## **Intrusion Detection/Prevention**

Intrusion detection and prevention can save companies heaps of money that would be spent on damages/recovery of a network. Using Snort (for detection/prevention) in tandem with Wireshark (for looking at the contents of the alert) allows for a cybersecurity/IT professional to determine the origins and causes of an intrusion. Even simply scanning a network for vulnerabilities can be detected (any good hacker scans first to determine a plan of action). In order to properly set up a program through pfsense (Snort) that detects/prevents intrusions, it must first be configured with the proper settings.

The first step is to locate the package manager in pfsense. From your internal network, open a browser window and type in the LAN interface IP address for pfsense (your firewall) and hit enter. To locate Package Manager, click on System>Package Manager in pfsense (screenshot below).



Under available packages, locate Snort and select Install (screenshot next page).

pa - system rac X +				
Not secure https://192.	168.101.1/pkg_mgr	php		
		Package Dependencies: @ lightpd-1.4.59 @ jq-1.6 @ whois-5.5.7 @ rsync-3.2.3_1 @ py-maxminddb-2.0.3 @ libmaxminddb-1.6.0 @ iprange-1.0.4 @ grepcidr-2.0 @ python38-3.8.10 @ php74-7.4.20 @ php74-intl-7.4.20 @ py-sqlite3- 3.8.10_7		
pimd	0.0.3_4	PIMD Multicast Routing. Lightweight, stand-alone implementation of Protocol Independent Multicast-Sparse Mode. Conflicts with Quagga OSPF. These packages cannot be installed at the same time.	+ Install	
		Package Dependencies: Ø pimd-2.3.2_2		
RRD_Summary	2.0_1	RRD Summary Page, which will give estimated month-over-month traffic passed In/Out during the specified period.	+ Install	
Service_Watchdog	1.8.7_1	Monitors for stopped services and restarts them.	+ Install	
Shellcmd	1.0.5_2	The shellcmd utility is used to manage commands on system startup.	+ Install	
siproxd	1.1.4_1	Proxy for handling NAT of multiple SIP devices to a single public IP.	+ Install	
		Package Dependencies: Ø siproxi-0.8.2_1		
snmptt	1.0.0_1	SNMPTT (SNMP Trap Translator) is an SNMP trap handler written in Perl for use with the Net-SNMP. Easy to setup and use.	+ Install	
-		Package Dependencies: @ snmptt-1.4.2_1		
snort	4.1.4_3	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	+ Install	
		Package Dependencies: Ø snort-2.9.18_1		
softflowd	P (2016a)	SoftBowd semi-stated network traffic analyser capable of CISco Network und export. SoftBowd semi-statefully track traffic flows recorded by listening on a network interface or by reading a packet capture file. These flows may be reported via NetFlow to a collecting host or summarised within softflowd itself. Softflowd supports Netflow versions 1, 5, 9 and 10 (IPFIX) and is fully IPv6-capable - it can track IPv6 flows and send export datagrams via IPv6. It also supports export to multicast groups, allowing for redundant flow collectors.	+ Install	
		Package Dependencies: Softflowd-1.0.0		
squid	0.4.45_5	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C- ICAP.	+ Install	
		Package Dependencies:		

Hit confirm install and you should see the following screen when completed (below).

System / Package Manager / Package Installer	0
pfSense-pkg-snort installation successfully completed.	
Installed Packages Available Packages Package Installer	
Package Installation Please note that, by default, snort will truncate packets larger than the	_
default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.	
This can be done by appending '-lro' to your ifconfig_ line in rc.conf.  Message from pfSense-pkg-snort-4.1.4_3:	
 Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets. >>> Cleaning up cache done. Success	•

Once installed, Snort will be located under Services (below).

COMMUNITY EDITION	Services - VPN -	Status <del>-</del>	Diagnostics 👻	Help 🗕	
WARNING: The 'admin' account password is set to the default value	Auto Config Backup Captive Portal	the User Manager.	Ĩ		
System / Package Manager / Package In	DHCP Relay DHCP Server DHCPv6 Relay				0
pfSense-pkg-snort installation successfully completed.	DHCPv6 Server & RA DNS Forwarder				
Installed Packages Available Packages Package Insta	DNS Resolver Dynamic DNS IGMP Proxy NTP				
Package Installation	PPPoF Server				
Please note that, by default, snort will truncate pack default snaplen of 15158 bytes. Additionally, LRO may Stream5 target-based reassembly. It is recommended to your card supports it.	SNMP Snort UPMP & NAT-PMP				ŕ
This can be done by appending '-lro' to your ifconfig  Message from pfSense-pkg-snort-4.1.4_3:	Wake-on-LAN				

Click Global settings in Snort, enable GPLv2 and set Rules Update to everyday and set remove

blocked hosts to everyday. Make sure to save/apply changes (below and next page).

Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Snort Subscriber	Rules									
Enable Snort V	RT 🗌 Click to e	nable downloa	d of Snort fr	ee Registered	User or paid Sub	scriber rules				
	Sign Up for a Sign Up for p	a free Registere baid Snort Subs	d User Rule criber Rule	s Account Set (by Talos)						
Snort GPLv2 Con	nmunity Rules									
Enable Snort GPI	Lv2 🔽 Click to e	nable downloa	d of Snort G	PLv2 Commu	nity rules					
	The Snort Co ruleset is up	ommunity Rule dated daily and	set is a GPL I is a subset	v2 Talos certifi of the subscri	ed ruleset that is ber ruleset.	distributed free	of charge with	iout any Snort Si	ubscriber License	e restrictions. This

Rules Update Setting	8
Update Interval	1 DAY 🗸
	Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	
	Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories	Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
General Settings	
Remove Blocked Hosts	1 DAY 🗸
Interval	Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall	✓ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	Click to retain Snort settings after package removal.
Startup/Shutdown Logging	Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.
	Save

Under Updates, update the rule set (you may need to click Force Update) (below).

Services / Snort	/ Updates									0
Snort Interfaces Glo	bal Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Installed Rule Set Mi	D5 Signature									
Rule Set Name/Publisher				M	D5 Signature Has	h		MD5 Signature	Date	
Snort Subscriber Ruleset				Ν	ot Enabled			Not Enabled		
Snort GPLv2 Community F	Rules			Ν	ot Downloaded			Not Download	led	
Emerging Threats Open R	ules			Ν	ot Enabled			Not Enabled		
Snort OpenAppID Detecto	rs			Ν	ot Enabled			Not Enabled		
Snort AppID Open Text Ru	les			Ν	ot Enabled			Not Enabled		
Feodo Tracker Botnet C2 I	P Rules			Ν	ot Enabled			Not Enabled		
Update Your Rule Se	t									
Last Update	Unknown	Resu	lt: Unknowr							
Update Rules	🗸 Update Ru	les				🛃 Ford	ce Update			
	Click UPDATE the MD5 hash	RULES to chines and force	eck for and the downloa	automatically a ad and applicat	apply any new position of the latest	sted updates fo versions of the e	r selected rule enabled rules p	s packages. Clic backages.	king FORCE UPD	ATE will zero out
Manage Rule Set Log	J									
	View Log						ar Log			
	The log file is	limited to 102	24K in size a	ind is automati	cally cleared whe	n that limit is e	xceeded.			
Logfile Size	Log file is em	pty								

The following is what it should look like once completed:

Update Your Rule Set	i	
Last Update	Nov-16 2021 20:55	Result: Success
Update Rules	Vpdate Rules	📩 Force Update
	Click UPDATE RULES to chee the MD5 hashes and force th	ck for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out he download and application of the latest versions of the enabled rules packages.

The next step is to create an alias for both interfaces (WAN and LAN) of pfsense. Navigate to Firewall>Aliases>Edit in pfsense and select Add Host. In the screenshot below, you can see I have added both interfaces and labeled them accordingly. Now hit save.

COMMUNITY EDITION	✓ Interfaces ✓	Firewall - Services	✓ VPN ✓	Status 👻	Diagnostics <del>-</del>	Help 👻	¢+
WARNING: The 'admin' acc	ount password is set to th	e default value. Change ti	ne password in t	he User Manage	er.		
Firewall / Aliases	s / Edit						Θ
Properties							
Name	pfsense interfaces The name of the alias r	nay only consist of the ch	aracters "a-z, A-Z	Z, 0-9 and _".			
Description	WAN and LAN for pfs A description may be e	ense ntered here for administra	tive reference (r	ot parsed).			
Туре	Host(s)			~			
Host(s) Hint	Enter as many hosts as re-resolved and update as 192.168.1.16/28 ma	s desired. Hosts must be s d. If multiple IPs are return ay also be entered and a li:	specified by their ned by a DNS qu st of individual If	IP address or fi ery, all are used 9 addresses will	ully qualified domain . An IP range such as be generated.	name (FQDN). FQDN s 192.168.1.1-192.168	hostnames are periodically 1.1.10 or a small subnet such
IP or FQDN	10.4.19.101		۷	/AN IP			Delete
	192.168.101.1			AN IP			Delete
	B Save + Add Ho	ost					

After this completed, you must locate Pass Lists under Services>Snort>Pass List>Edit. Select the Alias you just made and hit save. Make sure to uncheck LAN subnet to allow for alert logging (next page).

Services / Snort ,	/ Pass List	/ Edit									0
Snort Interfaces Glob	oal Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
General Information											
Name	passlist_4847 The list name r	'5 nay only con	sist of the cl	naracters 'a-z,	A-Z, 0-9 and _'.						
Description	You may enter	a descriptior	n here for you	ur reference.							
Auto-Generated IP A	ddresses										
Local Networks	🛃 Add firewal	l Locally-Atta	ched Netwo	rks to the list (	(excluding WAN)	Default is Chec	ked.				
WAN Gateways	🗹 Add WAN G	ateways to t	he list. Defa	ult is Checked.							
WAN DNS Servers	🛃 Add WAN D	NS servers t	o the list. De	fault is Check	ed.						
Virtual IP Addresses	🗹 Add Virtual	IP Addresse	s to the list.	Default is Che	cked.						
VPN Addresses	🛃 Add VPN A	ddresses to t	he list. Defa	ult is Checked							
Custom IP Addresses	s and Configu	red Firew	all Aliase	S							
Hint	Enter as many name) directly! and updated by	IP addresses To use a FQ / the firewall.	or alias nar DN, first crea You can als	nes as desirec ate the necess o provide an II	d. Enter ONLY an ary firewall alias, P subnet with a p	P address, IP su and then provid roper netmask o	ubnet or alias r le the alias nar of the form net	name! Do NOT er ne here. FQDN a work/mask such	nter a FQDN (fully Iliases are period h as 1.2.3.0/24.	/ qualified d ically re-reso	omain olved
IP or Alias	pfsenseInterf	aces				Dele	te				
	Save +	Add IP									

Next, add a Snort interface for WAN by selecting add interface. Open WAN settings and make

sure to check Enable Packet Cap	ptures and Block Offenders (below).
---------------------------------	-------------------------------------

General Settings	
Enable	☑ Enable interface
Interface	WAN (em0)
	Choose the interface where this Snort instance will inspect traffic.
Description	WAN
	Enter a meaningful description here for your reference.
Snap Length	1518
	Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings	
Send Alerts to System	□ Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	128
	Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em055794 is rotated and a new file opened.
Enable Unified2 Logging	Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
	Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.
Block Settings	
Block Offenders	Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

Joshua Lane IT419 11/23/2021 Next, navigate to Services>Snort>Interface Settings>WAN – Categories. Check the box to

enable Snort GPLv2 Community Rules (below).

non interraces	Global Settings	Updates	Alerts Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
/AN Settings V	VAN Categories	WAN Rules	WAN Variables	WAN Preprocs	WAN IP Rep	WAN	Logs		
utomatic Flowbi	t Resolution								
Resolve Flowb	Snort will ex automatica	xamine the enabl illy enabled and a	led rules in your chose dded to the list of files	n rule categories for in the interface rules	checked flowbits. directory.	Any rules th	at set these dep	pendent flowbits	will be
elect the rulese - Category is auto-e - Category is auto-o	ts (Categories) enabled by SID Mgn lisabled by SID Mgr	) Snort will la nt conf files mt conf files	oad at startup						
elect the rulese - Category is auto-e - Category is auto-c - Category is auto-c	ts (Categories) enabled by SID Mgn lisabled by SID Mgr Ruleset: Snort	) Snort will lo mt conf files mt conf files t GPLv2 Commun	ad at startup nity Rules					Select All Unse	elect All
elect the rulese - Category is auto-o - Category is auto-o category is auto-o	ts (Categories) enabled by SID Mgn lisabled by SID Mgn Ruleset: Snort Snort GPLv2 (	) Snort will lo mt conf files mt conf files t GPLv2 Commun Community Rule:	nad at startup hity Rules s (Talos certified)					Select All Uns	elect All 🕞

Proceed to WAN Rules under Interface Settings. Under Category Selection use the drop-down

menu to select GPLv2\_community.rules. Select enable all (next page).

	WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.	
	Services / Snort / Interface Settings / WAN - Rules	0
	Snort is 'live-reloading' the new rule set.	×
	Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt :	Sync
	WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs	
	Available Rule Categories	
	Category Selection:         GPLv2_community.rules         v           Select the rule category to view and manage.         Image: Category Select the rule category to view and manage.         Image: Category Select the rule category Select the rule category to view and manage.         Image: Category Select the rule category	
	Rule Signature ID (SID) Enable/Disable Overrides	
	SID Actions Reply C Reset All Current O Datable All C Enable All C Enable All C Enable All C Enable All	
	Rules View Filter	÷
	Selected Category's Rules	
	Legend: 🕗 Default Enabled 🗇 Enabled by user 🗞 Auto-enabled by SID Mgmt 💪 Action/content modified by SID Mgmt 🛕 Rule action is alert 🛞 Default Disabled by user 🗞 Auto-disabled by SID Mgmt	
	State Action GID SID Proto Source SPort Destination DPort Message	
1 Internet Informatio	A 1 105 tcp \$HOME_NET 2589 \$EXTERNAL_NET any MALWARE-BACK     Dagger_1.4.0	(DOOR -
	1 108 top \$EXTERNAL_NET any \$HOME_NET 7597 MALWARE-BACK Worm Client Log	DOOR QAZ
4	A 130 ALL APVTEDIAL NET ALIGNE NET 3024630246 MANUARE DAGY	10000

Next, add a Snort interface for LAN and open LAN settings. Check Enable Packet Captures and set Home Net to the pfSense only pass list (below and next page).

Snort Interfaces G	lobal Settings	Updates	Alerts Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
LAN Settings									
General Settings									
Enable	🛃 Enable inte	rface							
Interface	LAN (em1)				~				
	Choose the int	erface where th	is Snort instance will in	spect traffic.					
Description	LAN								
	Enter a meanir	ngful description	here for your referenc	e.					
Snap Length	1518	1		6 1.1 and 1.1					
	Enter the desir	ed interface sna	apien value in bytes. De	fault is 1518 and i	s suitable for m	iost applicatio	ns.		
Alert Settings									
Send Alerts to System Log	Snort will s	end Alerts to th	e firewall's system log.	Default is Not Che	cked.				
Enable Packet Captures	🗹 Checking t	his option will a	utomatically capture pa	ckets that genera	te a Snort alert	into a topdum	o compatible file		
Packet Capture File Size	128								
	Enter a value i directory /var/	n megabytes for log/snort/snort	the packet capture file _em115959 is rotated a	size limit. Default and a new file oper	is 128 megaby ned.	tes. When the	limit is reached,	the current packe	t capture file in
Enable Unified2 Logging	Checking t Default is N	his option will ca Not Checked.	ause Snort to simultane	ously log alerts to	a unified2 bina	ary format log	file in the logging	subdirectory for	this interface.
	Log size and r	etention limits f	or the Unified2 log shou	Id be configured o	on the LOG MGI	MT tab when t	his option is enal	oled.	

Choose the Networks	Snort Should Inspect and Whitelist
Home Net	passlist_48475 View List
	Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.
External Net	default View List Choose the External Net you want this interface to use.
	External Net is networks that are not Home Net. Most users should leave this setting at default. Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Repeat the steps you did for WAN Categories on LAN categories (enable ruleset for GPLv2 and under LAN Rules select GPLv2 from the drop-down menu, click enable all and apply).

Once this is completed, click Start Snort on this interface for both LAN and WAN (below).

Serv	ices / Sn	ort / Interfac	es									0
Snort I	Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Interf	ace Setting	gs Overview										
	Interface	Snor	t Status	Pat	ttern Match	E	locking Mode		Description		Actions	
0	WAN (em0)	<b>S</b>	C 💿	AC	C-BNFA		LEGACY MODE		WAN		Ø 🛅	
	LAN (em1)	0	C	AC	C-BNFA		DISABLED		LAN		e 🖉	
											Ē	Delete
-												

In order to simulate a threat, you need to download arachni to for vulnerabilities on your internal network. Make sure to download for the correct OS (download screenshot next page).



Open a command prompt window and change your directory to the location of arachni in your

downloads. Once this is done, change directories to bin under arachni (next page two pages).



C:\Users∖jl	ane003\Dowr	loads∖arachni	-1.5.1-0.5.12-windows-x86_64>cd bin
C:\Users\jl Volume in Volume Ser	ane003\Dowr drive C has ial Number	loads\arachni no label. is 266B-6AEB	-1.5.1-0.5.12-windows-x86_64\bin>dir
Directory	of C:\Users	∖jlane003\Dow	nloads\arachni-1.5.1-0.5.12-windows-x86_64\bin
03/28/2017	10:58 PM	<dir></dir>	
03/28/2017	10:58 PM	<dir></dir>	
03/28/2017	10:58 PM		108 arachni.bat
03/28/2017	10:58 PM		108 arachni_console.bat
03/28/2017	10:58 PM		108 arachni_multi.bat
03/28/2017	10:58 PM		108 arachni_reporter.bat
03/28/2017	10:58 PM		108 arachni_reproduce.bat
03/28/2017	10:58 PM		108 arachni_restore.bat
03/28/2017	10:58 PM		108 arachni_rest_server.bat
03/28/2017	10:58 PM		108 arachni_rpc.bat
03/28/2017	10:58 PM		108 arachni_rpcd.bat
03/28/2017	10:58 PM		108 arachni_rpcd_monitor.bat
03/28/2017	10:58 PM		108 arachni_script.bat
03/28/2017	10:58 PM		141 arachni_shell.bat
03/28/2017	10:58 PM		139 arachni_web.bat
33/28/2017	10:58 PM		127 arachni_web_change_password.bat
03/28/2017	10:58 PM		123 arachni_web_create_user.bat

As shown in the screenshot above, proceed to use arachni\_web command to start the scan. Once this is done, you will see a "accessible by tcp.localhost:9292" or similar syntax. Open a web browser and proceed to type http://localhost:9292 and it should bring you to a web UI for arachni. Log in with the default credentials (below and next page).



User Name: admin@admin.admin Password: administrator

Once logged in, we are greeted with a Welcome page that has some useful information on the homepage, such as Issues per scans and notifications about what you are involved with.



	Joshua Lane IT419 11/23/2021
$\leftrightarrow$ $\rightarrow$ $C$ O localhost:9292/d/users/sign_in	∽☆ J:
Arachni v1.5.1 - WebUI v0.5.12	Sign in
Sign in Please consult the Wiki for default credentials.	
Email admin@admin.admin	
Password	
Remember me	
Sign in	

Type in the IP address of your windows server and click scan. The following screen will show

when the scan is completed:

## http://192.168.101.2/ Edit description ✓ The scan completed in 00:00:22. Issues [3] All [3] \* Fixed [0] ✓ Verified [0] Pending verification [0] ✗ False positives [0] Awaiting review [0] Listing all logged issues. URL Input Element Missing 'X-Frame-Options' header 1 TOGGLE BY SEVERITY Reset Show all Hide all Interesting response 1 1 Allowed HTTP methods 1 Informational 2 NAVIGATE TO h 1 3 Interesting response 1 Allowed HTTP methods 1

Navigate to alerts under snort to view the alert logs that take place when this vulnerability scan

was done (below).

Alert Log View Filter         Oles         Source P         SPort         Pestination IP         OPer         GID:30         Description           2021-1123         1         TCP         Web Application Attack         101.101.1         5541         1/92.168.101.2         80         11020         SERVER-WEBAPP Admin. files access           2021-1123         1         TCP         Attempted Information         101.101.1         55413         1/92.168.101.2         80         11214         SERVER-WEBAPP Admin. files access           2021-1123         1         2         TCP         Attempted Information         101.101.1         55423         1/92.168.101.2         80         11214         SERVER-WEBAPP Admin. files access           2021-1123         1         2         TCP         Attempted Information         101.101.1         55423         1/92.168.101.2         80         11214         SERVER-WEBAPP hackup access           2021-1123         1         2         TCP         Attempted Information         101.101.1         55423         1/92.168.101.2         80         11214         SERVER-WEBAPP hackup access           2021-1123         1         1         TCP         Attempted Information         101.101.1         55423         1/92.168.101.2         80         11560 <th>Aler</th> <th>t Log Actio</th> <th>ons 🛃</th> <th>ownload Clear</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Aler	t Log Actio	ons 🛃	ownload Clear							
12 Ent/File         Event         Source IP         SPort         Destination IP         DPort         GID:SD         Description           2021-11:23         A         1         TCP         Web Application Attack         Q_III:X         SFAIL         QUI         SFEVER-WEBAPP Admin.,files access           2021-11:23         A         2         TCP         Attempted Information         Q_III:X         SFAIL         QUI         SERVER-WEBAPP Admin.,files access           2021-11:23         A         2         TCP         Attempted Information         Q_III:X         SFAIL         QUI         SERVER-WEBAPP Admin.,files access           2021-11:23         A         2         TCP         Attempted Information         Q_III:X         SFAIL         QUI         SERVER-WEBAPP Admin.,files access           2021-11:23         A         2         TCP         Attempted Information         Q_III:X         SFAIL         Q_III:X         SFAIL         SERVER-WEBAPP Admin.,files access           2021-11:23         A         2         TCP         Attempted Information         Q_III:X         SFAIL         Q_IIII:X         SFAIL         SERVER-WEBAPP Admin.,files access           2021-11:23         A         1         TCP         Attempted Information         Q_III:X         <	Alert Log	View Fi	lter							0	
ImageMationMainMainGeneSource/IP	12 Entrie	s in Acti	ive Log								
2201-11-23         1         TCP         Web Application Attack         10,1101         5541         102,168,1012         00         11222         SERVER-WEBAPP Admin., files access           2201-11-23         1         2         TCP         Attempted Information         10,1101         55413         102,1101         0         1222         SERVER-WEBAPP Admin., files access           2201-11-23         1         2         TCP         Attempted Information         10,1101         55423         102         0         122         SERVER-WEBAPP Admin., files access           2201-11-23         1         1         TCP         Attempted Information         10,1101         55423         102-188,1012         0         11224         SERVER-WEBAPP Admin., files access           2201-11-23         1         TCP         Attempted Information         10,1101         55423         102-188,1012         0         11224         SERVER-WEBAPP / doc/ access           2208-00         2         TCP         Attempted Information         10,1101         55423         102-188,1012         0         11224         SERVER-WEBAPP / doc/ access           2208-00         1         TCP         Recess to a potentially ublance         10,1101         55424         102-181,1012         0 <td< th=""><th>Date</th><th>Action</th><th>Pri Pro</th><th>to Class</th><th>Source IP</th><th>SPort</th><th>Destination IP</th><th>DPort</th><th>GID:SID</th><th>Description</th><th></th></td<>	Date	Action	Pri Pro	to Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description	
2021-11-23         2         TCP         Attempted Information         10.1 10.11         55415         192 148.101.2         80         1.212         SERVER-WEBAPP Admin_files access           22.08.40         2         TCP         Attempted Information         10.1 10.11         55415         10.2         10         12.2         SERVER-WEBAPP Admin_files access           22.08.40         2         TCP         Attempted Information         10.1 10.11         54423         10.2         8         12.2         SERVER-WEBAPP Intranet access           2025.11-123         A         2         TCP         Attempted Information         10.1 10.11         54423         10.2         10         11.213         SERVER-WEBAPP Intranet access           2025.11-123         A         2         TCP         Attempted Information         10.1 10.11         54423         10.2         11.560         SERVER-WEBAPP /doc/ access           2025.11-123         A         10         TCP         access to a potentially         10.110.11         5442         10.21.161.012         80         11.560         SERVER-WEBAPP /doc/ access           2021-11-23         A         10         TCP         access to a potentially         10.110.11         5442         12.168.1012         80         11.560<	2021-11-23 22:08:40	<b>A</b>	1 TC	P Web Application Attack	10.1.101.1 <b>Q</b> 🛨 🗙	55414	192.168.101.2 Q ⊕	80	1:1029	SERVER-IIS scripts-browse access	
2021-11-22       2       TCP       Attempted Information       10,110.11       5423       192,148.101.2       80       1.1214       SERVER-WEBAPP Intramet access         22.08.40       2       TCP       Attempted Information       10,110.11       5423       192,148.101.2       80       1.1214       SERVER-WEBAPP Intramet access         22.08.40       2       TCP       Attempted Information       10,110.11       11,010.1       SERVER-VTHEBAPP /optich/access       202,111.123.1       11       11,010.1       11,010.1       11,010.1       11,010.1       11,0	2021-11-23 22:08:40	4	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🕀 🗙	55415	192.168.101.2 <b>Q</b> 🛨	80	1:1212 <b>•</b> ×	SERVER-WEBAPP Admin_files access	
2021-11-23       2       TCP       Attempted Information       10.1101.1       55423       192.188.101.2       0       1.1233       SERVER-WEBAPP backup access         22.08.40       2       TCP       Attempted Information       10.1101.1       55423       12.112.3       0       1.1233       SERVER-WEBAPP backup access         22.08.40       2       TCP       Attempted Information       10.1101.1       10.1101.1       10.1101.1       10.1101.1       10.111.1       10.	2021-11-23 22:08:40	<u> </u>	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🛨 🗙	55423	192.168.101.2 <b>Q</b> ∰	80	1:1214	SERVER-WEBAPP intranet access	
2021-11-23         2         TCP         accesse to a potentially witherable web         10.1 10.11         55412         192.180.101.2         80         1.1560         SERVER-WEBAPP /doc/ access           2208.40         1         TCP         Web Application Attack         10.1 10.11         55412         192.180.101.2         80         1.1560         SERVER-WEBAPP /doc/ access           2208.40         1         TCP         Web Application Attack         10.1 10.11         55425         192.180.101.2         80         1.1668         SERVER-WEBAPP /doc/ access           2208.40         1         TCP         Web Application Attack         10.1 10.11         55425         192.180.101.2         80         11.288         SERVER-WEBAPP /doc/ access           2201-11-23         2         TCP         access to a potentially         10.1 10.11         55424         192.168.101.2         80         1.288         SERVER-OTHER Microsoft Frontpage           2021-11-23         2         1         TCP         Attempted Information         10.1 10.1         55409         192.168.101.2         80         1.1301         SERVER-WEBAPP admin, php access           2021-11-23         2         TCP         Attempted Information         10.101.1         55409         121.186.101.2         80 <t< td=""><td>2021-11-23 22:08:40</td><td>4</td><td>2 TC</td><td>P Attempted Information Leak</td><td>10.1.101.1 <b>Q</b> 🛨 🗙</td><td>55423</td><td>192.168.101.2 <b>Q</b> 🕀</td><td>80</td><td>1:1213</td><td>SERVER-WEBAPP backup access</td><td></td></t<>	2021-11-23 22:08:40	4	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🛨 🗙	55423	192.168.101.2 <b>Q</b> 🕀	80	1:1213	SERVER-WEBAPP backup access	
2021-11-23         1         TCP         Web Application Attack         10.1101.1         55425         102.168.101.2         80         11.069         SERVER-WEBAPP /og/bin/ access           22.08.40         1         1         TCP         Web Application Attack         10.1101.1         55425         102.168.101.2         80         11.069         SERVER-WEBAPP /og/bin/ access           22.08.40         1         TCP         access to a potentially         10.1101.1         5424         102.168.101.2         80         12.8         SERVER-OTHER Microard/ Frontpage           22.08.40         1         TCP         Web Application Attack         10.1101.1         5424         102.168.101.2         80         19.93         SERVER-OTHER Microard/ Frontpage           2021-11-23         A         1         TCP         Attempted Information         10.1101.1         5409         102.168.101.2         80         19.93         SERVER-WEBAPP admin php access           2021-11-23         A         2         TCP         Attempted Information         10.101.1         5409         102.168.101.2         80         11.301         SERVER-WEBAPP admin php access           2021-11-23         A         2         TCP         Attempted Information         10.101.1         5409         12.168	2021-11-23 22:08:40	•	2 TC	P access to a potentially vulnerable web application	10.1.101.1 Q	55412	192.168.101.2 <b>Q</b>	80	1:1560	SERVER-WEBAPP /doc/ access	
2021-11-23       A       2       TCP       access to a potentially vulnerable web application       10.1 10.1       55424       192.168.101.2       80       1.1288       SERVER-OTHER Microsoft Frontpage / Juli / Juli / access         2208.40       1       TCP       Web Application Attack       10.1 10.1       55494       192.168.101.2       80       1.928       SERVER-OTHER Microsoft Frontpage / Juli / access         2208.40       1       TCP       Web Application Attack       10.1 10.11       55490       192.168.101.2       80       1.993       SERVER-WEBAPP admin access         2208.40       1       TCP       Attempted information       10.1 10.11       10.1 10.11       80       1.993       SERVER-WEBAPP admin php access         2208.40       2       TCP       Attempted information       10.1 10.11       10.1 10.11       80       1.1281       SERVER-WEBAPP admin php access         2208.40       2       TCP       Attempted information       10.1 10.11       10.1 10.11       80       1.1281       SERVER-WEBAPP admin php access         2208.40       2       TCP       Attempted information       10.1 10.11       10.1 10.11       80       1.1281       SERVER-WEBAPP Phorum admin access         2208.40       2       TCP       Attempted information <td>2021-11-23 22:08:40</td> <td>4</td> <td>1 тс</td> <td>P Web Application Attack</td> <td>10.1.101.1 <b>Q</b> 🕀 🗙</td> <td>55425</td> <td>192.168.101.2 <b>Q</b> 🛨</td> <td>80</td> <td>1:1668</td> <td>SERVER-WEBAPP /cgi-bin/ access</td> <td></td>	2021-11-23 22:08:40	4	1 тс	P Web Application Attack	10.1.101.1 <b>Q</b> 🕀 🗙	55425	192.168.101.2 <b>Q</b> 🛨	80	1:1668	SERVER-WEBAPP /cgi-bin/ access	
2021-11-23       A       1       TCP       Web Application Attack       10.1.101.1       55409       102.168.101.2       80       1993       SERVER4IS illaadmin access         2208.40       2       TCP       Attempted Information       10.1.101.1       55409       102.168.101.2       80       1993       SERVER4IS illaadmin access         2021-11-23       A       2       TCP       Attempted Information       10.1.101.1       55409       102.168.101.2       80       1932       SERVER-WEBAPP admin.php access         2021-11-23       A       2       TCP       Attempted Information       10.1.101.1       55409       102.168.101.2       80       11.301       SERVER-WEBAPP admin.php access         22.08.40       2       TCP       Attempted Information       10.1.101.1       55409       102.168.101.2       80       11.301       SERVER-WEBAPP admin.php access         22.08.40       2       TCP       Attempted Information       10.1.101.1       55409       102.168.101.2       80       11.301       SERVER-WEBAPP Phorum admin access         22.08.40       2       TCP       Attempted Information       10.1.101.1       10.1.101.1       80       11.301       SERVER-WEBAPP Phorum admin access         22.08.40       2       TCP	2021-11-23 22:08:40	4	2 TC	P access to a potentially vulnerable web application	10.1.101.1 <b>Q</b> 🕀 🗙	55424	192.168.101.2 <b>Q</b>	80	1:1288 🕀 🗙	SERVER-OTHER Microsoft Frontpage /_vti_bin/ access	
2021-11-23       A       TCP       Attempted Information       10.1.101.1       \$5408       192.168.101.2       80       11.301       SERVER-WEBAPP admin.php access         22.08.40       C       TCP       Attempted Information       10.1.101.1       \$5408       192.168.101.2       80       11.301       SERVER-WEBAPP admin.php access         2021-11-23       C       TCP       Attempted Information       Q.T ×       \$5409       192.168.101.2       80       11.301       SERVER-WEBAPP admin.php access         2021-11-23       C       TCP       Attempted Information       Q.T ×       \$5409       192.168.101.2       80       11.301       SERVER-WEBAPP Admin.php access         2021-11-23       C       TCP       Attempted Information       Q.T ×       \$5409       192.168.101.2       80       11.314       SERVER-WEBAPP Phorum admin         2021-11-23       C       TCP       Attempted Information       10.1.101.1       \$5409       192.168.101.2       80       11.314       SERVER-WEBAPP Phorum admin         2021-11-23       C       TCP       Attempted Information       10.1.101.1       \$5409       192.168.101.2       80       11.34       SERVER-WEBAPP Phorum admin         20.08.40       C       C       TCP       Attempte	2021-11-23 22:08:40	•	1 тс	P Web Application Attack	10.1.101.1 Q 🕀 🗙	55409	192.168.101.2 <b>Q</b>	80	1:993 🕂 🗙	SERVER-IIS lisadmin access	
2021-11-23       A       2       TCP       Attempted Information       Q I ×       S5409       102.168.101.2       80       11.921       SERVER-WEBAPP admin.php access         22:08.40       2       TCP       Attempted Information       Q I ×       S5409       102.108.101.2       80       11.921       SERVER-WEBAPP admin.php access         22:08.40       2       TCP       Attempted Information       101.101.1       S5409       102.108.101.2       80       11.921       SERVER-WEBAPP Phorum admin access         22:08.40       2       TCP       Attempted Information       101.101.1       Q I ×       S409       102.108.101.2       80       11.921       SERVER-WEBAPP Phorum admin access         22:08.40       2       TCP       Attempted Information       101.101.1       Q I ×       S409       102.108.101.2       80       11.921       SERVER-WEBAPP Phorum admin access         20:08.40       X<	2021-11-23 22:08:40	<b>A</b>	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🕀 🗙	55408	192.168.101.2 <b>Q</b> 🛨	80	1:1301	SERVER-WEBAPP admin.php access	
2021-11-23         Δ         2         TCP         Attempted Information         10.1.101.1         55409         192.168.101.2         80         1.1134         SERVER-WEBAPP Phorum admin           22.08.40         Leak         Q ↔ Q ↔         Q ↔         Image: Access	2021-11-23 22:08:40	4	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🕀 🗙	55409	192.168.101.2 <b>Q</b>	80	1:1301	SERVER-WEBAPP admin.php access	
	2021-11-23 22:08:40	<b>A</b>	2 TC	P Attempted Information Leak	10.1.101.1 <b>Q</b> 🕀 🗙	55409	192.168.101.2 <b>Q</b> ⊕	80	1:1134	SERVER-WEBAPP Phorum admin access	
2021-11-23 ▲ 3 TCP Unknown Traffic 216.92.33.104 80 192.148.101.2 49948 120.3 (http://angeocli) NO CONTENT-LENGTH 21.97.35	2021-11-23 21:07:35	Δ	3 тс	P Unknown Traffic	216.92.30.104 Q	80	192.168.101.2 <b>Q</b>	49948	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	

You can then create a rule under firewall rules on the WAN interface for blocking this IP address that scanned the internal network. It is possible to spoof your IP address, so this may not be an ample rule if the attacker has more resources at their disposal.

Next, proceed to access a website with a 'virus' to click on from the internal network. Make sure to disable any blocking rules preventing this to simulate a real intrusion (below).

Rules (Drag to Change Order)												
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	3 /3.64 MiB	*	*	*	LAN Address	443 80	×	*		Anti-Lockout Rule	\$
	×	0 /0 B	IPv4 TCP	*	*	216.92.30.104	80 (HTTP)	*	none			÷∕⊡⊡∎́
	~	10 /63.08 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	₺∥□०面
	~	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	₺∥₽०₫
											🕇 Add 🕽 Add 🛅 Delete 🕞	Save + Separate

Once you navigate to the virus (here we used it315.girlsgeekout.org/virus) and click HTTP

response with errors (below).



Here is the alert generate from this download on Snort:

Snort Interf	faces	Global	Settings	Updates	Alerts E	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
Alert Log	View S	ettings	8									
Interfa	ce to Insp	ect	WAN (em0 Choose inter	) 🗸	🗌 Auto-refr	resh view	250 Alert lines	s to display.		Save		
Alert	t Log Actio	ons	🛃 Download	Clear								
Alert Log	l View Fi	ilter										
Entries	in Activ	e Log										
ite	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description		
021-11-23 1:07:35	<b>A</b>	3	TCP	Unknown Traffic	216.92.30.104 <b>Q                                    </b>	80	192.168.101.2 <b>Q</b> 🛨	49948	120:3 🛨 🗙	(http_inspect) NO ( TRANSFER-ENCOD	CONTENT-LENG	TH OR ESPONSE

Before you begin with trying to view a log to investigate with Wireshark, you must first change firewall rules to allow a secure shell connection on WAN as well as download an SFTP client to connect to your pfSense firewall. Navigate to Firewall>Rules and add the following rule, click save and apply changes:

	whereas with block the pack	et is dropped silently. In either case, the o	riginal packet is disca	rded.	arried to the ochaely	•			
Disabled	Disable this rule Set this option to disable this	s rule without removing it from the list.							
Interface	WAN Choose the interface from w	WAN  Choose the interface from which packets must come to match this rule.							
Address Family	IPv4 Select the Internet Protocol v	version this rule applies to.	~						
Protocol	TCP Choose which IP protocol thi	is rule should match.	~						
Source									
Source	Invert match	Single host or alias	~	10.1.101.1	1	``			
Destination									
Destination	Invert match	WAN address	~	Destination Address	1				
Destination Destination Port Range	Invert match  SSH (22)  From	WAN address	<b>~</b> 22) <b>~</b>	Destination Address	1				
Destination Destination Port Range	☐ Invert match SSH (22) From Specify the destination port of	WAN address SSH ( Custom To or port range for this rule. The "To" field m	22) V ay be left empty if onl	Destination Address Custom y filtering a single port.					
Destination Destination Port Range Extra Options Log	Invert match SSH (22) From Specify the destination port of Log packets that are han Hint: the firewall has limited the Status: System Logs: Set	WAN address Custom To or port range for this rule. The "To" field m dled by this rule local log space. Don't turn on logging for t titings page).	<ul> <li>✓</li> <li>22)</li> <li>✓</li> <li>ay be left empty if online</li> <li>everything. If doing a leverything.</li> </ul>	Destination Address Custom y filtering a single port.	/	(see			
Destination Destination Port Range Extra Options Log Description	Invert match SSH (22) From Specify the destination port of Log packets that are hand Hint: the firewall has limited the Status: System Logs: Set SSH on WAN A description may be entered log.	WAN address         Custom       To         or port range for this rule. The "To" field m         dled by this rule         local log space. Don't turn on logging for rtings page).         d here for administrative reference. A max	v 22)     v ay be left empty if onl everything. If doing a imum of 52 character	Destination Address Custom y filtering a single port.	ernote syslog server i displayed in the firew	(see vall			

Navigate to System>Advanced>Admin Access to enable Secure Shell:

System / Advance	ed / Admin Access	0
Admin Access Firew	all & NAT Networking Miscellaneous	System Tunables Notifications
webConfigurator		
Protocol	ОНТТР	HTTPS (SSL/TLS)
SSL/TLS Certificate	webConfigurator default (612df251bf277) Certificates known to be incompatible with use fo	✓ or HTTPS are not included in this list.
TCP port	Enter a custom port number for the webConfigur after save.	ator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately

Secure Shell Server	✓ Enable Secure Shell
SSHd Key Only	Password or Public Key 🗸
	When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure she access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding	Enables ssh-agent forwarding support.
SSH port	22
	Note: Leave this blank for the default of 22.

Next, download SFTP client as shown on the next page:

WinS Free SFTP; SCP;	CP S3 and FTP client for Windows						
Home				Install			
		Free F	Award-W File Manag	'inning ger			
	Copy file between a local computer and remote servers using						
		FTP, FTPS, SC	P, SFTP, WebDAV or S3 file	transfer protocols.			
		DOWNLOAD NOW		ABOUT WINSCP			
		166 million downloads t	to date				

Once this is downloaded and installed, proceed to connect to your pfSense firewall through the SFTP client. Click the folder with 2 dots and type in the Public IP address for your pfSense firewall in the host box. Insert your credentials for pfSense and click Login (screenshot on next page).

			Joshua Lane IT419
1			11/23/2021
SCP WinSCP			- 🗆 ×
Local Mark Files Commands Session	Options Remote Help		
🖽 📰 🔂 Synchronize 🗾 🔐 🔝	🐼 🗃 Queue 👻 Transfer Settings Default	- 🥵 -	
🚅 New Session			
📑 My documents 🔹 🚰 👻 💌	⊨ • → • 🗈 🖬 🎧 🎜 🔚		🏠 🤁 🖻 Find Files 🚼
🗄 🕼 Upload 👻 📝 Edit 👻 💢 🕞 I	Login	- 🗆 X	i New ▼ I + - ♥
C:\Users\jlane003\Documents\			
Name Size	Tools  Manage  Show Login dialog on startup and when the last ses	Session File protocol: SFTP V Host name: Port number: 10.4.19.101 22 User name: Password: admin • ••••••• Save V Advanced V sion is closed	Rights Owner
0.P. of 5.50 (P. in 0 of 2		Abidan	
Not connected.	-	4 moden	

Click Yes at the Unknown Server prompt (next page):

Joshua Lane IT419

admin@10.418.101 · WinSCP				11/23/202
Local Mark Files Commands Session Options Remote Help Synchronize Synchronize Occure Transfer Settings Default Wy documents Occure to Properties New Construction Common	admin@10.4.19.101 - WinSCP			- 🗆 ×
Image: Synchronize	Local Mark Files Commands Session Option	Remote Help		
admin@104.19.101 * wew Session         Wy documents       Image: Comparison of the compari	🛨 🎇 🚔 Synchronize 🗾 🧬 🖬 🚳	Queue  Transfer Settings Default	• 👩 •	
Wy documents Image: Control of the second sec	admin@10.4.19.101 × 📑 New Session			
W pload	📔 My documents 🛛 🕶 🚰 🕶 🕎 🔹 🦛 😁	- 🗈 🗈 🏠 🗶 🔚	$[ \  \  \  \  \  \  \  \  \  \  \  \  \ $	🗈 🗊 🏠 🤔 🖻 Find Files
Alusers/jlane003/Documents/     Name     Size   Type   Parent dire   File foldie   File foldie   Stab   Ohsen Hi   Continue connecting to an unknown server and add its host key to a cache? The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's bost key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.   The server's host key was not found in the cache. You have no guarantee that the server is the computer you think i	🗊 Upload 👻 📝 Edit 👻 🗶 📝 🕞 Propertie	՝ New 🗸 🛨 🖃 🔽	🗄 📄 Download 👻 📝 Edit 👻 🗶 🕞 Pro	operties 🔐 New 🕶 🛨 🖃 🗹
Name Size Type   Parent dire   File folder   Etest.pdf   SKB   Chonisue connecting to an unknown server and add its host   key to a cache?   The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is. The server's Ed25519 key details are: Algorithm: ssh-ed25519 255 SHA-256: BrwiwqSCjmyY3bqRe26jgPpBVnC+tJT1Ydz6Yox1aGo= MD5: 64:e3:95365:e67:rcDee:0e:54:9e:79:78:69:39 If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel. Key fingerprints to dipboard Yes No Cancel Help B of 5.59 GB in 0 of 3 4 hidden	:\Users\jlane003\Documents\			
<ul> <li>Parent dire File folder best.pdf</li> <li>S KB</li> <li>Continue connecting to an unknown server and add its host key to a cache?</li> <li>The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.</li> <li>The server's Ed25519 key details are: Algorithm: sth-ed25519 255 SHA-256: Bhwiwq5CjmyY3bgRs26jgPpBWnC+UTIYdz6Yox1aGo= MDS: 64-8349585ee67:c0:ee:0:54:9ef79:87:86939</li> <li>If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.</li> <li>Copy key fingerprints to clipboard</li> <li>Yes No</li> <li>Cancel</li> <li>Help</li> </ul>	Name Size Type	Warning	? ×	ged Rights Owner
B of 5.59 GB in 0 of 3 4 hidden	It419     File fold       Itest.pdf     5 KB       Windows Server 2016     5,865,808	r continue connecting to an u key to a cache? The server's host key was not found i server is the computer you think it is. The server's Ed25519 key details are: Algorithm: ssh-ed25519 255 SHA-256: BfwiwqSCjmyY3bgRs2 MD5: 64:e3:19:58:5e:67:c0:ee If you trust this host, press Yes. To co- press No. To abandon the connectio	unknown server and add its host in the cache. You have no guarantee that the toggPpBVnC+tJT1Ydz6Yox1aGo= .0e:54:9e:f9:9f:78:69:39 nnect without adding host key to the cache, n press Cancel. Copy key fingerprints to clipboard	
4 Haden	R of 5 59 GB in 0 of 3	4 hidden		
NOT CONNECTED.	ot connected.	4 hidden		

In order to locate exactly where the alert log you want is, you must navigate to

Services>Snort>Interface Settings>LAN – Logs. The file path will be displayed there

(screenshot on next page):

Joshua Lane IT419 11/23/2021 • - • × 👷 plSense.home.arpa - Services: Sri 🗙 🥹 it315.girlsgeekout.org/virus/ 🗙 🕇 🕂 ← → C ▲ Not secure | https://192.168.101.1/snort/snort\_interface\_logs.php?id=1 ☆ 😩 : DESCENSE System + Interfaces + Firewall + Services + VPN + Status + Diag 2 🗘 WARNING: The 'admin' account password is set to the default value. Change the pa ord in the User Manager Services / Snort / Interface Settings / LAN - Logs 0 Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs Log File Selection Log File to View alert ~ Choose which log you want to vie Log file contents File successfully loaded. Log File Path /var/log/snort/snort\_em152389/alert Log Contents 😐 🤌 🛤 皆 🔕 🗎 ∧ 🖫 d<mark>8</mark> 1:45 PM

Go back into the SFTP client and navigate to the file path previously as shown and click OK (next page):

						11	/23/20
🚇 snort_em152389 - adm	in@10.4.19.101 - WinSCP					_	
Local Mark Files Comm	ands Session Options Remote H	Help					
🕀 🛃 📮 Synchronize	토 🥐 💽 🛞 🗿 Queue 🗸	Transfer Settings Default	<ul> <li>✓ <i>6</i> →</li> </ul>				
🚽 admin@10.4.19.101 ×	🚔 New Session						
🐛 C: Local Disk 🔹 🗧	🖥 • 🕎 • < • -> • 🔁 🛍	û 🗶 🐁	📕 snort_em1! 🝷 🚰 👻 🝸	• 🔶 • 🔶 • 💼	🗖 🏠 🎜 🗖	Find Files	
🗐 🔄 Upload 👻 📝 Edit 🗣	🗙 📝 🕞 Properties 📑 New	- + - V	🕞 Download 👻 📝 Edit	- 🗙 📝 🕞 Properti	es 📔 New 🗸	+ - V	
C:\Users\jlane003\			/var/log/snort/snort_em1523	89/			
Name	Size Type	Changed	Name	Size Changed		Rights	Owner
<u>t</u>	Parent directory	11/4/2021 9:31:50 AM	<u> </u>	11/16/202	1 10:18:34 AM	rwxr-xr-x	root
.VirtualBox	File folder	11/23/2021 9:17:56 AM	barnyard2	11/16/202	1 10:18:34 AM	rwxr-xr-x	root
E Contacts	File folder	8/31/2021 8:27:16 AM	alert	1 KB 11/23/202	1 10:08:12 AM	rw-rr	root
E Desktop	System Folder	8/31/2021 8:27:16 AM	app-stats.log	0 KB 11/16/202	1 10:18:34 AM	rw-rr	root
Documents	System Folder	10/28/2021 9:42:38 AM	snort.log.1637699899	1 KB 11/23/202	1 10:08:12 AM	rw	root
Downloads	System Folder	11/23/2021 10:14:00 AM					
Ravorites	File folder	8/31/2021 8:27:16 AM					
🕞 Links	File folder Dowr	load		? ×			
Music	System Folder						
Password Assignment	File folder	Download file 'snort.log.163769989	9' to local directory:				
E Pictures	System Folder	C:\Users\jianeuu3\*.*		✓ Browse			
Me Saved Games	File folder Tra	nsfer settings					
Searches	File folder Tra	nster type: Binary					
Videos	System Folder						
VirtualBox VMs	File folder	ransfer in background (add to transfer	queue)				
		Transfer settings	OK Cancel	Help			
		o not show this dialog box again					
0 B of 0 B in 0 of 14		18 hid	den 590 B of 770 B in 1 of 4				
		101114			A	SETD-3	0.15.58

Once this is done, the file should be transferred and observable in Wireshark. Open up the Wireshark Application and look at the file as shown. Here you can see the destination IP address that shows who downloaded the 'virus' from a bad website (on next page):

				Joshua Lane
				IT419
				11/23/2021
snort.log.16376998	99			
File Edit View Go	Capture Analyze Statistics Teles	phony Wireless Tools Help		
🖌 🔳 🖉 💿 📘 🗎	🕅 🙆 🔍 🖛 🔿 🖀 Ŧ 🛓 📑			
📕 tcp				×
No. Time	Source D	Destination Protocol	Length Info	
1 0.000000	216.92.30.104 1	192.168.101.2 TCP	550 80 → 49948 [PSH, ACK] Seq=1 Ack=1 Win=2054 Len=496 [TCP segment of a reassembled PDU]	
> Frame 1: 550 by	tes on wire (4400 bits), 550	0 bytes captured (4400 bits		
> Internet Protoc	ol Version 4, Src: 216.92.30	0.104, Dst: 192.168.101.2	(08:00:27:07:a5:71)	
> Transmission Co	ntrol Protocol, Src Port: 80	0, Dst Port: 49948, Seq: 1,	Ack: 1, Len: 496	
0000 08 00 27 6f	a3 71 08 00 27 44 87 9b 08	8 00 45 02 ···'o·q·· 'D···	E-	^
0010 02 18 00 00	40 00 32 06 2a 6f d8 5c 1e	e 68 c0 a8 ····@·2· *o·∖· d 21 50 18 e. P √	D.	
0030 08 06 da 86	00 00 48 54 54 50 2f 31 2e	e 31 20 32HT TP/1.	2	
0040 30 30 20 4f	4b 0d 0a 44 61 74 65 3a 20	0 54 75 65 00 OK- D ate:		
0050 2c 20 32 33 0060 3a 30 37 3a	20 4e 6f 76 20 32 30 32 31 33 35 20 47 4d 54 6d 6a 53	1 20 32 31 , 23 Nov 2021 3 65 72 76 :07:35 6 MTS		
0070 65 72 3a 20	41 70 61 63 68 65 0d 0a 43	3 6f 6e 74 er: Apac heC	int	
0080 65 6e 74 2d	4c 65 6e 67 74 68 3a 20 0d	d 0a 54 72 ent-Leng th: •	Tr	
0090 61 6e 73 66	65 72 2d 45 6e 63 6f 64 69	9 6e 67 3a ansfer-É ncodi 5 3a 20 74 Koop Alivo	κ: -	
00b0 69 6d 65 6f	75 74 3d 35 2c 20 6d 61 78	8 3d 31 30 imeout=5 . max	10	
00c0 30 0d 0a 43	6f 6e 6e 65 63 74 69 6f 6e	e 3a 20 4b 0··Conne ction		v
Internet Protocol	Version 4 (ip), 20 bytes		Packets: 1 ' Displayed: 1 (100.0%)	Profile: Default

Adding these various rules can keep clients/staff from accidentally downloading viruses and protect your enterprise from outside threats. Snort and custom firewall rules can go a long way prohibiting misuse and making up for the weakest link in the cybersecurity chain (humans).