ESERCIZIO W13D1

L'obiettivo viene esposto dalla seguente traccia in piattaforma:

- Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.
- Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.
- Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Preparazione macchine virtuali

Configuriamo le nostre macchine su rete interna in modo che riescano a comunicare tra di loro.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

Settaggio rete Kali
Linux

#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.32.100/24
netmask 255.255.255.0
gateway 192.168.32.1
```

```
GNU nano 2.0.7
                           File: /etc/network/interfaces
* Reloading OpenBSD Secure Shell server's configuration sshdr system
 and how to activate them. For more information, see interfa
                                                                                  * Reloa
ding Postfix configuration...ace
auto lo
                                    ...done.
iface lo inet loopback
                                                   Settaggi rete
 The primary network interface
                                                  Metasploitable2
auto eth0
iface ethO inet static
#iface eth0 inet dhcp
address 192.168.32.101
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.32.1
                                  [ Wrote 16 lines ]
                             ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^W Where Is ^V Next Page ^U UnCut Text^T To Spell
              1 WriteOut
G Get Help
```

```
(kali® kali)-[~]
$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
64 bytes from 192.168.32.101: icmp_seq=1 ttl=64 time=0.942 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=64 time=0.762 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=64 time=0.784 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=64 time=0.689 ms
^C
— 192.168.32.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.689/0.794/0.942/0.092 ms

Kali ping Meta
Kali ping Meta
```

```
msfadmin@metasploitable:~$ ping 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data.
64 bytes from 192.168.32.100: icmp_seq=1 ttl=64 time=0.936 ms
64 bytes from 192.168.32.100: icmp_seq=2 ttl=64 time=0.647 ms
64 bytes from 192.168.32.100: icmp_seq=3 ttl=64 time=0.657 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=64 time=0.784 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=64 time=0.784 ms
64 bytes from 192.168.32.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
67tt min/aug/max/mdev = 0.647/0.756/0.936/0.117 ms
68squared msgadmin@metasploitable:~$
```

Intercettazione richieste

Grazie all'aiuto dell'intercepting proxy Burpsuite, possiamo intercettare le richieste inviate dal nostro browser fino al web server.

```
Pretty
             Raw
 1 POST /dvwa/login.php HTTP/1.1
                                                                                                  Richiesta GET
 2 Host: 192.168.32.101
 3 Content-Length: 44
                                                                                                       durante
 4 Cache-Control: max-age=0
                                                                                                     immissione
 5 Upgrade-Insecure-Requests: 1
                                                                                                     credenziali
 6 Origin: http://192.168.32.101
7 Content-Type: application/x-www-form-urlencoded
 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
   text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, image/appg, */*; q=0.8, application/signed-exchange; v=b3; q=0.7
10 Referer: http://192.168.32.101/dvwa/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; PHPSESSID=be96029d7b436d9d57e322c0423d3a03
14 Connection: close
16 username=admin&password=password&Login=Login
```

La prima ci mostra il passaggio di credenziali da nostro browser fino alla pagina di login

```
POST /dvwa/security.php HTTP/1.1

Host: 192.168.32.101

Content-Length: 33

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://192.168.32.101

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://192.168.32.101/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Accept-Encoding: gzip, deflate, br
Consection: close

Security=low&seclev_submit=Submit

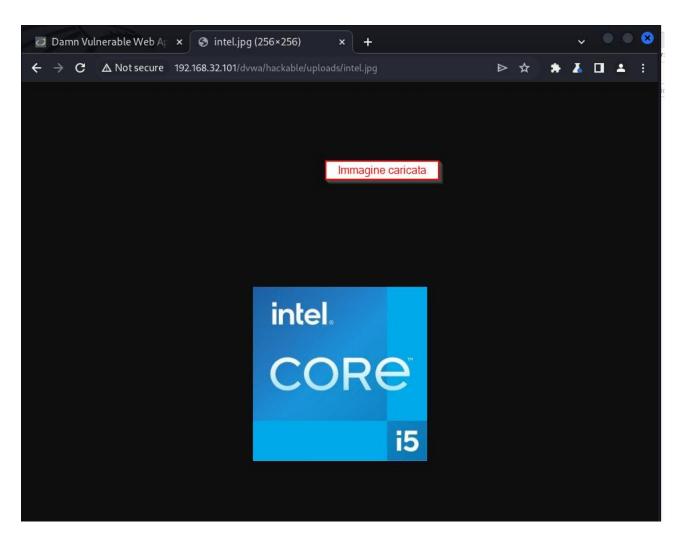
RIchiesta POST inserimento low e submit
```

La seconda ci da un idea di ciò che viene consegnato al web server quando schiacciamo un pulsante, come ad esempio submit per il cambio di sicurezza. Scegliamo low.

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.32.101
Content-Length: 8253
 Cache-Control: max-age=0
Upgrade-Insecure-Requests:
Origin: http://192.168.32.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarydpagjeKdSHFxOqfp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, image/apng, */*; q=0.8, application/signed-exchange; v=b3; q=0.8, applic
Referer: http://192.168.32.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=956cb05f283f902c0328782b6796c249
Connection: close
                                                                                                                                                                                                                   Immagine caricata
        ---WebKitFormBoundarydpagjeKd5HFxOgfp
Content-Disposition: form-data; name="MAX_FILE_SIZE"
   ----WebKitFormBoundarydpagjeKd5HFxOgfp
Content-Disposition: form-data; name="uploaded"; filename="intel.jpg"
Content-Type: image/jpeg
ÿØÿàJFIFÿÛ
 ) )/'%'/9339GDG]]}
,
)/'%'/9339GDG]]}ÿÂ"ÿÄ5ÿÚçRWÒ\ý$óéII%j⊚9´£RIQ:HjI>4sIÑxÁ+\$'\±1ÐI I\Neñ}"\$2Mé¦\œcçOXù>πĐ¡{ĒċÌÝ\Ē[&MYI$èÒIbI%íyiwc }icúc²ñÎßs-\\ê;{××ûª
)/'%'/9339GDG]}}¾"ÿA"ÿASÿUcRWOţÿţoEII%jo9'ERIO;HjI>4sINka+¾±iDI I\Neñ}"$=MeļţoeçOXù>kDj{EōIY*EL6MYIşeOIDI%Iyıvc_jrcuc*nIKs-ţe;{xxus
Y/İţK«Kcţcyv. DiàRK«åRICI*FDIxob+aèiK#òV )cÄeRîÓijÿjjősåu"70ïQV;xPot*PÛµ40DI9èOU0i>51Egözö\Zòò*Wxkjī%bÖV;äxVţ$RnTŌIÑ
+TPO-Ö¥Ü, ú'|ÉòdINV%å-kUymè-HIñ±EPiö"'»LÔm ţmÄdO^£xòÄx_BmòT-?Om+ţ)[úçïvx'òù¶y6th+§ä³uŐRßièO9ieb)Moz-£ô'Ó_ĒïTóYţ*Ox/b,VÖ;g;S«r*Oz_ú
y*bÖbAKK7kb5.å{-óFRÍ 'Éāe'èNDù-ŞQÜ'ĭiâo%zĬoŤ(éyxş, zpÄñ[+ß5D»y=ĬNzæbóYŪÚŤc[-ePOODlé9pĨ xD*Ü£jízo#:jÄŤţĄC,úáä<çIi<kkó3alVî^-òé;yô=[|ê
çA'ÜåUKoO(g¥Aj;ţ*"w)$èùAówÓ-* ŞÄ-L]\K_wéPzYŶpäTöÖç84#O+wÛ+YQKÔ: 'ĒG?Iµjt ·OÑÓóPc>Cyū']&¥ôùV\Ø+prJj«U¤ÄOPdRR*4Q("9D0xy<RÎ
IDSió]¤ETÖ*D(4Y5Ē(NJPD*4(jÁAxyLNYE'@,¥vő-nJeŐ
l¹-,ÂÜRðyJaLII'[60*eAúÉţ*]Üaè'èh'ÎYasBjţ7^Ê]OZÎNScos,?Üß-äöñ«EXŚsBJ{PÑ+mCioōÚç®]ä*jó®ÜoDPLLLL}ôjô}ô}ó}ó}ó}ó}ó}ó}ó}ó}ó}ójófájófæicJ%{ösE7ÆTöÿÄ/
012P!35@"$%46ÿÚýú½~~XRæ«42"~ÝøNäxæf3+"W£WÏ?NÜG§,úÈ622vî5R#2§557Û7ðÚçáèÐÒå;M:k¢ËT äÌ
ÖNŐO<HÑIk×¥Hd=48¢ÔA.² jHÑÉ-}þ|ü=ÿdÜ?þÖ.k/
æfUmÌMcö«³TþFhà,2Ê\YÚĒt¤óc>dÍÚ°±µSÛ°ðÛçáèÓ¥œM «â5Âu°åR9¬¶çë
4hh(vµðPr047SX¥òO,àiÊåkéÉ'Ý\pygldü|ùù|ý~ÀÏ?`g°3ÏÅDU_qÍN+Ýä¬AS**yø5[ÖùcLmåKJª«²få¶!=[øœSéòODlĶ´|[ñºœ<OëlÄÖúyðÑæ]lä¤E/_WuZý2e5|æ*äèe
!à.TÓÍÛ³-ems7l×^þ},ôîÆ,°£Êp[79F$í/ZÙ(··?
OFldÄ6@³\Dpn/bÆT°>!5}ñVERd¹fH|*D2!YbÊ(ÛòòA»4¿ä-§·KM*«ŐSd⊛,lÚòF««-%Y\LJ;Ok×XMEfÉ{OS.ÎãÚKUîiA£cÊ.j≪æ]Í6uőj#;¦¿"¹¨Àyl@Đü*Ë>e5$$çŐ2Ú÷+t
"ÑdÉ&]@d!MÒòÚ¹òÔϡùj^WòĔ(fĔÆ!+Oß 2>ø>\Ce+sK:y#ÍJ%I/sN_=I"Ä<Ó\<X׿:ìksÀÝYÉ{ÜG¹ïÔåFÉ<·±=pA·TIrç̺3æYó,zy WϡŚg¤s:1.
4{"êÂd82&¿h¬éz14ÁøŇKk> ì#(ÖDSE"°.ÆD`«¡2ϡ>Ì.ÖĖpwé=sR'ŌAÙSâI a²-ÂÁ#ÆøRPh,b+rE|V~SÈá¿]±-ϡŌ§3ºº«Ça
x-5»euÄä"¬
k8'Ä+mñÇp[+5ÉGB"5c·OĬú:+őFœÙcÊÛbÀ]_S[Á«[ËÇ(QrL»[ïyç¿ÀETòæS÷y¥Ï?^¬ælUWÏ÷Cêöú½>'``Àå@l\س'6.m\Ú³'6@l\س'±sbæÁÎZç-sìå;9NÎS°iä»9.ÎCñ;þNç
```

La terza slide ci mostra una richiesta POST che passa un'immagine di tipo jpg alla pagina di upload. Se il caricamento va a buon fine, dovrebbe uscire un avviso rosso come questo, contenente la parte di percorso che ci permette di accedere all'immagine.





Inserimento file .php

Inserendo il nostro file .php dentro upload, possiamo lanciare un attacco Cross scriping. Dopo averlo caricato con successo, possiamo eserguire comandi di varia natura, ad esempio ls(file presenti) oppure pwd(percorso Web server.





