SPC-Project2-Part 2

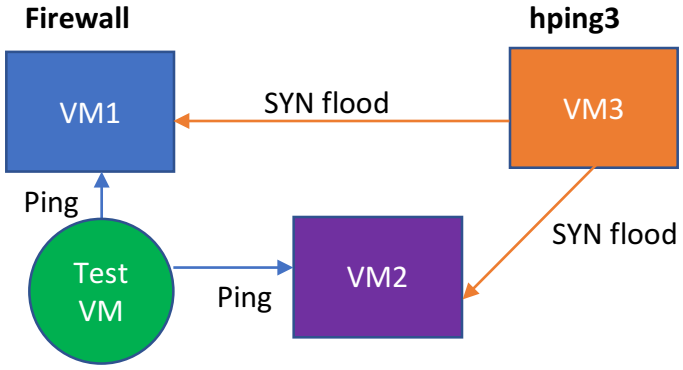
Yue Guan

1. Firewall

For the firewall section, because we need to launch SYN flood DoS attack as three different types: basic SYN flood, SYN flood with spoofed IP and SYN flood with SYN rule on Firewall. So, we set up firewall and architecture as this:

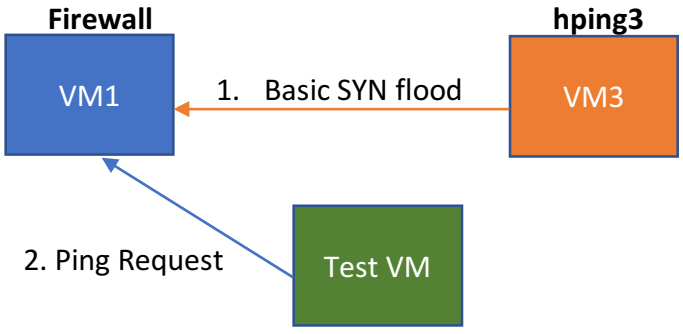
1. Basic SYN flood

a. The very first basic test:



For the basic SYN flood attack test on the firewall, I first actived firewall on VM1 with specific rules that block the SYN request from VM3 and disabled firewall on VM2. Then I launched basic SYN flood on VM3 to attack VM1 and VM2 using hping3. With another test VM sending ping request to both, VM1 responses much faster than VM2. So, the firewall is fully configured.

b. Basic SYN flood as required:

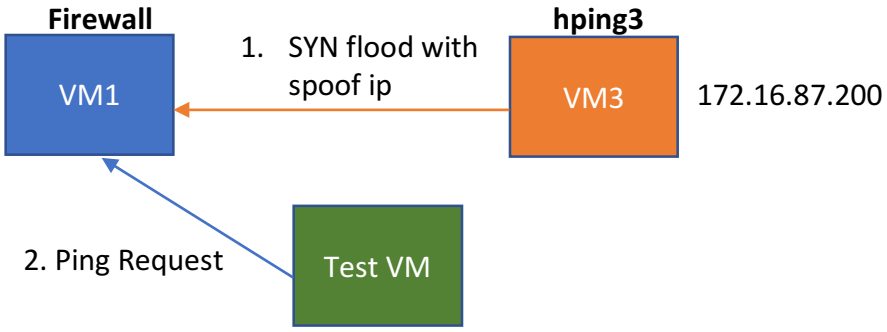


For the basic SYN flood, I use nmap to scan the open port and use one of the open port 22 to do SYN flood attack. We set up vm3 with hping3, and

configure ufw on VM1 with the rule that deny all SYN request from vm3 IP: 172.16.87.137.

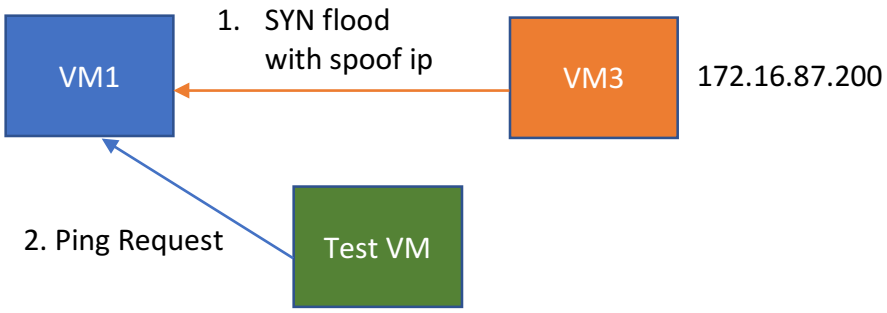
After we exploit basic attack from vm3 to vm1, we choose Test VM(vm2, IP: 172.16.87.136) to ping vm1 to test vm1's responsive capability. VM1 is still working. The pcap file captured on vm1 is *syn1basicvim.pcap*. The pcap file captured on vm3 is *syn1basicattack.pcap*.

2. SYN flood with spoofed IP



For the spoofing IP one, I didn't change the ufw configure on VM1. So, the ufw on VM1 is just deny on SYN from ip 172.16.87.137. Then we use a spoof ip address: 172.16.87.200 on hping3 on vm3 to do SYN flood attack on VM1. And use test VM to do ping request on vm1 to test the responsive capability here. It shows that the ping request didn't work so well now. The related pcap file *syn2attack.pcap* on VM3 and *syn2vim.pcap* on VM1.

3. SYN flood with SYN rule on Firewall

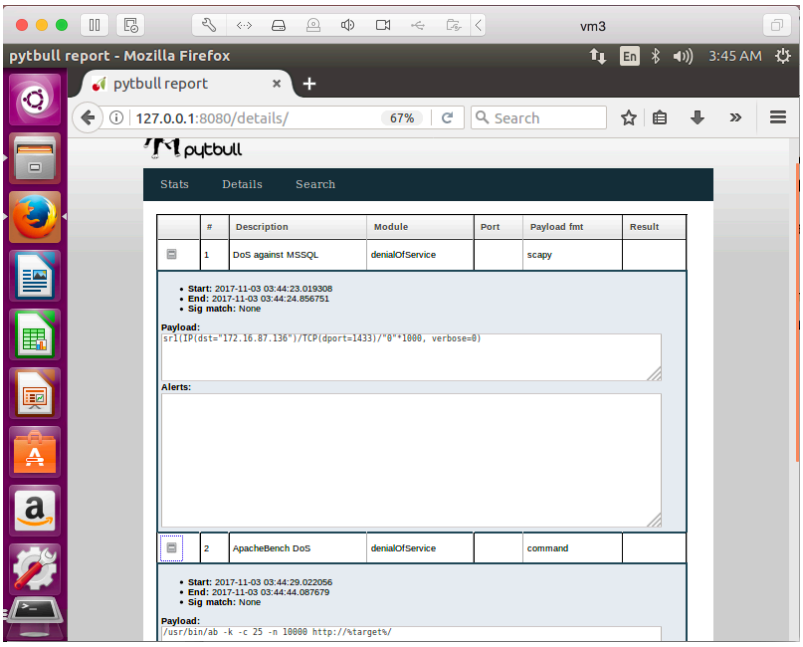


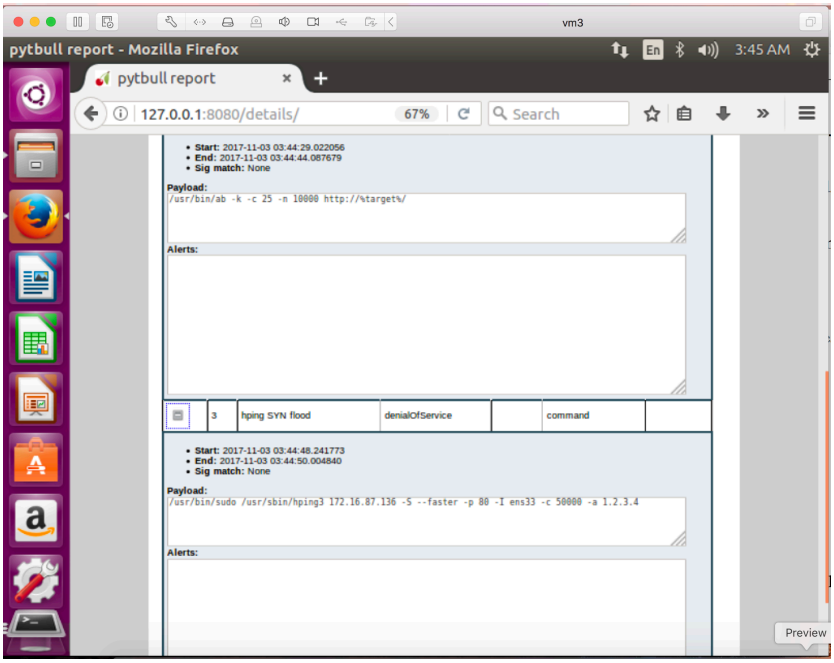
To fully detect SYN flood using ufw, I modify the firewall before.rules by blocking all SYN request when it receives 5 per second or more. Then we still test VM1 from VM3 using spoofing IP and hping3. With the ping test from Test VM(IP: 172.16.87.136), it shows VM1 is work great now. The related pcap files are *syn3attack.pcap, syn3vim.pcap*.

IDS/IPS

Run 2 tests for each category of Pytbull (one that fails and one that passes) for each of the IDSs. Mainly we require you to run tests for the below categories:

a. Denial of Service
    1. The failed DoS Screenshots:

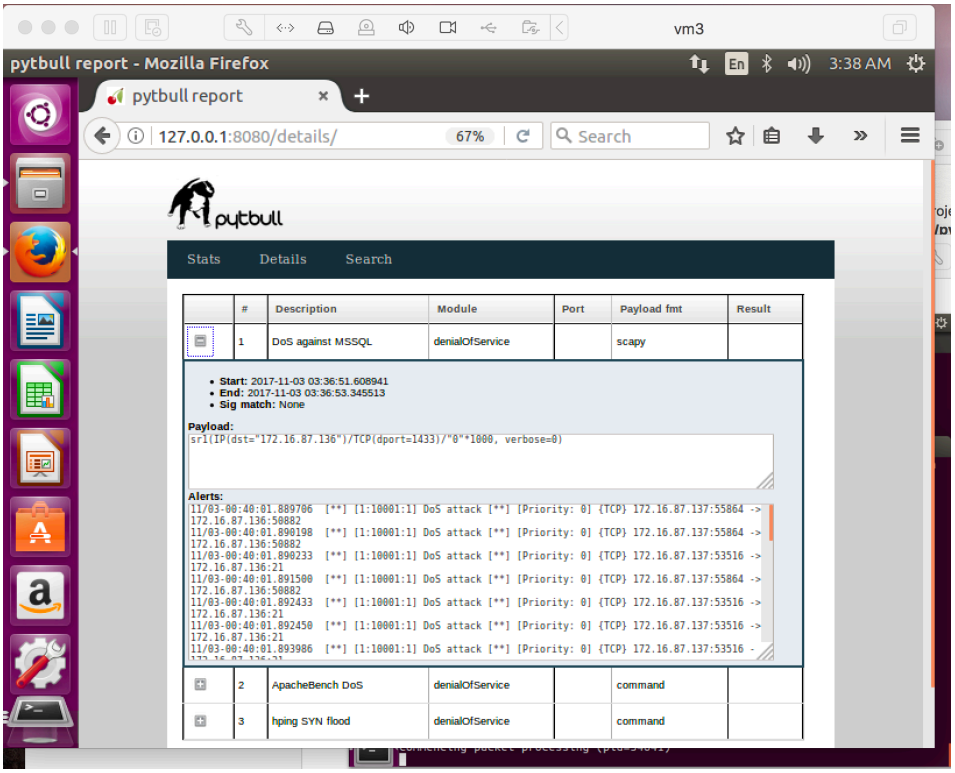


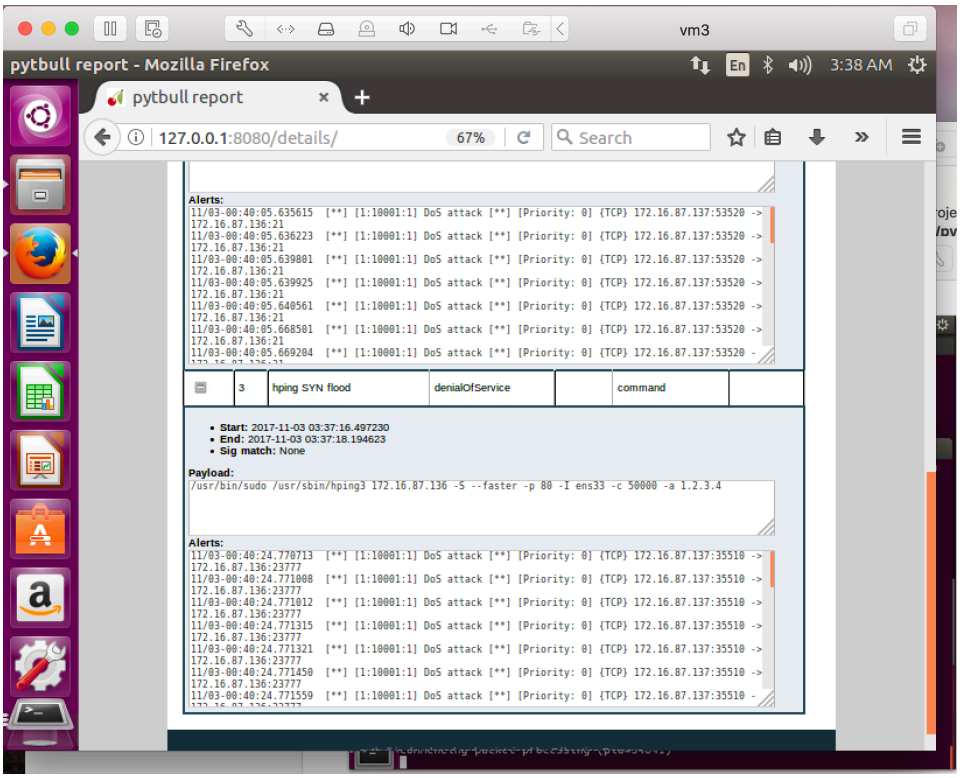


The reason why I failed this time: I didn't set up correct snort rules to detect those DoS attack. At the meantime, there is some configuration mistakes I have on snort too.

2. The Success One:

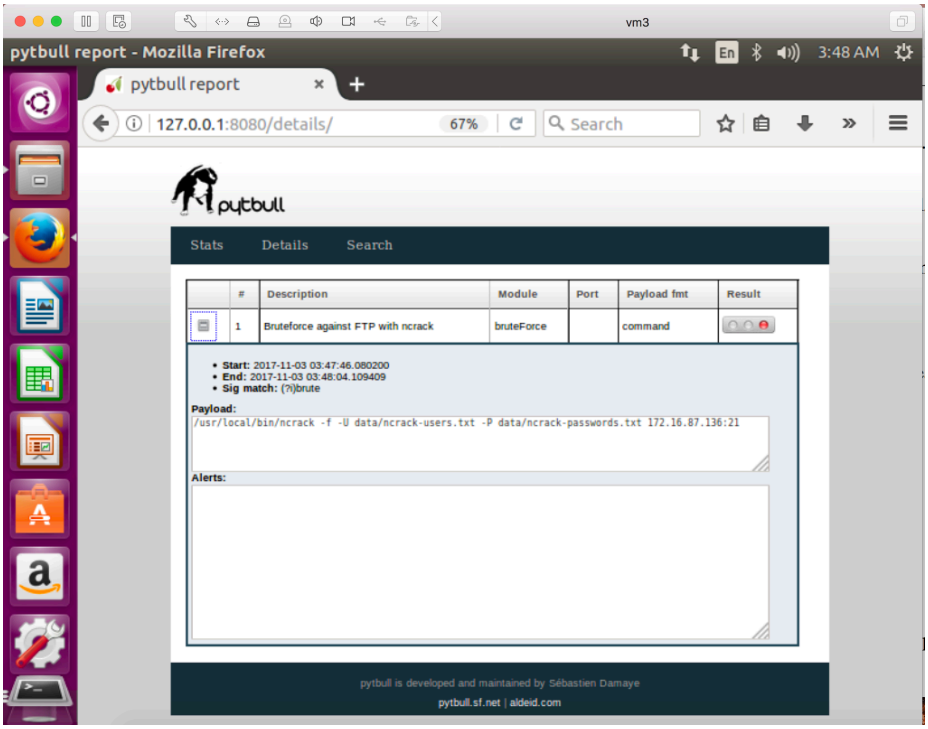
The corresponding alert logs file looks like this:





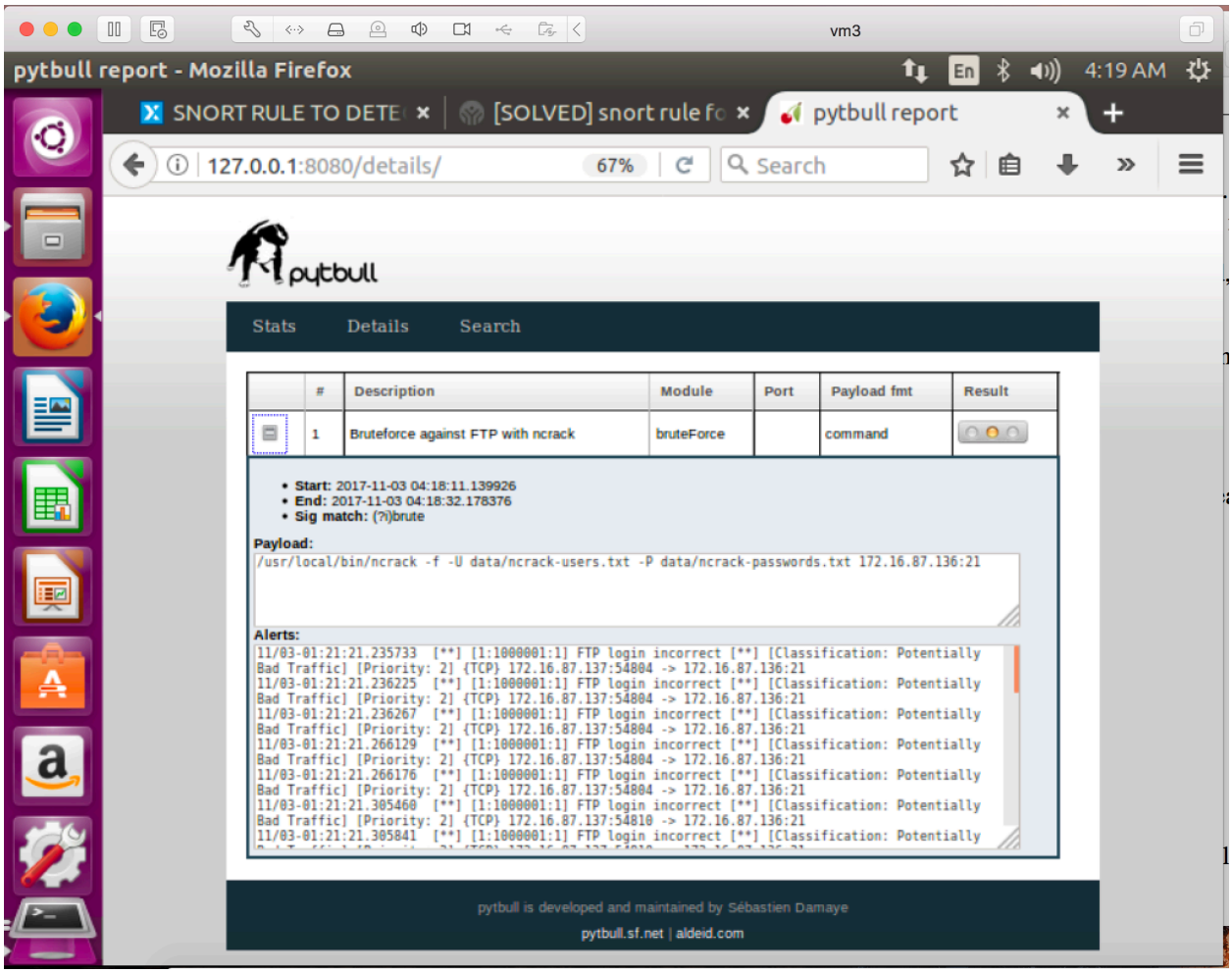
b. Brute Force

1. The failed one:



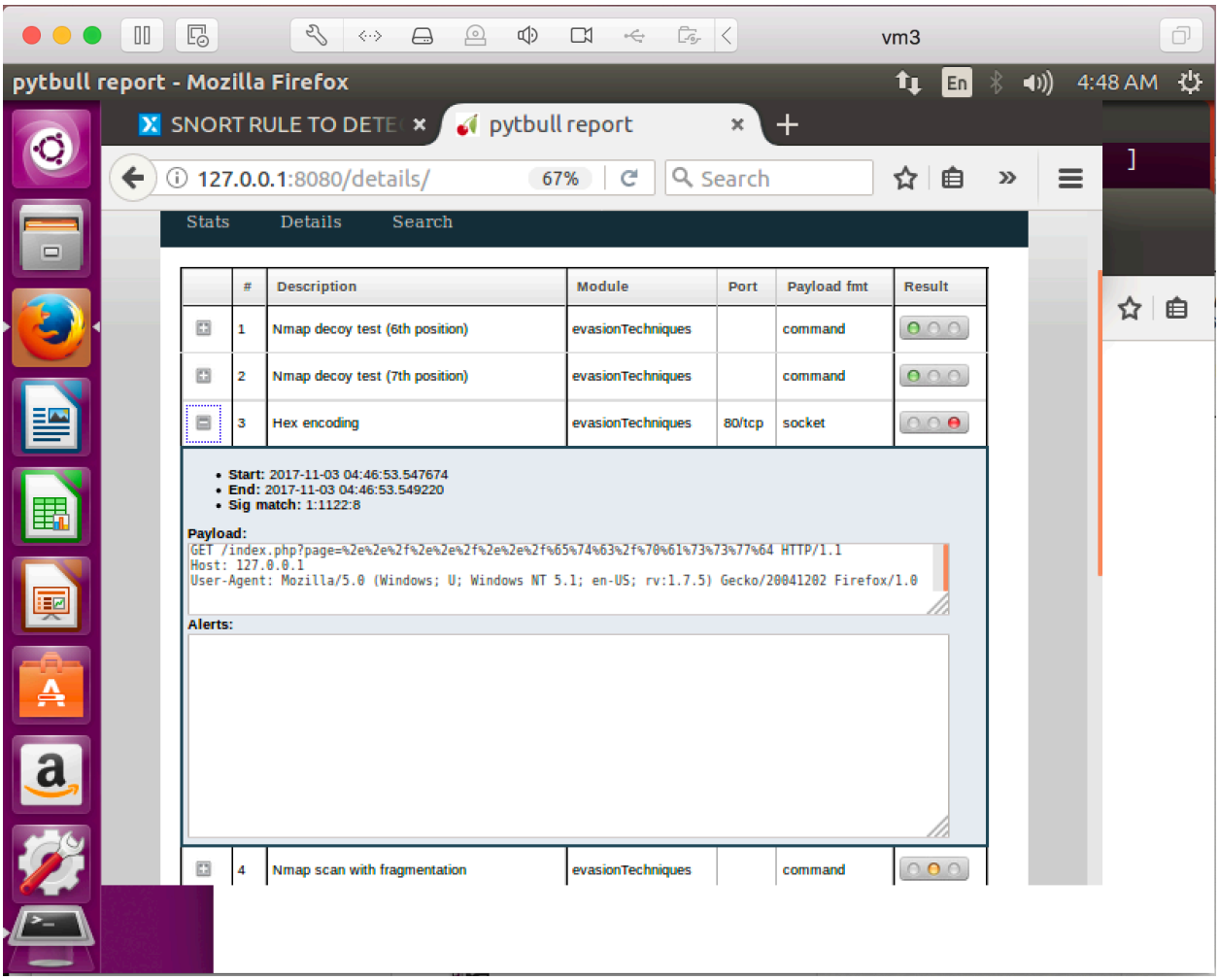
The reason why I failed: I set up some snort rules that just detect the content where has ftp, however, it should be has some content with 530 (not found).

The Successful one with correspond alert log files:



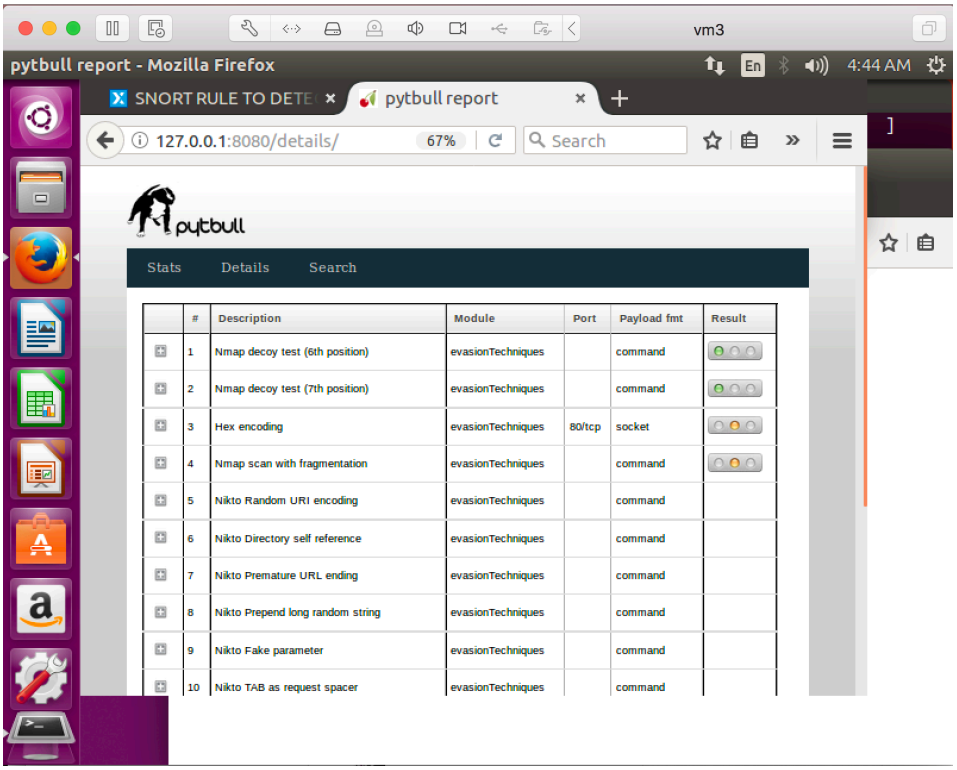
c. Evasion Techniques:

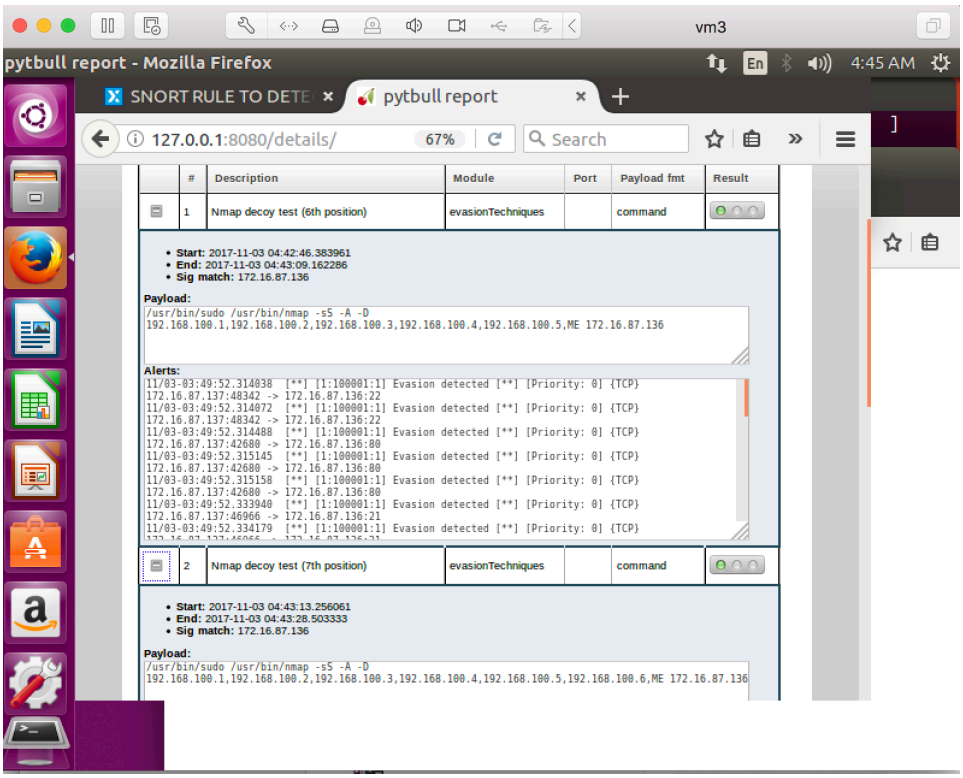
1. The failed one:



The reason why I failed: The reason why I failed for Hex encoding here is because I didn't detect the specific HTTP things in my snort rule. I didn't set the rule properly.

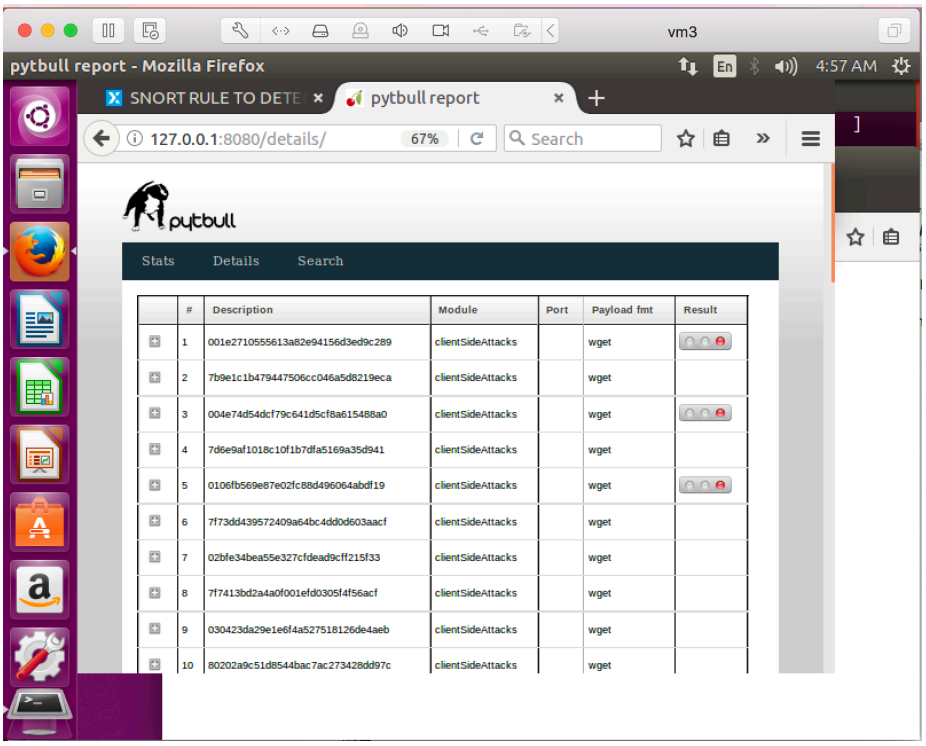
2. The successful one with alert files:





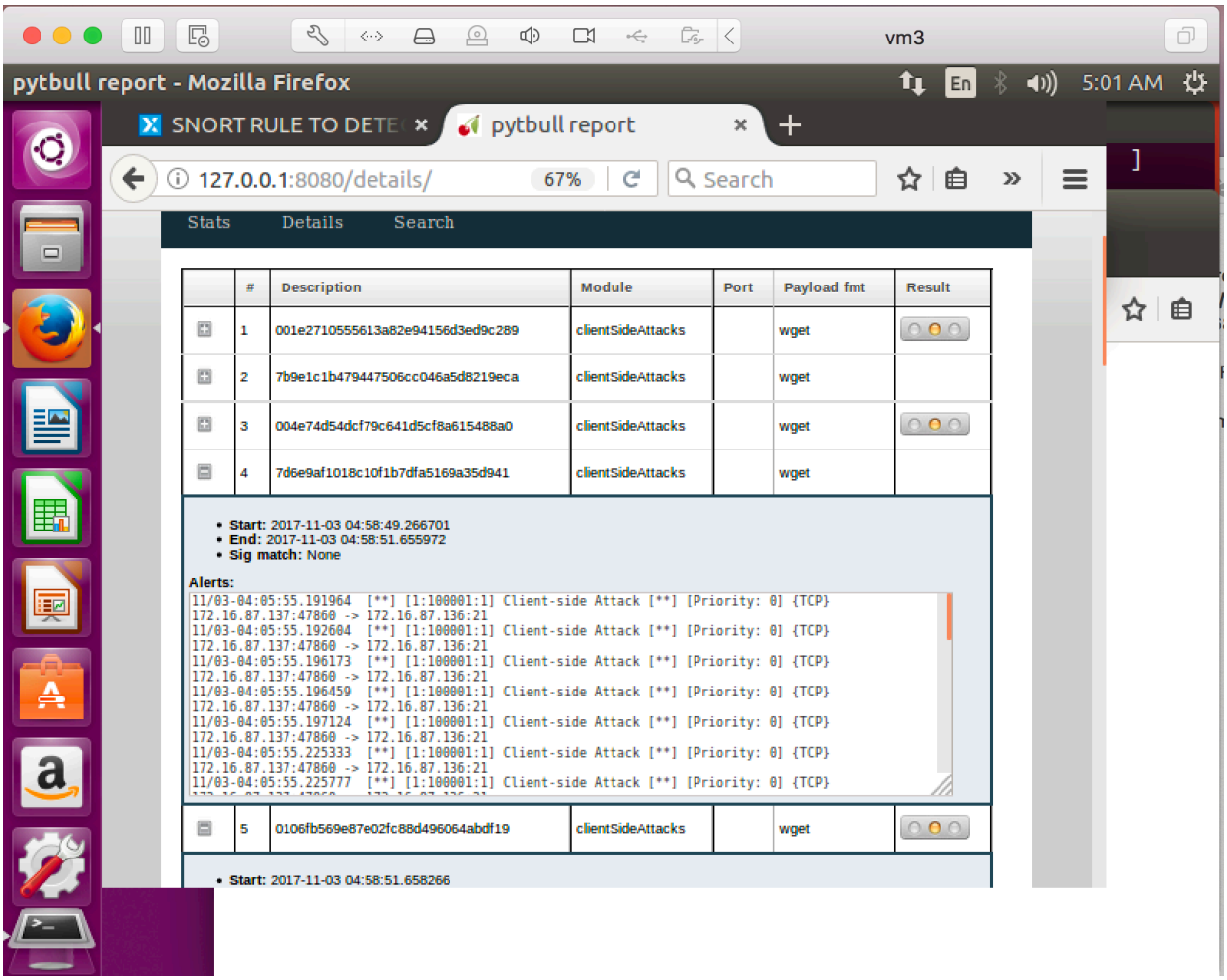
d. Client Side Attacks

1. The failed one:



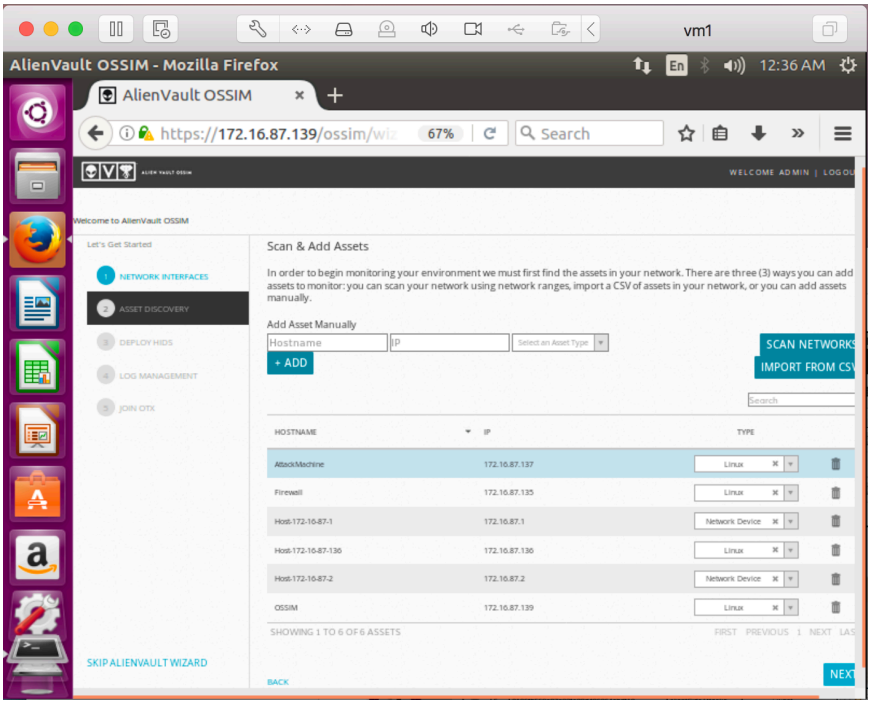
The reason why I failed: I didn't set up a snort rule related to the client side attack. It all relates to something else.

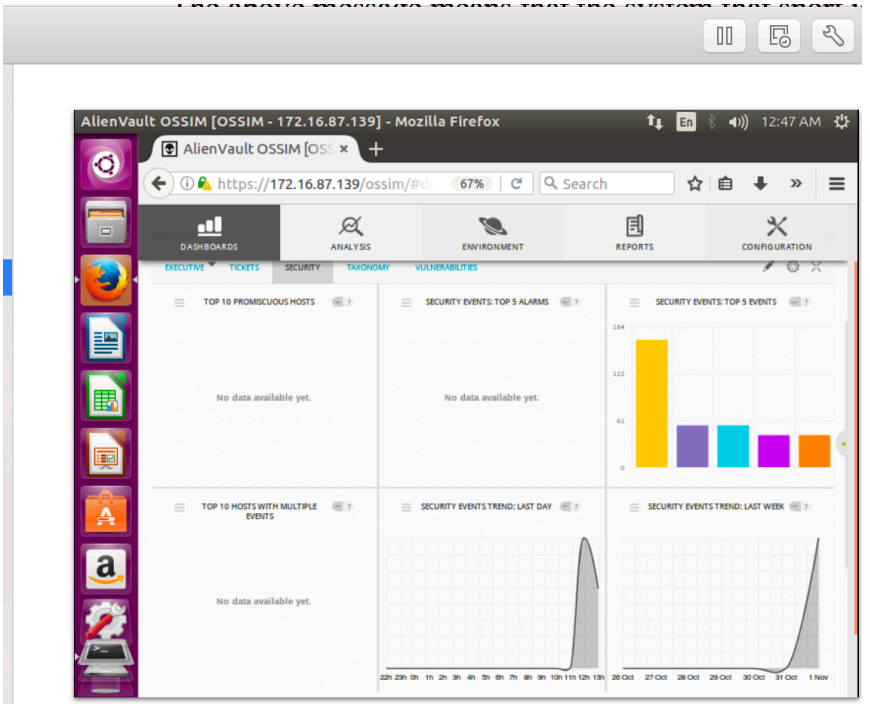
2. The successful one with alert logs:



e. SIEM

1. Some Screenshot on SIEM:





2. The reason why I failed on OSSIM:

   However, the OSSIM part didn't succeed this time. Fortunately, professor Ayo understand us about the situation on OSSIM that we faced this time and let us to write the reason why we failed this time on OSSIM and will still give us scores on that. It's great.

   So, the reason why I failed OSSIM here is I met with some trouble to integrate snort into my OSSIM. Also, there is some issue with my own computer here because of the large plenty amount of VMs I need to open at the same time. My laptop failed for hundreds of time on opening 4 or more VMs at the same time. In addition, failed thousands of time to integrate snort into OSSIM. The screenshot shows where I was going through, and I look forward to seeing where it should be. It would be great if you could show us on class about how OSSIM should work and integrate all the security devices together in one platform.