**CYBER DEFENSE OVERVIEW**

**PCAP Forensic Examination of Attack**

**Setting Up the Environment:**

To perform the cyber kill chain forensic analysis, we need to download Security OS and install it in VirtualBox. This is how the steps were performed:

1. Download and Import Appliance the Security Onion OS.ova and run it on Virtual Box.

2. Run setup from the desktop for ELSA, SQUIRL, SQUERT and OSSEC from” Quick Setup” option.

3. Make sure that eth0 is set up for Management Interface and eth1 is made for Snipping Interface.

4. Click OK and Run through the setup and reboot the system. Now, that the setup is rebooted again setup the username and password from the Quick Setup which is later used.

5. Since, the packet size is greater than the default size, increase the packet size by running these commands on the terminal.

6. ***sudo ifconfig eth0 mtu 6000*** and ***sudo ifconfig eth1 mtu 6000***.

7. To generate the BRO logs and alerts, tcpreplay the pcap file that is downloaded with the command.

***sudo tcpreplay -ieth1 -M10 /Downloads/Lab3.pcap***

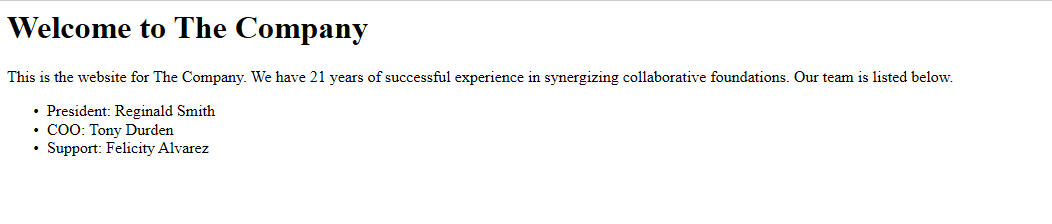
8. Now, first launch ELSA from Desktop to access the BRO logs.

9. Choose BRO\_CONN as a filter and hit submit query button to list all the connections captured in the PCAP file.

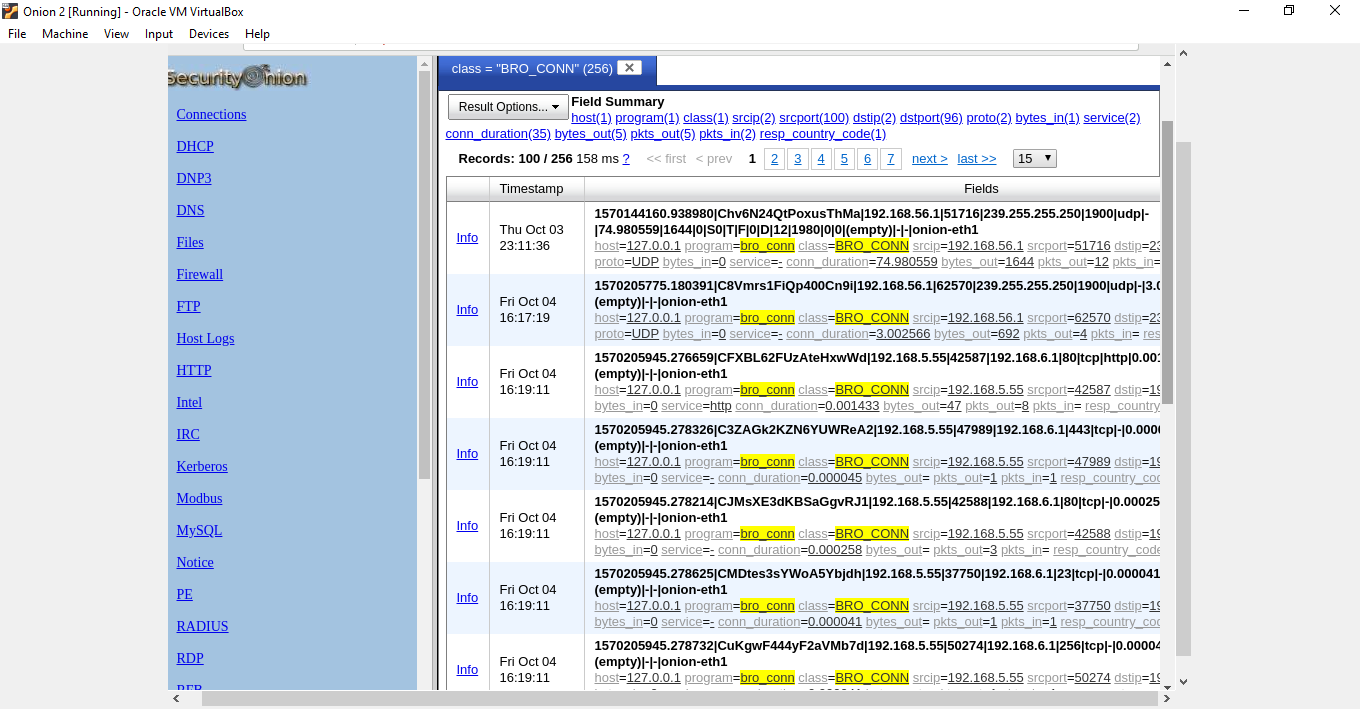
**CYBER KILL CHAIN PHASES:**

It defines the steps used by cyber attackers in today’s cyber-based attacks. Now that the environment is ready, the attacks are categorized and carried out through the cyber kill chain phase manner.

**1.** **Reconnaissance:** The intruder was able to find the employee names (President: Reginald Smith, COO: Tony Durden and Support: Felicity Alvarez) of “The Company” by accessing their website. Below steps describe in detail how this was cracked using ELSA.



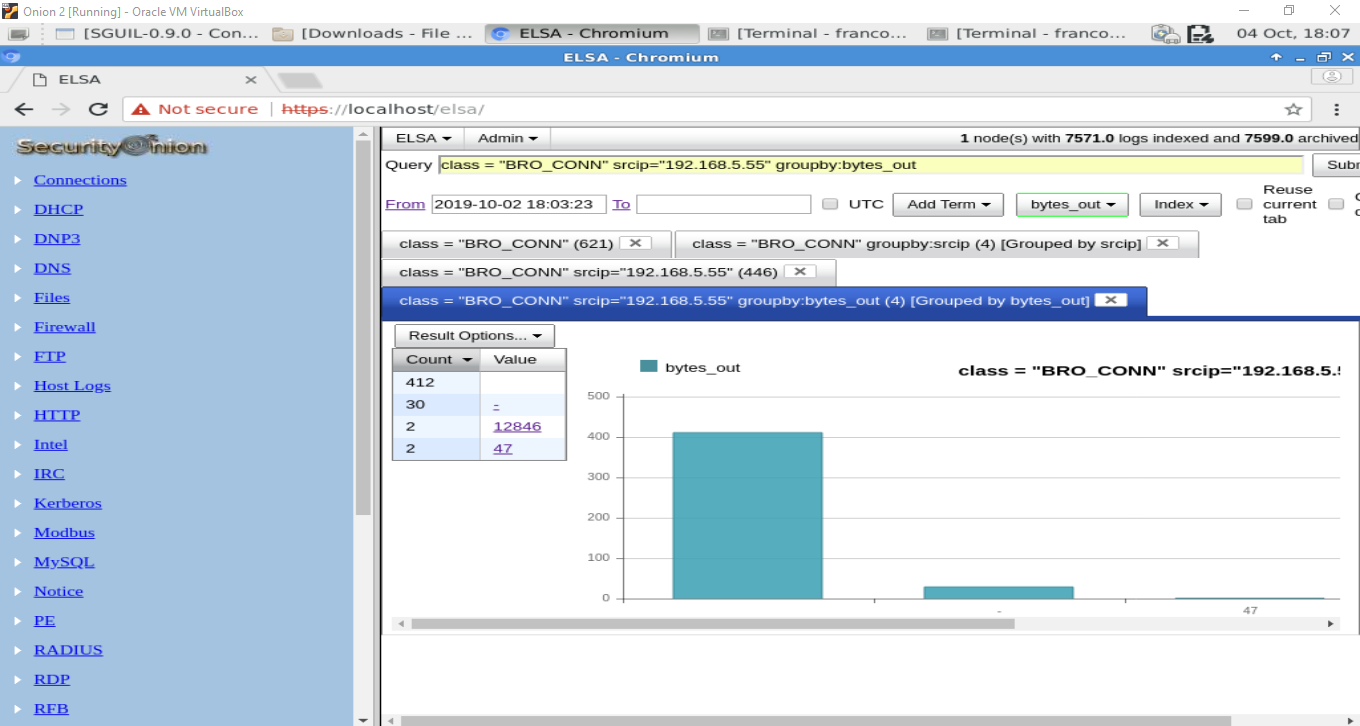
1. Based on the BRO\_CONN logs, we see that there was network traffic generated from 3 different IP addresses (this is represented by the number in the srcip column). Clicking on this number will group all the connections based on the source IP address.



B) Since the intruder IP address was already provided as 192.168.5.55 and also from the logs, we see large number of connections (223) being created from this machine, it was the prime contender for analysis.

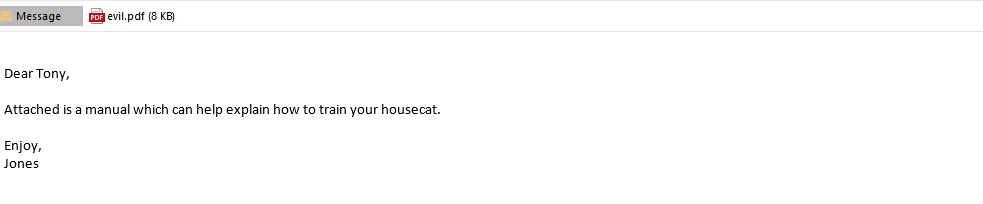
C) Clicking on the 192.168.5.55 will further filter the bro logs based on this IP address.

D) Now from this list of connections, we notice that there are 3 unique bytes out (refer to column bytes\_out (3)), representing different data bytes transferred.



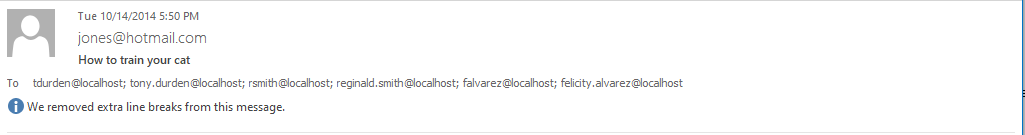
E) Clicking on the number 3 in the (bytes\_out) column will group by the bytes sent out from 192.168.5.55. Here we notice that there are two connections: one with 47 bytes and another with 12846 bytes.

**2. Weaponization:** In this method, the email is sent to Tony. Once the Tony Dorden opens the particular mail and clicks on the evil.pdf file present in the mail, the file is opened and a backdoor is created in his system. The document does not contain any visible text/data value.



**3. Delivery:** Here, this step involves the transmission of the attack to the intended victim(s). For example, this would be sending the actual phishing email to the attacker delivered. Below attached is the reference that contains the long list of mailing recipients list the attacker attacked.

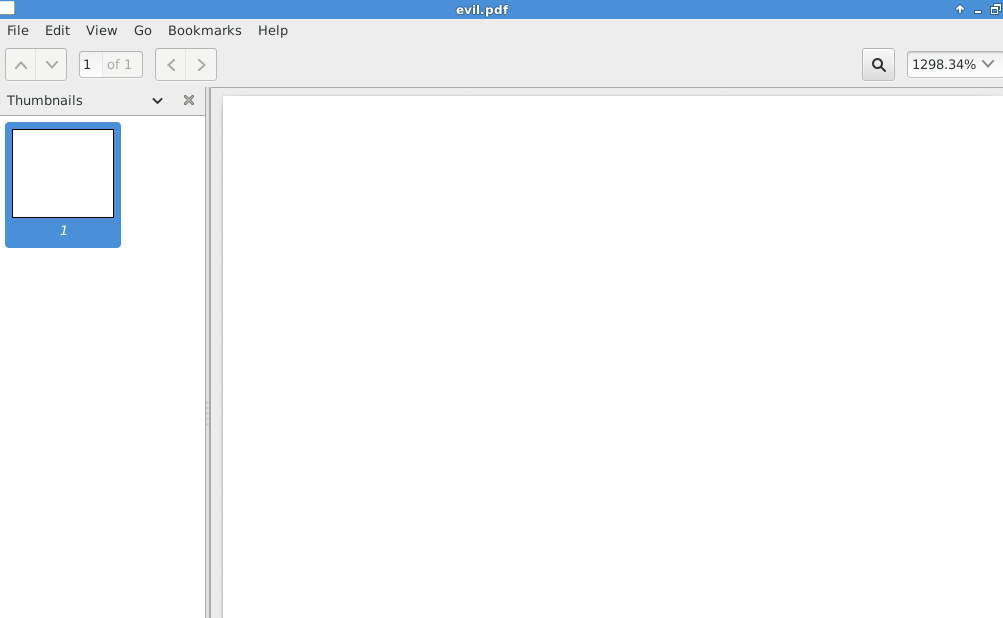
The mail was sent by Jones from [jones@hotmail.com](mailto:jones@hotmail.com) to Tony the victim of this attack who happens to be an employee in this company.



Now, that the .eml file was obtained. It was opened using a mail explorer to get the evil.pdf attachment. The evil.pdf is downloaded and attached herewith for your reference.

This is the (8 bytes) sized evil.pdf attachment from the mail that was sent out.

**4. Exploitation:**  During the exploitation phase, the APT malware code is executed on the target network through network through remote or local mechanism, taking advantage of discovered vulnerably to gain super user access to targeted organizational information systems.



**5. Command & Control:** In this phase, the software allows the attacker to fully manage the APT code in the environment and allows the attacker to fully manage the APT code in the environment and allows the attacker to move deeper into the network, exhilarate data and conduct destruction or denial of the service operations.

Here the anonymous user takes the control of all the system features like My Documents and Pictures.

The number of bits transferred and transmitted is also given in the log.dir file as shown below.



**6. Actions On Objectives**: The actions and objectives of the APT are dependent on its specific mission. The APT could be focused on data exfiltration, denial of service or destruction.

In the case of data exfiltration, the APT maybe interested in organizational proprietary data such as engineering designs or employee and customer .Personally Identifiable Information(PII).

The images are obtained in Xplico in the following way:

