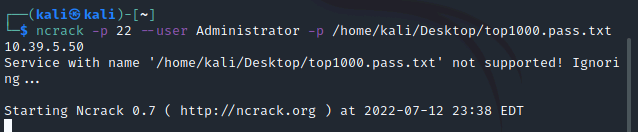
Analyzing Attacks on Computing and Network Environments

LAB-01

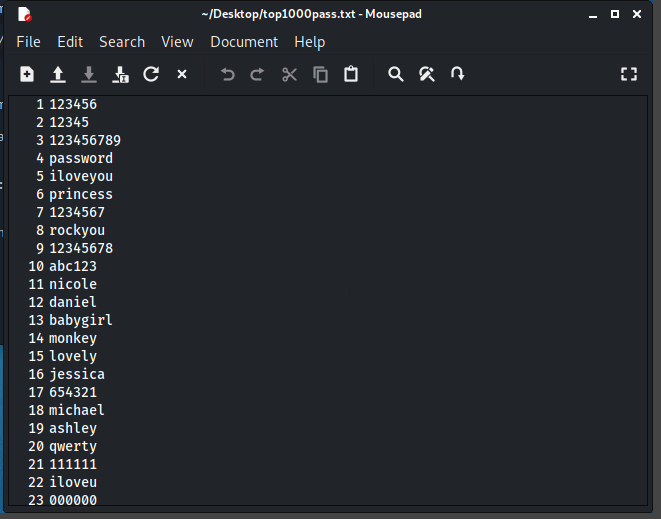
Objective: Using Kali Linux machine to use Ncrack to crack Windows Server Administrator password.

Scenario: Looking at reconnaissance attacks has led you to think about the next steps for the attackers going after the Develetech network. The company has been lax in password policy before, and you decide to see if an attacker could get easy access to your critical servers by cracking passwords. You'll therefore perform an online password cracking attempt against your SSH server using a pre-generated password dictionary. If you manage to breach the server, you'll see just how much damage you can do with a successful hacking attack.

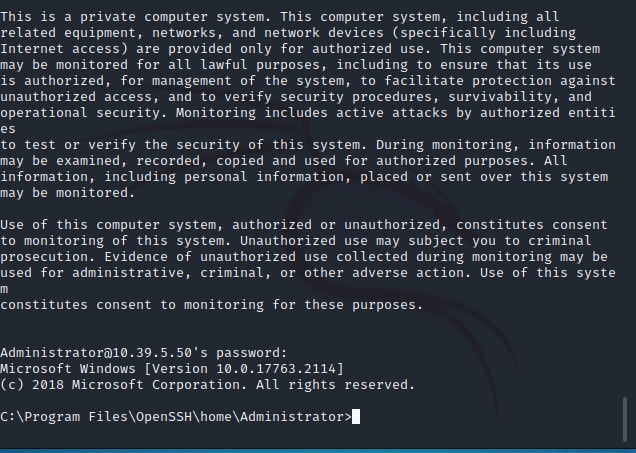
* I begun this lab by spinning up a Kali Linux Virtual Machine (VM) in order to utilize Ncrack program.



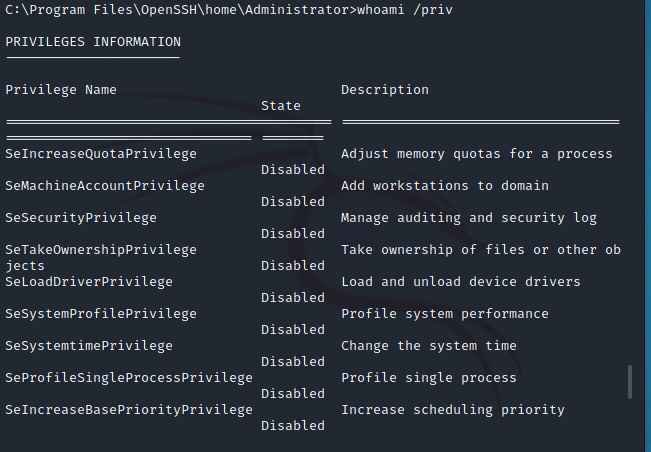
* I am starting the password cracking/harvesting process by issuing the follow command **ncrack -p 22 --user Administrator -P /home/kali/Desktop/top1000pass.txt 10.39.5.50**
* Note: 10.39.5.50 is the Windows Server IP



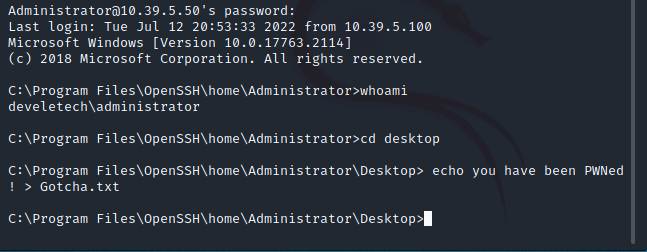
* I started analyzing the results from the harvested and notice that every password did not meet today’s password complexity standards.
* Note: Most organizational policies force password length, must include a Lower and Uppercase, numbers and special characters. Also configuring failed password attempts to a low number causing the machine to lock up and present a stalemate situation to the attacker.



* I was able to log into the Windows server using the collected credentials collected. In a Terminal first issue the ssh [Administrator@10.39.5.50](mailto:Administrator@10.39.5.50) to ssh into the server and use the password Pa22w0rd



* I verified that the system I was able to log into was the correct one by issue 2 commands: whoami for user information and whoami /priv for user privileges



* I then played with the Administrator just a tad by sending him a little message stating that I got him/her. This can be verified by logging into the Windows Server VM and look at the text file that is now on that machine’s desktop.

This now completes this lab. Go back to the Kali Linux machine and close the ssh connection by using the command CTRL +C in the terminal.

Questions for thought:

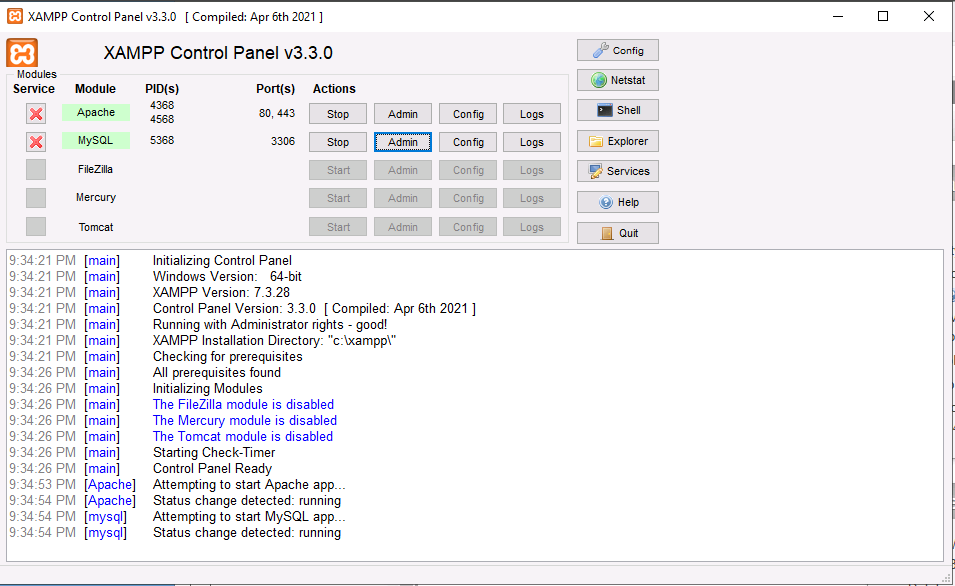
* What other harm could an attacker do with this level of access?
  1. This is a wide-open question as a attacker has a buffet of things he/she could exploit such as deleting/locking files or system for a ransomware attack, installing malicious programs containing trojans or downloading malware or scripts for a zero day attack, setting up control and command by installing a backdoor. The possibilities are endless.
* How would someone defend against a type of attack?
  1. As mention early the simplest and most effective recommendation is to implement the password complexity, utilizing Multifactor for logging in or configuring a failed password length lockout. Also, you could disable SSH connections entirely.

Assessing Impact of Web-Based Threats

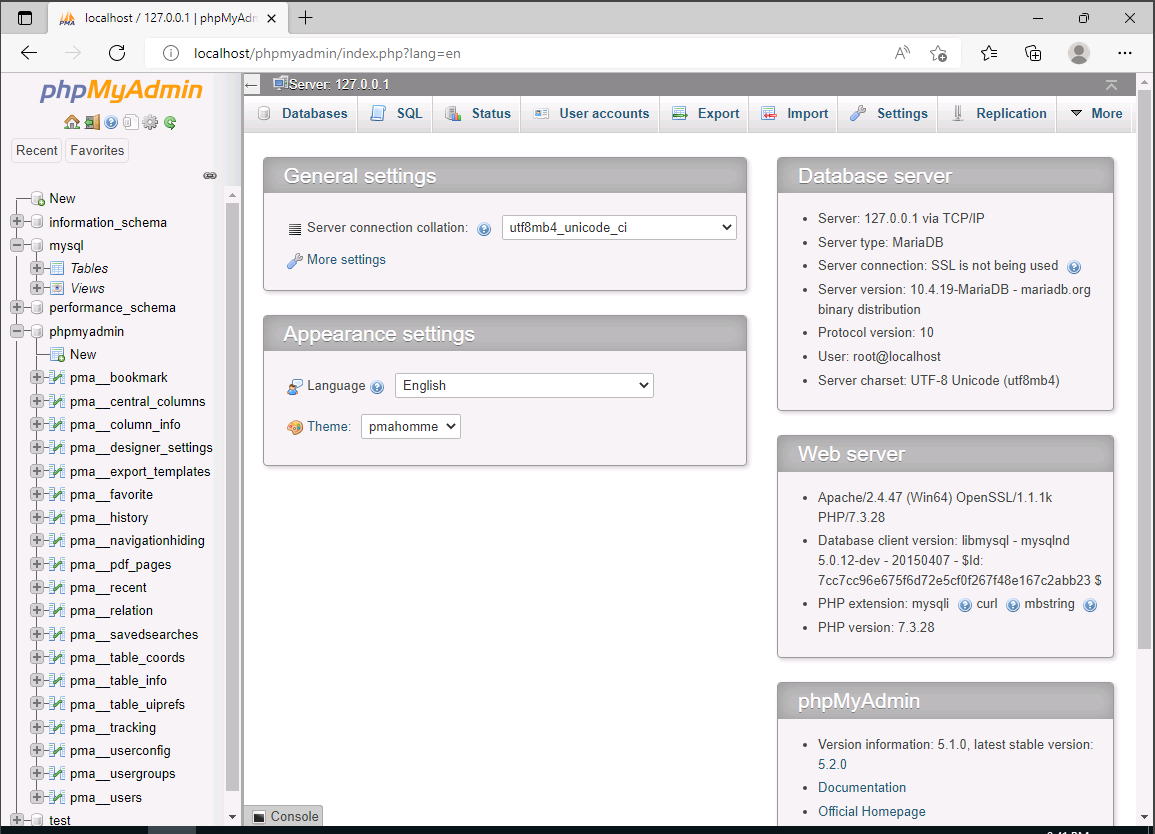
LAB-02

Objective: A SQL-Based Server has already been configured on Windows Server Machine. The Web server uses XAMPP, an open source software.

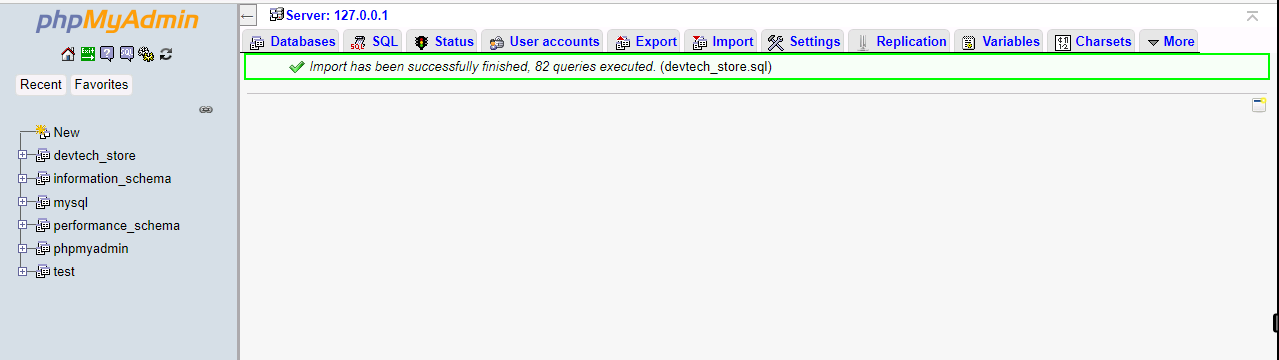
Scenario: Develetech's storefront website was unfortunately published in a hurry, and not much attention was paid to securing the site. You're especially concerned that the site is vulnerable to injection attacks on its SQL database. An attacker may be able to hijack an account in the database to deface the site or tamper with the product data. So, you'll test the website's vulnerabilities to SQL injection to assess how web-based threats can compromise your organization's security.



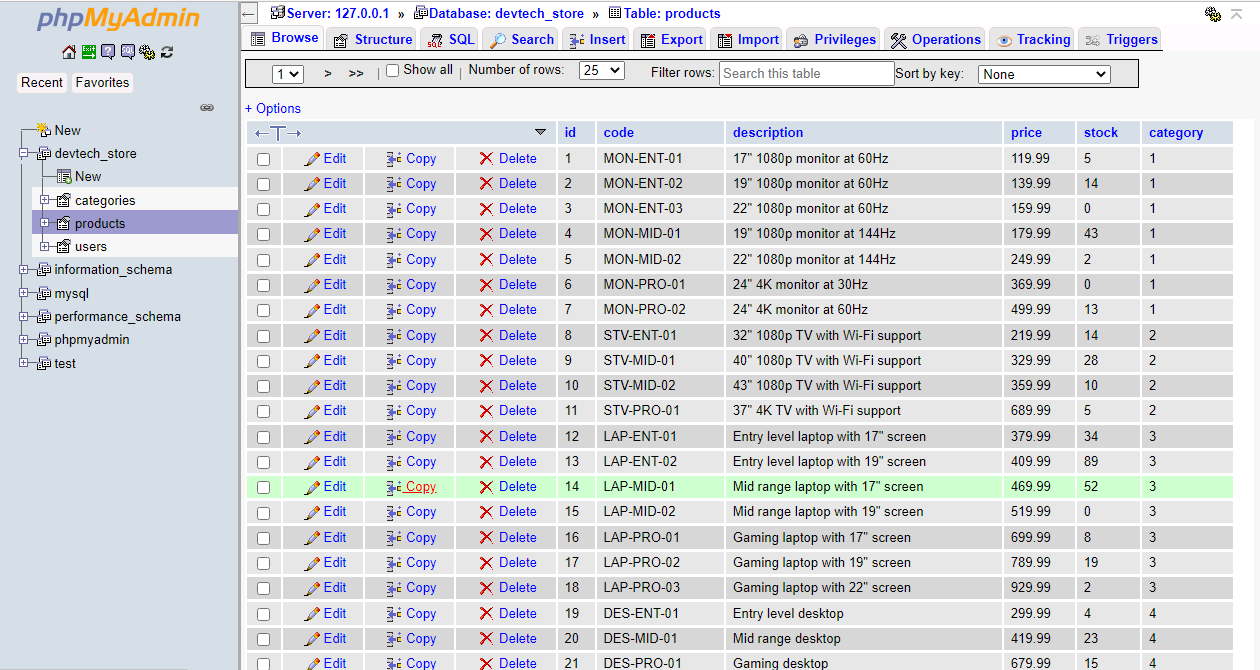
To begin this Lab, I had to login into the Windows Server. After logging in I had to start the SQL server where I started apache and MySQL servers. I also selected the Admin user as I must import some database files.



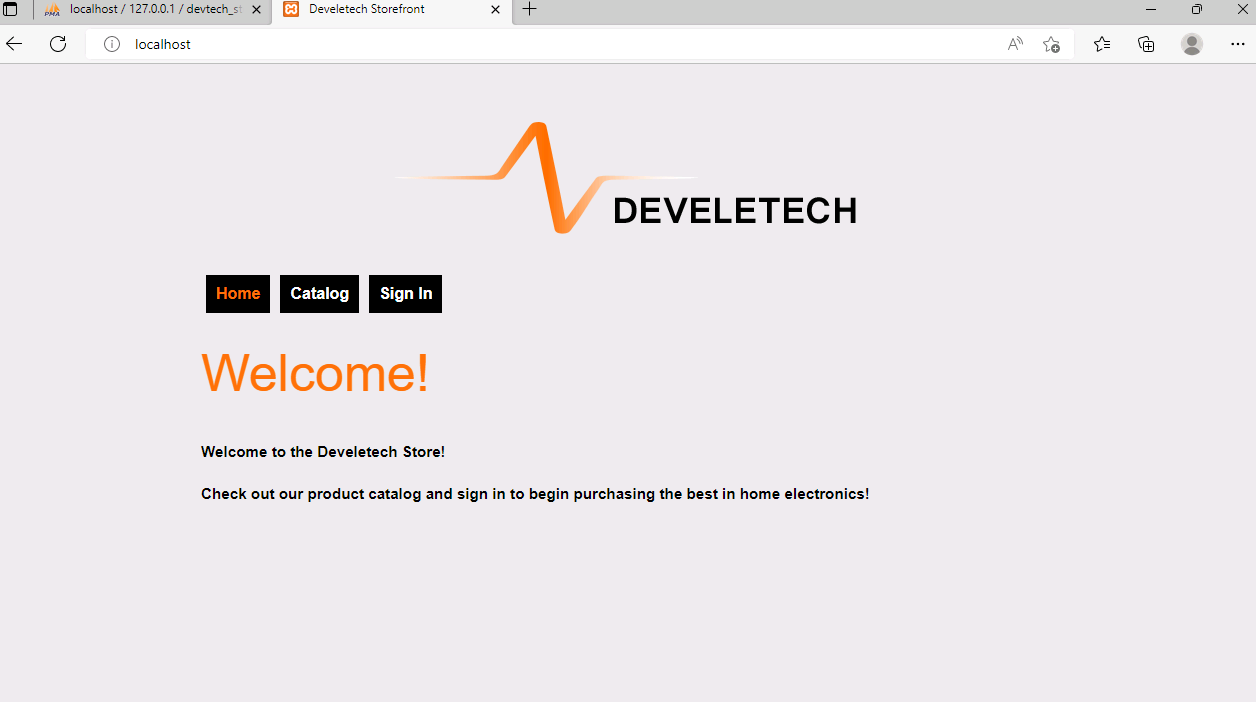
After I enable the Admin user, this GUI started up.



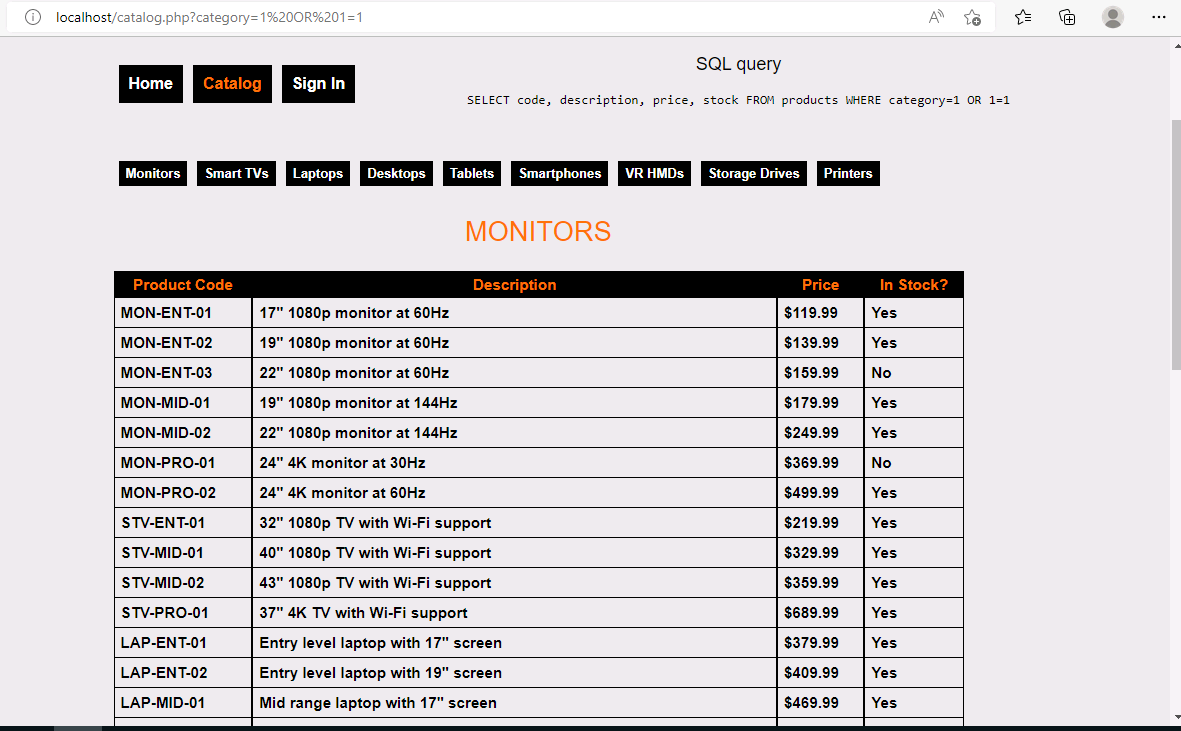
I was successfully able to import the database. Now it is time to analyze the database.



I am just going the 3 tables looking at the information seeing if anything malicious or out of place sticks out and catches my attention.



I setup Develetech website and I verified It was successful by going to <http://localhost:80>. To set it up I had to move the config folder to the correct directory and extract the package files.



I executed a injection under the monitor category simply adding OR 1=1 to the end of <http://localhost/catalog.php?category=3> 🡺🡺http://localhost/catalog.php?category=3 OR 1=1



Now its time to see if I can get in. I inputted my credentials and was denied access. Looking at the SQL query and see that it automatically made my credentials into strings.



Attempted to login again, but this time with password manipulation. Before, the injection I was working with true statements such username = Kevin password = password, yet now I am working with statements to cause the output to be false. This was done by x’ OR x’=’x and using that as my password.

Note: The "always true" statement applies to every row of the users table, so it logs you in as the first user in that table. In this case, the first user is Laura Anderson, who has administrator privileges. It's common for the first accounts in a database of users to have administrator privileges.

Other:

Some other ways an attacker can use a SQL injection against a database is dropping entire tables, editing individual rows, dumping contents of members table to see user login information or even log in as specific users.

To defend against SQL injections, you can initiate input validation or use of parametrized queries/statements

This is the end to this lab, but don’t worry there is more coming.

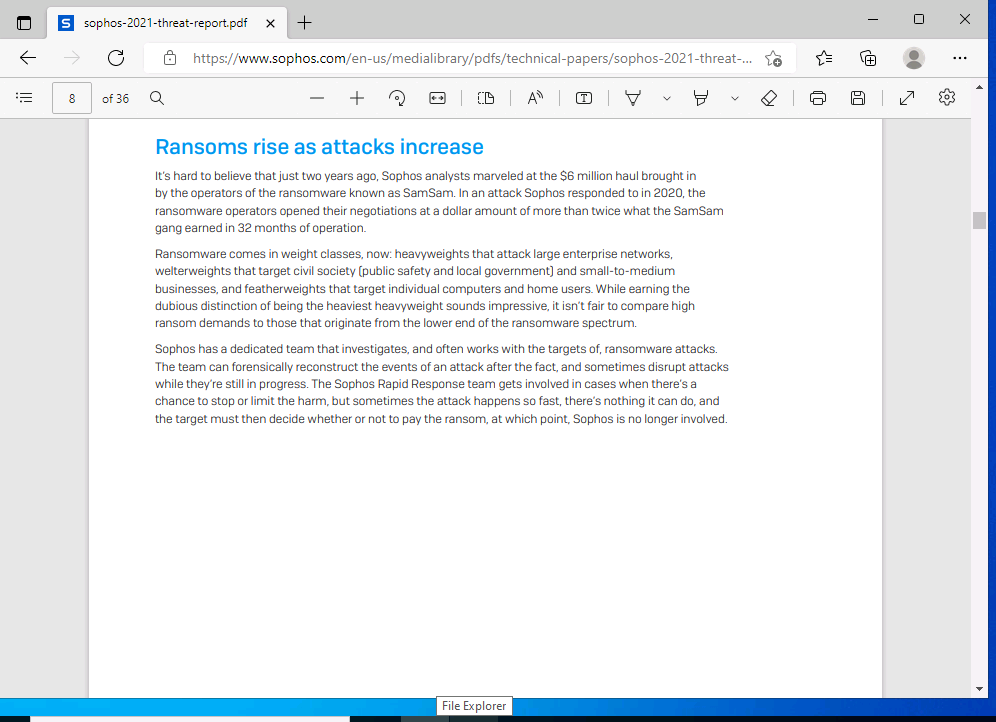
Assessing Impact of Malware

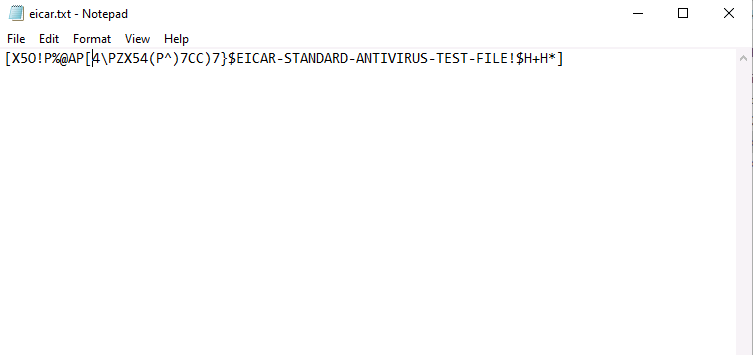
LAB-03

Objective: Stimulating Malware in a text file without harming Windows 10 VM

Scenario: You are growing concerned about the volume of malware undoubtedly striking Develetech as the company rapidly grows. Is your anti-malware sufficient to discover these attacks? You need to identify what the latest threats are and test your end-station anti-malware to ensure that it works properly.

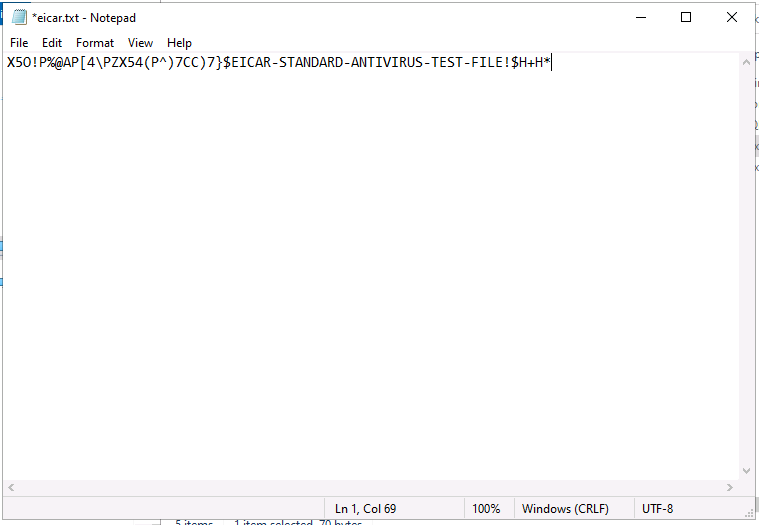
To begin with this project I had to spin up my Windows 10 VM. From there I had to open a browser and go to [**https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf**](https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf)in order to review the information on the ransom rise of attacks increase.



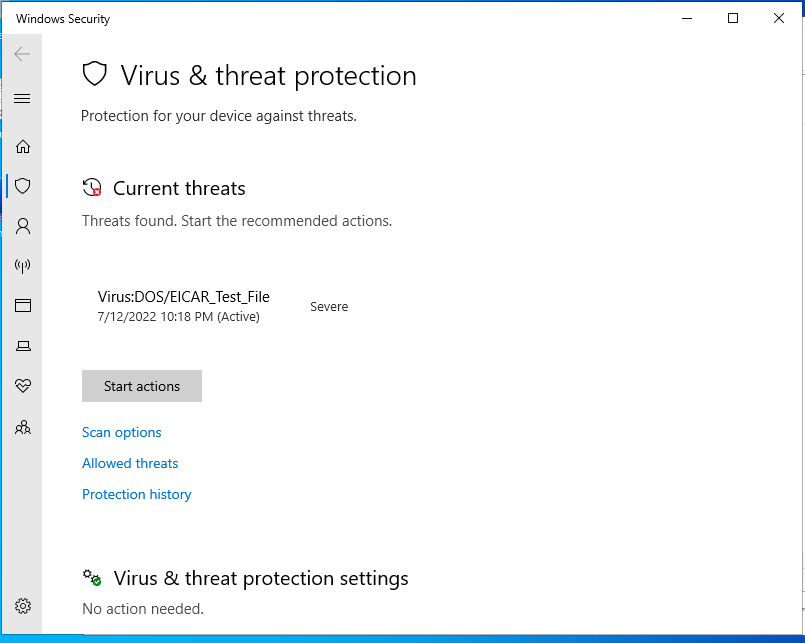


Next, we will get to the good stuff, by testing out my VMs anti-ware by activating the test text file I’m using for this lab. The random string is an example of an EICAR testing file designed to trigger anti-malware systems without being malicious resulting in a false positive.

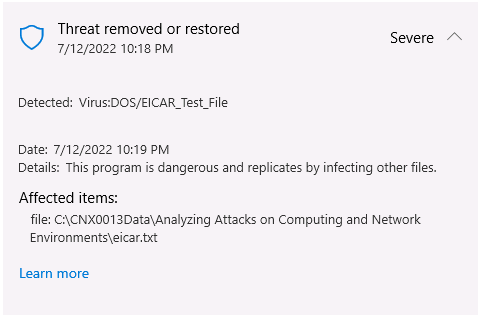
Note: For more information on EICAR please visit here: [www.eicar.org/?page\_id=3950](http://www.eicar.org/?page_id=3950).



I removed the beginning and closing brackets [] to really activate the malicious malware in order to see if my anti-malware results again in a false positive.



Immediately saving the text file, I received a windows security pop up notification. Clicking the notification to continue my investigation brings me to the virus and threat protection screen where I can see it registered the now file as a threat, true positive.



I analyzed the quarantine file and found that the virus works like a worm malware. The severity level of this malware was severe but was placed into a restricted zone after detection to avoid affecting rest of computer and network.

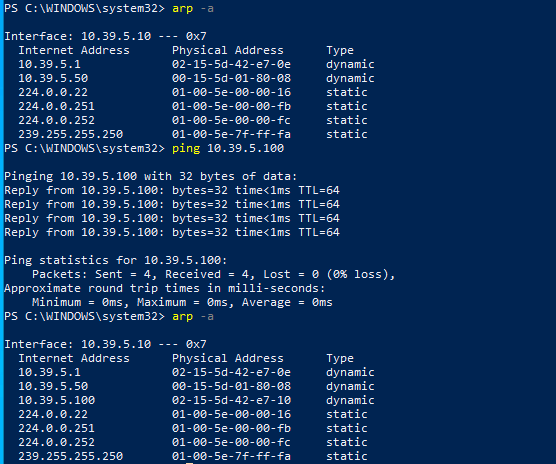
Note: To remove the file before it is sent to the quarantine you simply would select action from the drop down and select remove.

Assessing Impact of Hijacking and Impersonation Attacks

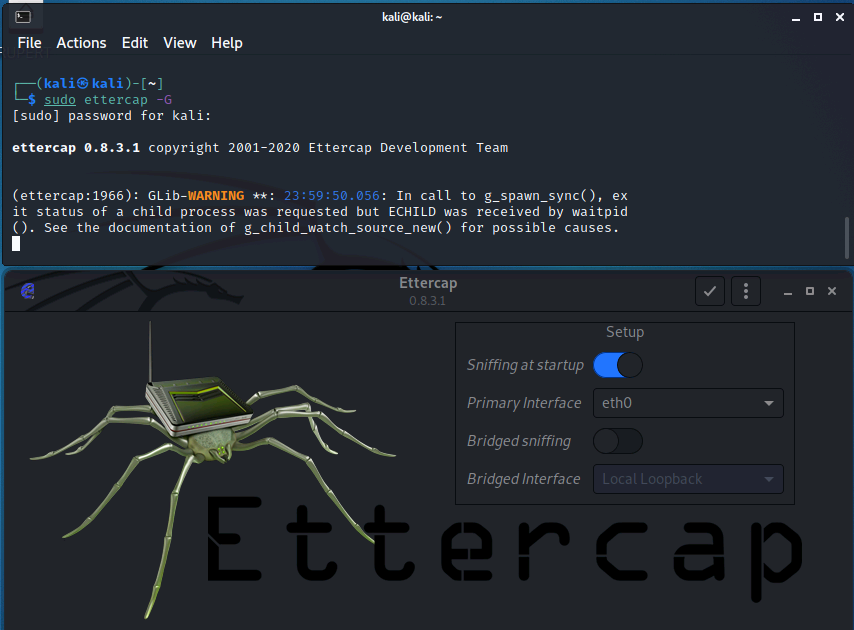
LAB-04

Objective: Using Ettercap on Kali Linux Machine to perform a ARP Poisoning attack on my Windows 10 Machine

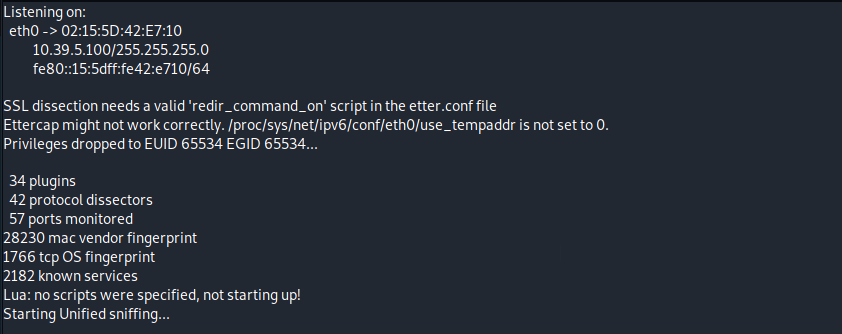
Scenario: You have been getting numerous complaints from people connected to Develetech's guest wireless network today complaining of timeouts and slow service. You connect your analysis laptop to the network and find that the performance is unusually bad. You'll investigate further by viewing your ARP cache and monitoring Wireshark for any unusual traffic.



Beginning this lab, I verified which devices was connected to my network. I don’t see my Linux machine under the devices found. To get it discovered I had to initiate a ping then rerun my ARP command.

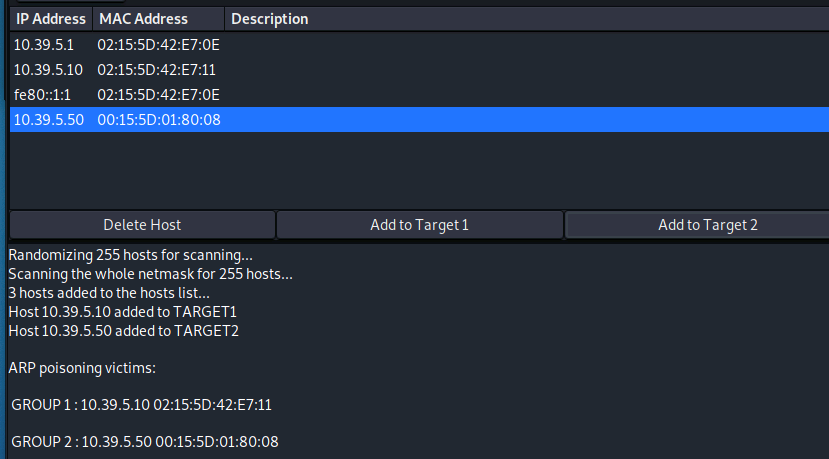


Now I know what devices the network is using. Its time to configure Ettercap to carry out my attack. To get to Ettercap, I simply went into a kali Linux CMD prompt and issued the following command: sudo Ettercap -G. That then allowed the application to generate a pop-up window. I had to configure the subnet mask of the network by clicking on the 3 dots and selecting netmask.

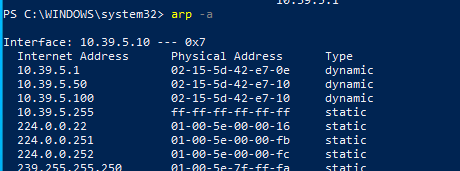




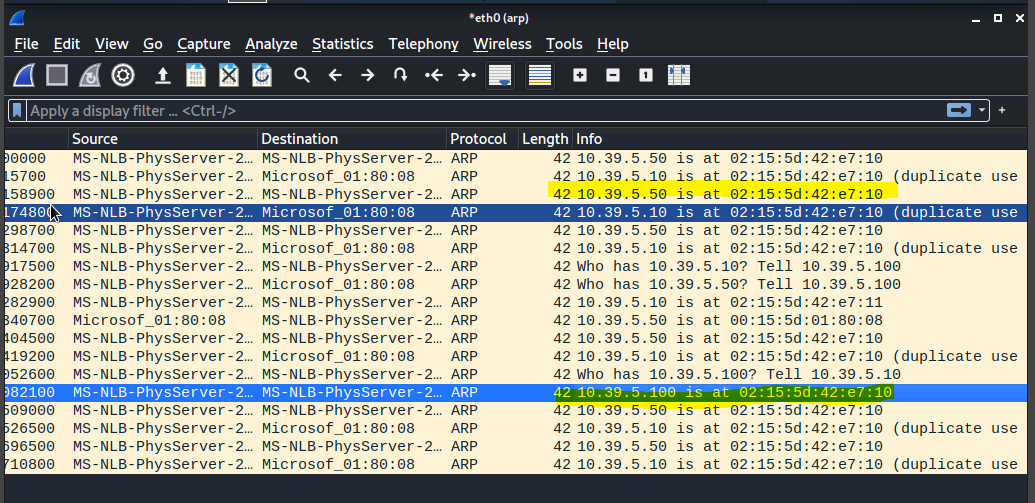
I started the scan then went to the 3 dots 🡪 host 🡪 scan for host. Once host scan was completed, I went back to the 3 dots 🡪 host 🡪 host list. I Verified that all my devices were discovered and listed in the ARP table.



Selected my Windows 10 and Windows 2019 server to add to target 1 and 2. Then I went back to the 3 dots selected ARP poisoning from the MITM menu. I insured that remote connections were selected



I went back to my Windows machine to see what has changed and after running an ARP commands I see that now my server and kali Linux machine share the same mac address. To verify that this was in fact an ARP attack I initiated a scan in Wireshark to look at my network activity.



Filtering the traffic for ARP made this easier for analyzing the packets. Scrolling down the packet list I’m seeing a lot of duplicate use under the information tab. After inspecting further, I can confirm that the ARP attack was a success.

Notes:

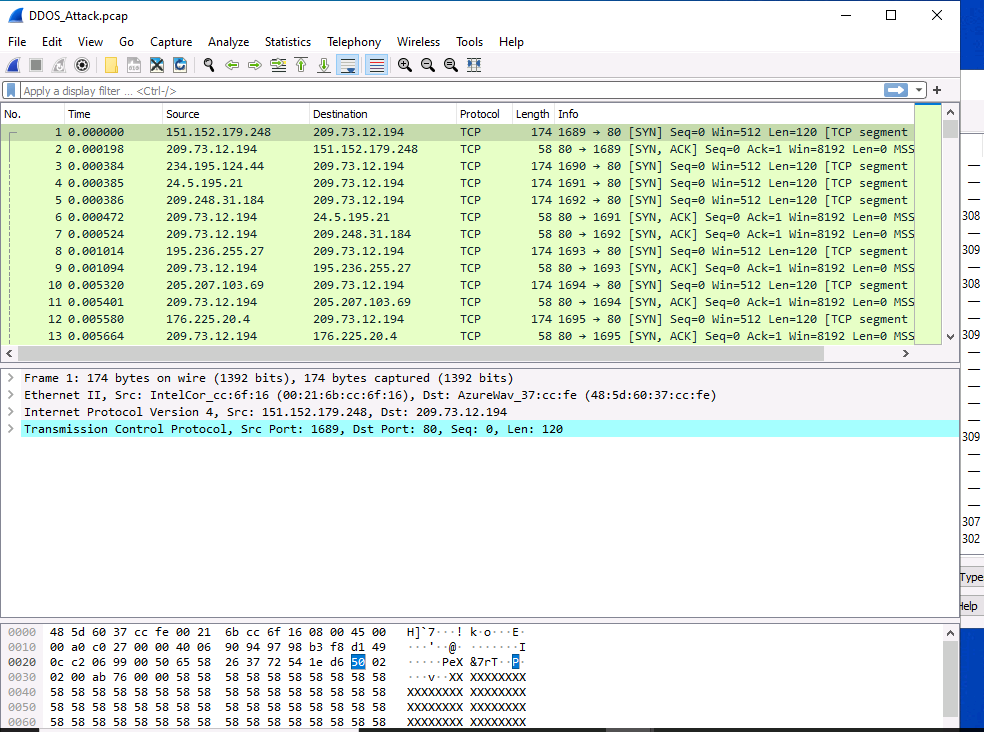
* Attackers would use an attack like this to generate a MITM attack or even a DOS attack
* To defend against an attack like this you can use subnets, IDS, Port Security, DHCP snooping and ARP inspection.

Assessing Impact of DDOS Incidents

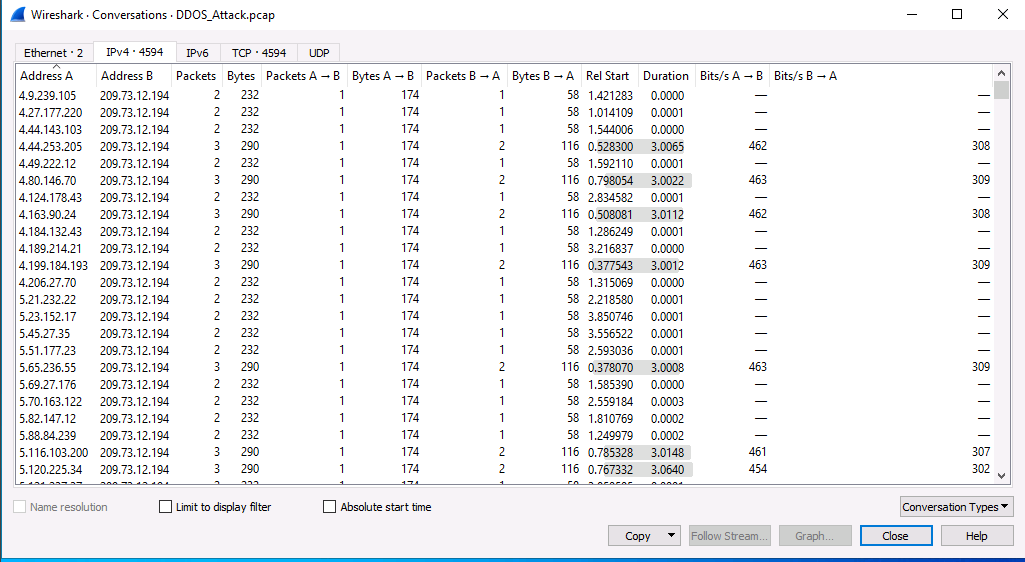
LAB-05

Objective: Examine PCAP for signs of a DDOS attack.

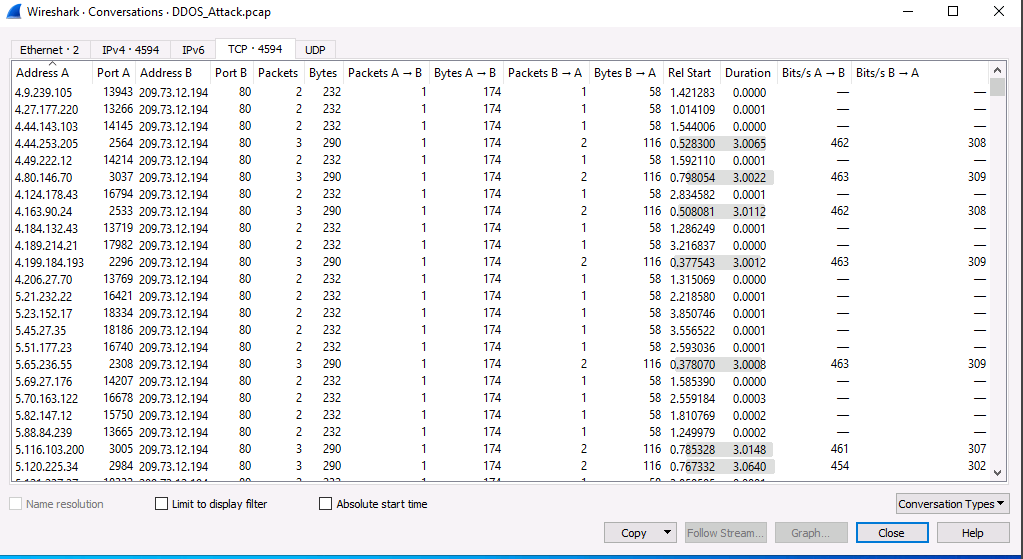
Scenario: You get a frantic call from the Develetech web administrator telling you the site has been down more than an hour, although the server itself is up and seems to be working. You see the flashing of the switch lights and realize your server is receiving massive amounts of traffic. You plug your analysis laptop into the switch and capture the traffic hitting the web server at 209.73.12.194. You want to see if there is a pattern of DDoS activity currently hitting the web, so you'll do some research to that effect. Detecting or not detecting a pattern could indicate the severity of the attack on your systems.



Loaded in Test PCAP for this lab to be analyzed



Knowing we are looking for signs of a DDOS attack. I decided to see how many packets the network devices are receiving. This was achieved by going to Statistics 🡪Conversations and focusing on the IPV4 column and Packets from A🡪B. You can see in the snippet all packets coming from the site is receiving 174 packets from each hit on the site.



Looking at the TCP table I see that port 80 is the highly requested port being hit. Therefore, with the large packets being received and the only port targeted is port 80 for http it can certainly be said a DDOS attack is or has happened.

Mitigation against DDOS Attacks:

* You can recommend the organization to buy extra bandwidth that would absorb the overload of traffic or ask about redundant internet connections (works a Primary and Secondary methodology if the primary went down the secondary would immediately turn on.
* Consult with your ISP about offering DDOS protection
* Implementing network perimeter defenses such as firewalls, IDS/IPS, Antivirus, or load balancers would be an option, but it’s just a temporary solution