## Download and install Security Onion

|  |  |
| --- | --- |
| SecurityOnion | 16.04.7.1 |
| CPU | 2 with 2 Cores |
| RAM | 8 GB |
| Hard Drive | 60 GB |
| Interfaces | Ens33: 192.168.156.4 | Ens34: monitoring |

|  |  |
| --- | --- |
| WIN7-BASE & WIN7-VICTIM | Win7 SP1 Build 7601 |
| CPU | 1 with 2 Cores |
| RAM | 2 GB |
| Hard Drive | 60 GB |
| Interfaces | 192.168.156.11 & 192.168.156.10 |

I already had a known working Security Onion 16.04.7.1 iso file, so I used that to create a virtual machine (VM) in VMware Workstation Pro 16.1.0 build-17198959. This Security Onion VM was placed on a /25 (255.255.255.128) subnet (192.168.156.0) behind a pfSense 2.50.0 firewall (192.168.156.2). One of the SecurityOnion interfaces is for maintenance access (ens33) and the other is for monitoring. Next, I set up more expansive monitoring rules by running the *sudo vim /etc/nsm/rules/local.rules* command. Once the Vim editor is opened I added the following rules:

* *alert tcp any any -> 192.168.156.0/25 any*
* *alert udp any any -> 192.168.156.0/25 any*
* *alert icmp any any -> 192.168.156.0/25 any*
* *sdrop udp 192.168.156.2 57621 -> 192.168.156.4 57621*
* *sdrop udp 192.168.156.2 57621 -> 192.168.156.10 57621*
* *sdrop udp 192.168.156.2 57621 -> 192.168.156.11 57621*

The first three rules (alert) are set up such that they would trigger an alert on any TCP, UDP, or ICMP traffic that traveled across the 192.168.156.0 /25 subnet. The three (sdrop) rules were set up to drop any UDP packets sent past the gateway to either the SecurityOnion, WIN7-BASE, or WIN7-VICTIM VMs on port 57621. I did this because I have Spotify installed on my host machine and I knew from experience that it has an unannounced P2P feature that trawls networks and I didn’t want that to interfere with the results. Additionally, I also blocked this behavior on the host machine using Windows firewall. In order to apply the rules and verify that all of the monitoring is working I ran the *sudo rule-update && sudo so-status* commands. All modules reported [OK] status, so I proceeded to adjust Wireshark permissions by running the *sudo dpkg-reconfigure wireshark-common* and selecting the <yes> option which will allow any user to capture traffic with Wireshark. Finally, I opened Wireshark’s options and configured it to capture on the monitoring interface (ens34), stored captures in /Desktop/captures, enabled promiscuous mode on all interfaces, set the capture file type to pcap, and checked the option to create a new file automatically after the pcap reaches 512 MB in size. Before beginning to get WIN7-VICTIM infected, I made sure to start the network captures in the previously configured Wireshark on SecurityOnion and verified that I was capture traffic with a ping from WIN7-VICTIM to 192.168.156.2.

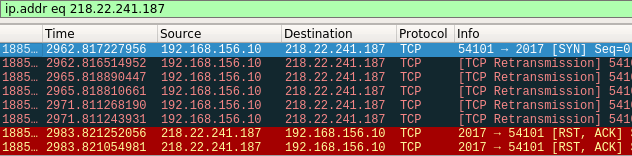
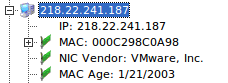
## Honeypot Configuration

Next, I created a ‘golden image’ Windows 7SP1 VM, because Windows 7 is less noisy than Windows 10. In order to properly install VMware tools, I manually installed the Windows update windows6.1-kb4474419, set the floppy drive and optical drive to auto, rebooted, and then installed VMware Tools from the VM menu. Next, I disabled IPv6, installed Google Chrome (Version 89.0.4389.9) since most modern webpages wouldn’t work properly in the natively installed Internet Explorer 7, and disabled Windows Firewall. I then created some baselines by running the *netstat -ano* and *netstat -abn* commands on WIN7-BASE. After this I ran an port scan from SecurityOnion using the *sudo nmap -sS -p0- -v -a 192.168.156.11* command. Once this was completed, I cloned WIn7-BASE and renamed this clone to WIN7-VICTIM for the actual infection.

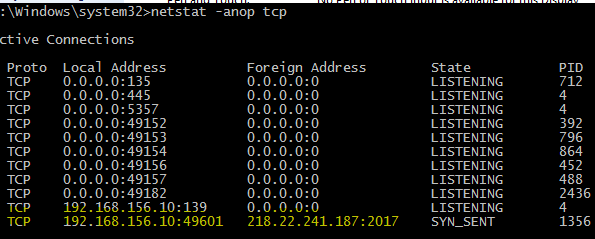
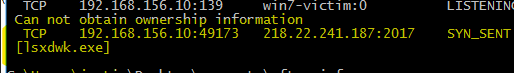
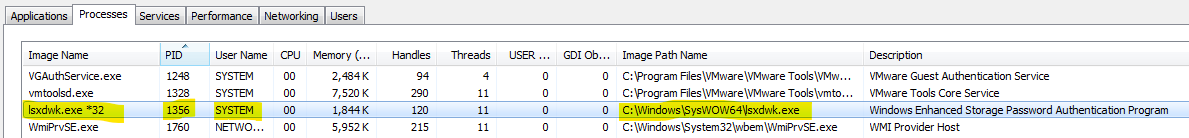
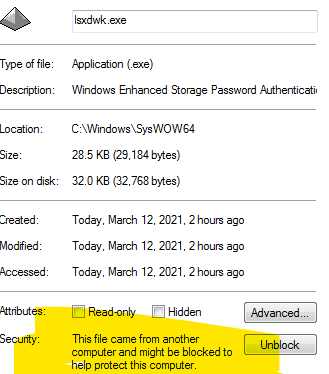
## Initial Analysis

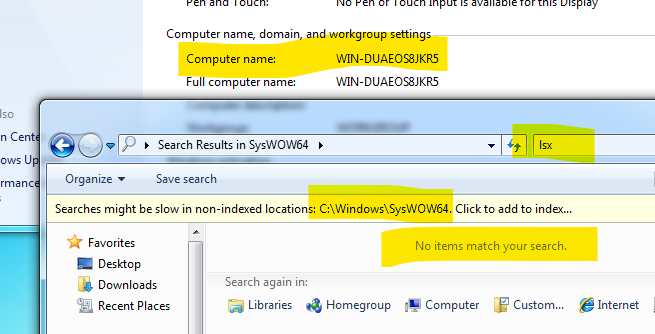
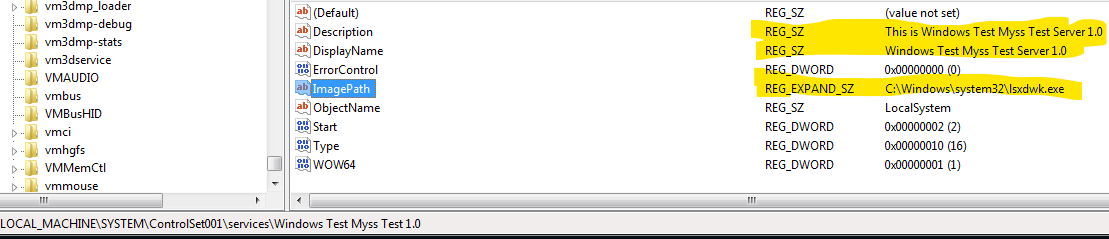
The above picture shows a section of suspicious traffic, from which I was able to determine a preliminary timeline of events: access to a ‘likely hostile’ .tk (Tokelau) domain from BitTorrent traffic, potential reconnaissance actions in the form of pings and SSH scans. Next, there were possible attempts to access the machine (Http Client Body contains pass = in cleartext). Finally, we see a packed executable is downloaded, I was able to determine was from IP address 218.22.241.187.

## Identify Conversations

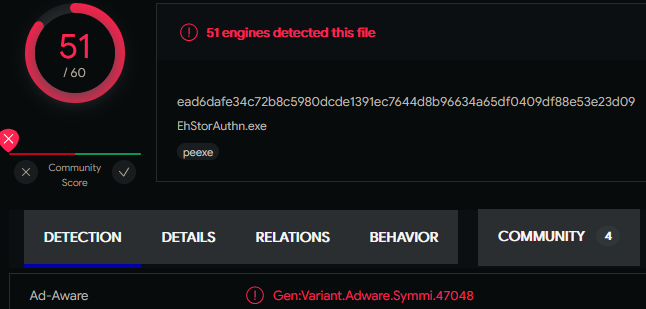
   
The above screenshot shows some of the traffic captured, filtered by the attackers IP address. It appears that it was making contact with the impacted machine several times a second, using a TCP connection on port 2017. The attacker appears to be using a virtualized environment:  


## Extract Malware

Using the information I’d gathered up until this point, I went looking for the malware. The first Thing I did was to run *netstat -anop tcp* to show me that active TCP connections, their state, destination, port, and associated PID:  
Here we can see that 218.22.214187:2017 was running with PID 1356. Because of this, my next step was to run *netstat -abp tcp* in order to see associated processes, which revealed that this connection was tied to lsxdwk.exe:  
  
To further corroborate this, I looked at Task Manager to see if I could cross reference that:  
  
This gave me a path to the file:  
  
Next I checked Win7-BASE to see if this is a hollowed out file and didn’t find it:

  
Next I searched in the Registry as that is a common persistence method:  


## Analyze DNS Traffic

This malware did not appear to make much use of DNS, but I was able to determine that the IP address 218.22.241.187 is registered to ChinaNet Anhui Province Network (chinatelecom.com.cn) in Suzhou, Anhui, China. It appears that lsxdwk.exe may be a modified form of EhStorAuthn.exe and has been thoroughly cataloged by the community:  


## File List

|  |  |
| --- | --- |
| File Name | SHA1 Hash |
| SecurityOnion16.04.7.1.iso | 7f436c7b27102a76aafb2ba682e18774d0eac8cd |
| lsxdwk.exe | 040D184883540187F9FE4F6646228CB895F250EA |
| 03102021-INFECTIONTIMEBB\_00009\_20210313010946.pcap | baad04507e6eb91ce7fcac860bf6c7498d5d8732 |
| 03102021-INFECTIONTIMEBB\_00010\_20210313011046.pcap | 6c4c239317e342920814b06d32088166d5b2b2b9 |
| 03102021-INFECTIONTIMEBBagain\_00001\_20210313034711.pcap | 7c0c3c0b52fa68f0d43207b534206def377c0094 |