Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

Lab 6.5.6 Poisoning and Spoofing DNS

From TestOut CompTIA Security+ Course

In this lab I will be carrying out a DNS Spoofing attack to redirect traffic as part of a Man-In-The-Middle approach.

The scenario for this lab is as follows:

"You are the IT security administrator for a small corporate network. You want to spoof the DNS to redirect traffic as part of a man-in-the-middle attack.

In this lab, your task is to:

- (Optional) From the **Exec** computer, access **rmksupplies.com** and verify that site can be accessed.
- From the Linux **Support** computer, use Ettercap to begin sniffing and scanning for hosts.
- Configure the **Exec** computer (192.168.0.30) as the target 1 machine.
- Initiate DNS spoofing.
- From the **Exec** computer, access **rmksupplies.com** and verify that it has been redirected to a different site."

To start I will begin with verifying that I can reach this website from the **Exec** Computer.

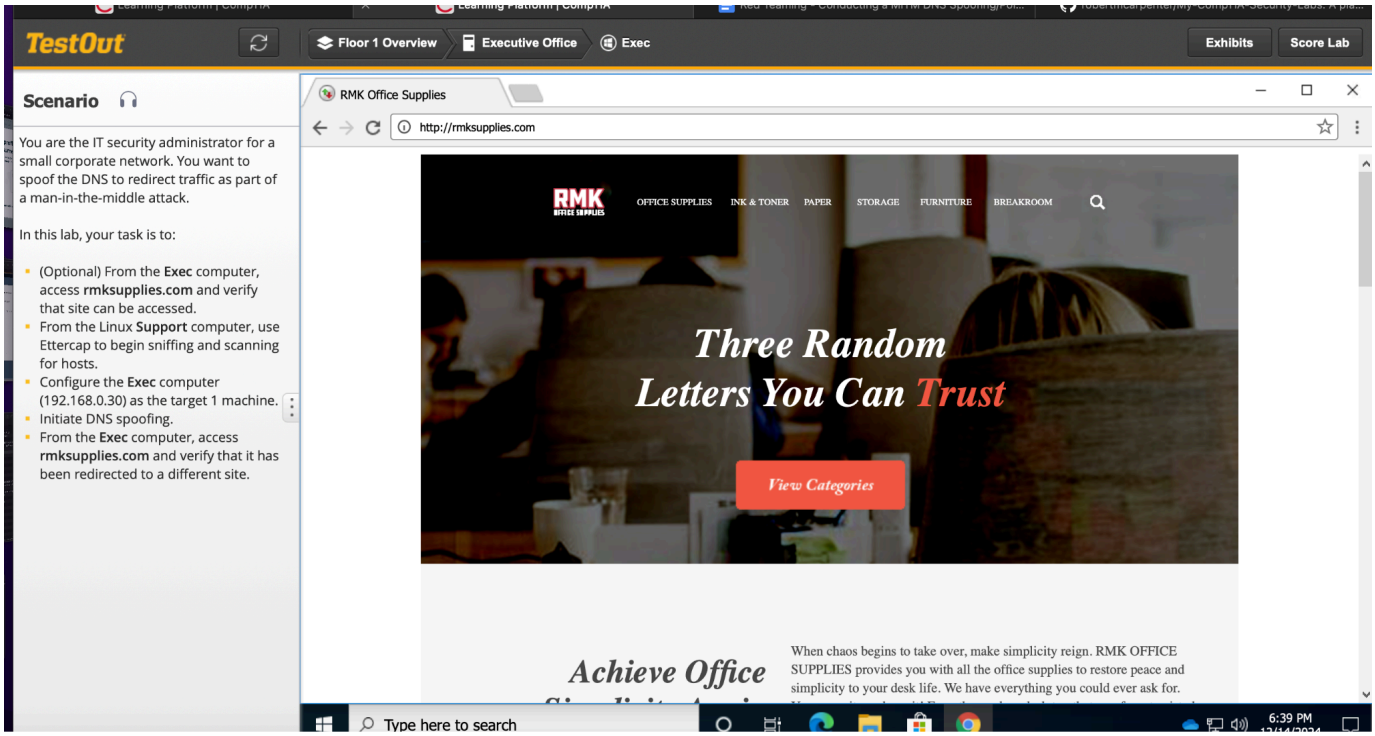
Note: This Lab takes place in a hypothetical office with the ability of the user/learner (myself) to change workstations and navigate through a virtual space.

See picture below:

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

I will first click on the Windows machine in the Exec office. Opening a web browser and navigating to **rmksupplies.com** to verify it is online.

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

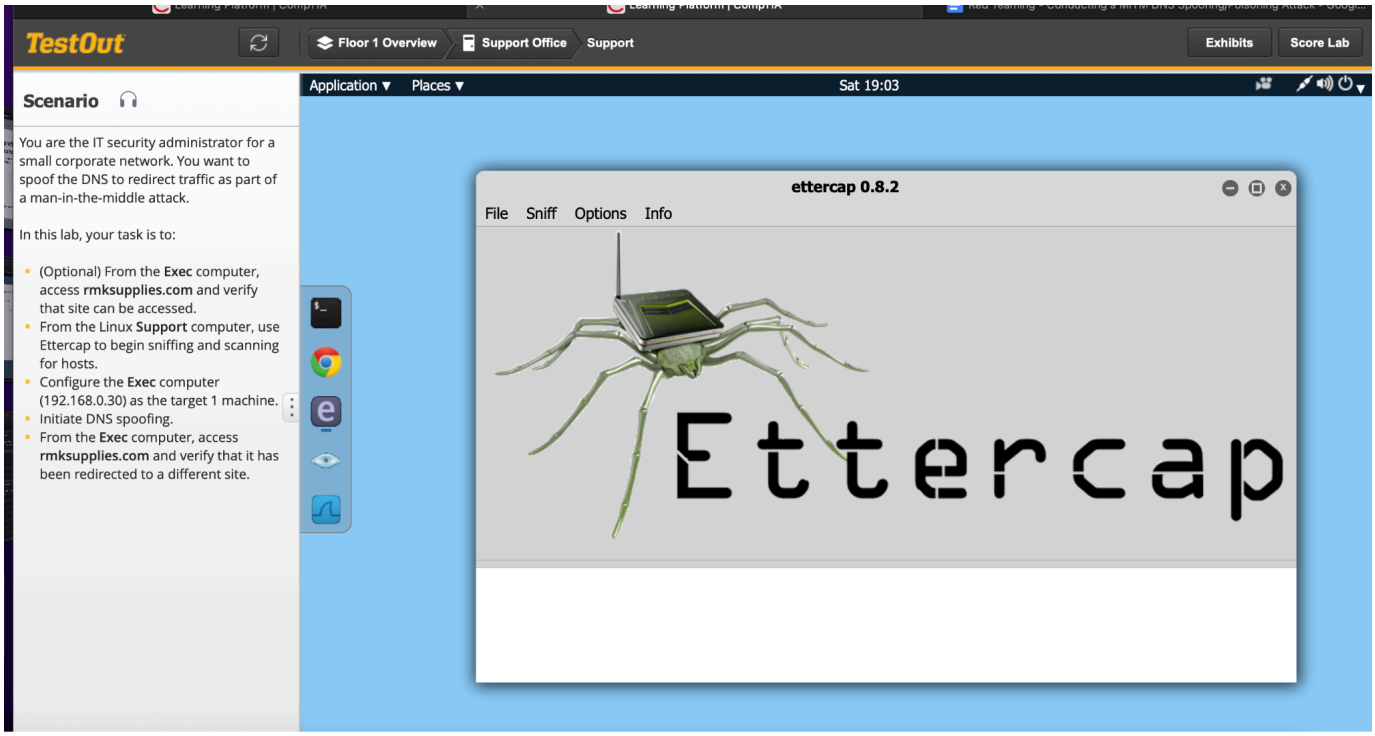


That means that we are able to access the company's website. I will now put my **Ethical Hacker** hat on and attempt to carry out a DNS Spoofing attack.

I'll switch back to my Linux Machine called **support** within the office.

To start my attack I will use Ettercap on my attacking Kali Linux machine.

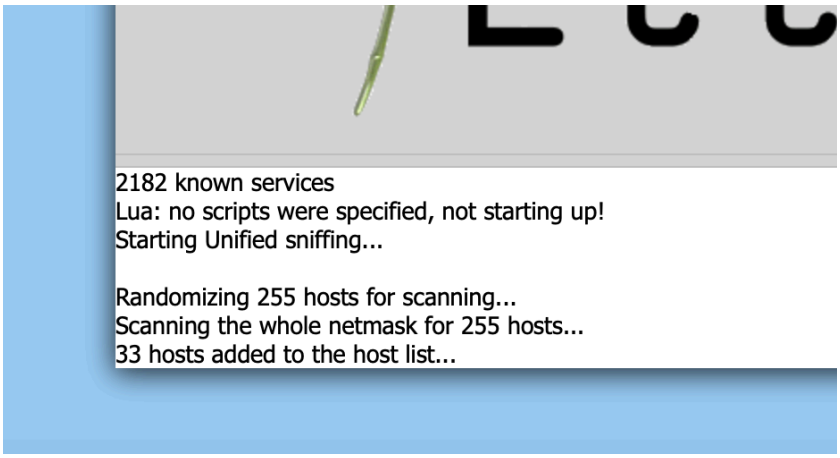
Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



From here at the top menu bar I'll select **Sniff > Unified Sniffing.** After selecting that I see the logging start at the bottom.

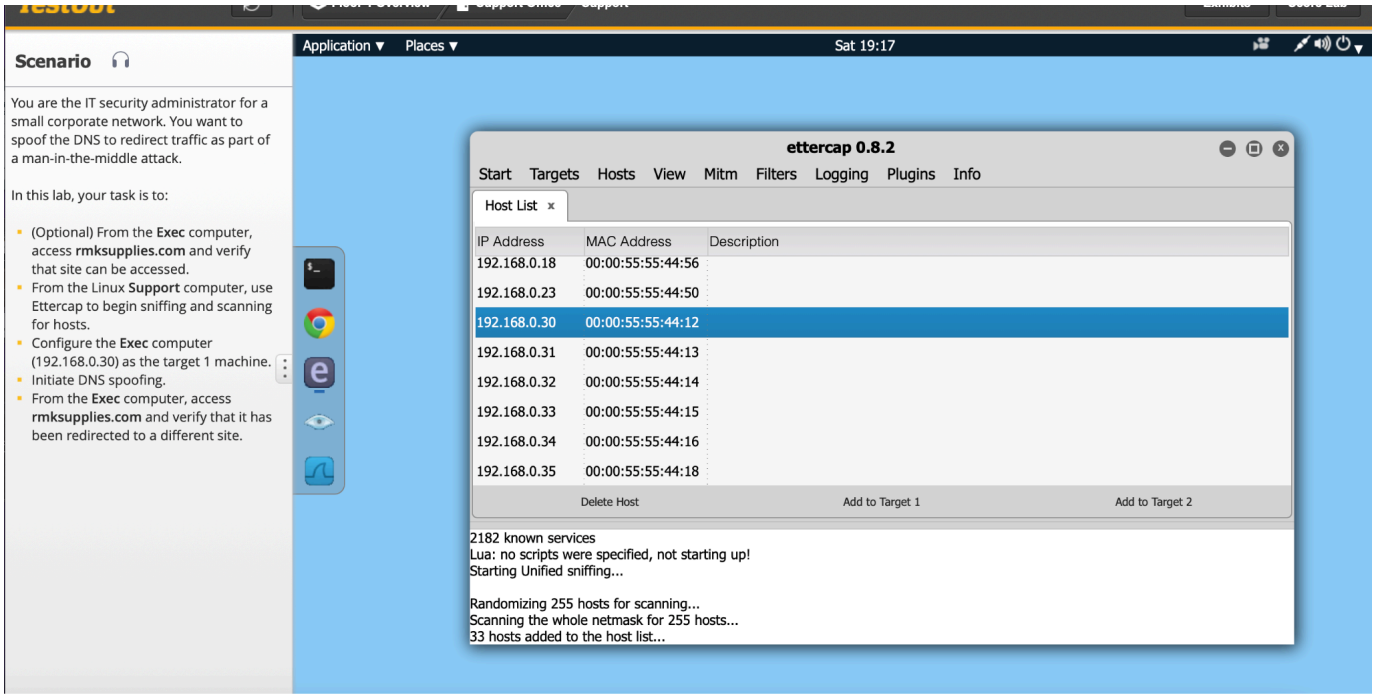
Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

Now we need to scan the network for hosts to attack. I'll click **Hosts > Scan for Hosts** at the top menu.



According to the Lab we want to attack the **Executive's** Computer which resides on **192.168.030.** To select the IP, I'll open the **Hosts > Hosts list** and select it from there.

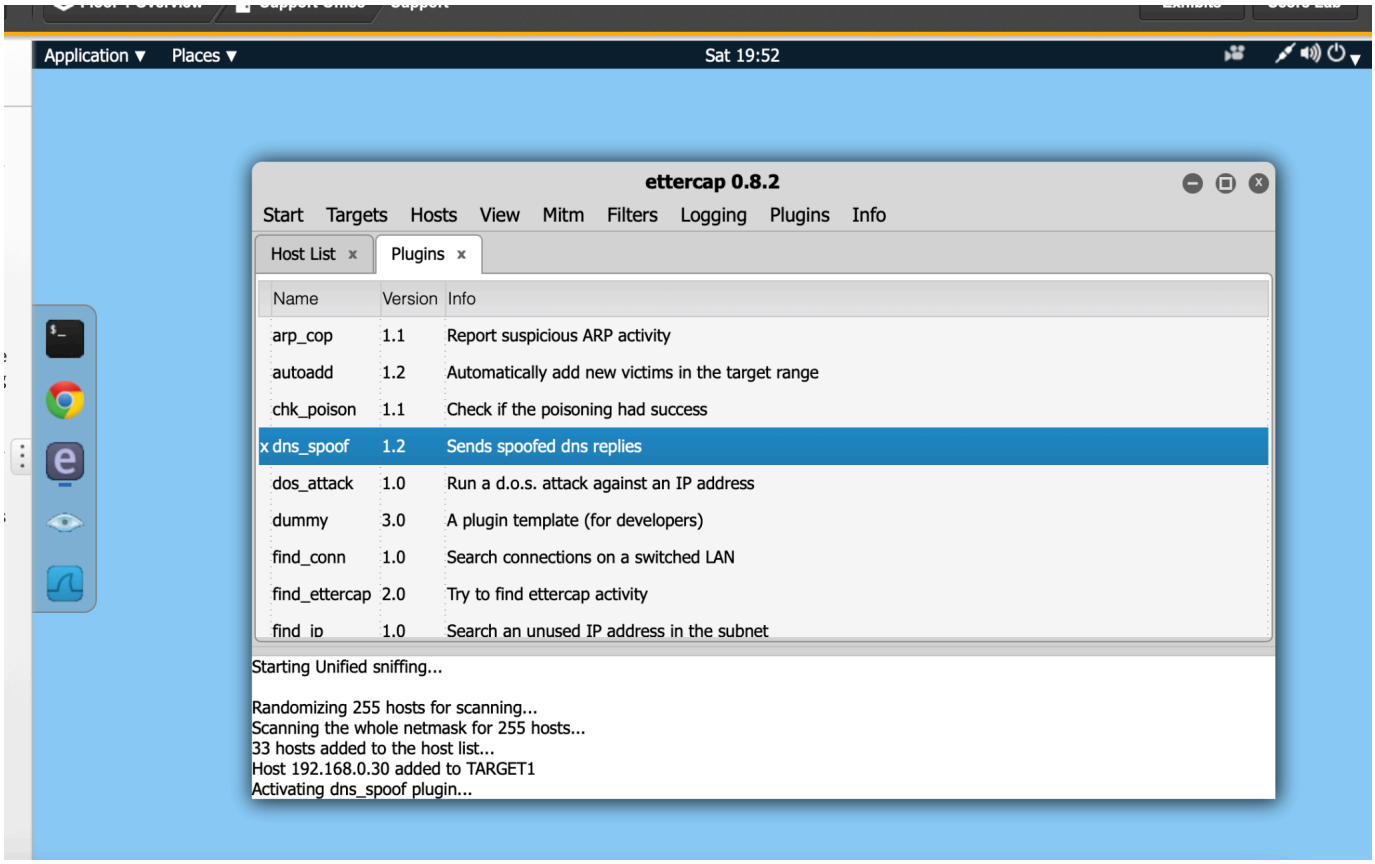
Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



Once highlighted I'll click **Add to Target 1** and I see in the logging that **192.168.0.30** was indeed added.

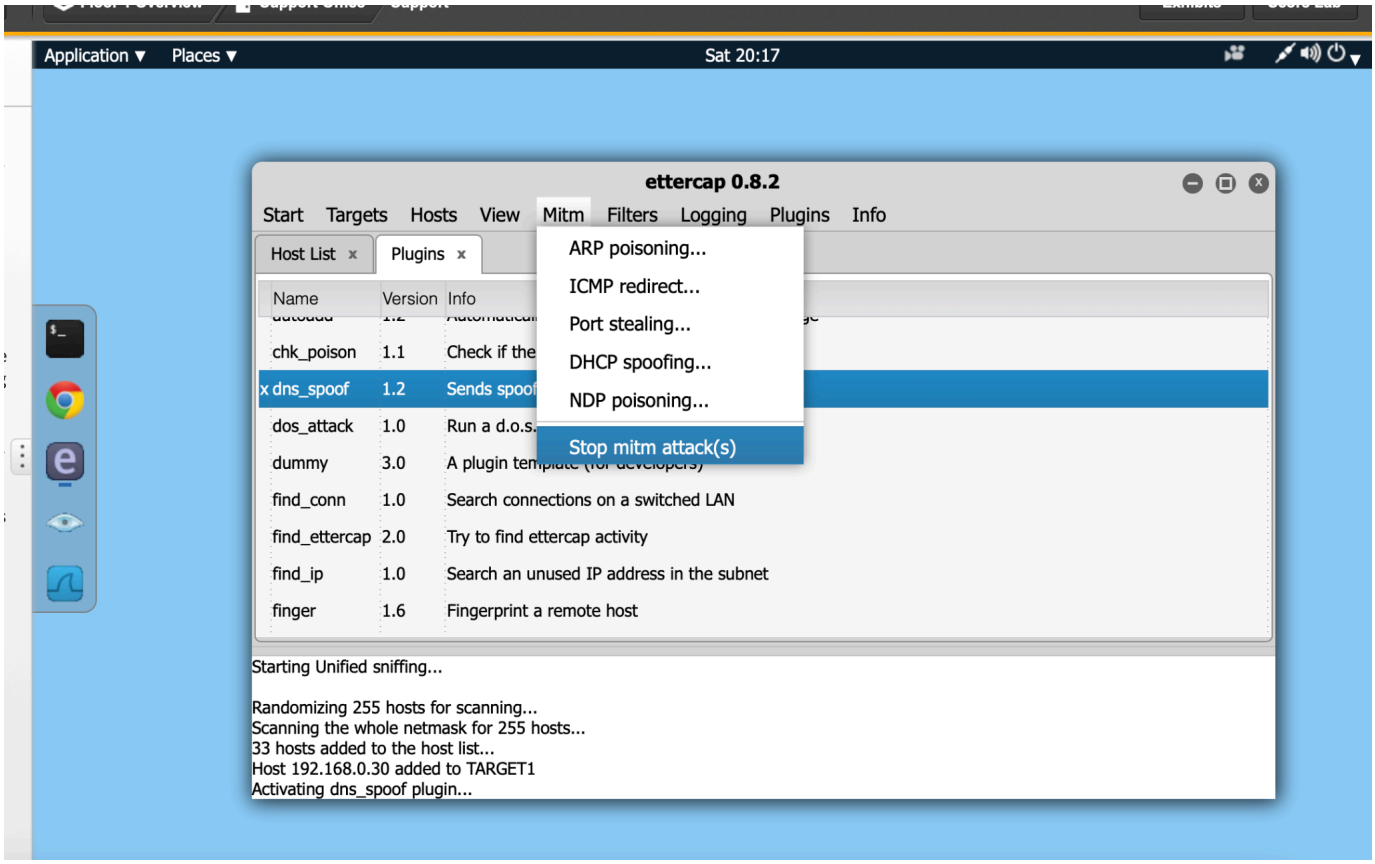
To start the DNS Spoofing attack I'll need to install the plug in within Ettercap. Clicking **Plugins,** I will select **dns_spoof** plugin.

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



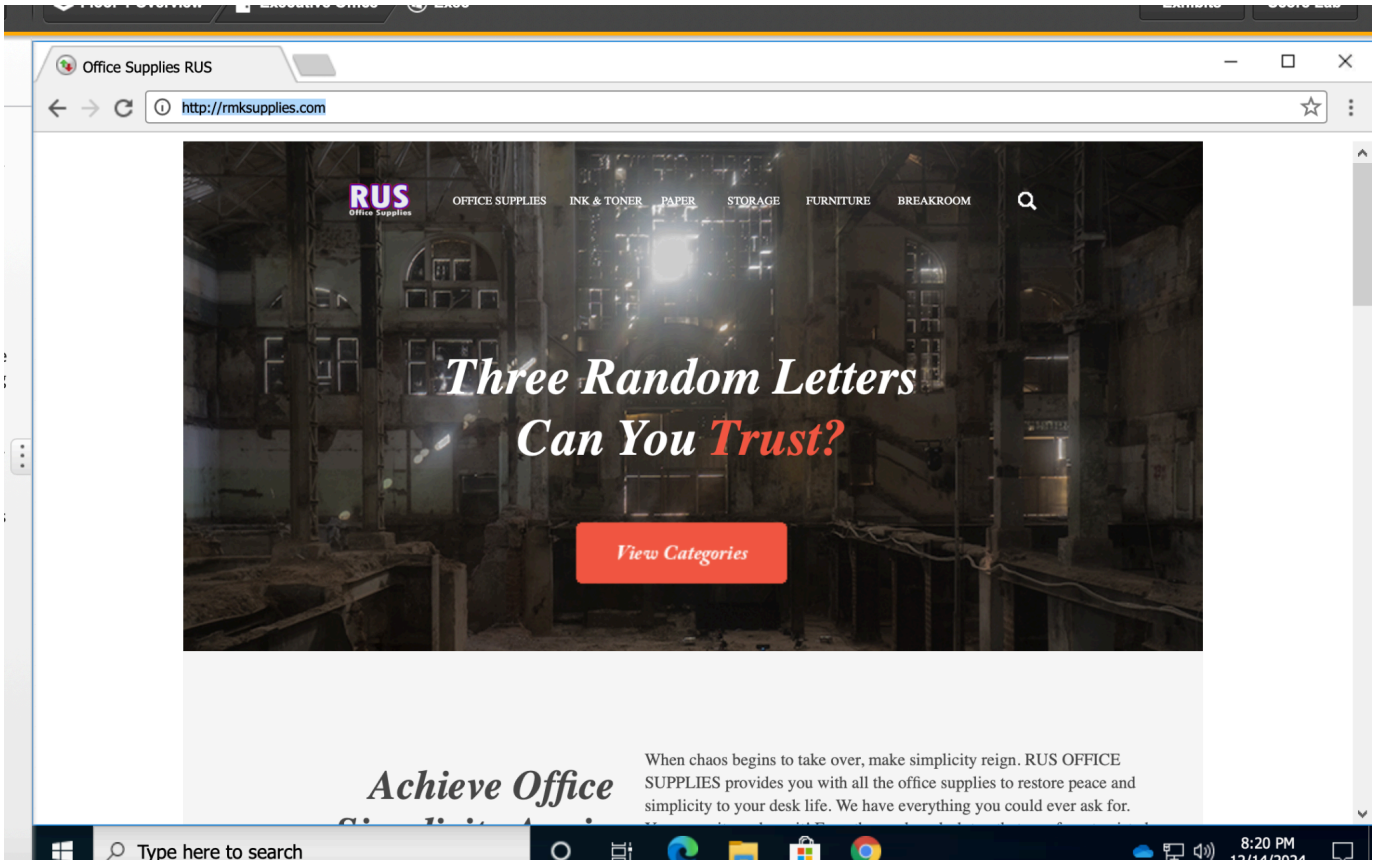
Now that the plugin is loaded I will select MiTm tab in ettercap and select **MiTM > ARP Poisoning**. We will use ARP Poisoning to carry out the attack.

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



I see that the attack is running because in the menu above it prompts me if I want to Stop MiTM attack, which means it must be running. Now let's check on the victim machine to see what is happening.

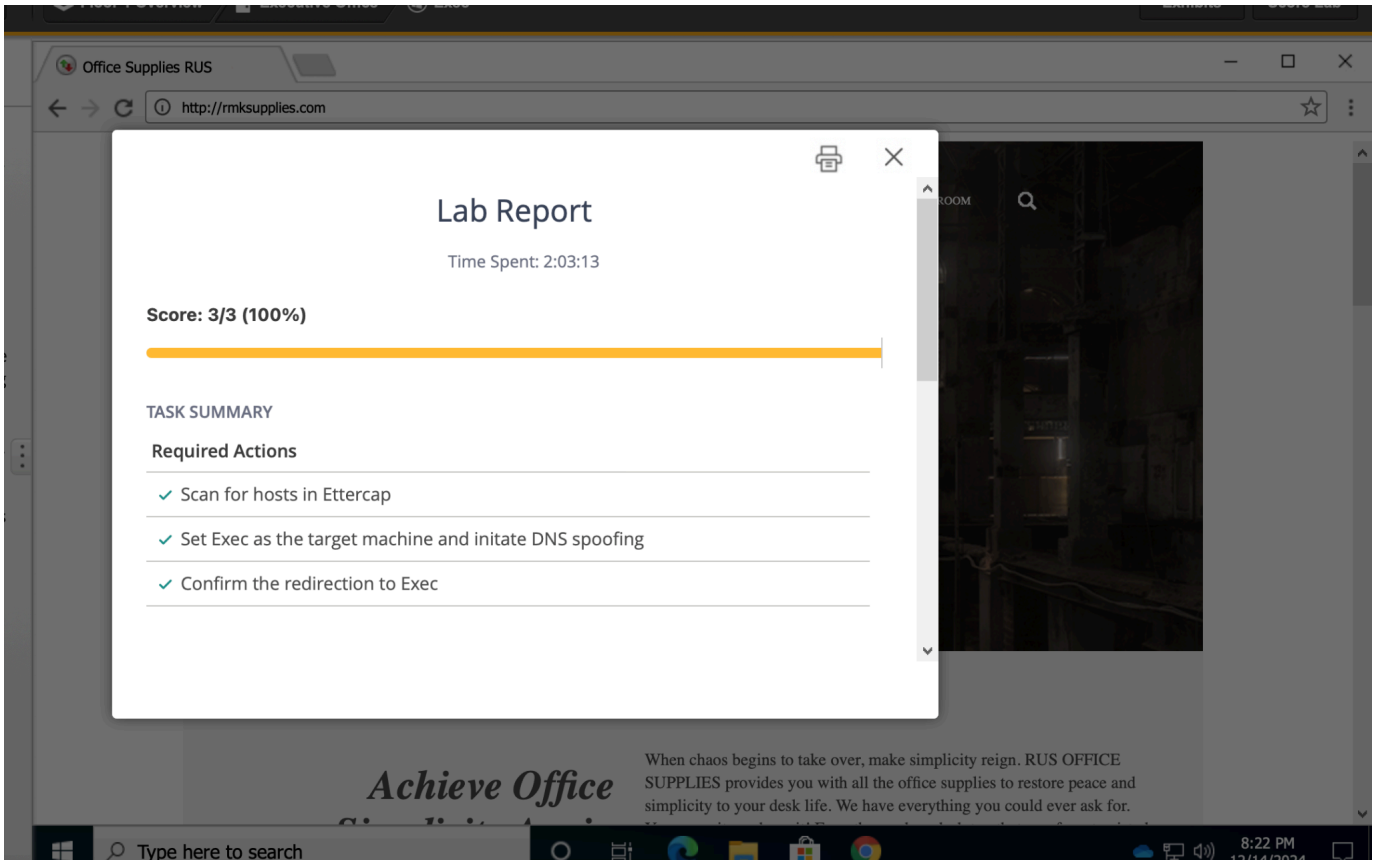
Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



Notice how the site has been redirected to **RUS** office supplies which is not RMK. This means our attack has been successful!

This now concludes this lab.

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024