

PROGETTO BONUS 2 S7L5

TRACCIA:

Effettuare una simulazione di un attacco al sito

<http://testphp.vulnweb.com/> passando da TOR.

Lo scopo dell'esercizio non è riuscire nell'attacco ma appunto attaccando dall'interno della rete TOR.

NOTA: attaccare il sito testphp.vulnweb.com è totalmente legale quindi non rischiate nulla, basta che non facciate un Ddos.

Per svolgere questo esercizio, utilizzerò proxychains, uno strumento che consente di indirizzare il traffico attraverso la rete TOR.

Per installarlo, basta eseguire il comando ***“sudo apt install proxychains”***:

```
francesco@kali:~$ sudo apt install proxychains
[sudo] password for francesco:
The following packages were automatically installed and are no longer required:
  ibverbs-providers libcephfs2 libgfxdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal
  libboost-iostreams1.83.0 libgfapi0 libglusterfs0 librados2 python3.11 samba-vfs-modules
  libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev
Use 'sudo apt autoremove' to remove them.

Installing:
  proxychains

Installing dependencies:
  libproxychains3

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1975
  Download size: 22.7 kB
  Space needed: 74.8 kB / 37.0 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libproxychains3 amd64 3.1-9+b2 [13.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 proxychains all 3.1-9 [9140 B]
Fetched 22.7 kB in 1s (34.9 kB/s)
Selecting previously unselected package libproxychains3:amd64.
(Reading database ... 404434 files and directories currently installed.)
Preparing to unpack .../libproxychains3_3.1-9+b2_amd64.deb ...
Unpacking libproxychains3:amd64 (3.1-9+b2) ...
Selecting previously unselected package proxychains.
Preparing to unpack .../proxychains_3.1-9_all.deb ...
Unpacking proxychains (3.1-9) ...
Setting up libproxychains3:amd64 (3.1-9+b2) ...
Setting up proxychains (3.1-9) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for libc-bin (2.38-13) ...
```

Una volta installato, posso procedere con la configurazione.

Per aprire il file di configurazione, utilizzo il seguente comando:

“`sudo nano /etc/proxychains.conf`”, successivamente scorro fino all’ultima riga, e come unica modifica cambio socks4 in socks5, salvo e chiudo il file.

Perché utilizzare il protocollo socks5?

Socks5 supporta l’autenticazione, è più sicuro e può gestire il traffico UDP, mentre socks4 è più vecchio e limitato.

```
File Actions Edit View Help
GNU nano 8.2 /etc/proxychains.conf
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

# Proxy DNS requests - no leak for DNS data
proxy_dns

# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
# type host port [user pass]
# (values separated by 'tab' or 'blank')
#
# Examples:
# socks5 192.168.67.78 1080 lamer secret
# http 192.168.89.3 8080 justu hidden
# socks4 192.168.1.49 1080
# http 192.168.39.93 8080
#
# proxy types: http, socks4, socks5
# ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 9050
```

Dopo aver installato e configurato nikto, procedo con l’installazione di tor:

```
francesco@kali: ~  
File Actions Edit View Help  
  
(francesco@kali)-[~]  
$ sudo apt install tor  
The following packages were automatically installed and are no longer required:  
  ibverbs-providers libcephfs2 libgfxdr0 libpython3.11-dev python3-lib2to3 python3.11-minimal  
  libboost-iostreams1.83.0 libgfs2 libglusterfs0 librados2 python3.11 samba-vfs-modules  
  libboost-thread1.83.0 libgfrpc0 libibverbs1 librdmacm1t64 python3.11-dev  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
  tor  
  
Installing dependencies:  
  tor-geoipdb torsocks  
  
Suggested packages:  
  mixmaster torbrowser-launcher apparmor-utils nylx obfs4proxy  
  
Summary:  
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 1975  
  Download size: 4541 kB  
  Space needed: 26.3 MB / 37.0 GB available  
  
Continue? [Y/n] y  
Get:2 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.8.13-2 [2414 kB]  
Get:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 tor amd64 0.4.8.13-2 [2053 kB]  
Get:3 http://kali.mirror.garr.it/kali kali-rolling/main amd64 torsocks amd64 2.4.0-2 [74.4 kB]  
Fetched 4541 kB in 2s (2483 kB/s)  
Selecting previously unselected package tor.  
(Reading database ... 404450 files and directories currently installed.)  
Preparing to unpack .../tor_0.4.8.13-2_amd64.deb ...  
Unpacking tor (0.4.8.13-2) ...  
Selecting previously unselected package tor-geoipdb.  
Preparing to unpack .../tor-geoipdb_0.4.8.13-2_all.deb ...  
Unpacking tor-geoipdb (0.4.8.13-2) ...  
Selecting previously unselected package torsocks.  
Preparing to unpack .../torsocks_2.4.0-2_amd64.deb ...  
Unpacking torsocks (2.4.0-2) ...  
Setting up tor (0.4.8.13-2) ...  
Something or somebody made /var/lib/tor disappear.  
Creating one for you again.  
Something or somebody made /var/log/tor disappear.  
Creating one for you again.
```

Successivamente avvio il servizio tor con il comando “**sudo service tor start**” e subito dopo controllo il suo stato con il comando “**sudo service tor status**”:

```
(francesco@kali)-[~]  
$ sudo service tor start  
  
(francesco@kali)-[~]  
$ sudo service tor status  
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)  
   Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)  
   Active: active (exited) since Fri 2025-01-24 12:43:11 CET; 7s ago  
  Invocation: bf372f2a970b4194a75de0bde3c2423d  
    Process: 9929 ExecStart=/bin/true (code=exited, status=0/SUCCESS)  
   Main PID: 9929 (code=exited, status=0/SUCCESS)  
  
Jan 24 12:43:10 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master) ...  
Jan 24 12:43:11 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).  
  
(francesco@kali)-[~]  
$
```

Possiamo vedere che lo stato è “active”.

È arrivato il momento di testare Proxychains con Tor e verificarne il funzionamento.

Per farlo, utilizzo il comando “**proxychains curl** <https://checktorproject.org>”:

```
(francesco@kali)-[~]
$ proxychains curl https://check.torproject.org
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:9050 ... check.torproject.org:443 ... OK
<!doctype html>
<html lang="en_US">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>

    Congratulations. This browser is configured to use Tor.

</title>
<link rel="icon" type="image/x-icon" href="/torcheck/img/tor-not.png" />
<style>
  html { height: 100%; }
  body {
    height: 100%;
    text-align: center;
    font-family: Helvetica, sans-serif;
```

Si può intuire che la prova è andata a buon fine per aver ricevuto la risposta “**Congratulations. This browser is configured to use Tor**”.

Ora che tutto è pronto, posso utilizzare Nikto per scansionare il sito <http://testphp.vulnweb.com/> passando dalla rete TOR.

Utilizzerò il seguente comando: “**proxychains nikto -h** <http://testphp.vulnweb.com/>”.

Proxychains: reindirizza il traffico attraverso TOR

Nikto: avvia Nikto

-h: specifica l’host da scansionare (in questo caso, testphp.vulnweb.com).

Vediamo quindi qual è il risultato della scansione:

```
(francesco@kali)-[~]
$ proxychains nikto -h http://testphp.vulnweb.com/
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
- Nikto v2.5.0

[proxychains] Strict chain ... 127.0.0.1:9050 ... testphp.vulnweb.com:80 ... OK
+ Target IP: 224.0.0.1
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2025-01-24 12:47:35 (GMT1)

+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
[proxychains] Strict chain ... 127.0.0.1:9050 ... testphp.vulnweb.com:80 ... OK

[proxychains] Strict chain ... 127.0.0.1:9050 ... testphp.vulnweb.com:80 ... OK
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-01-24 12:50:11 (GMT1) (156 seconds)

+ 1 host(s) tested
documento
(francesco@kali)-[~]
```

Mi accorgo però, che alla fine della scansione vengono riportati degli, e dopo 20 errori Nikto interrompe la scansione.

Per provare ad ottenere una scansione migliore, ho provato ad aumentare il timeout, quindi il tempo di attesa di Nikto per ricevere una risposta dal server, utilizzando il flag “**-timeout**”.

Nell'immagine sopra, infatti, possiamo notare alcuni particolari come:

Server: nginx/1.19.0

Header mancanti:

- X-frame-options, la mancanza di questo header consente attacchi di clickjacking.
- X-Content-type-options, la sua assenza potrebbe permettere MIME sniffing.

Questi sono degli esempi delle vulnerabilità che ci fornisce Nikto dopo la scansione.

Conclusioni:

Nikto non esegue attacchi attivi, ma segnala possibili punti deboli.

Con l'output ricevuto possiamo eseguire un'**analisi del rischio**, ulteriori **test**, **documentare i risultati** elencando le **vulnerabilità** e le **misure correttive**.