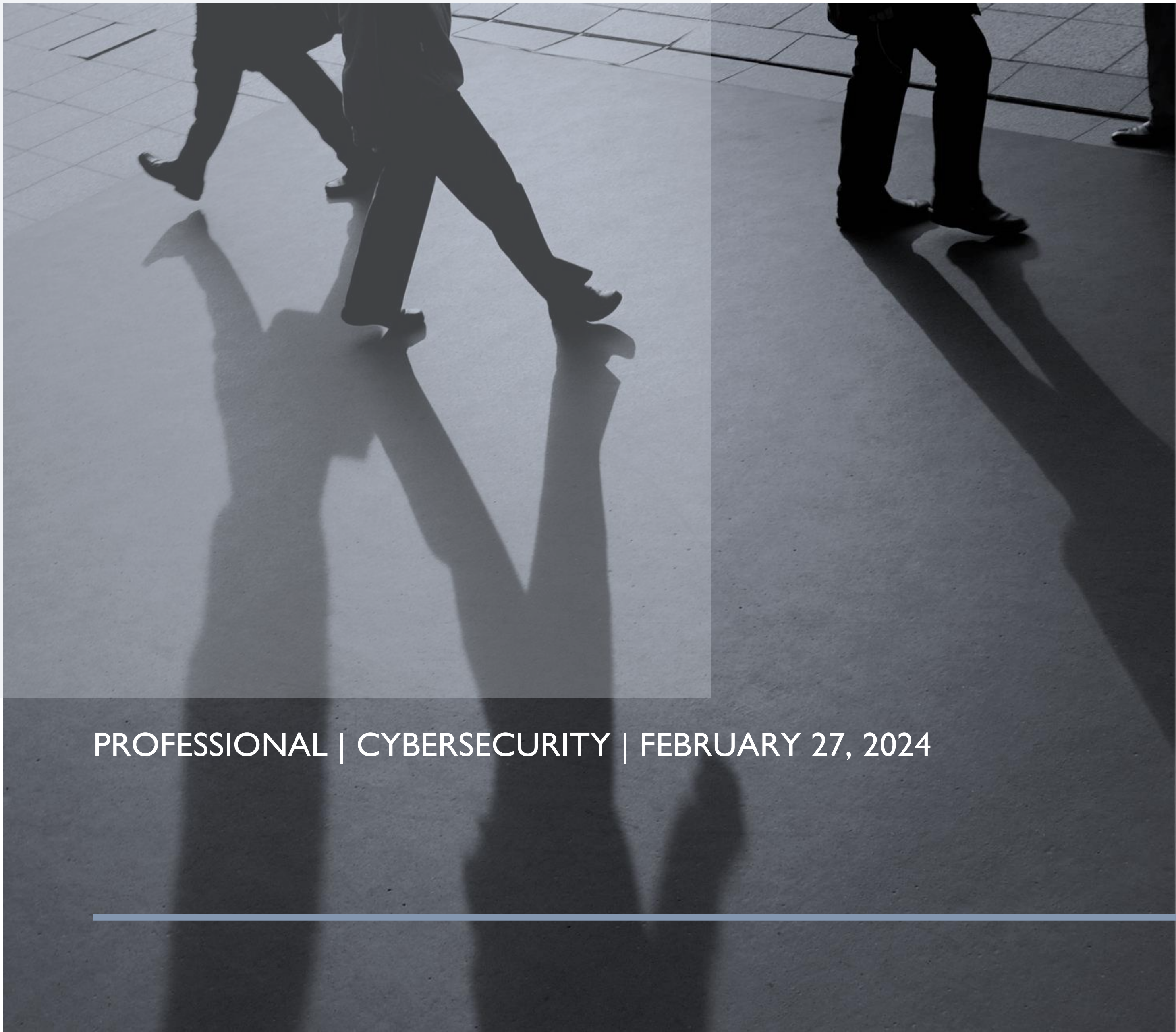
SMB ENUMERAION

BY JAMES ROBERSON



PROFESSIONAL | CYBERSECURITY | FEBRUARY 27, 2024

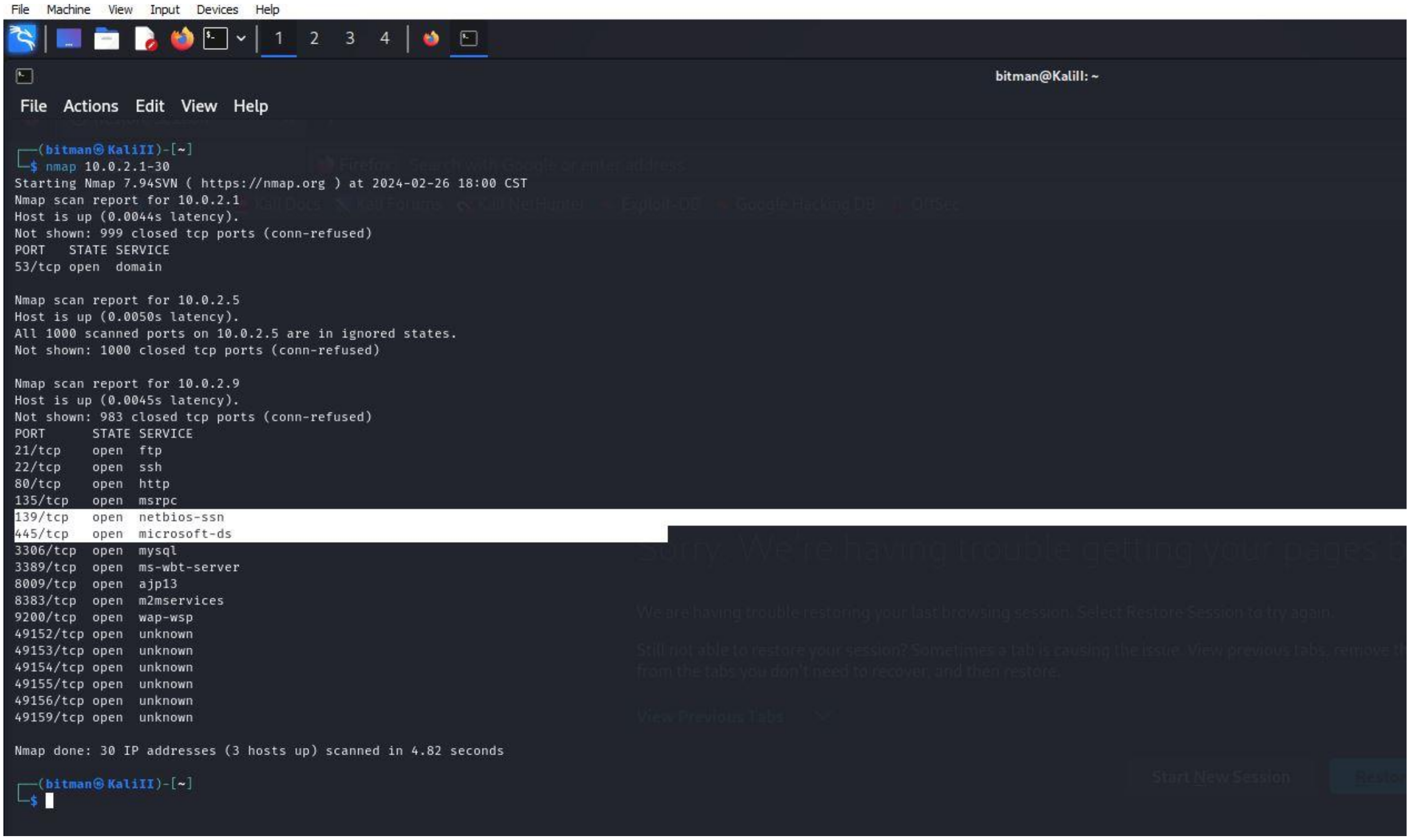
WHAT HAPPENED?

In this particular assignment from the client, I was asked to aggregate results from various information gather tools. Those tools include, but are not limited to, nmblookup, nmap scripts, smbmap, smbclient, and as well as rpcclient.

- Showcased the output for each nmblookup, network mapper scripts, and smbmap. Check.
- Identified the available shares that go along with smbclient. Check.
- A list of users identified through the rpcclient. Check and check.

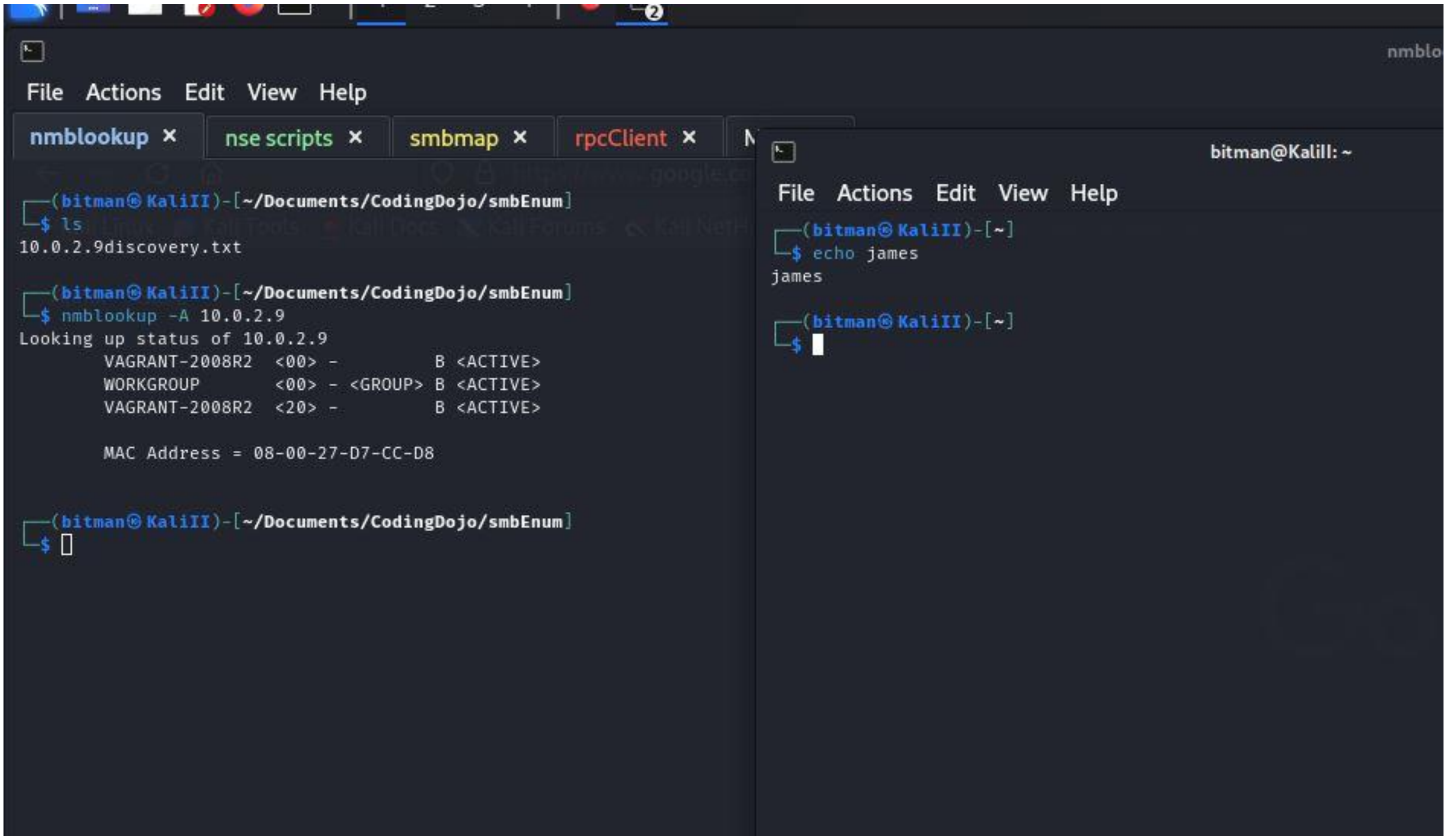
I must highlight the initial difficulty I had determining the difference in command structure between each tool. Smbclient kept giving me the same unable to connect with SMB1 – no workgroup available. It seemed no matter how I structured the command, I would receive the same output. After a bit of research, I concluded that the smb.conf may need to be reconfigured to correct the error. Once I navigated over to /etc/samba/smb.conf, where I was able to configure the file as shown in Figure 6 and 7, I was able to pull those shares from the site.

PROOF:


File Machine View Input Devices Help
1 2 3 4
bitman@KaliII: ~
File Actions Edit View Help

```
┌──(bitman㉿KaliII)-[~]
└─$ nmap 10.0.2.1-30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 18:00 CST
Nmap scan report for 10.0.2.1
Host is up (0.0044s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.5
Host is up (0.0050s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.9
Host is up (0.0045s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
8009/tcp  open  ajp13
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown

Nmap done: 30 IP addresses (3 hosts up) scanned in 4.82 seconds

┌──(bitman㉿KaliII)-[~]
└─$ 
```

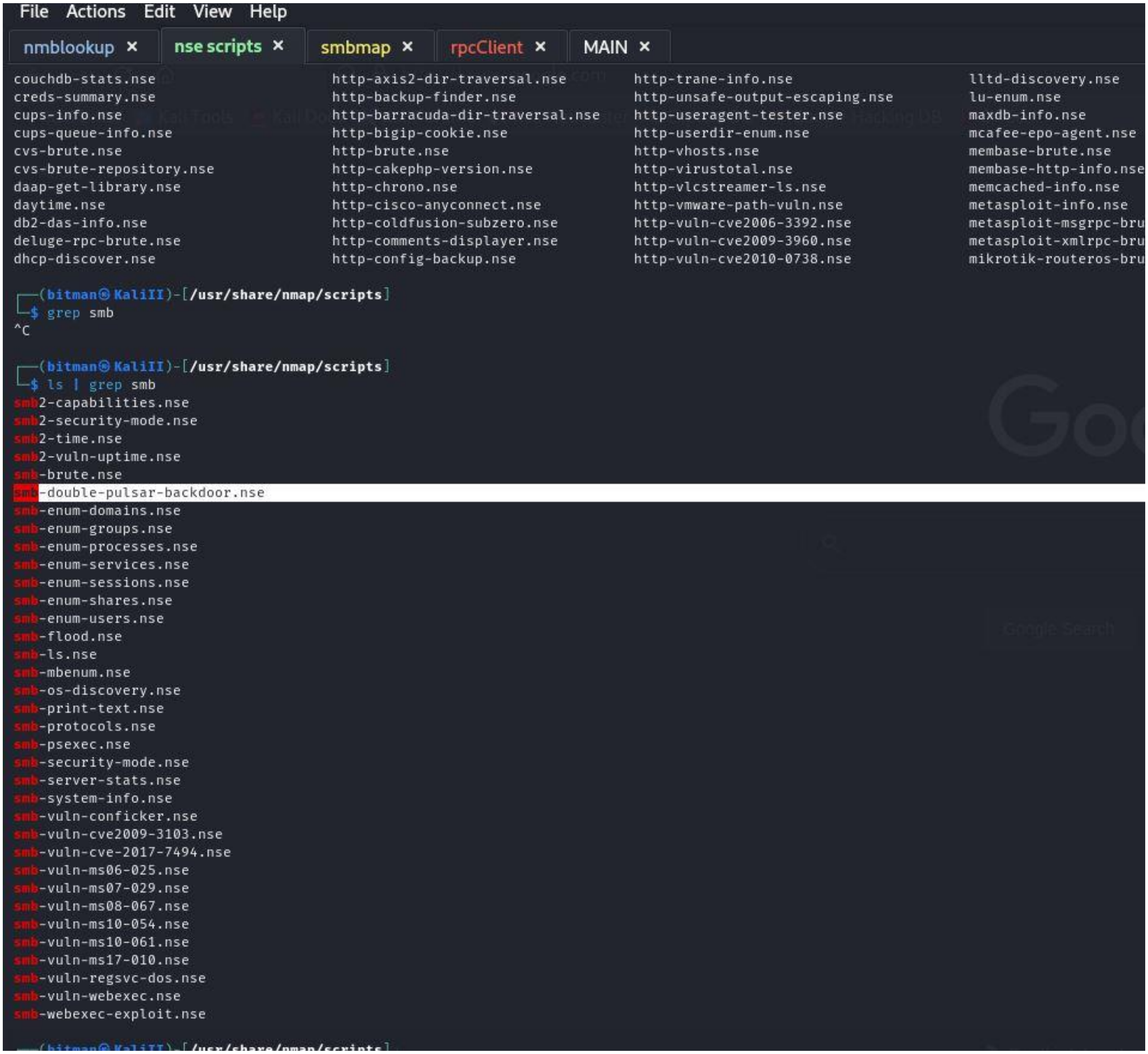
Figure 1. Discovery scan of machines.



```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ ls
10.0.2.9discovery.txt

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ nmblookup -A 10.0.2.9
Looking up status of 10.0.2.9
        VAGRANT-2008R2  <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        VAGRANT-2008R2  <20> -         B <ACTIVE>

        MAC Address = 08-00-27-D7-CC-D8


┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ 
```

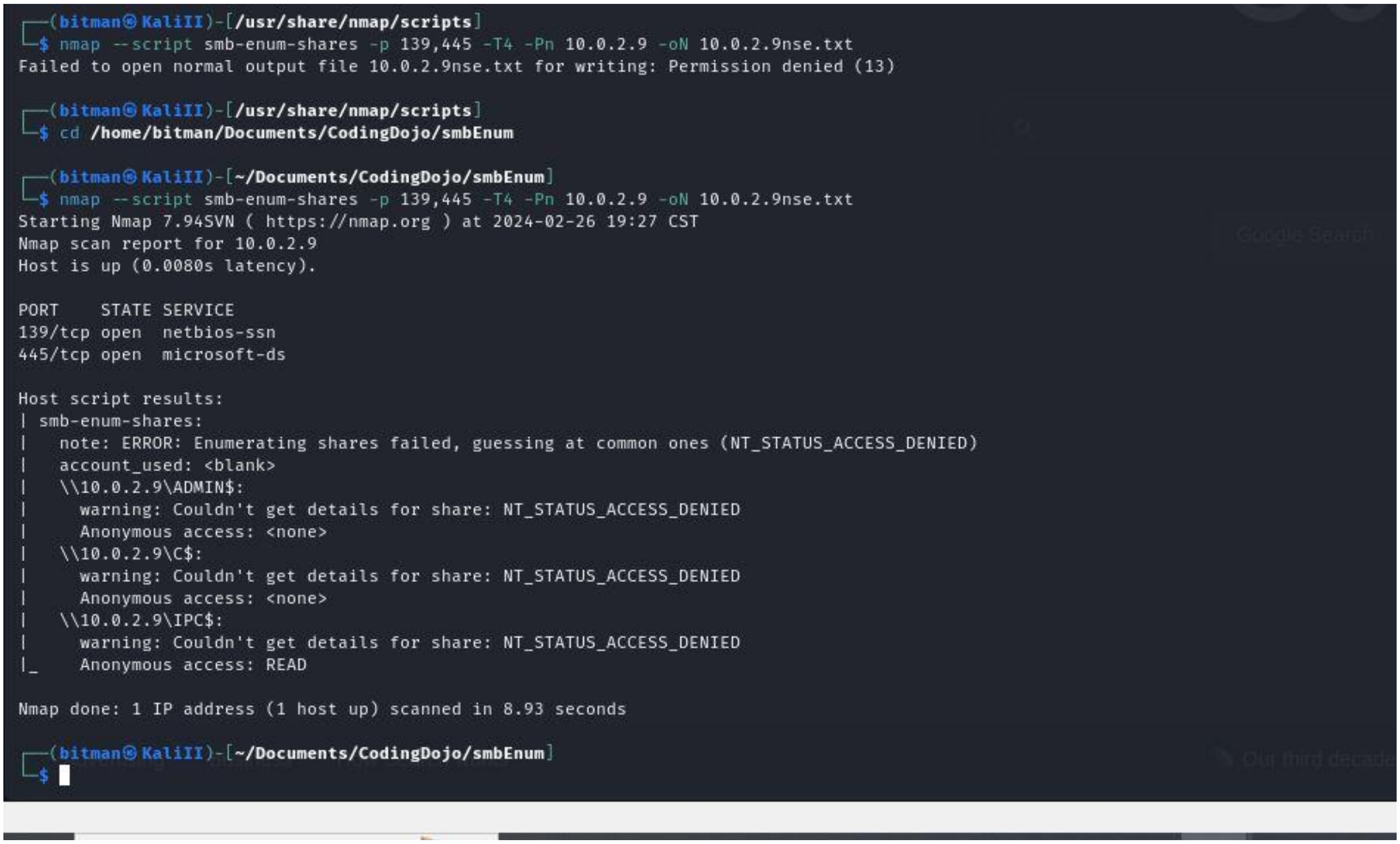
```
┌──(bitman㉿KaliII)-[~]
└─$ echo james
james

┌──(bitman㉿KaliII)-[~]
└─$ 
```

Figure 2. Per our agreement, I began enumerating the target starting with the first tool, nmblookup.



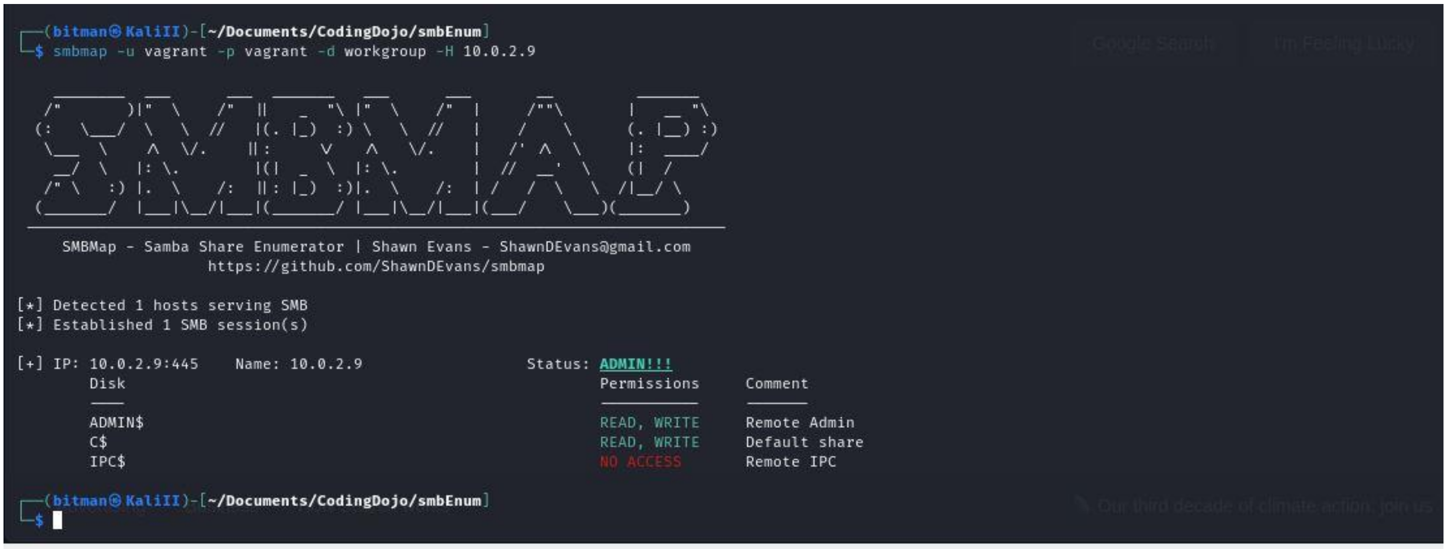
```
couchdb-stats.nse              http-axis2-dir-traversal.nse       http-trane-info.nse                lltd-discovery.nse
creds-summary.nse              http-backup-finder.nse             http-unsafe-output-escaping.nse    lu-enum.nse
cups-info.nse                  http-barracuda-dir-traversal.nse   http-useragent-tester.nse          maxdb-info.nse
cups-queue-info.nse            http-bigip-cookie.nse              http-userdir-enum.nse              mcafee-epo-agent.nse
cvs-brute.nse                  http-brute.nse                     http-vhosts.nse                    membase-brute.nse
cvs-brute-repository.nse       http-cakephp-version.nse           http-virustotal.nse                membase-http-info.nse
daap-get-library.nse           http-chrono.nse                    http-vlcstreamer-ls.nse            memcached-info.nse
daytime.nse                    http-cisco-anyconnect.nse          http-vmware-path-vuln.nse          metasploit-info.nse
db2-das-info.nse               http-coldfusion-subzero.nse        http-vuln-cve2006-3392.nse         metasploit-msgrpc-bru
deluge-rpc-brute.nse           http-comments-displayer.nse        http-vuln-cve2009-3960.nse         metasploit-xmlrpc-bru
dhcp-discover.nse              http-config-backup.nse             http-vuln-cve2010-0738.nse         mikrotik-routeros-bru

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$ grep smb
^C

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$ ls | grep smb
smb2-capabilities.nse
smb2-security-mode.nse
smb2-time.nse
smb2-vuln-uptime.nse
smb-brute.nse
smb-double-pulsar-backdoor.nse
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-services.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
smb-flood.nse
smb-ls.nse
smb-mbenum.nse
smb-os-discovery.nse
smb-print-text.nse
smb-protocols.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smb-webexec-exploit.nse

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
```

Figure 3. Next, were the nmap scripts. This is just a list of potential scripts to run.



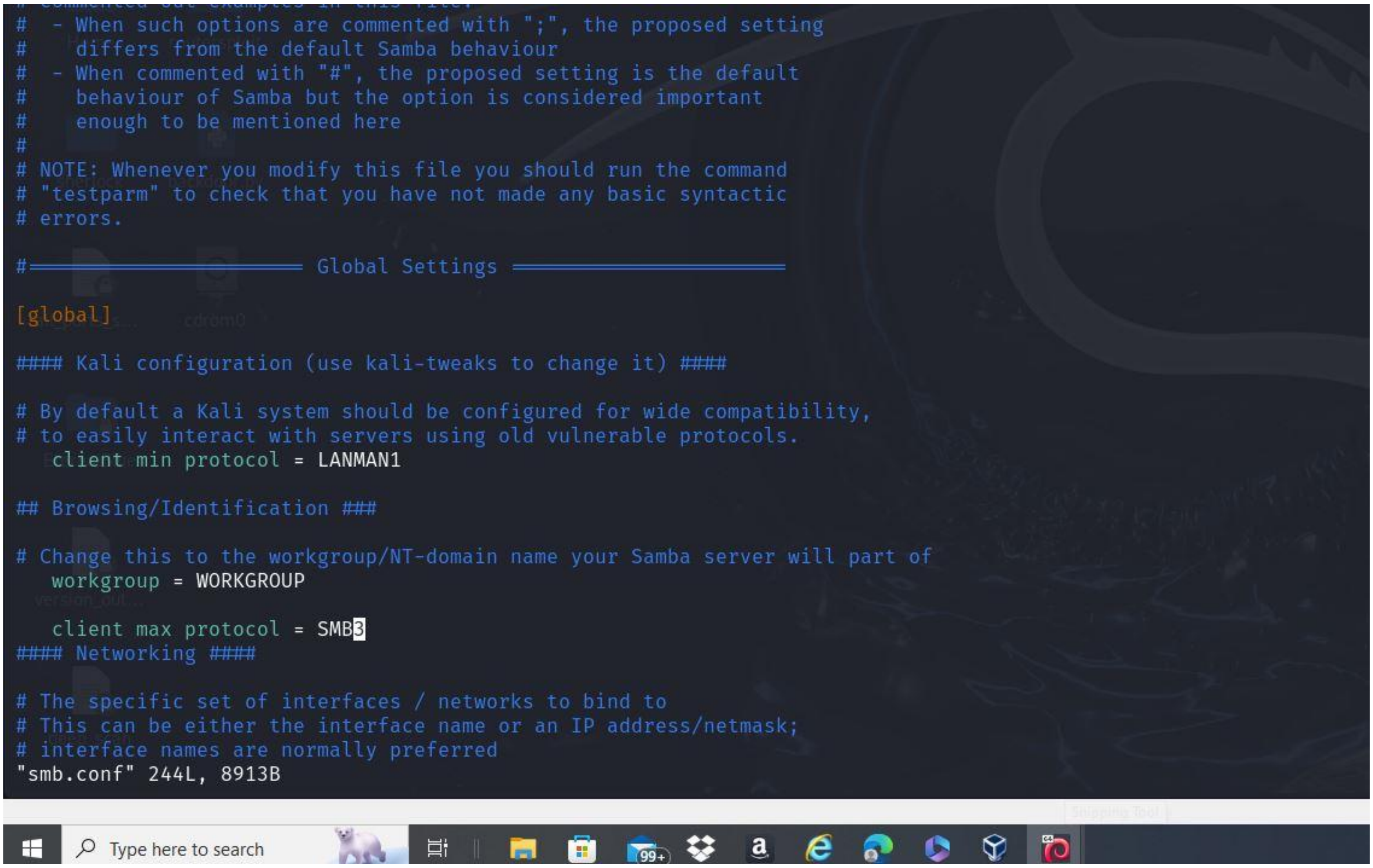
```
┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$ nmap --script smb-enum-shares -p 139,445 -T4 -Pn 10.0.2.9 -oN 10.0.2.9nse.txt
Failed to open normal output file 10.0.2.9nse.txt for writing: Permission denied (13)

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$ cd /home/bitman/Documents/CodingDojo/smbEnum

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ nmap --script smb-enum-shares -p 139,445 -T4 -Pn 10.0.2.9 -oN 10.0.2.9nse.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 19:27 CST
Nmap scan report for 10.0.2.9
Host is up (0.0080s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.0.2.9\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.2.9\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.0.2.9\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 8.93 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ 
```

Figure 4. The actual script I decided to run was to gather the shares from target IP. Not a requirement but I wanted to know if it would work and it did. As you can see the script may say that it failed when trying to enumerate shares, but it still lists them out anyway.



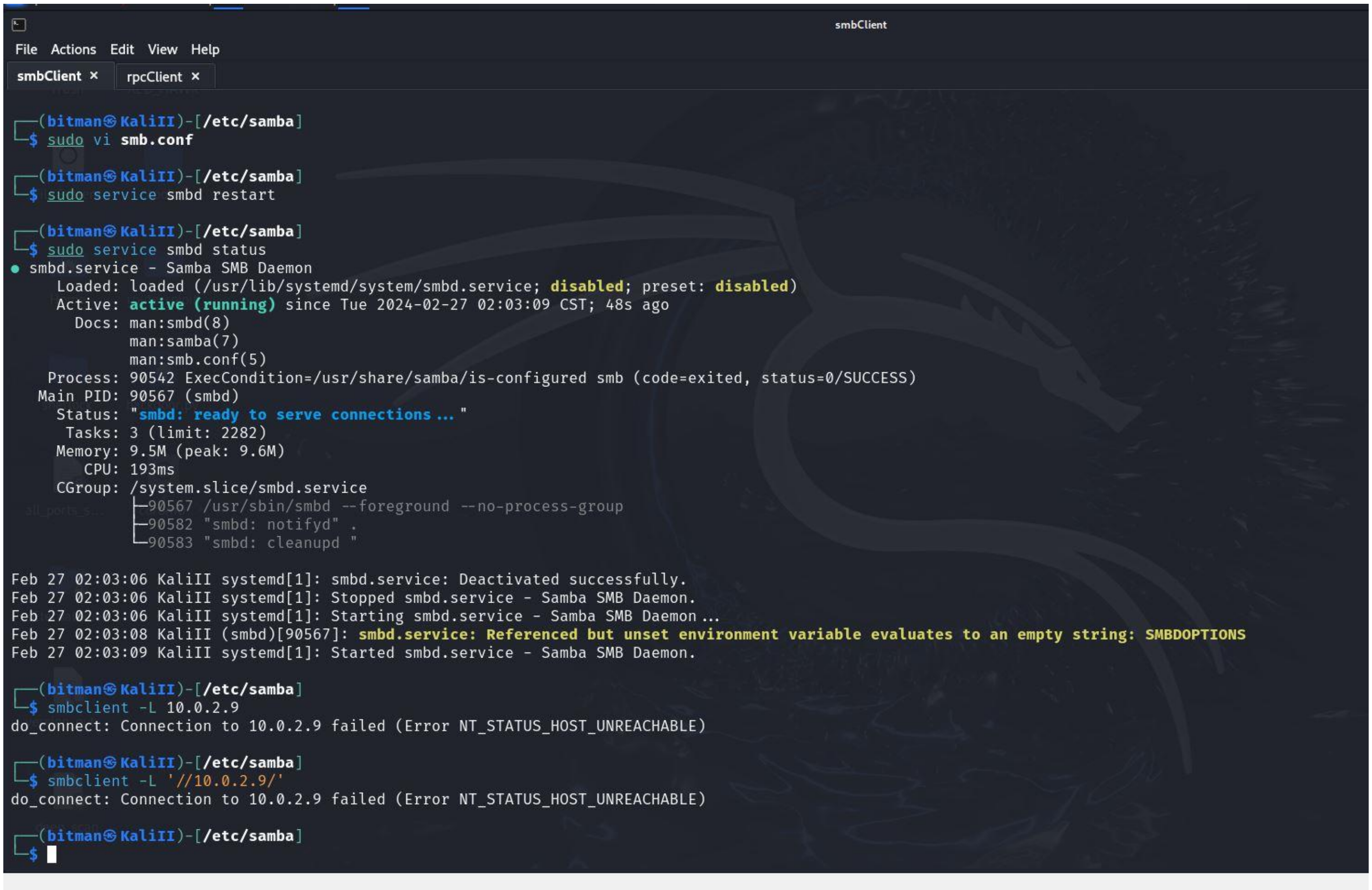
```
┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ smbmap -u vagrant -p vagrant -d workgroup -H 10.0.2.9

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.0.2.9:445    Name: 10.0.2.9                  Status: ADMIN!!!
        Disk                                            Permissions     Comment
        ----                                            -----------     -------
        ADMIN$                                          READ, WRITE     Remote Admin
        C$                                              READ, WRITE     Default share
        IPC$                                            NO ACCESS       Remote IPC

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/smbEnum]
└─$ 
```

Figure 5. smbmap showed off the shares by passing in the username and password as parameters. As well as setting domain as workgroup.



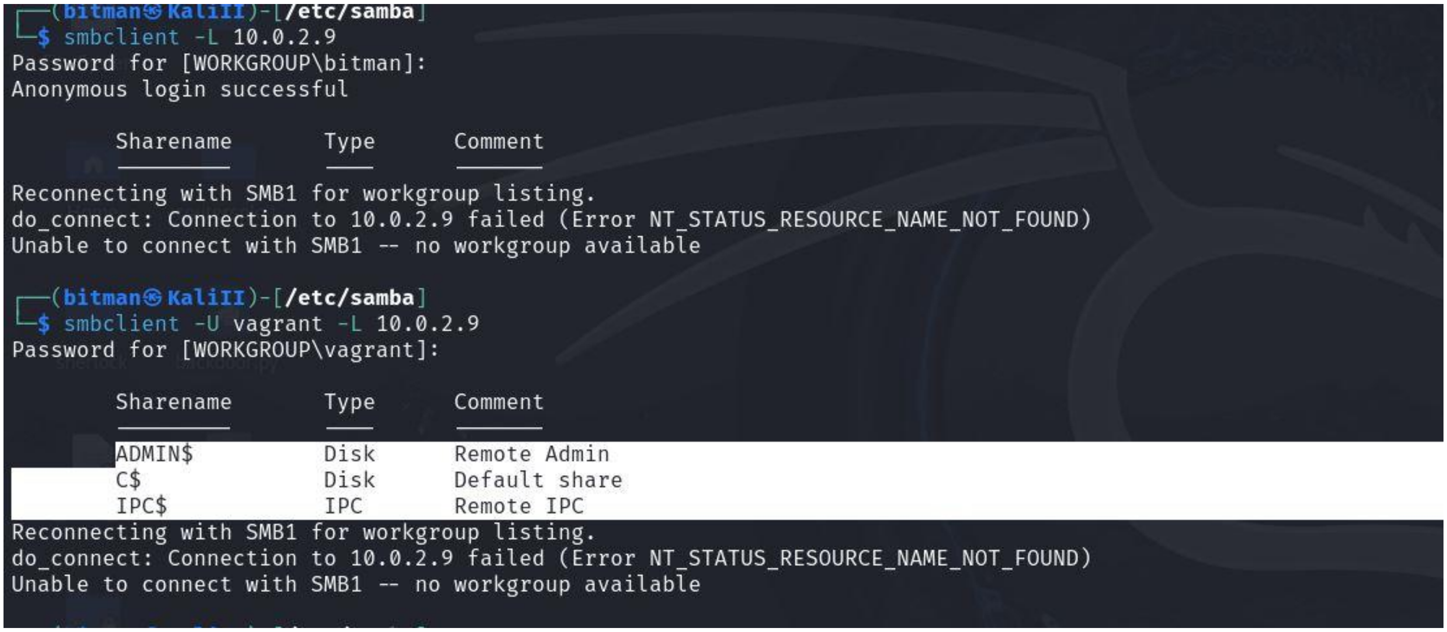
```
# commented out examples in this file.
#   - When such options are commented with ";", the proposed setting
#     differs from the default Samba behaviour
#   - When commented with "#", the proposed setting is the default
#     behaviour of Samba but the option is considered important
#     enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#======================= Global Settings =======================

[global]

#### Kali configuration (use kali-tweaks to change it) ####

# By default a Kali system should be configured for wide compatibility,
# to easily interact with servers using old vulnerable protocols.
   client min protocol = LANMAN1

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = WORKGROUP

   client max protocol = SMB3
#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
"smb.conf" 244L, 8913B
```

Figure 6. I added client max protocol = SMB3 to the smb.conf file. Saved and closed it. On to Figure 7.



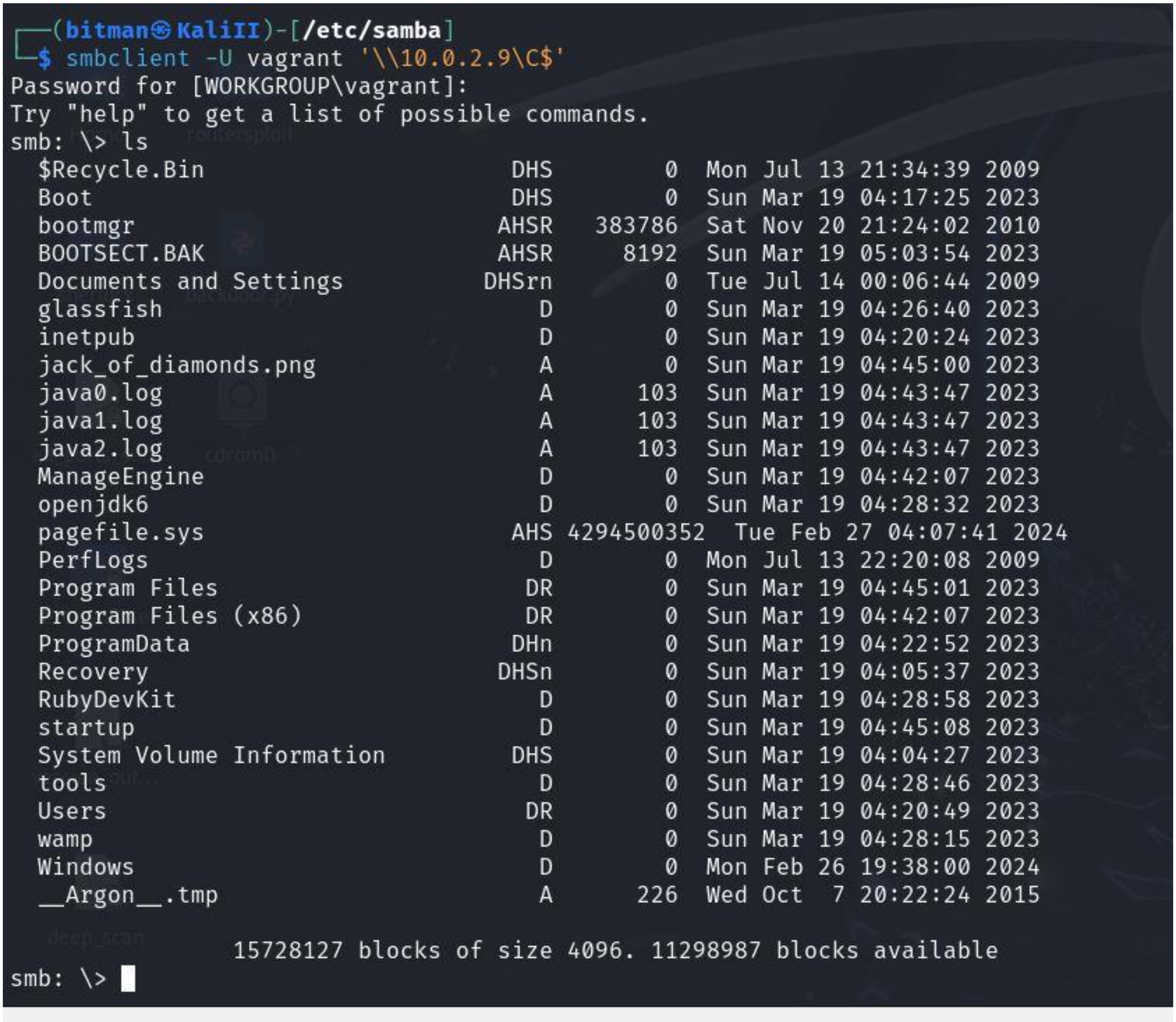
```
┌──(bitman㉿KaliII)-[/etc/samba]
└─$ sudo vi smb.conf

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ sudo service smbd restart

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ sudo service smbd status
● smbd.service - Samba SMB Daemon
     Loaded: loaded (/usr/lib/systemd/system/smbd.service; disabled; preset: disabled)
     Active: active (running) since Tue 2024-02-27 02:03:09 CST; 48s ago
       Docs: man:smbd(8)
             man:samba(7)
             man:smb.conf(5)
    Process: 90542 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
   Main PID: 90567 (smbd)
     Status: "smbd: ready to serve connections ..."
      Tasks: 3 (limit: 2282)
     Memory: 9.5M (peak: 9.6M)
        CPU: 193ms
     CGroup: /system.slice/smbd.service
             ├─90567 /usr/sbin/smbd --foreground --no-process-group
             ├─90582 "smbd: notifyd" .
             └─90583 "smbd: cleanupd "

Feb 27 02:03:06 KaliII systemd[1]: smbd.service: Deactivated successfully.
Feb 27 02:03:06 KaliII systemd[1]: Stopped smbd.service - Samba SMB Daemon.
Feb 27 02:03:06 KaliII systemd[1]: Starting smbd.service - Samba SMB Daemon ...
Feb 27 02:03:08 KaliII (smbd)[90567]: smbd.service: Referenced but unset environment variable evaluates to an empty string: SMBDOPTIONS
Feb 27 02:03:09 KaliII systemd[1]: Started smbd.service - Samba SMB Daemon.

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ smbclient -L 10.0.2.9
do_connect: Connection to 10.0.2.9 failed (Error NT_STATUS_HOST_UNREACHABLE)

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ smbclient -L '//10.0.2.9/'
do_connect: Connection to 10.0.2.9 failed (Error NT_STATUS_HOST_UNREACHABLE)

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ ▌
```

Figure 7. After reconfiguring the smb file, I wanted some kind of indication that the change was being implemented; so I looked up smb's status to see it running. The error had disappeared and then reappeared when I finally realized that my command structure was the reason for the smbclient difficulties, as shown in Figure 8.



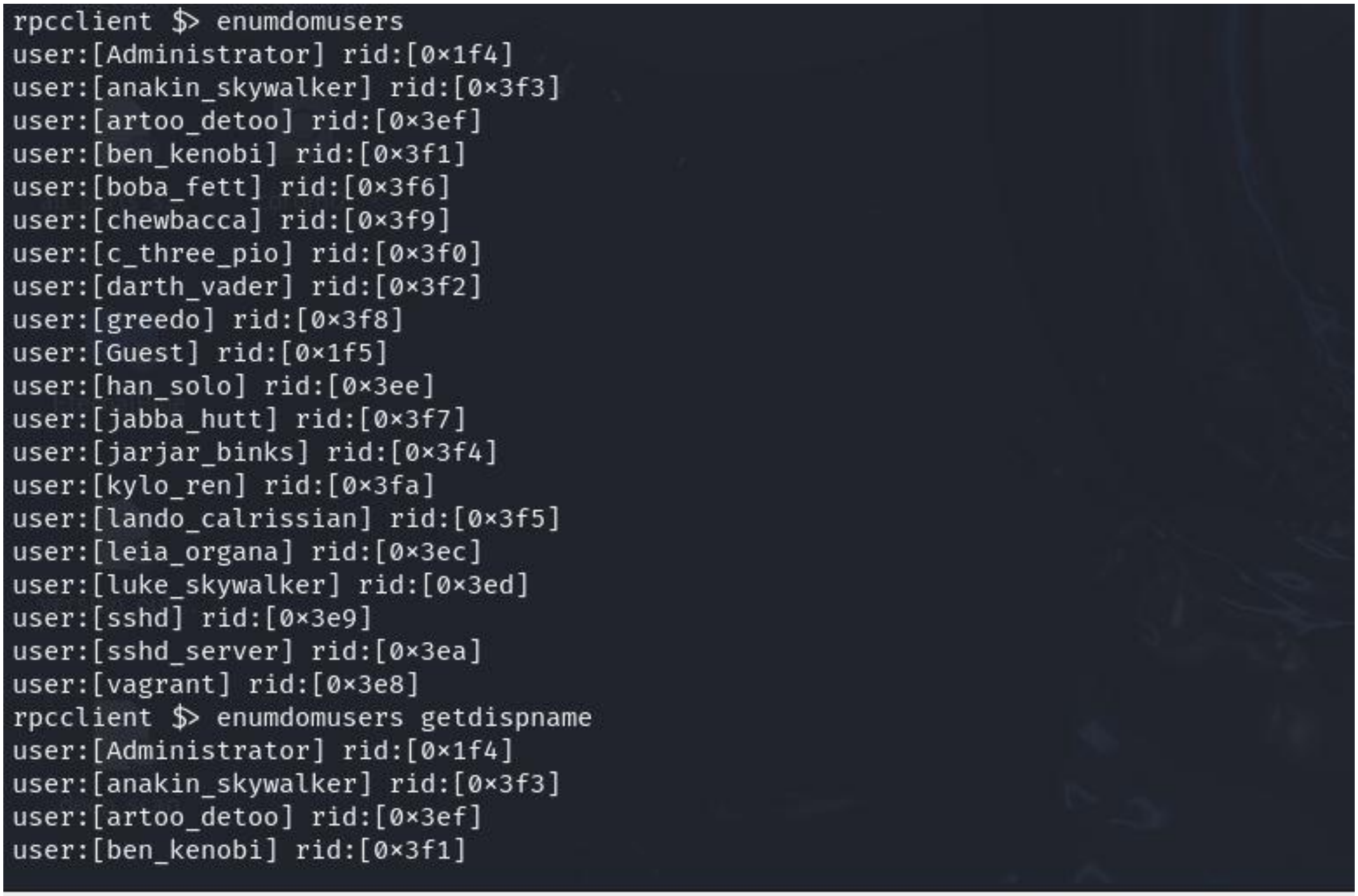
```
┌──(bitman㉿KaliII)-[/etc/samba]
└─$ smbclient -L 10.0.2.9
Password for [WORKGROUP\bitman]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.0.2.9 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(bitman㉿KaliII)-[/etc/samba]
└─$ smbclient -U vagrant -L 10.0.2.9
Password for [WORKGROUP\vagrant]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.0.2.9 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Figure 8. Yes, the connection failure came back, but this time it wasn't coming alone. The shares began to appear once I specified the user with -U vagrant.



```
┌──(bitman㉿KaliII)-[/etc/samba]
└─$ smbclient -U vagrant '\\10.0.2.9\C$'
Password for [WORKGROUP\vagrant]:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Mon Jul 13 21:34:39 2009
  Boot                              DHS        0  Sun Mar 19 04:17:25 2023
  bootmgr                          AHSR   383786  Sat Nov 20 21:24:02 2010
  BOOTSECT.BAK                     AHSR     8192  Sun Mar 19 05:03:54 2023
  Documents and Settings          DHSrn        0  Tue Jul 14 00:06:44 2009
  glassfish                           D        0  Sun Mar 19 04:26:40 2023
  inetpub                             D        0  Sun Mar 19 04:20:24 2023
  jack_of_diamonds.png                A        0  Sun Mar 19 04:45:00 2023
  java0.log                           A      103  Sun Mar 19 04:43:47 2023
  java1.log                           A      103  Sun Mar 19 04:43:47 2023
  java2.log                           A      103  Sun Mar 19 04:43:47 2023
  ManageEngine                        D        0  Sun Mar 19 04:42:07 2023
  openjdk6                            D        0  Sun Mar 19 04:28:32 2023
  pagefile.sys                      AHS 4294500352  Tue Feb 27 04:07:41 2024
  PerfLogs                            D        0  Mon Jul 13 22:20:08 2009
  Program Files                      DR        0  Sun Mar 19 04:45:01 2023
  Program Files (x86)                DR        0  Sun Mar 19 04:42:07 2023
  ProgramData                       DHn        0  Sun Mar 19 04:22:52 2023
  Recovery                         DHSn        0  Sun Mar 19 04:05:37 2023
  RubyDevKit                          D        0  Sun Mar 19 04:28:58 2023
  startup                             D        0  Sun Mar 19 04:45:08 2023
  System Volume Information         DHS        0  Sun Mar 19 04:04:27 2023
  tools                               D        0  Sun Mar 19 04:28:46 2023
  Users                              DR        0  Sun Mar 19 04:20:49 2023
  wamp                                D        0  Sun Mar 19 04:28:15 2023
  Windows                             D        0  Mon Feb 26 19:38:00 2024
  __Argon__.tmp                       A      226  Wed Oct  7 20:22:24 2015

                15728127 blocks of size 4096. 11298987 blocks available
smb: \> 
```

Figure 9. List out the current directory.



```
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[anakin_skywalker] rid:[0×3f3]
user:[artoo_detoo] rid:[0×3ef]
user:[ben_kenobi] rid:[0×3f1]
user:[boba_fett] rid:[0×3f6]
user:[chewbacca] rid:[0×3f9]
user:[c_three_pio] rid:[0×3f0]
user:[darth_vader] rid:[0×3f2]
user:[greedo] rid:[0×3f8]
user:[Guest] rid:[0×1f5]
user:[han_solo] rid:[0×3ee]
user:[jabba_hutt] rid:[0×3f7]
user:[jarjar_binks] rid:[0×3f4]
user:[kylo_ren] rid:[0×3fa]
user:[lando_calrissian] rid:[0×3f5]
user:[leia_organa] rid:[0×3ec]
user:[luke_skywalker] rid:[0×3ed]
user:[sshd] rid:[0×3e9]
user:[sshd_server] rid:[0×3ea]
user:[vagrant] rid:[0×3e8]
rpcclient $> enumdomusers getdispname
user:[Administrator] rid:[0×1f4]
user:[anakin_skywalker] rid:[0×3f3]
user:[artoo_detoo] rid:[0×3ef]
user:[ben_kenobi] rid:[0×3f1]
```

Figure 10. I looked through the –help menu to locate the command enumdomusers and ran it. Yahtzee!