SIT716 Computer Networks and Security

Week 9: Working with Sguil

Below you will find instructions for conducting an experiment designed to explore concepts of networking and/or security. Before referring to the instructions below, make sure you take the time to research and design your own experiment – even if you can't work out everything that is required. After completing your study of this unit, the skills you develop in designing your own experiments will be a critical skill for learning about new network protocols and security attacks, enabling you to work successfully as a valued professional in these fields.

Host	IP Address	Role
Security Onion	192.168.1.3/24	PCAP analysis

Outline:

In this lab we will be using Security Onion to analyse captured traffic stored in a packet capture (PCAP) file that is suspected to contain malicious traffic. Security Onion SO has many useful tools pre-packaged that allow you to analyse deeply pcaps; Kibana, Sguil, Squert, Wireshark, NetworkMiner, and more. We will be using a combination of all those tools to dive deep into the pcap, as well as additional tools and websites available online.

Important Notice:

In this lab we will be examining network traffic that contains real malware. Although most of this malware is quite old and well recognised by anti-virus products, you should never attempt to extract or work with that malware directly as you could inadvertently cause damage to your computer or data, or that of others (leading to criminal charges). To keep yourself and other users safe, ensure that all your analysis activity remains strictly within your isolated virtual machine.

Instructions:

1. Load VirtualBox and confirm that you have taken a snapshot of Security Onion before proceeding so that you can rewind the virtual machine to a clean state at the end of your work. Review the screencast in Course 4 Week 2 if you are uncertain how to do this.

2. Start Security Onion and open a terminal window.

3. Security Onion includes many sample PCAP files in the folder `/opt/samples`, however for this lab we will focus on `2014-12-05-phishing-email-traffic.pcap` found in the `mta` subdirectory. Start by browsing through the captured traffic using Wireshark, and see if you can identify anything unusual in the traffic, as follows:

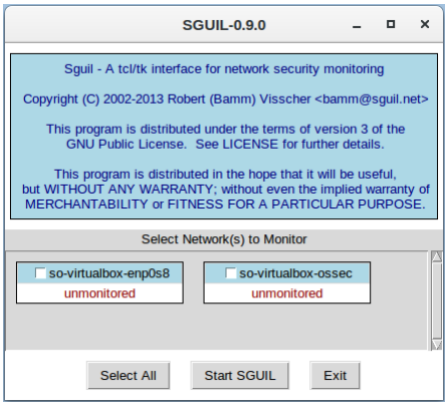
   ```
   wireshark /opt/samples/mta/2014-12-05-phishing-email-traffic.pcap
   ```

4. It should be clear that it's difficult to identify any problems without the aid of tools, so let's use Security Onion to help us. Import this PCAP file into Security Onion by executing the following command:

   ```
   sudo so-import-pcap /opt/samples/mta/2014-12-05-phishing-email-traffic.pcap
   ```

5. This will take a few minutes to complete the import operation, however once complete start the Sguil tool by double-clicking its icon on the desktop and login with the username and password you used when setting up Security Onion in Course 4 Week 2.

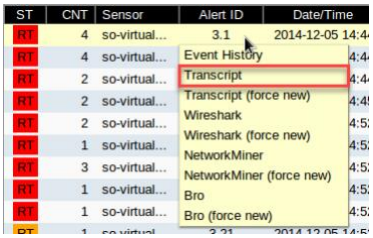
6. Once you've logged in, Sguil will display the dialog shown below. Click on the **Select All** button, then **Start SGUIL** button.



7. Once Sguil loads you will see a number of alerts at the top of the window. The events that we are interested in are dated 2014 (ignore the OSSEC events in 2018). What we are trying to establish is what happened in this particular attack. There is quite a lot of useful information displayed in this interface, In particular:
    a. ST column: indicates the status of the alert, indicating the likely severity (yellow, orange, then red in order of least to most severity).
    b. CNT column: indicates how many equivalent alerts have been detected, i.e., a number of 5 indicates there are five separate but equivalent alerts;
    c. Alert ID: a unique identifier for each alert (correlated events show the ID of the first alert);
    d. Date/Time: timestamp for the event (correlated events show the timestamp of the first alert);
    e. Source and Destination IP/port: indicates the endpoints for associated network traffic;
    f. Event Message: descriptive message indicating the rule triggered by the relevant events.

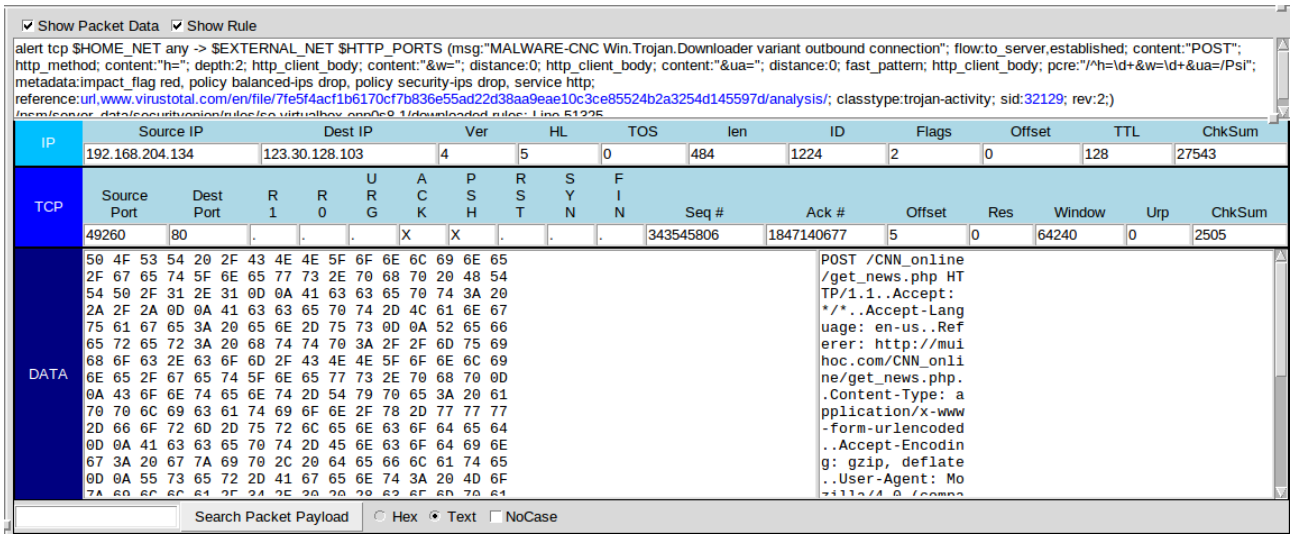
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	so-virtual...	3.1	2014-12-05 14:44:58	192.168.204.134	49260	123.30.128.103	80	6	MALWARE-CNC Win.Trojan.Downloader variant outbound connection
RT	4	so-virtual...	3.3	2014-12-05 14:44:58	192.168.204.134	49260	123.30.128.103	80	6	ET CURRENT_EVENTS Upatre redirector 29 Sept 2014 - POST
RT	2	so-virtual...	3.5	2014-12-05 14:44:59	123.30.128.103	80	192.168.204.134	49260	6	ET CURRENT_EVENTS suspicious embedded zip file in web page
RT	2	so-virtual...	3.6	2014-12-05 14:45:09	192.168.204.134	49262	123.30.128.103	80	6	ET CURRENT_EVENTS Upatre redirector GET Sept 29 2014
RT	2	so-virtual...	3.13	2014-12-05 14:52:30	192.168.204.134	49268	177.124.228.4	46521	6	MALWARE-CNC User-Agent known malicious user-agent string - realupdate - Win.Backdoor.Upatre
RT	1	so-virtual...	3.14	2014-12-05 14:52:30	192.168.204.134	49268	177.124.228.4	46521	6	ET TROJAN Upatre Common URI Struct Dec 01 2014
RT	3	so-virtual...	3.15	2014-12-05 14:52:30	192.168.204.134	49268	177.124.228.4	46521	6	MALWARE-CNC Win.Trojan.Upatre variant outbound connection
RT	1	so-virtual...	3.17	2014-12-05 14:52:31	192.168.204.134	49269	177.124.228.4	46521	6	ET TROJAN Common Upatre URI/Headers Struct
RT	1	so-virtual...	3.19	2014-12-05 14:52:32	192.168.204.134	49270	205.134.224.148	80	6	ET TROJAN Common Upatre Header Structure 2
RT	1	so-virtual...	3.21	2014-12-05 14:52:34	205.134.224.148		192.168.204.134		254	sensitive_data: sensitive data global threshold exceeded
RT	6	so-virtual...	3.22	2014-12-05 14:52:50	192.168.204.2	53	192.168.204.134	55828	17	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt
RT	16	so-virtual...	3.23	2014-12-05 14:53:07	212.56.214.129	443	192.168.204.134	49273	6	ET TROJAN Possible Dyre SSL Cert (fake state)
RT	3	so-virtual...	3.32	2014-12-05 14:53:36	85.10.194.10	443	192.168.204.134	49282	6	ET TROJAN Possible Dyre SSL Cert (fake state)
RT	4	so-virtual...	3.41	2014-12-05 14:53:51	192.168.204.134	54188	192.168.204.2	53	17	ET POLICY I2P Reseed Domain Lookup (reseed.i2p-projekt.de)
RT	1	so-virtual...	3.47	2014-12-05 15:06:35	192.168.204.134	18856	77.72.174.163	3478	17	ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag true change port flag true)
RT	1	so-virtual...	3.49	2014-12-05 15:06:53	192.168.204.134	18856	77.72.174.163	3478	17	ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag false change port flag true)
RT	1	so-virtual...	3.52	2014-12-05 15:09:13	192.168.204.134	49568	192.168.204.2	53	17	MALWARE-OTHER dns request with long host name segment - possible data exfiltration attempt
RT	1	so-virtual...	3.53	2014-12-05 15:09:13	192.168.204.134	49568	192.168.204.2	53	17	ET POLICY DNS Query for Invisible Internet Project Domain (I2P)
RT	1	so-virtual...	3.54	2014-12-05 15:09:14	192.168.204.2	53	192.168.204.134	49568	17	PROTOCOL-DNS domain not found containing random-looking hostname - possible DGA detected

8. Notice how the first three alerts (3.1, 3.3, and 3.5) have the same endpoints, which tells us that these three events are part of the same set of network traffic (a web request and response). Given the use of port 80, it is likely that these events are related to a HTTP exchange. For TCP connections it's possible to call up the transcript of the connection (the data passed over the connection) by right-clicking on the **Alert ID** and selecting **Transcript**. If you call up the transcript for the first three events, you'll notice that the output is identical (the three events are generated by the same traffic).



Note that there can be useful information found this way also. For example, looking at the transcripts you will see that the site being accessed is supposed to be CNN (US news network), however the hostname 'muihoc.com' is popping up. Why would CNN provide content from muihoc.com? If you search for this domain name you'll quickly find this is part of the malware attack.

9. The first event indicated (3.1) shows that a trojan was detected, so let's begin our investigation there. Click on the row to select that event, then down the bottom right of the window, click on the checkboxes to "Show Packet Detail" (shows the raw data in the packet) and "Show Rule" (shows how the event was detected/generated). You should see the following information:



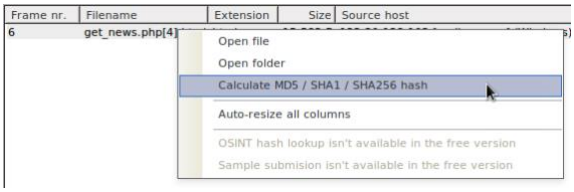
This information will quickly show you the packet data that caused the alert, along with the actual signature rule that raised the alert. This is useful for a quick look at data and rules to see what was detected.

10. Interestingly, this event gives us a link to VirusTotal, a free (for non-commercial use) database which stores information about malware files and detected by different virus scans (the URL links to the relevant page using the SHA-256 hash of the relevant file). The VirusTotal page (relinked here) can tell us about the malware that it thinks it has identified.

11. Notice the regular mention of the name 'Upatre' on the web page. Every anti-virus vendor uses their own naming scheme, however the regular appearance of 'Upatre' suggests a common name for this malware. Do a web search for this name and see what you can learn. For example, Symantec's web site indicates that Upatre was first discovered on November 20, 2013, which would make sense given this data was captured in 2014. It also tells you that Upatre will download other Malware, which we should keep an eye out for.

12. First, let's start by verifying the presence of Upatre. If something malicious were downloaded, it would be received in the response to a web request. If we examine event 3.5 in the above list, we can see that the source port and destination port have reversed, and the source is now port 80, commonly used by web servers. If there is any malware, it would likely be in here. We can preview any files included in the HTTP stream by using NetworkMiner. Right click on the event ID for event 3.5 and select NetworkMiner.

13. Change to the Files tab in NetworkMiner and you will see that one file has been detected. The file is just under 16KB in size, and although the file appears to be html from this entry, if you review the transcript from Step 8 above you'll see the filename is actually 'BreakingNews_pdf34.zip'. We can search VirusTotal for this particular file if we get its SHA-256 hash, which we can do by right clicking on the file entry and selecting Calculate MD5 / SHA1 / SHA256 hash.

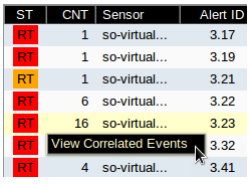


14. Copy the SHA-256 hash discovered in the previous step and paste it into the search box on VirusTotal's home page. If you review the resulting page (relinked here), you'll notice that this particular file contains Upatre (note that even the file size matches!).

15. At this point all we have confirmed is that the Upatre trojan was detected, we don't know that it has been run yet. Given that Upatre is a "downloader" of malware, we can scan forward through the events to identify if this has occurred. Look through the next events to try and find any activity that might involve downloading a file – this can be done quickly by looking for a long response by using the Transcript feature above, or you can load each event into NetworkMiner to be more thorough.

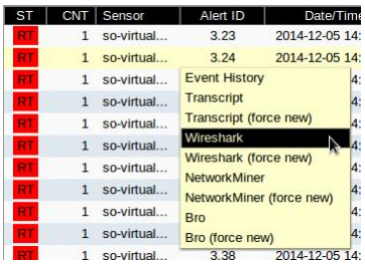
16. You will come across event 3.19 downloading a file inf13.jpa.txt, however if you look up the SHA-256 on VirusTotal (relinked here) this appears to be benign. Keep looking!
Note: if you do a web search for inf13.jpa.txt you'll see this is part of Upatre's behavior but we don't know that yet!

17. Next you will find event some SSL certificates being exchanged in events 3.23 and 3.32. There seems to be a lot of events here, let's have a look and see what's going on. If you right click on the event count (CNT field) for a particular row, you can see the correlated events. Do this for event 3.23 which shows 16 correlated events.



18. The list of correlated events here indicates the same source IP address and source port, and the same destination IP address, however the destination port is changing, suggesting 16 separate data connections. It's possible to have a look at the traffic generated for a particular event in Wireshark by right clicking on the Alert ID and selecting Wireshark – try this on any of the alerts, and have a

look at the exchange here. We can see that the exchange is encrypted, so we can't see the contents.



19. Returning to the event however, note how the name of 'Dyre' is mentioned twice. What is Dyre? Is it the malware? Try a web search for 'dyre malware' or similar and conduct some research to find out what it is. If successful, you will learn that Upatre and Dyre are regularly combined together through phishing emails with supposed invoices (zip file with an executable within). Together they are used for capturing online banking information. Symantec has some good information on this combination (follow this link), including a whitepaper with further information linked at the bottom.

The above shows some of the ideas you can use for investigating strange behaviour on the network detected by systems such as the various IDS included in Security Onion. There are many other samples in the /opt/samples folder, now would be a great time to rewind your VM back to the snapshot before you loaded data in and try something different! See what else you can learn about different attacks and malware behaviour in particular.