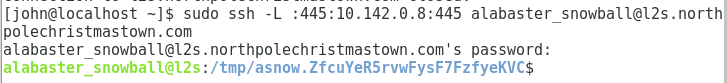
# Santa’s SMB Server--Exploiting Letters to Santa Part 3, Connecting to the Share

## List the Shares

Using the instructions from Part 2, we attempt to list the shares on an SMB server we found, 10.142.0.8. First, establish an SSH tunnel through l2s to 10.142.0.8. We won’t need to enter commands into SSH once the session is opened, though.  
sudo ssh -L :445:10.142.0.8:445 alabaster\_snowball@l2s.northpolechristmastown.com



Then we use smbclient in a new terminal window on our Linux VM to connect to 127.0.0.1. It uses port 445, and the SSH tunnel will pass the traffic on to 10.142.0.8.  
smbclient -L 127.0.0.1 -U alabaster\_snowball



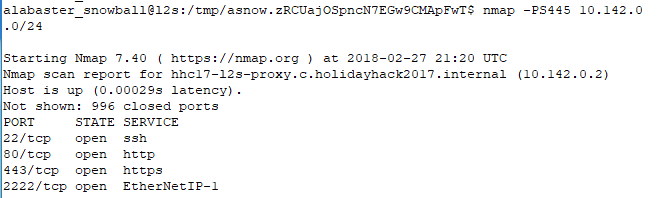
Rats! It won’t let us in. What’s wrong?

**<It’s a trap!>**

If you just ran nmap -A 10.142.0.0/24 you missed the real SMB server. The server we need is on 10.142.0.7. Holly Evergreen’s Hint 1 tells us the default host discovery may not find all hosts and recommends using the -PS### option, as in -PS123 to check for NTP running on TCP port 123. Also note that all the hosts we discovered are listening on the default host discovery ports of 80 and 443. Since we are interested in finding SMB servers, we should add -PS445 to our Nmap scan. If you didn’t find a server on 10.142.0.7, go back and do that now.

**</It’s a trap!>**

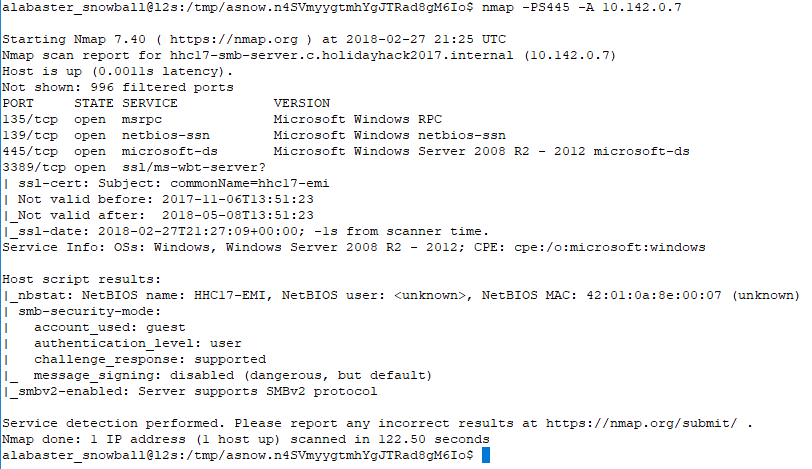
Here’s a scan with the -PS445 option to run a TCP SYN probe (PS) against port 445.  
nmap -PS445 10.142.0.0/24



<SNIP> The only new host in the scan is 10.142.0.7 so the rest are omitted.

## 

Now, we can run a full scan only on the new host we’ve found at 10.142.0.7 with  
nmap -PS445 -A 10.142.0.7.  
We could use -Pn to tell Nmap to skip host discovery and go straight to the port scan, instead of using -PS445, since we are only scanning one address and we know it is there.



Note that 10.142.0.7 is not listening on the default ports that Nmap probes during host discovery (80, 443). It is probably blocking the ICMP probes in its firewall. There is something strange, in that l2s and the SMB server should be on the same network and Nmap should do an ARP request. See the questions and the end of this lesson.

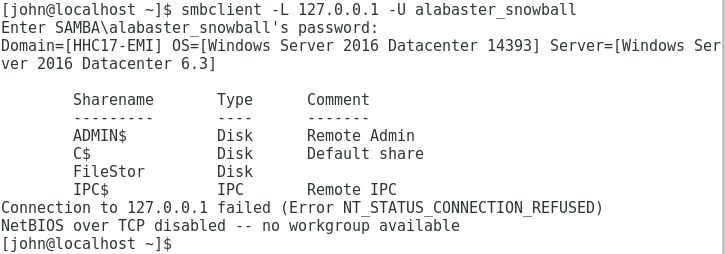
Here is an updated spreadsheet with 10.142.0.7 included.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IP address | DNS name | ports | Certificate Names | Web Server | OS | robots.txt | NetBIOS name |
| 10.142.0.2 | hhc17-l2s-proxy | 22, 80, 443, 2222 | dev, l2s | nginx | Linux |  |  |
| 10.142.0.3 | hhc17-apache-struts1 | 22, 80 |  | nginx | Linux |  |  |
| 10.142.0.5 | mail, ewa | 22, 25, 80, 143, 2525 |  | nginx | Linux | cookie.txt | x |
| 10.142.0.6 | edb | 22, 80, 389, 8080 |  | nginx | Linux | /dev | x |
| 10.142.0.7 | hhc17-smb-server | 135, 139, 445, 3389 | hhc-17-emi |  | Windows |  | HHC17-EMI |
| 10.142.0.8 | hhc17-emi | 80, 135, 139 ,445, 3389 | hhc17-smb-server | IIS | Windows |  | HHC17-SMB-SERVE |
| 10.142.0.11 | hhc17-apache-struts2 | 22, 80 |  | nginx | Linux |  |  |
| 10.142.0.13 | eaas | 80, 3389 | hhc17-elf-manufacturing | IIS | Windows |  |  |

Note that the DNS names and the Certificate names/NetBIOS names are reversed for for .7 and .8. I’m not sure if Alabaster is trying to confuse us or just made a mistake. None of the Windows servers are running HTTPS (port 443), so they don’t need web server certificates. They all run Remote Desktop Protocol (RDP, port 3389) and use the certificates there.

So, let’s try listing the shares on 10.142.0.7 this time.





Success! The share name that we are looking for is FileStor. The other shares (with ‘$’s) are Windows defaults. The error just means that when smbclient tried to connect using NetBIOS, it failed. That’s fine, we weren’t forwarding the NetBIOS ports anyway.

## Connect to the File Share (Commence Pillaging)

While we are here, let’s connect to the FileStor share and see if we can find anything interesting. [This site](https://help.ubuntu.com/community/Samba/SambaClientGuide), especially the section “Samba Client--Manual Configuration should be helpful. Download any interesting files you find.

## Question

The internal address of the l2s server is 10.142.0.3, and the address of the SMB server is 10.142.0.7. When Nmap probes an address on the local network it uses an ARP request. Why didn’t the Nmap scan find 10.142.0.7?

