Lab 4

Virtual Private Network (VPN) Configuration and Testing

Encrypt and test the encryption of transmission of cardholder data across open, public networks.

Summary:

Strong cryptography and security protocols (e.g. TLS, IPSec, SSH, etc.) should be used to safeguard sensitive cardholder data during transmission over open, public networks that could easily be accessed by malicious individuals. Examples of open, public networks include the Internet, wireless technologies (e.g. Bluetooth), GPRS (general packet radio service) and satellite communications. Industry best practices must be followed to implement strong encryption for authentication and transmission. Security policies and procedures for encrypting the transmission of cardholder data must be documented and made known to all affected parties.

Contents:

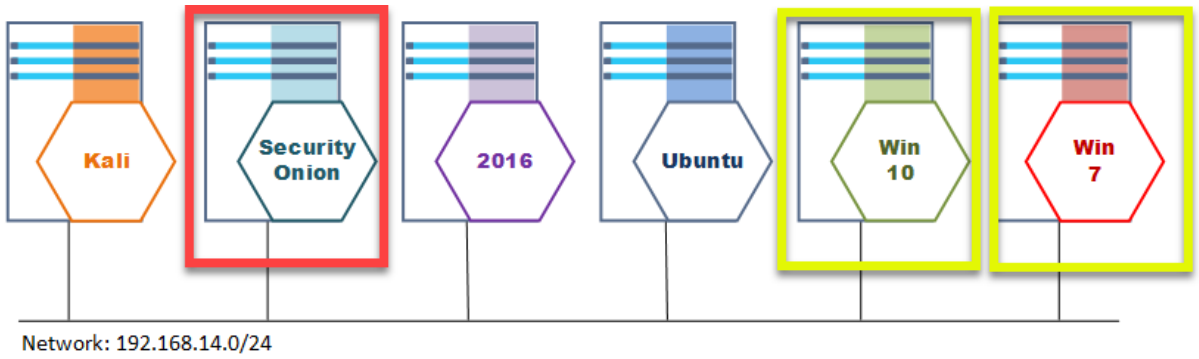
Lab Setup:

Security onion is collecting Packet Capture (pcap) data of traffic from all of the systems on the network and processing it using the Zeek (formerly Bro) Security Monitor framework. Zeek splits out unique sessions based on the source and destination IP address and the protocol that is being used. The result of this in Kibana is the "bro_conn" Log Type. This makes it trivial with a few simple Kibana queries to confirm if any given host is making connections using unencrypted protocols.

In this exercise we will be filtering these connections looking for traffic that is using non encrypted protocols where the policy indicated they should be. For this particular lab we are looking specifically for non https (port 443) traffic coming from a particular host. The same techniques can be used to confirm if any given protocol that we want to test is within policy or not.

PCI_DSS Mapping:

4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.



Zeek (Bro) logs:

In Kibana:

Key Fields for Confirming Encrypted Traffic:

Field	Description
source_ip	IP address that the connection was from
source_port	Source port of the connection
destination_ip	IP address that the connection was to
destination_port	Destination port of the connection
event_type	In this case we want to select [bro_conn]

Basic Search strings:

To search for any SSL connections seen on the network (We can also do this in the GUI)

```
>_ event_type:bro_ssl
```

To find all SSL connections from a specific ip address:

```
>_ source_ip:<ip address> AND event_type:bro_ssl
```

To find all NON-SSL connections from a specific ip address:

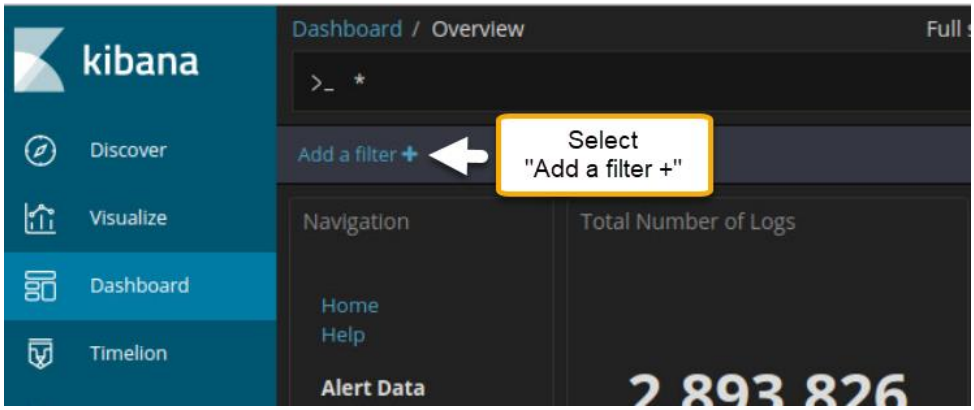
```
>_ source_ip:<ip address> AND NOT event_type:bro_ssl
```

Audit HowTo:

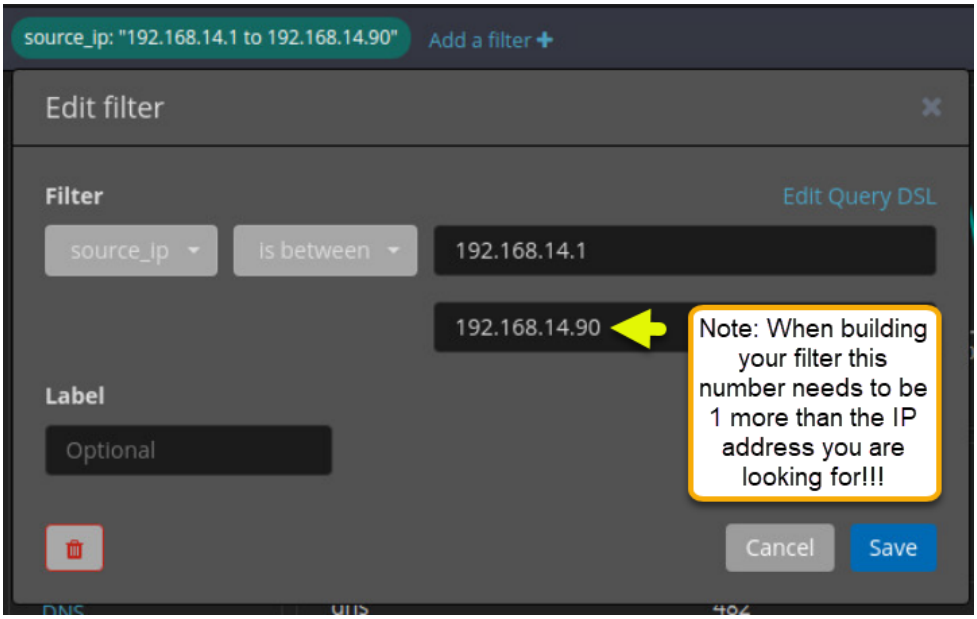
What we are trying to do with an audit here is prove that devices that are supposed to be doing only encrypted communications (POS - Point Of Sale devices for example) are not using non-encrypted connections. The easiest way to do this is to get the IP addresses of the POS systems and write a query that checks for any connections that are not encrypted. Note: We can use this same strategy for any encryption protocol we want (TLS, IPSec, SSH, etc) and the media that is transporting the connection (Fiber,Ethernet,Wireless) is not relevant as long as we can sniff it.

Build a filter for the IP address range that the interesting machines are in:

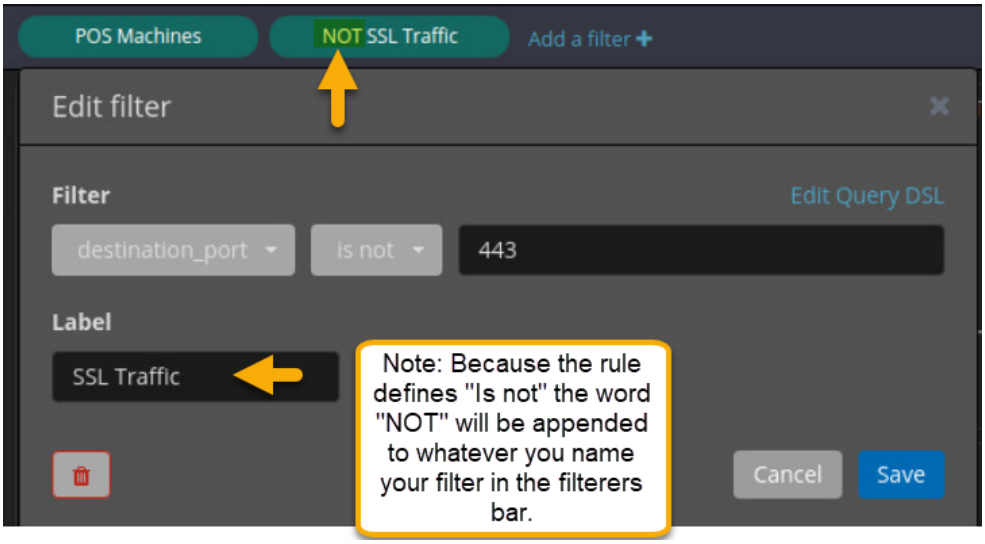
Step 1)



Step2) Enter the address range you want and save the filter.



Step 3) At this point we can make a second filter to find any network sessions that are not following the policy (not SSL in this case). The easiest way is to simply look for traffic not going to port number 443.



ToDo:

Find any IP addresses that are in the POS range that are not using encrypted SSL connections.

1. Were any of the POS IP's defined in the policy communicating via unencrypted connections? _____
2. If so what type of communication was non encrypted? _____
3. Would this be defined as against policy? _____