>> 60 1,7</td><td>54 chrome -</td><td>Shortcu</td><td>ut.lnk</td><td></td><td></td><td></td><td>Data</td></dir:<></dir: 	> 60 1,7	54 chrome -	Shortcu	ut.lnk				Data
05/20/20 06/09/20 11/06/20 C:\Users' Entire co	14 11:59 PM 14 08:33 PM 16 11:47 AM 4 Fil 3 Dir \Administrat	<pre><dir: e(s) (s) 1,(or\Deskto 53 bytes)</dir: </pre>	7: 85 4,1 601,343,4 0p거	79 hMailServ 55 Internet Updates 009 bytes 488 bytes fr	ver Admi Explore	nistrator. er.lnk	. lnk	Helvetica Helvetica For homogenetica Brett Logan June 9, 2021	- Edited ~) Data (CK] Seq=272) Data (CK] Seq=272) Data (CK] Seq=272) Data) Data
05/20/20 06/09/20 11/06/20 C:\Users' Entire col	14 11:59 PM 14 08:33 PM 16 11:47 AM 4 Fil 3 Dir \Administrat nversation (10 Save As	<dir e(s) (s) 1,4 or\Deskto 53 bytes) Print</dir 	7: 8: 601,343,4 야거 〇 ASCII	79 hMailServ 55 Internet Updates 09 bytes 488 bytes fr	ree	nistrator er.lnk Hex Dump	. lnk	Helvetica The Helvet	Edited ~	Data CK] Seq=272 Data CK] Seq=272 Data CK] Seq=272 Data Data CK] Seq=276
05/20/20 06/09/20 11/06/20 C:\Users' Entire col Find Help	14 11:59 PM 14 08:33 PM 16 11:47 AM 4 Fil 3 Dir \Administrat nversation (10 Save As	<dir: e(s) (s) 1,e or\Deskto 53 bytes) Print</dir: 	7 8 4,(601,343,4 야거 〇 ASCII	79 hMailServ 35 Internet Updates 009 bytes 488 bytes fr	ree IC O Filter	Hex Dump	. lnk O ream	Theiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica To Heiretica	Edited ~ C Reg T C Reg C R	Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=276 Data (CK) Seq=276 Data (CK) Seq=276 Data (CK) Seq=276 Data
05/20/20 06/09/20 11/06/20 C:\Users' Entire co Find Help Secure S	14 11:59 PM 14 08:33 PM 16 11:47 AM 4 Fil 3 Dir Administrat nversation (10 Save As Sockets Laye	<dir e(s) (s) 1,4 or\Deskto 53 bytes) Print</dir 	7 8 4,(601,343,4 0p>	79 hMailSeri 55 Internet Updates 009 bytes 488 bytes fr	ree IC O Filter	Hex Dump	. lnk O ream	The Helvestica The Helvestica	 Edited ~ Reg Pr Pr	Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=272 Data (CK) Seq=276 Data (CK) Seq=276 Data (CK) Seq=276 Data (CK) Seq=272 Data (CK) Seq=276 Data (CK) Se

5.3 Viewing Network Topologies

While Wireshark doesn't specifically offer a topology illustration, it is still possible to determine network topology by monitoring traffic and paying close attention to IP/MAC addresses within the network. Monitoring traffic between these addresses helps to create a picture of network locations and establish norms for network activity. Note the source and destination columns in your Wireshark Capture revealing IP addresses:



Section Six: Auditing and Log Collection

Network auditing is a key responsibility of IT personnel at NSSD. A properly executed audit provides information such as security risks, allowing for changes to the network to keep our data safe. These audits also help map and inventory the network to ensure visibility and proper administration efforts.

When auditing to diagnosing a specific network problem, Wireshark is especially useful due to the specificity of data that it reveals. Among the tools that personnel can use to garner deeper levels of information is the analyze menu:



A breakdown of menu items and their description is as follows:

Menu Item	Accelerator	Description
Display Filters		Displays a dialog box that allows you to create and edit display filters. You can name filters, and you can save them for future use.
Display Filter Macros		Shows a dialog box that allows you to create and edit display filter macros. You can name filter macros, and you can save them for future use.
Apply as Column	Shift+Ctrl+I	Adds the selected protocol item in the packet details pane as a column to the packet list.

Apply as Filter		Change the current display filter and apply it
		immediately. Depending on the chosen menu
		item, the current display filter string will be
		replaced or appended to by the selected protocol
		field in the packet details pane.
Prepare as Filter		Change the current display filter but won't apply
		it. Depending on the chosen menu item, the
		current display filter string will be replaced or
		appended to by the selected protocol field in the
		packet details pane.
Conversation		Apply a conversation filter for various protocols.
Filter		
Enabled	Shift+Ctrl+E	Enable or disable various protocol dissectors
Protocols		
Decode As		Decode certain packets as a particular protocol
Follow \rightarrow TCP		Open a window that displays all the TCP
Stream		segments captured that are on the same TCP
		connection as a selected packet
Follow \rightarrow UDP		Same functionality as "Follow TCP Stream" but
Stream		for UDP "streams".

Follow \rightarrow TLS	Same functionality as "Follow TCP Stream" but
Stream	for TLS or SSL streams. See the wiki page
	on <u>TLS</u> for instructions on providing TLS keys.
Follow \rightarrow HTTP	Same functionality as "Follow TCP Stream" but
Stream	for HTTP streams.
Expert Info	Open a window showing expert information
	found in the capture. Some protocol dissectors
	add packet detail items for notable or unusual
	behavior, such as invalid checksums or
	retransmissions. Those items are shown here. The
	amount of information will vary depend on the
	protocol

(Wireshark 2021)

Loopback Traffic

Useful for diagnostics and troubleshooting, loopback traffic is the communications a device has with itself. To view this traffic, be sure to install ncap along with Wireshark. This creates the loopback interface, and on the initial Wireshark screen select and double click the *adapter for loopback traffic capture*. This traffic can be analyzed like other captured traffic using the above menu to gain greater detail.

Creating/Saving Logs

Logs are useful for IT personnel because they allow revisiting of network activity, giving the ability to search, troubleshoot, and compare. Using Wireshark, follow these directions to save captured traffic in files for later use and regulatory compliance:

- 1. Open Wireshark
- 2. Run Capture
- 3. If there is a known issue of concern on the network, reproduce it
- 4. Stop the capture
- 5. Click File \rightarrow Save As and enter file name (such as case number)
- 6. The log file will be saved in .pcapng format

				K 🔶 🖌 🖉	🕈 👱 🛛		G		e	11					3
Ap	ply a	display filter	. <\$/>>												and the second
0.		Time	Source	Destination	Protocol	Length	Info								20
1	.145	39.519691	13.107.136.9	10.0.0.70	TCP	56	443 →	60385	[ACK]	Seq=4069	Ack=821	Win=524544	Len=0		1
	.146	39.519692	13.107.136.9	10.0.0.70	TLSV1	92	Applic	callon	Data	See-4107	A ek-2261	Win-EDEECO	1 00-0		1
1	147	39.519694	13.107.130.9	10.0.0.70	TCP	56	443 -	60305	[ACK]	Seq=4107	ACK=2201	Win=525566	Len=0		
	140	39.519696	13, 107, 136, 9	10.0.0.70	TCP	56	443 -	60385	[ACK]	Seq=4107	Ack=4233	Win=525568	Len=0		
	150	39.519819	10.0.0.70	13,107,136,9	TCP	54	60384	→ 443	[ACK]	Seg=1411	Ack=4107	Win=262080	Len=0		6.3
	151	39.519820	10.0.0.70	13.107.136.9	TCP	54	60383	- 443	[ACK]	Seg=1449	Ack=4107	Win=262080	Len=0	-	1
	152	39.519820	10.0.0.70	13.107.136.9	TCP	54	60385	→ 443	[ACK]	Seg=4233	Ack=4107	Win=262080	Len=0		1
1	153	39.567176	13.107.136.9	10.0.0.70	TLSv1	1050	Applie	ation	Data						
1	154	39.567258	10.0.0.70	13.107.136.9	TCP	54	60384	→ 443	[ACK]	Sea=1411	Ack=5103	Win=261120	Len=0		1
	lTin	ne delta fr	om previous captured	frame: 0.000002000 se	condsJ										1
	[Tin	me delta fr	om previous displaye	d frame: 0.000002000 s	econds]					Wiresh	ark - Save C	apture File As			
	[Tin	me since re	ference or first fram	ne: 39.519691000 secon	ds]										
	Fran	ne Number:	1145			Look in	. 7	1					000	00	
	Fran	ne Length:	56 bytes (448 bits)			LOOK III.		- /							
	Cap	ture Length	: 56 Dytes (448 Dits)			amputor	1	Name			^ Size	Kind	Date Modif	fied
	(Fr	ame is mark	ed: raisej				omputer		Applica	tions			Folder	7/2/21 12	:21 PM
	[Pr	ane is igno	frame: eth:ethertype	in:tcn:vssmonitorinal		1 b	rettlogar	(📄 💼	Library				Folder	6/11/21 3	:48 AN
	[Co	loring Rule	Name: TCP]	ip. ccp.vasmonicoring)					System	č.			Folder	7/13/20 2	2:43 AM
	[Co	loring Rule	String: tcpl		-			1.00	Users				Folder	7/13/20 2	:41 AN
)00)10)20)30	3c 00 08	22 fb 9b 5 28 2f fb 4 46 01 bb e 01 f6 a9 0	d 6b f4 c1 14 b5 b3 0 00 74 06 37 1b 0d b e1 8a f7 61 4c a7 0 00 f6 a9	37 08 00 45 00 <" 6b 88 09 0a 00 (f) 7b 8f 93 50 10 (F) (▼) Helvetica C ▼]k7 @.t. 7k aL Reg			0							
				o 1 Brett Logan July 1, 2021	2	File nar	me: Ent	er Case	a Numbr	er Here as F	ile Name	>			Save
						-									Cance
1	* -	The frame match	ed this coloring rule string (fra	me.coloring_rule.string)		Save as	a: V	lireshar	k/ po	capng				÷	Help
						Con	npress w	ith gzip	,						

Troubleshooting Tip:

Creating two Wireshark analysis sets can help IT personnel in diagnosing errors. Running an analysis on a problematic machine and also on a functional machine and then comparing the results can offer valuable insight.

Tools Overview

Wireshark

The focus of this manual, "wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998" (Wireshark 2021). IT personnel at NSSD will benefit from familiarization with Wireshark and its many useful features in ensuring better network understanding and security.

<u>Nmap</u>

Short for "network mapper", this utility for network discovery and security auditing provides useful functions such as determining open ports.

<u>Snort</u>

This is an intrusion detection and prevention system that offers real-time traffic analysis and packet logging.

<u>Kali 2</u>

Used for penetration testing to ensure network defenses are adequate.

Windows Firewall

Built in firewall that filters traffic and can be used to block unwanted connections.

Section Eight: References

Berkeley. 2021. Berkeley Information Security Office. Intrusion Detection Guideline. https://security.berkeley.edu/intrusion-detection-guideline

Guim, Timothy. 2021. PCH Technologies. Why Do I Need Network Security Monitoring For My Network? <u>https://pchtechnologies.com/why-do-i-need-network-security-</u> monitoring-for-my-network/

Hassan, Waqar UI. 2017. Mena Entrepreneur. The Importance of Network Traffic Analysis. <u>https://menaentrepreneur.org/2017/02/importance-network-traffic-analysis/</u>

Infosec Matters Blog. 2021. Detecting Network Attacks with Wireshark. <u>https://lab.infoseclearning.com/lab/intrusion-detection-using-snort</u>

Keary, Tim. 2020. Comparitech. Wireshark Cheat Sheet. Commands, Captures, Filters, and Shortcuts. <u>https://www.comparitech.com/net-admin/wireshark-cheat-sheet/</u>

National Institute of Standards and Technology (NIST). 2021. https://www.nist.gov

Profitap. 2018. Profitap Blog. 14 Powerful Wireshark Filters Our Engineers Use.

https://insights.profitap.com/14-powerful-wireshark-filters-to-use

Wireshark. 2021. User Reference, Chapter 3. The Analyze Menu.

https://www.wireshark.org/docs/wsug_html_chunked/ChUseAnalyzeMenuSection.

<u>html</u>