## Week 16 Homework Submission File: Penetration Testing 1

#### Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is:

Yes, it’s right on their website:

**Karl Fitzgerald**

Chairman & Chief Executive Officer

Altoro Mutual

- How can this information be helpful to an attacker:

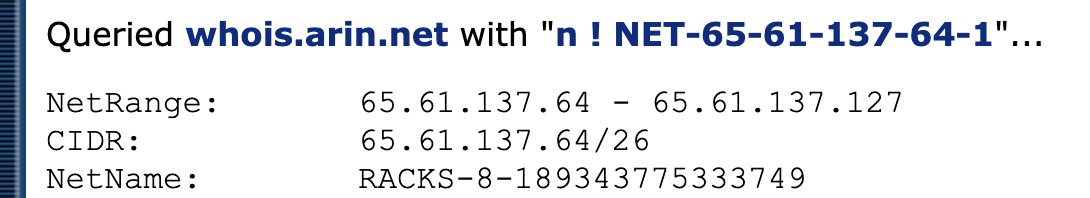
They may want to conduct whaling attacks or spearfish to get access to what the CEO has access to. IT is safe to assume the CEO has pretty powerful access to a lot of files and folders and may even have access to customer PII.

#### Step 2: DNS and Domain Discovery

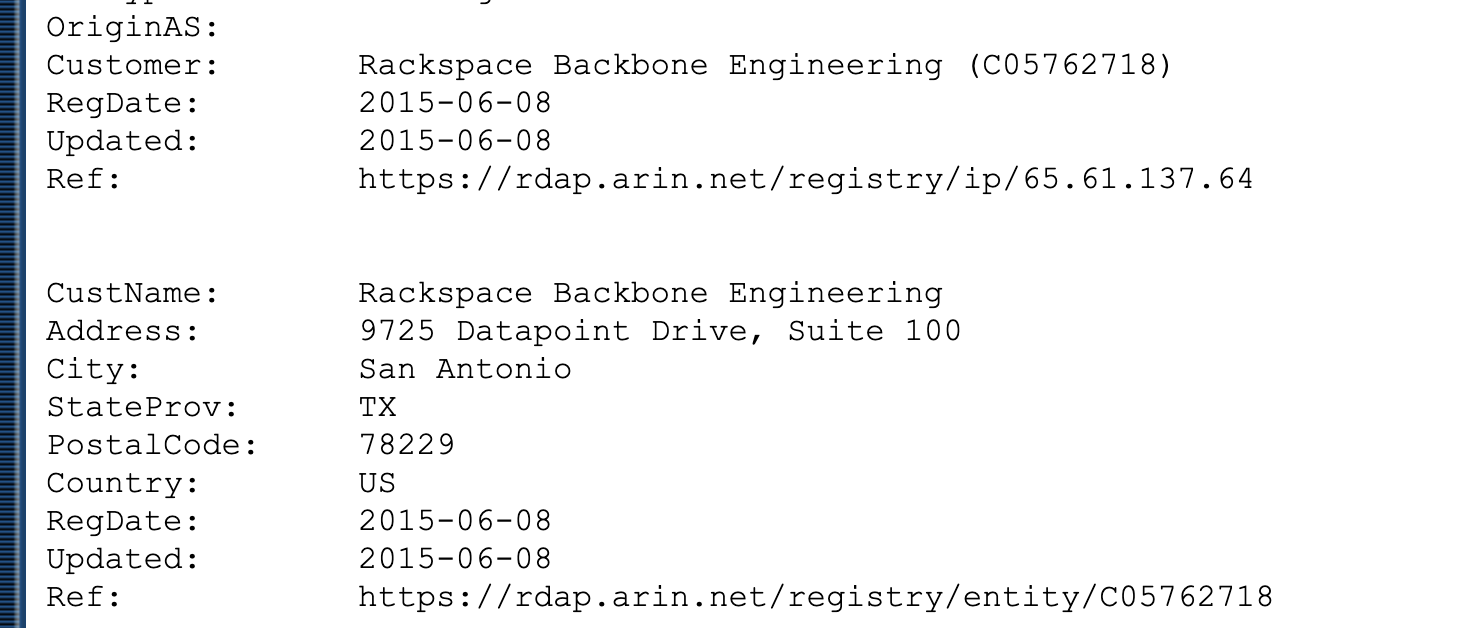
Enter the IP address for `demo.testfire.net` into Domain Dossier and answer the following questions based on the results:

1. Where is the company located: Sunnyvale, CA

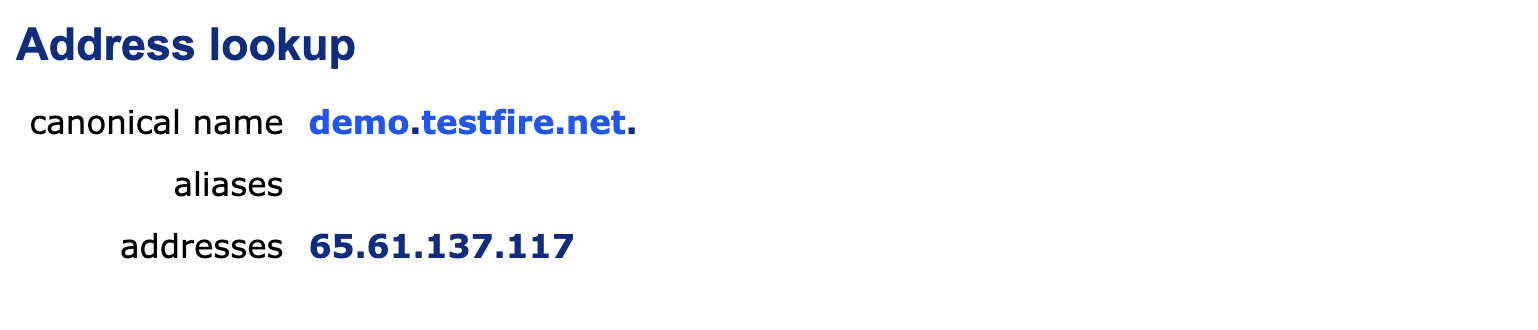
2. What is the NetRange IP address:



3. What is the company they use to store their infrastructure:

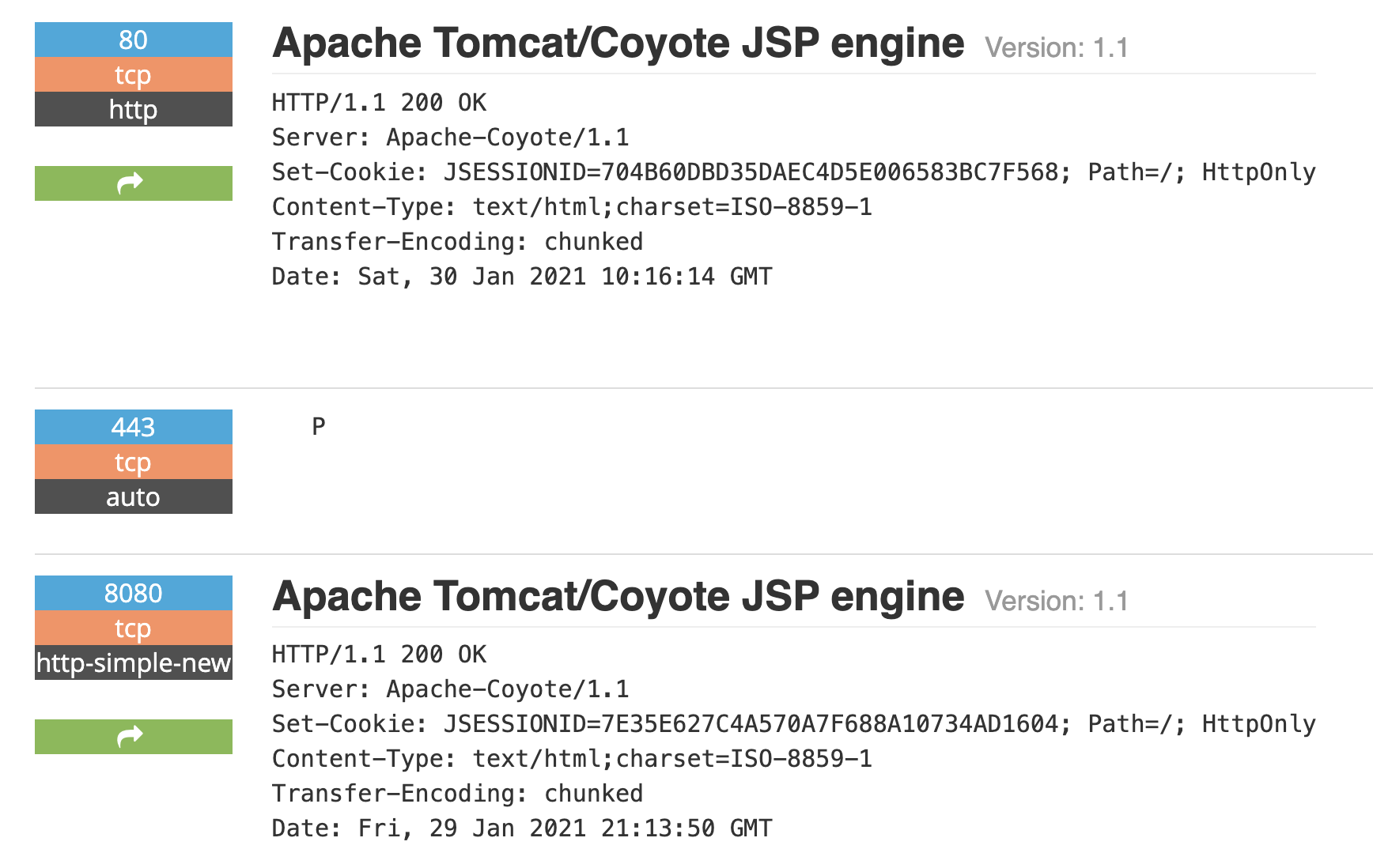


4. What is the IP address of the DNS server:



#### Step 3: Shodan

- What open ports and running services did Shodan find:



The open ports are listed in blue which are 80, 443, and 8080.

#### Step 4: Recon-ng

- Install the Recon module `xssed`.

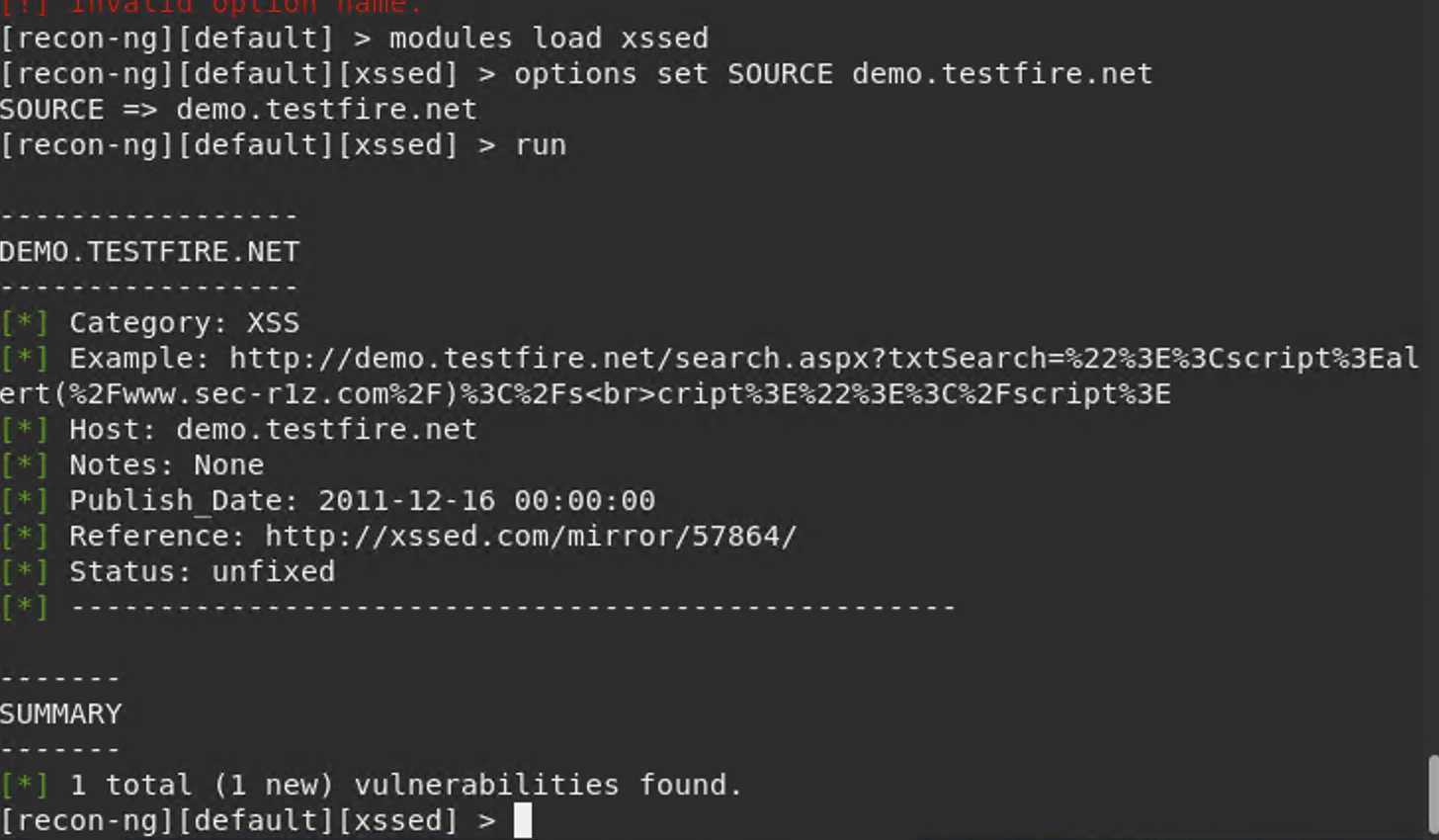
- Set the source to `demo.testfire.net`.

- Run the module.

For this, I logged into the Kali machine and ran <recon-ng>

Once there, I went to install xssed by running <marketplace install xssed>

I then set the source as directed: <options set SOURCE demo.testfire.net>



Is Altoro Mutual vulnerable to XSS:

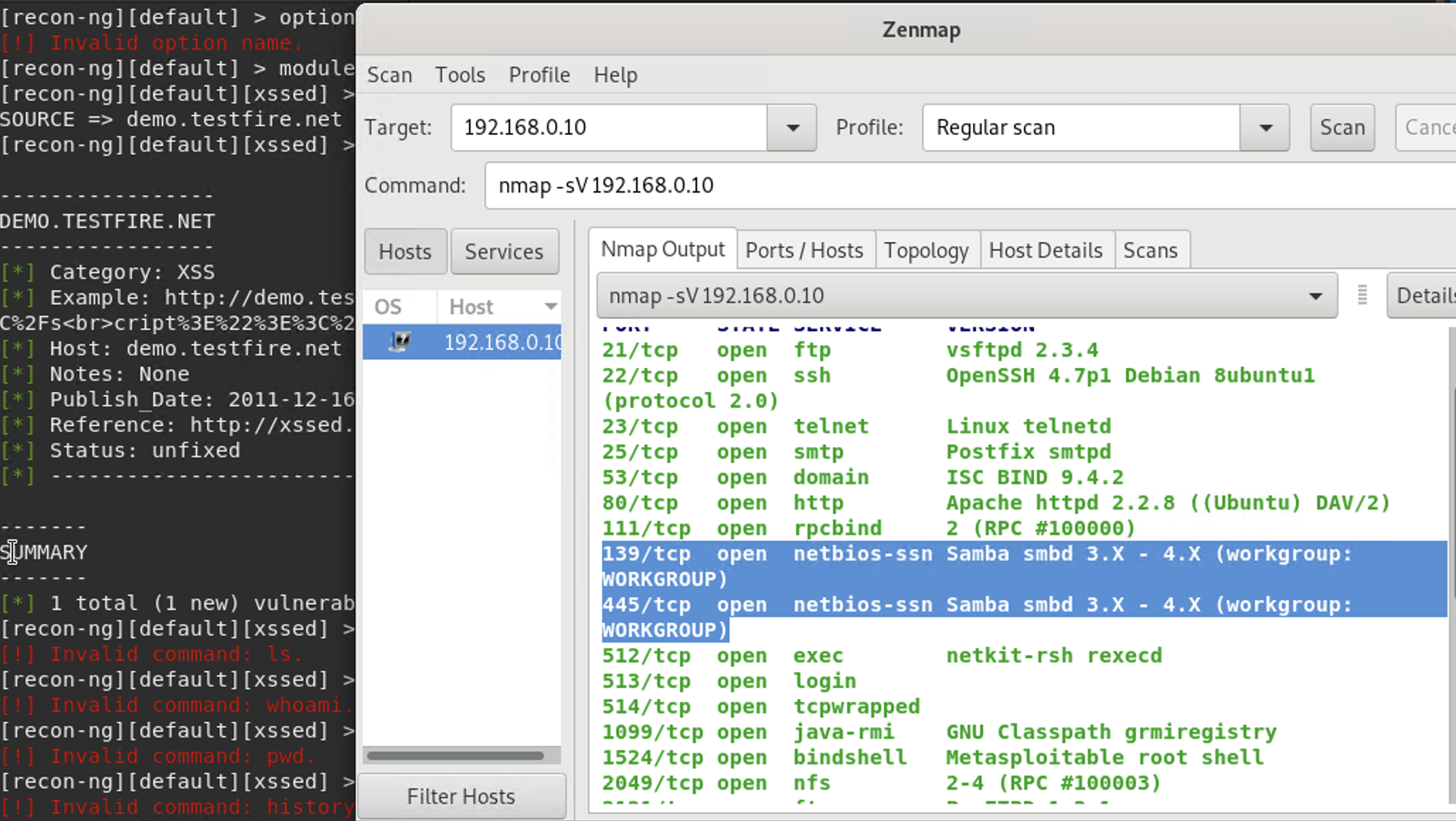
Simply put; yes they are.

### # Step 5: Zenmap

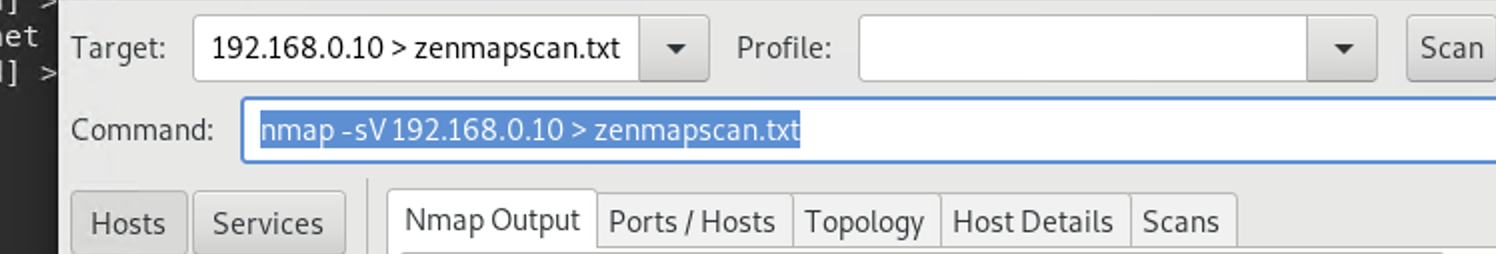
Your client has asked that you help identify any vulnerabilities with their file-sharing server. Using the Metasploitable machine to act as your client's server, complete the following:

Use Zenmap to run a service scan against the Metasploitable machine.

From within the command line, I ran <zenmap>. That opened up a GUI interface window that allowed me to set some parameters. There was no specific service san to run in the drop down. That was created by adding the <-sV> to the command. That allowed the following:



Once within, I highlighted the two vulnerabilities assigned to look into which involve ports 139 and 445. Additionally, I later added the following to write out the results to the <zenmapscan.txt> as requested.



Use Zenmap's scripting engine to identify a vulnerability associated with the service running on the 139/445 port from your previous scan. Once you have identified this vulnerability, answer the following questions for your client:

What is the vulnerability?

The most critical vulnerability is that the remote host may now be compromised because of a vulnerability that allows for a backdoor shell installation. This means that a hacker could very well gain access to the command line using a shell (whatever version necessary depending on the OS used) and steal or manipulate data.

According to the report, the remote SSH host key was generated on a Debian or Ubuntu system that contains a bug in the random number generator of its OpenSSL Library. Due to this, an attacker can easily obtain the private part of the remote key and use this to set up a decipher or man in the middle (MiTM) attack.

Why is it dangerous?

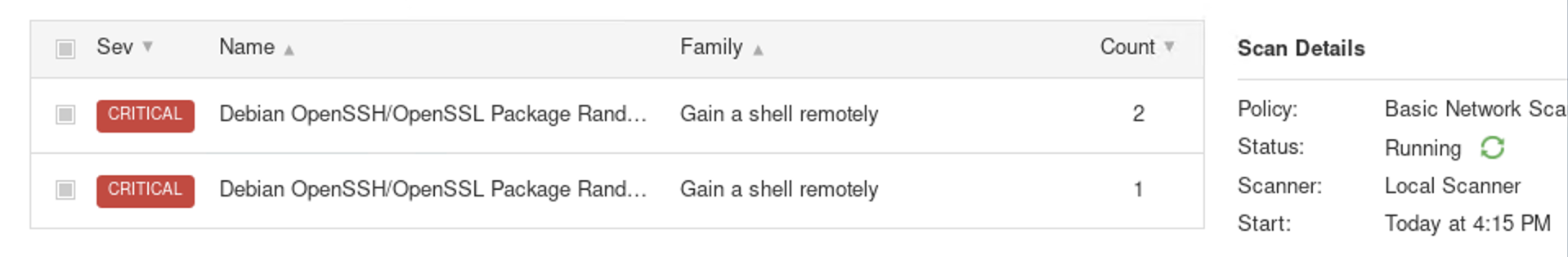
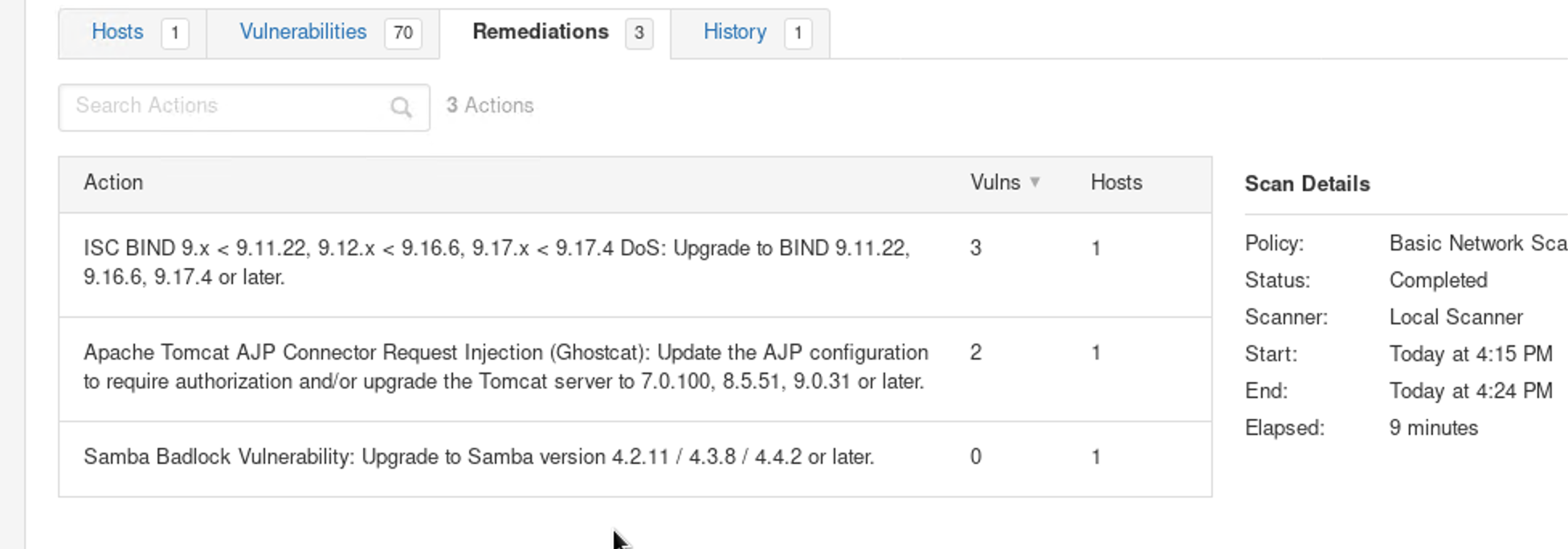
See above.

What are your recommendations for the client to protect their server?

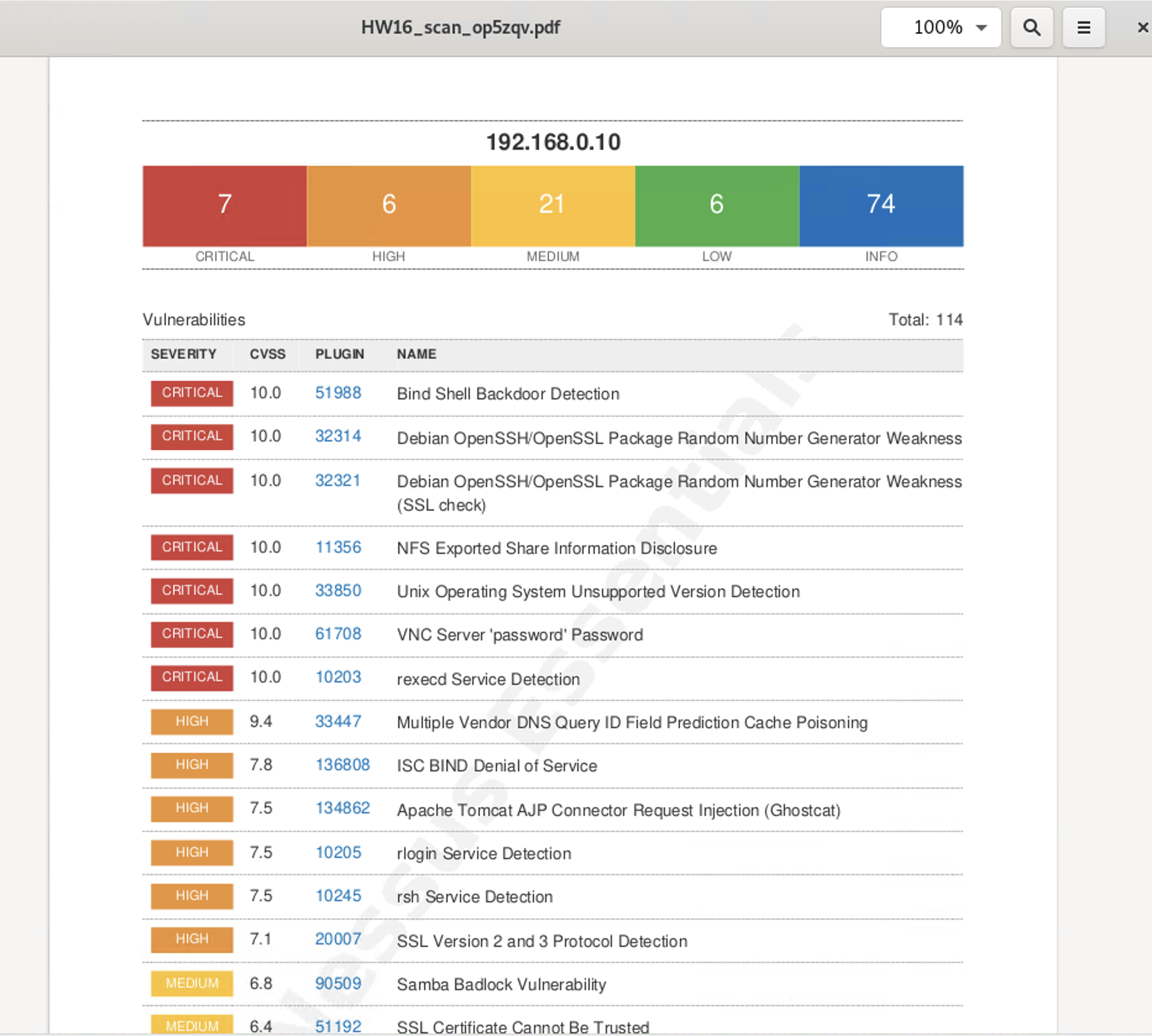
First, there are two critical updates that need to take place. The Apache Tomcat server needs to be upgraded to the latest version which would be 7.0 100 8.5 51. 9.031 or later. Also, the version of Samba installed is also out of date and should be updated to 4.4.2 or later. Since programs throughout the client’s infrastructure communicate through different operating systems, this is critical. Samba allows machines of different operating systems to communicate and share files effectively. Once completed, all SSH keys should be regenerated and configured to work without access to the old keys.

An upgrade like this will require you to take machines offline and not allow communication between these servers for the duration.

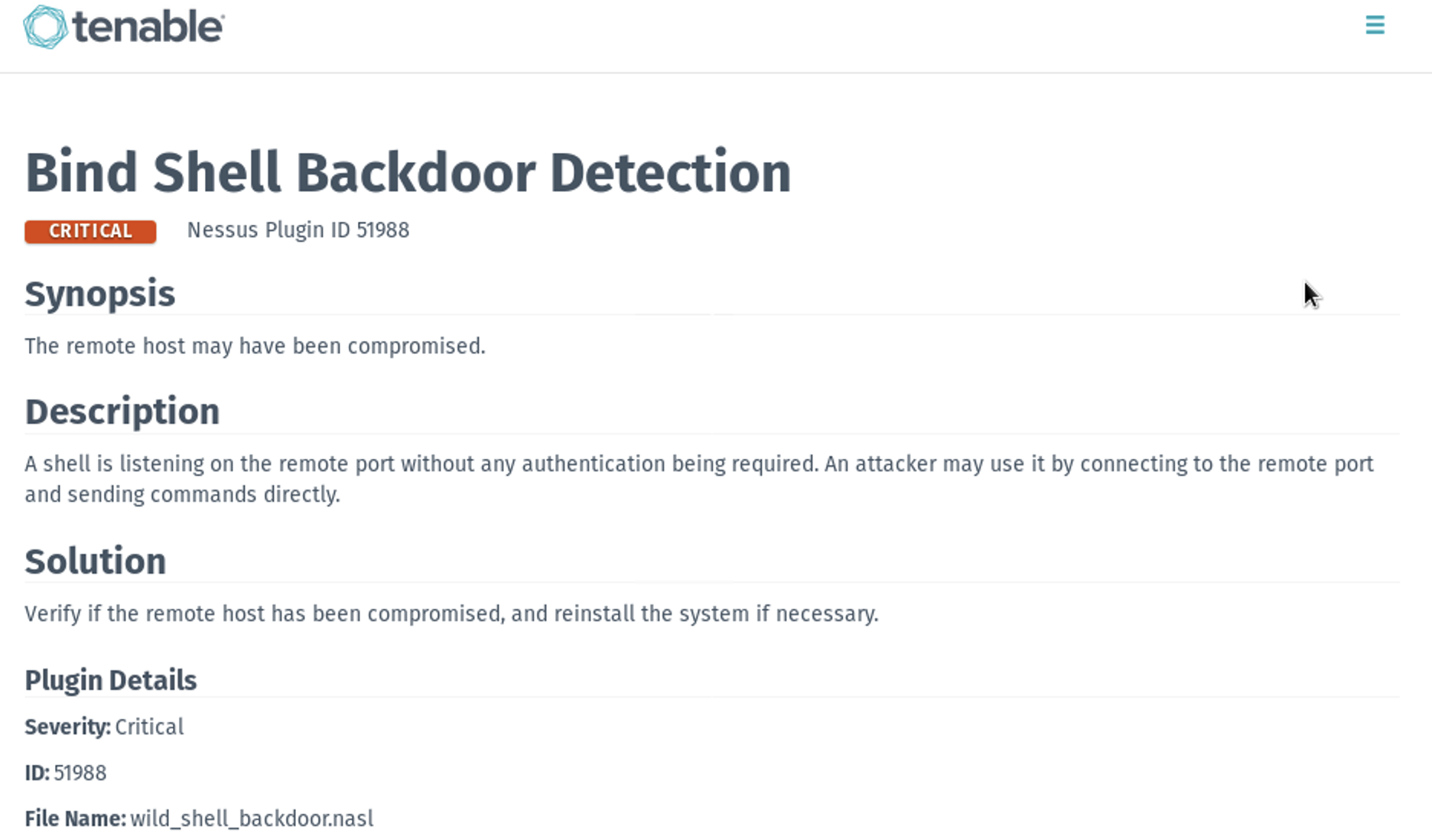
For some additional responses to this request, I ran a metasploitable scan by using Nessus to generate an executive summary of vulnerabilities. Within the report, there were (5) critical vulnerabilities to include issues with access to ports 139 and 445. I have included some screenshots of the executive summary below to back up the arguments:



The first screenshot shows the remediations suggested to correct vulnerabilities. Within it, you can see the tabs at the top with 70 vulnerabilities listed and 3 remediations.



Once a report was generated (labeled HW16), you can see issues listed in a weighted order. There are 7 critical issues that need addressing as well as 6 that are of high priority.



This is the backdoor detection alert on the remote client.

