Labs: Threats, Attacks, and Vulnerabilities

Kyle M. Stecki

University of Advancing Technology

2019/11/02 - 11:27

Lab 1: Vulnerabilites part 1

practicing footprinting, spoofing, and DoS attack strategies

Using Kali machine to use nmap

Did a scan on 192.168.27.0/24

Saved file to hosts.txt

Performed a syn scan using nmap on the same ip

Using leafpad to view the results of the scan in host.txt

Now using Zenmap to perform similiar tasks

performed a scan on kali box using zenmap on 192.168.27.18 and used wireshark on win 10 box to capture the data

Performed another scan in zenmap on 192.168.27.0/24

Using win 10 machine to learn about wireshark

using wireshark to view the packets from a previously saved snapshot

A screenshot of a cell phone

Description automatically generated

2019/11/03 - 21:10

Lab 2: vulnerabilites part 2

Using wireshark to scan tcp port 80

On the server instance i am going through the settings

deleted browser history

Using the kali machince to ping an ip

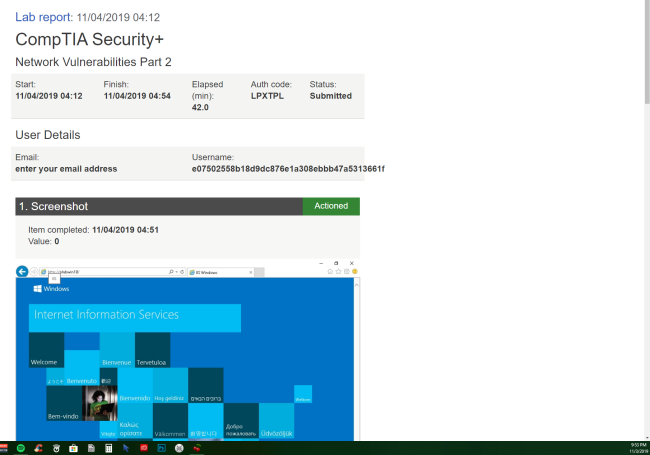
observing the pings in wireshark on the windows machine

Now moving on to the anti-phising toolbar

installing firefox on the win10 machine

downloading the netcraft toolbar for firefox

checking for phishing websites



2019/11/03 - 21:55

Lab 3: Firewall Rule Based Management

Using one of the server machines to ping the win 10 machine

went into the firewall settings for win10 machine

changed the firewall rule for file and printer sharing and turned on the firewall

tried ping again from server machine and it did not go through as expected

Swtiched back the firewall rule on the win10 machine and pinged from the server and it worked again

performing the ping actions in reverse

Performing a remote desktop connection from the win10 machine

used RDP to change the firewall rule on the server from the win10 machine

pinged the server and got no response

reversed the process to turn the friewall rule back on

Using the server machine to change more firewall rules

used the CLI to set all the firewall rules to the off state

pinged from the win10 machine to the server and got a reply

Used the CLI to turn back on all firewall rules

pinged again from win10 machine with no reply

