



Project D -Cybersecurity Analyst

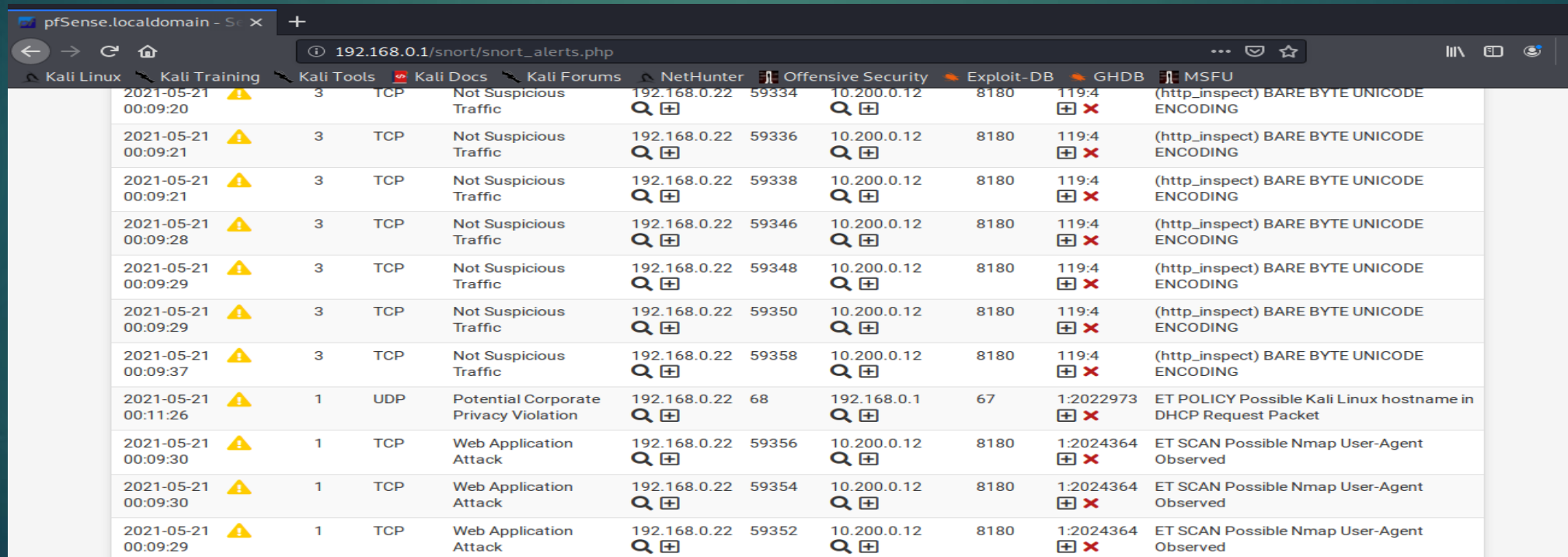
BY: MALCOLM BROWN

Executive Summary

- ▶ Improve the security of the network.
- ▶ Implement a way to identify and log attacks against their web and production servers.
- ▶ Install an IDS/IPS

Vulnerabilities found

- ▶ While searching for vulnerabilities I came across a web server application attack.
- ▶ There were also several traffic logs that are unknown and potentially bad.



The screenshot shows a web browser window with the address bar displaying '192.168.0.1/snort/snort_alerts.php'. The browser's address bar also shows 'pfSense.localdomain - S'. The browser's tab bar shows several tabs: 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MSFU'. The main content area displays a table of snort alerts. The table has 11 columns: 'Time', 'Alert ID', 'Priority', 'Protocol', 'Action', 'Source IP', 'Source Port', 'Destination IP', 'Destination Port', 'Interface', and 'Message'. The table contains 11 rows of data. The first 7 rows show 'Not Suspicious Traffic' alerts. The 8th row shows a 'Potential Corporate Privacy Violation' alert. The last 3 rows show 'Web Application Attack' alerts.

Time	Alert ID	Priority	Protocol	Action	Source IP	Source Port	Destination IP	Destination Port	Interface	Message
2021-05-21 00:09:20	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59334	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:21	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59336	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:21	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59338	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:28	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59346	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:29	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59348	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:29	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59350	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:09:37	3	3	TCP	Not Suspicious Traffic	192.168.0.22	59358	10.200.0.12	8180	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2021-05-21 00:11:26	1	1	UDP	Potential Corporate Privacy Violation	192.168.0.22	68	192.168.0.1	67	1:2022973	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
2021-05-21 00:09:30	1	1	TCP	Web Application Attack	192.168.0.22	59356	10.200.0.12	8180	1:2024364	ET SCAN Possible Nmap User-Agent Observed
2021-05-21 00:09:30	1	1	TCP	Web Application Attack	192.168.0.22	59354	10.200.0.12	8180	1:2024364	ET SCAN Possible Nmap User-Agent Observed
2021-05-21 00:09:29	1	1	TCP	Web Application Attack	192.168.0.22	59352	10.200.0.12	8180	1:2024364	ET SCAN Possible Nmap User-Agent Observed

Snort

- ▶ Snort was used to improve the security of the network. Alerting against attacks that were being made.
- ▶ Firewall rules were put in place to alert or log attacks.
- ▶ Captured real-time traffic analysis and packet-logging on IP networks.

Firewall rules

- Several firewall rules were made to test connections and alert vulnerabilities.

Firewall / Rules / TRUSTED

Floating

UNTRUSTED

TRUSTED

DMZ

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 9.66 MiB	*	*	*	TRUSTED Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	*	*	DMZ net	21 (FTP)	*	none		Block FTP from Trusted to DMZ	
<input type="checkbox"/>	✓ 0 / 2 KiB	IPv4 TCP	*	*	DMZ net	443 (HTTPS)	*	none		Allow HTTPS traffic to DMZ	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	192.168.0.30	*	DMZ net	443 - 990	*	none			
<input type="checkbox"/>	✓ 0 / 22.93 MiB	IPv4 *	TRUSTED net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	TRUSTED net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add


Delete

Save

Separator

Recommendations

- ▶ Configure firewall rules to the attacks you want to be alerted by.
- ▶ Block websites by URL if needed I would advise to download SquidGuard.
- ▶ Daily automated vulnerability scans with alerts of detected vulnerabilities.
- ▶ Adjust snort to your company's needs.



Thank You
Any Questions