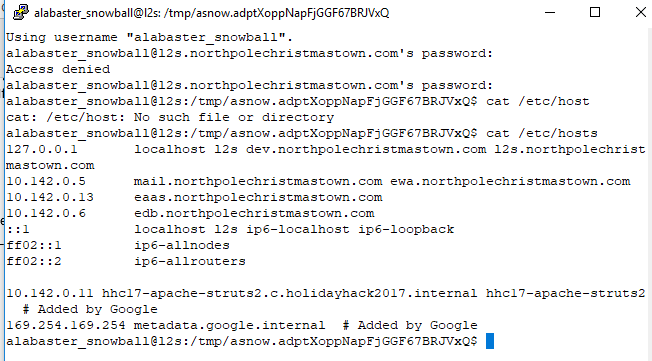
# Santa’s SMB Server--Exploiting Letters to Santa Part 2, Evaluating the Nmap Scan

## Questions from Part 1

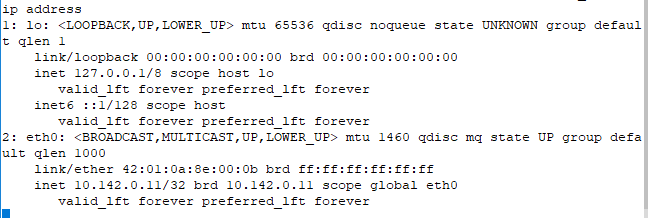
[Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) or Common Internet File System (CIFS) is a Microsoft adaptation of a protocol originally developed at IBM around 1990. It was used over the NetBIOS ports of UDP 137 and 138, and TCP ports 137 and 139, but that is no longer recommended. Instead, SMB usually runs over TCP port 445. TCP Port 445 is what we will be looking for. SMB has many functions besides file sharing and has several versions. SMB v1 is insecure and [should be disabled](https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/) wherever possible. You can find [detailed information about SMB here](https://msdn.microsoft.com/en-us/library/windows/desktop/aa365233(v=vs.85).aspx).

If you search for “enumerate SMB shares” on your favorite search engine, you will find several tools available to you. There are tools built in to [Metasploit](https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_enumshares), [Nmap](https://nmap.org/nsedoc/scripts/smb-enum-shares.html), and [Kali](https://hackercool.com/2016/07/smb-enumeration-with-kali-linux-enum4linuxacccheck-smbmap/). Basic tools are all we will need: SSH with port forwarding, Linux [Samba](https://www.samba.org/samba/) [smbclient](https://help.ubuntu.com/community/Samba/SambaClientGuide), or Windows [net use](https://www.lifewire.com/net-use-command-2618096).

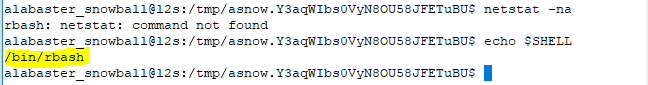
The /etc/hosts file has some of the information we are looking for.



It looks like there are servers mail or ewa at 10.142.0.5, eaas at 10.142.0.13, and edb at 10.142.0.6. Since both l2s and dev point to local host, we can assume that both are hosted on this VPS. Running the command ip address shows us that the internal IP of this server is 10.142.0.11.



The netstat command does not work through the SSH connection to l2s. It turns out the connection is running [rbash](https://www.tecmint.com/rbash-a-restricted-bash-shell-explained-with-practical-examples/), which is a restricted Bash instance. It is interesting to note that the shell we obtained through the Apache Struts vulnerability was a standard shell which can run netstat. However, if you go back and run the command it turns out that it doesn’t give any useful information.



There was a lot of talk during the contest about [escaping the rbash shell](https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells), but our SSH connection will provide us with everything we need.

From the [Nmap site](https://nmap.org/book/man-host-discovery.html):

*If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. (For IPv6, the ICMP timestamp request is omitted because it is not part of ICMPv6.) These defaults are equivalent to the -PE -PS443 -PA80 -PP options. The exceptions to this are the ARP (for IPv4) and Neighbor Discovery**(for IPv6) scans which are used for any targets on a local ethernet network.*

To prevent your host from being discovered in a default Nmap scan, you would block ICMP echo request (ping), TCP ports 80 and 443 (hard to do for a web server) and ICMP timestamp request (or just block all ICMP.) On the local network, it is harder since Nmap just sends an ARP request. If you block ARP, your server won’t be able to communicate unless you also configure a static ARP table for all hosts it needs to reach.

## Nmap Scan

If you ran your scan with the standard “blast away at everything” syntax,  
nmap -A 10.142.0.0/24  
you got the following results. I’ve summarized them in a table, and the raw results are in Appendix A.

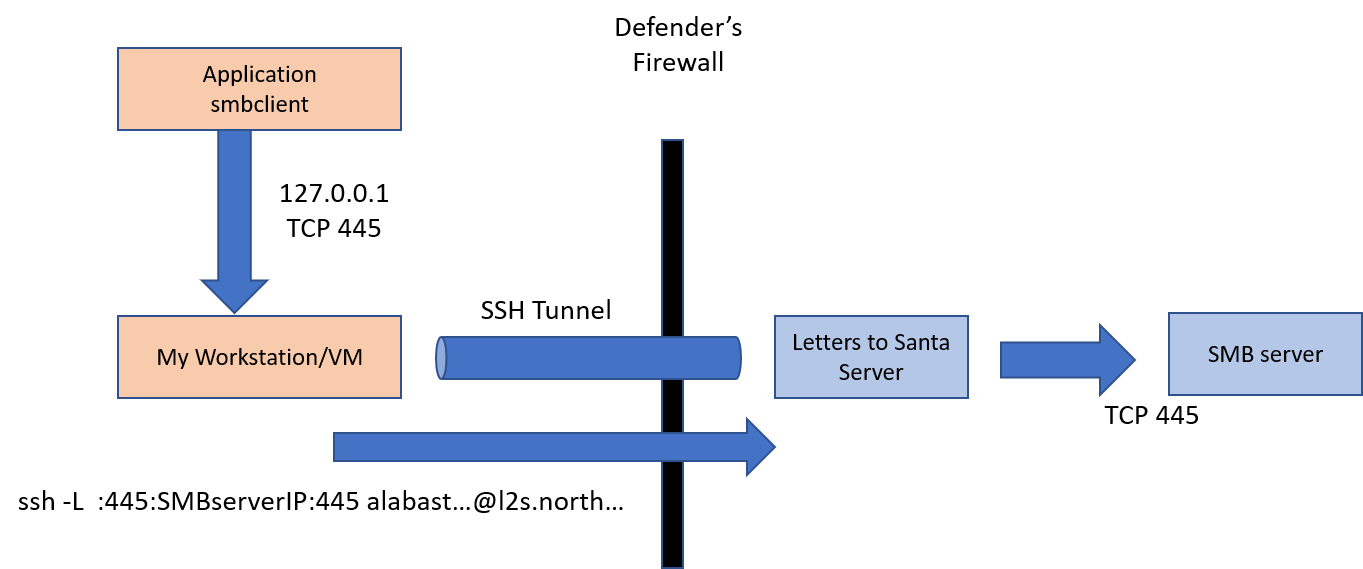
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IP address | Name | ports | Certificate Names | Web Server | OS | robots.txt |
| 10.142.0.2 | hhc17-l2s-proxy | 22, 80, 443, 2222 | dev, l2s | nginx | Linux |  |
| 10.142.0.3 | hhc17-apache-struts1 | 22, 80 |  | nginx | Linux |  |
|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

Whenever you are surveying a network, you will find it well worth your while to create such a table. The servers at 10.142.0.2, 3, and 11 run the servers for Letters to Santa challenge. The only server in the table above that listens on the SMB port, 445, is 10.142.0.8 (hhc17-emi). If you discovered more than one SMB server, you should try to connect to all of them.

## SSH Tunnel

The Linux implementation of SMB (used for Windows compatibility, not because Linux people like SMB) is Samba. If you were lucky, Alabaster would have installed the Samba client, smbclient, on the l2s server. He did not, but you can work around that with an SSH tunnel, or SSH port forwarding. You should find Holly’s Hints 2-7 very helpful. Please study the links she gives you.

The SSH daemon (server running on l2s) allows clients to “forward” ports. We will use local port forwarding in this case--other choices are dynamic and remote port forwarding. Our SSH client and the SSH server on l2s will work together to send our traffic through the l2s server to another server in Alabaster’s network. Here’s a picture:



The command ssh -L :445:SMBserverIP:445 alabaster\_snowball@l2s.northpolechristmastown.com will create an SSH tunnel between our VM and the l2s server. When an application on our VM sends data to 127.0.0.1:445, the SSH client will grab it and send it on to the l2s server. The first 445 in the command is what tells our SSH client to intercept incoming traffic on port 445. When the SSH server on l2s receives the traffic inside the SSH tunnel, it will forward the traffic to SMBserverIP on port 445. That’s why the SMBserverIP:445 part is there. How does the SSH client know it should connect to the SSH server on l2s, you ask? That’s what alabaster\_snowball@l2s.northpolechristmastown.com is for.

The SSH tunnel is great for administrators who need to manage systems remotely. It’s also a boon to attackers if they gain access to it. That’s why, at a minimum, SSH servers should use certificates and not passwords for authentication. Best practice is to require Two Factor or Multi Factor Authentication (2FA or MFA) for **all** VPN and SSH connections.

## List SMB Shares

It used to be that you could query and sometimes log into SMB shares without a user name or password using the share for Inter-Process Communication, IPC$ or null session. That allowed an attacker to gain much information, quickly. Fortunately, Windows Server 2003 and later do not allow anonymous access to IPC$. You will probably have to have a user name and password to list shares. We already caught Alabaster reusing passwords once, and Holly’s Hint 2 suggests Alabaster is known for password reuse.

Holly’s Hint 7 gives you the syntax you need to use smbclient to list the shares on an SMB server. If you don’t have smbclient installed on your Linux VM, you can get it with yum install samba-client (RedHat or CentOS, note that it says samba-client and not smbclient) or apt-get install smbclient (Debian or Ubuntu.) Remember that you are going through your SSH tunnel, so smbclient thinks it is connecting to 127.0.0.1 and not the server on the far end.

1. Establish an SSH connection to l2s that will forward all SMB traffic (TCP 445) to the SMB server you wish to connect to.
2. Use smbclient on Linux to list the shares on that server.

## Question

What is the name of the SMB file share? What SSH and smbclient commands did you use? Is more than one share available?

Note: If the SMB server denies access even when you use a correct user name and password, it could be that you didn’t discover all the SMB servers. Reread Holly’s Hint 1. If that doesn’t help, talk to your instructor or see the **<It’s a trap!>** section of the next lesson.

# Appendix--Complete Nmap Listing

alabaster\_snowball@l2s:/tmp/asnow.DyeAsSxPTTdgLs3JMzFWQUMH$ nmap -A 10.142.0.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2018-02-27 14:51 UTC

Nmap scan report for hhc17-l2s-proxy.c.holidayhack2017.internal (10.142.0.2)

Host is up (0.00021s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)

| ssh-hostkey:

| 2048 81:aa:b0:de:e0:4a:b5:23:7e:e8:cd:14:f3:fa:e2:f3 (RSA)

|\_ 256 dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba (ECDSA)

80/tcp open http nginx 1.10.3

|\_http-server-header: nginx/1.10.3

|\_http-title: Did not follow redirect to https://hhc17-l2s-proxy.c.holidayhack2017.internal/

443/tcp open ssl/http nginx 1.10.3

|\_http-server-header: nginx/1.10.3

|\_http-title: Toys List

| ssl-cert: Subject: commonName=dev.northpolechristmastown.com

| Subject Alternative Name: DNS:dev.northpolechristmastown.com, DNS:l2s.northpolechristmastown.com

| Not valid before: 2018-02-13T14:01:38

|\_Not valid after: 2018-05-14T14:01:38

|\_ssl-date: TLS randomness does not represent time

| tls-nextprotoneg:

|\_ http/1.1

2222/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)

| ssh-hostkey:

| 2048 81:aa:b0:de:e0:4a:b5:23:7e:e8:cd:14:f3:fa:e2:f3 (RSA)

|\_ 256 dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba (ECDSA)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for hhc17-apache-struts1.c.holidayhack2017.internal (10.142.0.3)

Host is up (0.00015s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)

| ssh-hostkey:

| 2048 81:aa:b0:de:e0:4a:b5:23:7e:e8:cd:14:f3:fa:e2:f3 (RSA)

|\_ 256 dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba (ECDSA)

80/tcp open http nginx 1.10.3

|\_http-server-header: nginx/1.10.3

|\_http-title: Toys List

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for mail.northpolechristmastown.com (10.142.0.5)

Host is up (0.00017s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 97:19:45:74:46:2d:76:d3:29:68:a2:af:27:ba:9b:64 (RSA)

|\_ 256 e9:ec:cd:7d:52:1b:4e:6c:92:d3:52:bf:10:bd:0c:86 (ECDSA)

25/tcp open smtp Postfix smtpd

|\_smtp-commands: mail.northpolechristmastown.com, PIPELINING, SIZE 10240000, ETRN, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

80/tcp open http nginx 1.10.3 (Ubuntu)

| http-robots.txt: 1 disallowed entry

|\_/cookie.txt

|\_http-server-header: nginx/1.10.3 (Ubuntu)

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

143/tcp open imap Dovecot imapd

|\_imap-capabilities: listed LOGIN-REFERRALS Pre-login LITERAL+ more ENABLE capabilities IMAP4rev1 AUTH=LOGINA0001 post-login have IDLE SASL-IR ID AUTH=PLAIN OK

2525/tcp open smtp Postfix smtpd

|\_smtp-commands: mail.northpolechristmastown.com, PIPELINING, SIZE 10240000, ETRN, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

Service Info: Host: mail.northpolechristmastown.com; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for edb.northpolechristmastown.com (10.142.0.6)

Host is up (0.00016s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)

| ssh-hostkey:

| 2048 39:b8:4e:46:f6:bd:68:49:12:41:5e:51:c1:01:68:36 (RSA)

|\_ 256 a1:05:5f:a4:e2:88:a3:83:44:63:08:3e:2d:d2:d8:97 (ECDSA)

80/tcp open http nginx 1.10.3

| http-robots.txt: 1 disallowed entry

|\_/dev

|\_http-server-header: nginx/1.10.3

| http-title: Site doesn't have a title (text/html; charset=utf-8).

|\_Requested resource was http://edb.northpolechristmastown.com/index.html

389/tcp filtered ldap

8080/tcp open tcpwrapped

| http-robots.txt: 1 disallowed entry

|\_/dev

|\_http-server-header: Werkzeug/0.12.2 Python/2.7.13

|\_http-title: Did not follow redirect to http://edb.northpolechristmastown.com/index.html

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for hhc17-emi.c.holidayhack2017.internal (10.142.0.8)

Host is up (0.00029s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: IIS Windows Server

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

3389/tcp open ssl/ms-wbt-server?

| ssl-cert: Subject: commonName=hhc17-smb-server

| Not valid before: 2017-11-06T13:46:55

|\_Not valid after: 2018-05-08T13:46:55

|\_ssl-date: 2018-02-27T14:53:26+00:00; 0s from scanner time.

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|\_nbstat: NetBIOS name: HHC17-SMB-SERVE, NetBIOS user: <unknown>, NetBIOS MAC: 42:01:0a:8e:00:08 (unknown)

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smbv2-enabled: Server supports SMBv2 protocol

Nmap scan report for hhc17-apache-struts2.c.holidayhack2017.internal (10.142.0.11)

Host is up (0.00018s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)

| ssh-hostkey:

| 2048 81:aa:b0:de:e0:4a:b5:23:7e:e8:cd:14:f3:fa:e2:f3 (RSA)

|\_ 256 dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba (ECDSA)

80/tcp open http nginx 1.10.3

|\_http-server-header: nginx/1.10.3

|\_http-title: Toys List

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for eaas.northpolechristmastown.com (10.142.0.13)

Host is up (0.00062s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: Index - North Pole Engineering Presents: EaaS!

3389/tcp open ssl/ms-wbt-server?

| ssl-cert: Subject: commonName=hhc17-elf-manufacturing

| Not valid before: 2017-11-23T20:53:55

|\_Not valid after: 2018-05-25T20:53:55

|\_ssl-date: 2018-02-27T14:53:25+00:00; 0s from scanner time.

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Post-scan script results:

| clock-skew:

| 0s:

| 10.142.0.8 (hhc17-emi.c.holidayhack2017.internal)

|\_ 10.142.0.13 (eaas.northpolechristmastown.com)

| ssh-hostkey: Possible duplicate hosts

| Key 256 dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba (ECDSA) used by:

| 10.142.0.2

| 10.142.0.3

| 10.142.0.11

| Key 2048 81:aa:b0:de:e0:4a:b5:23:7e:e8:cd:14:f3:fa:e2:f3 (RSA) used by:

| 10.142.0.2

| 10.142.0.3

|\_ 10.142.0.11

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (7 hosts up) scanned in 116.06 seconds

alabaster\_snowball@l2s:/tmp/asnow.DyeAsSxPTTdgLs3JMzFWQUMH$