# SMB & NetBIOS

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos

# Server Message Block (SMB)

**Server Message Block** (**SMB**) is a communication protocol[1] that Microsoft created for providing shared access to files and printers across nodes on a network. It also provides an authenticated inter-process communication (IPC) mechanism. Microsoft first implemented SMB in the LAN Manager operating system, at which time SMB used the NetBIOS protocol as its underlying transport. Later, Microsoft implemented SMB in Windows NT 3.1 and has been updating it ever since, adapting it

هو بروتكول يتيح للمستخدمين انهم يتصلوا مع سيرفر بغرض فتح ومشاركه وتعديل ملفات ومبني علي مبدأ CLIENT & SERVER

يعني ايه المبدأ دا ؟

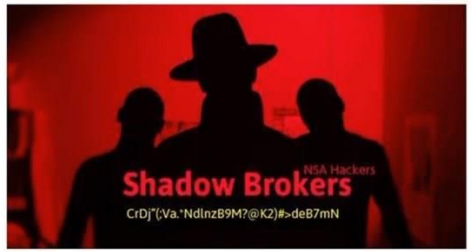
يعني السيرفر بيكون عنده الفايل ال بيعمله SHARE والناس تعمل Connect عليه وتستخدام هذا الفايل ويكونوا هما Client زي Dropbox

SMB ليه إصدارات كتيره ومهم جدا تحديد نوع الإصدار ال شغال علي Target Machine

* Vulnerability الموجوده في SMBv1 أحيانا تسمي EternalBlue

المعلومات ال بقدر استخرجها من SMB أسماء المستخدمين والدومين والطابعات والملفات المتاحة ال معمول لها SHARE ودي بتكون حاجات موجوده بداخل السيستم ومهم جدا اننا نجمعها

**EternalBlue**, sometimes stylized as **ETERNALBLUE**, is an exploit generally believed to have been developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on 14 April 2017, and was used as part of the worldwide WannaCry ransomware attack on 12 May 2017.




https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://support.kaspersky.com/general/products/13698

**Microsoft Security Bulletin MS17-010 - Critical**
**Security Update for Microsoft Windows SMB Server**

Published: March 14, 2017

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

16

SMB بيشتغل علي بروتكول 445/TCP

اما NetBIOS بيشتغل نفس وظيفة SMB لكن بالنسبه لل NetBIOS بيكون متوزع وشغال ء
137/UDP خاص ب NAME SERVICE
138/UDP خاص ب DATAGRAM SERVICE
139/TCP ماسك Session الخاص ب service دي

فاحنا هنركز علي 139/TCP الخاص ب NetBIOS و 445/TCP الخاص ب SMB

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

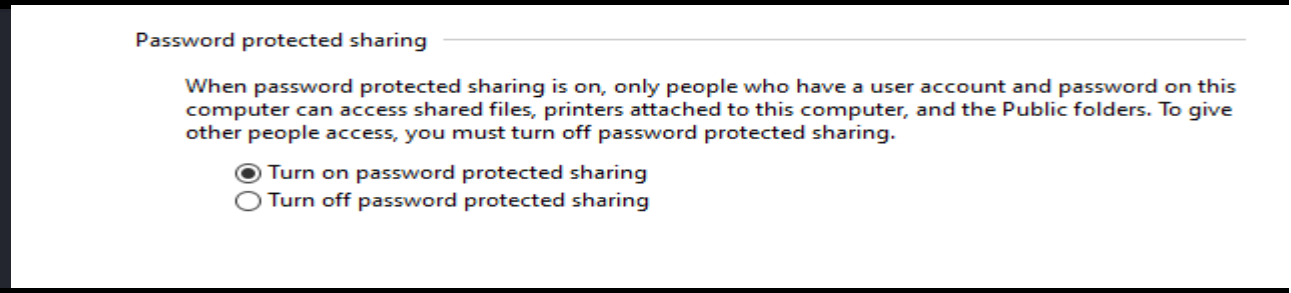
**GitHub** : https://github.com/0xDos

```
┌──(kali㉿kali)-[~]
└─$ sudo nbtscan -r 192.168.1.0/24 -vv
Doing NBT name scan for addresses from 192.168.1.0/24

NetBIOS Name Table for Host 192.168.1.2:

Incomplete packet, 155 bytes long.
Name                Service            Type
---------------------------------------------
MYPC                <20>               UNIQUE
MYPC                <00>               UNIQUE
WORKGROUP           <00>                GROUP

Adapter address: 3c:d9:2b:49:d5:f3
---------------------------------------------

NetBIOS Name Table for Host 192.168.1.10:

Incomplete packet, 48 bytes long.
Name                Service            Type
---------------------------------------------
---------------------------------------------

NetBIOS Name Table for Host 192.168.1.30:

Incomplete packet, 335 bytes long.
Name                Service            Type
---------------------------------------------
METASPLOITABLE      <00>               UNIQUE
METASPLOITABLE      <03>               UNIQUE
METASPLOITABLE      <20>               UNIQUE
METASPLOITABLE      <00>               UNIQUE
METASPLOITABLE      <03>               UNIQUE
METASPLOITABLE      <20>               UNIQUE
__MSBROWSE__   <01>                  GROUP
WORKGROUP           <00>                GROUP
WORKGROUP           <1d>               UNIQUE
WORKGROUP           <1e>                GROUP
WORKGROUP           <00>                GROUP
WORKGROUP           <1d>               UNIQUE
WORKGROUP           <1e>                GROUP

Adapter address: 00:00:00:00:00:00
---------------------------------------------
192.168.1.255    Sendto failed: Permission denied
```

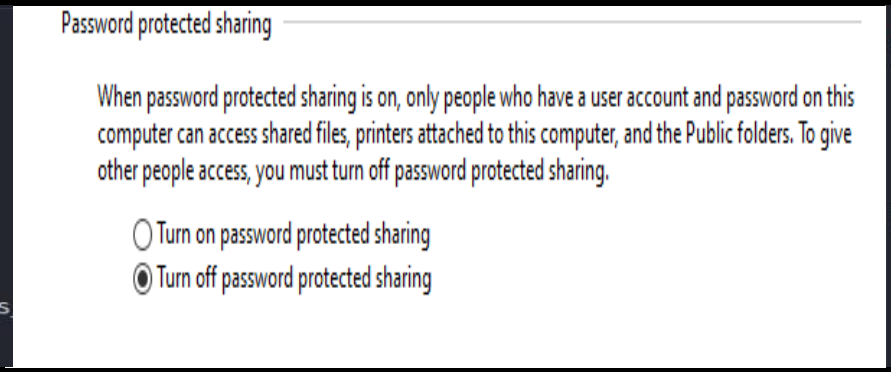
- nbtscan

# • Smbclient

```
┌──(kali㉿kali)-[~]
└─$ smbclient  -L 192.168.1.2
Enter WORKGROUP\kali's password:
session setup failed: NT_STATUS_ACCESS_DENIED
```




```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 192.168.1.2
Enter WORKGROUP\kali's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        data            Disk
        E$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.1.2 failed (Error NT_STATUS
Unable to connect with SMB1 -- no workgroup available
```




```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 192.168.1.30
Enter WORKGROUP\kali's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient  //192.168.1.2/users
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Mon Dec
  ..                                  DR        0  Mon Dec
  Default                            DHR        0  Thu Apr
  desktop.ini                        AHS      174  Sat Dec
  Public                              DR        0  Thu Apr

                26216109 blocks of size 4096. 12609535 blo
smb: \>
```

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos

# • Smbmap & enum4linux

```
┌──(kali㉿kali)-[~]
└─$ sudo smbmap -H 192.168.1.2 -u ahmed
[+] Guest session       IP: 192.168.1.2:445     Name: unknown
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        data                                                    READ, WRITE
        E$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        Users                                                   READ ONLY
```

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo enum4linux 192.168.1.30
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.30
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on 192.168.1.30            |
 ============================================================
[+] Got domain/workgroup name: WORKGROUP

 =====================================================
|    Nbtstat Information for 192.168.1.30             |
 =====================================================
Looking up status of 192.168.1.30
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ===================================================
|    Session Check on 192.168.1.30                  |
 ===================================================
[+] Server 192.168.1.30 allows sessions using username '', password ''

 ===================================================
|    Getting domain SID for 192.168.1.30            |
 ===================================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ================================================
|    OS information on 192.168.1.30              |
 ================================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl l
[+] Got OS info for 192.168.1.30 from smbclient:
[+] Got OS info for 192.168.1.30 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03

 ==========================
|    Users on 192.168.1.30 |
 ==========================
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games     Desc: (null)
```

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos

# • Nmap SMB NSE Scripts

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  192.168.1.17 -sV -p T:445,139 U:137 --script="smb-enum-*" --script-args=user=ahmed

Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-02 08:18 EST
Failed to resolve "U:137".
Failed to resolve "U:137".
Nmap scan report for 192.168.1.17
Host is up (0.00042s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: ABC)
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:BE:C6:21 (VMware)
Service Info: Host: CLIENT7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.1.17\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.1.17\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.1.17\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\192.168.1.17\USERS:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: <none>

Failed to resolve "U:137".
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  192.168.1.17 -sV -p T:445,139 --script="smb-os-discovery.nse" --script-args=user=ahmed
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-02 08:24 EST
Nmap scan report for 192.168.1.17
Host is up (0.00041s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: ABC)
MAC Address: 00:0C:29:BE:C6:21 (VMware)
Service Info: Host: CLIENT7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: client7-PC
|   NetBIOS computer name: CLIENT7-PC\x00
|   Workgroup: ABC\x00
|_  System time: 2022-02-02T15:25:04+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.78 seconds
```

"smb-enum-*" معناها جرب جميع Scripts

*ممكن اطبق نفس script ولكن بدل "smb-enum-*" هيكون "smb-vuln-*

ودا هيشوف ايه exploit المتاحة علي service دي

* لو مش عارف script دا وظيفته ايه وبيعمل ايه وازاي استخدمه اكتبله

الامر دا <<< nmap --script-help scriptname

LinkedIn : https://www.linkedin.com/in/mohamed-elsayaad

GitHub : https://github.com/0xDos

# What is NetBIOS?

NetBIOS stands for **Net**work **B**asic **I**nput **O**utput **S**ystem.
IBM developed it along with Sytek.

**The primary intention of NetBIOS** was developed as Application Programming Interface (API) to enable access to LAN resources by the client's software.

NetBIOS naming convention starts with 16-ASCII character string used to identify the network devices over TCP/IP; 15-characters are used for the device name, and the 16th character is reserved for the service or name record type.

NetBIOS software runs on port 139 on Windows operating system.
File and printer service needs to be enabled to enumerate NetBIOS over Windows Operating system.

**NetBIOS Enumeration Tools:**

The following table shows the list of tools to perform NetBIOS Enumeration:

| Sl.no | Name of the tool | Web Links |
|---|---|---|
| 01 | Nbtstat | www.technet.microsoft.com |
| 02 | SuperScan | http://www.mcafee.com/in/downloads/free-tools/superscan.aspx |
| 03 | Hyena | http://www.systemtools.com/hyena/ |
| 04 | Winfingerprint | https://packetstormsecurity.com/files/38356/winfingerprint-0.6.2.zip.html |
| 05 | NetBIOS enumerator | http://nbtenum.sourceforge.net/ |

# NetBIOS Enumeration

NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP, 15 characters are used for the device name and 16th character is reserved for the service or name record type


**Attackers use the NetBIOS enumeration to obtain:**

- List of computers that belong to a domain
- List of shares on the individual hosts in the network
- Policies and passwords

### NetBIOS Name List

| Name | NetBIOS Code | Type | Information Obtained |
|---|---|---|---|
| <host name> | <00> | UNIQUE | Hostname |
| <domain> | <00> | GROUP | Domain name |
| <host name> | <03> | UNIQUE | Messenger service running for that computer |
| <username> | <03> | UNIQUE | Messenger service running for that individual logged-in user |
| <host name> | <20> | UNIQUE | Server service running |
| <domain> | <1D> | GROUP | Master browser name for the subnet |
| <domain> | <1B> | UNIQUE | Domain master browser name, identifies the PDC for that domain |

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

# NetBIOS Enumeration

### NetBIOS Name List

| Name | NetBIOS Code | Type | Information Obtained |
|---|---|---|---|
| <host name> | <00> | UNIQUE | Hostname |
| <domain> | <00> | GROUP | Domain name |
| <host name> | <03> | UNIQUE | Messenger service running for that computer |
| <username> | <03> | UNIQUE | Messenger service running for that individual logged-in user |
| <host name> | <20> | UNIQUE | Server service running |
| <domain> | <1D> | GROUP | Master browser name for the subnet |
| <domain> | <1B> | UNIQUE | Domain master browser name, identifies the PDC for that domain |

**nbtstat -a 10.1.1.1**

<20> UNIQUE this machine running file server services
<00> UNIQUE this machine running workstation services
<00> Group this is the name od domain
<1c> Group this machine run IIS

<1b> UNIQUE this machine run master browser OS , so its AD DS

https://support.microsoft.com/en-us/kb/163409

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos

# NetBIOS Enumeration (Cont'd)

Nbtstat utility in Windows displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache

Run **nbtstat** command "**nbstat.exe -c**" to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses


Run **nbtstat** command "**nbtstat.exe -a <IP address of the remote machine>**" to get the NetBIOS name table of a remote computer

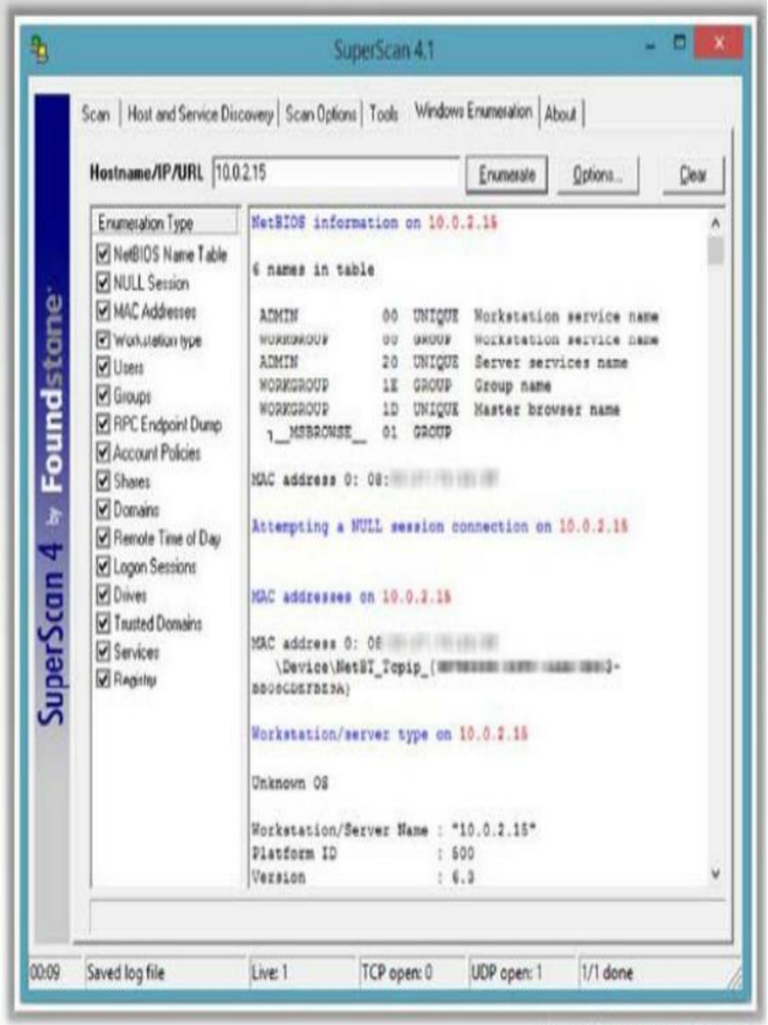

http://technet.microsoft.com

# NetBIOS Enumeration Tool: SuperScan

SuperScan is a connect-based TCP port scanner, pinger, and hostname resolver

**Features:**

1. Support for unlimited IP ranges
2. Host detection by multiple ICMP methods
3. TCP SYN and UDP scanning
4. Simple HTML report generation
5. Source port scanning
6. Hostname resolving
7. Banner grabbing
8. Windows host enumeration



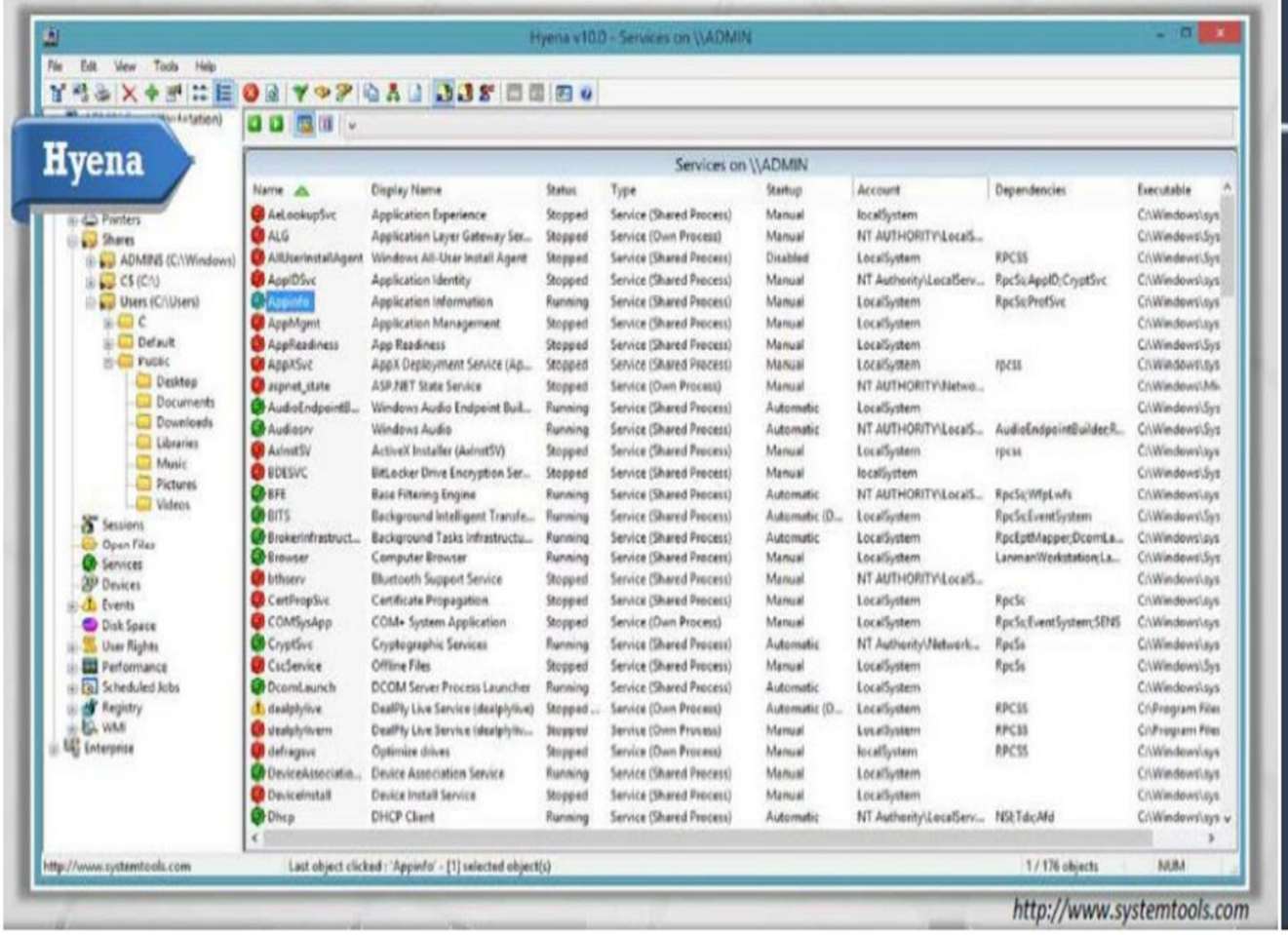

http://www.mcafee.com

**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos

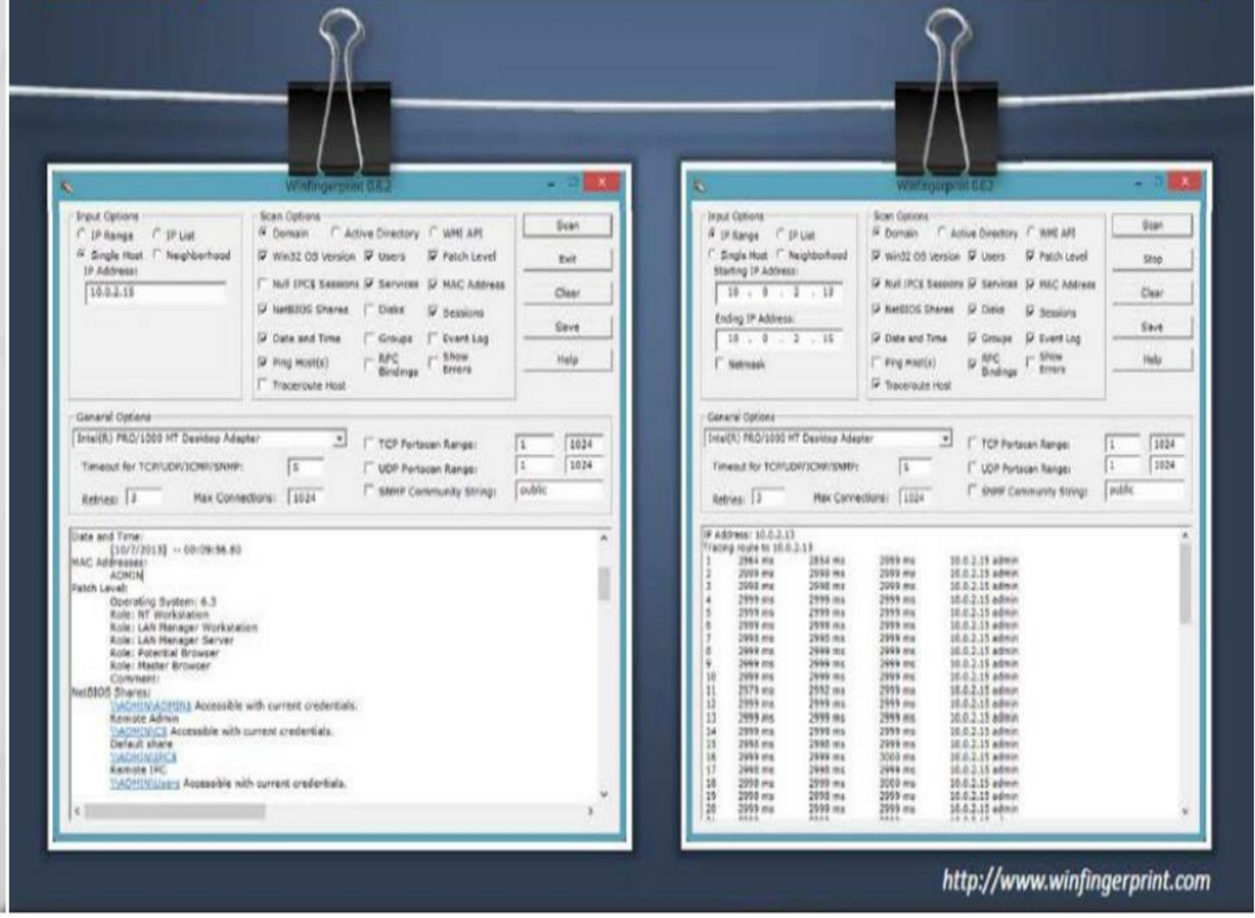
# NetBIOS Enumeration Tool: Hyena

- Hyena is a GUI product for managing and securing **Microsoft operating systems**. It shows **shares** and **user logon names** for Windows servers and domain controllers
- It displays **graphical representation** of Microsoft Terminal Services, Microsoft Windows Network, Web Client Network, etc.



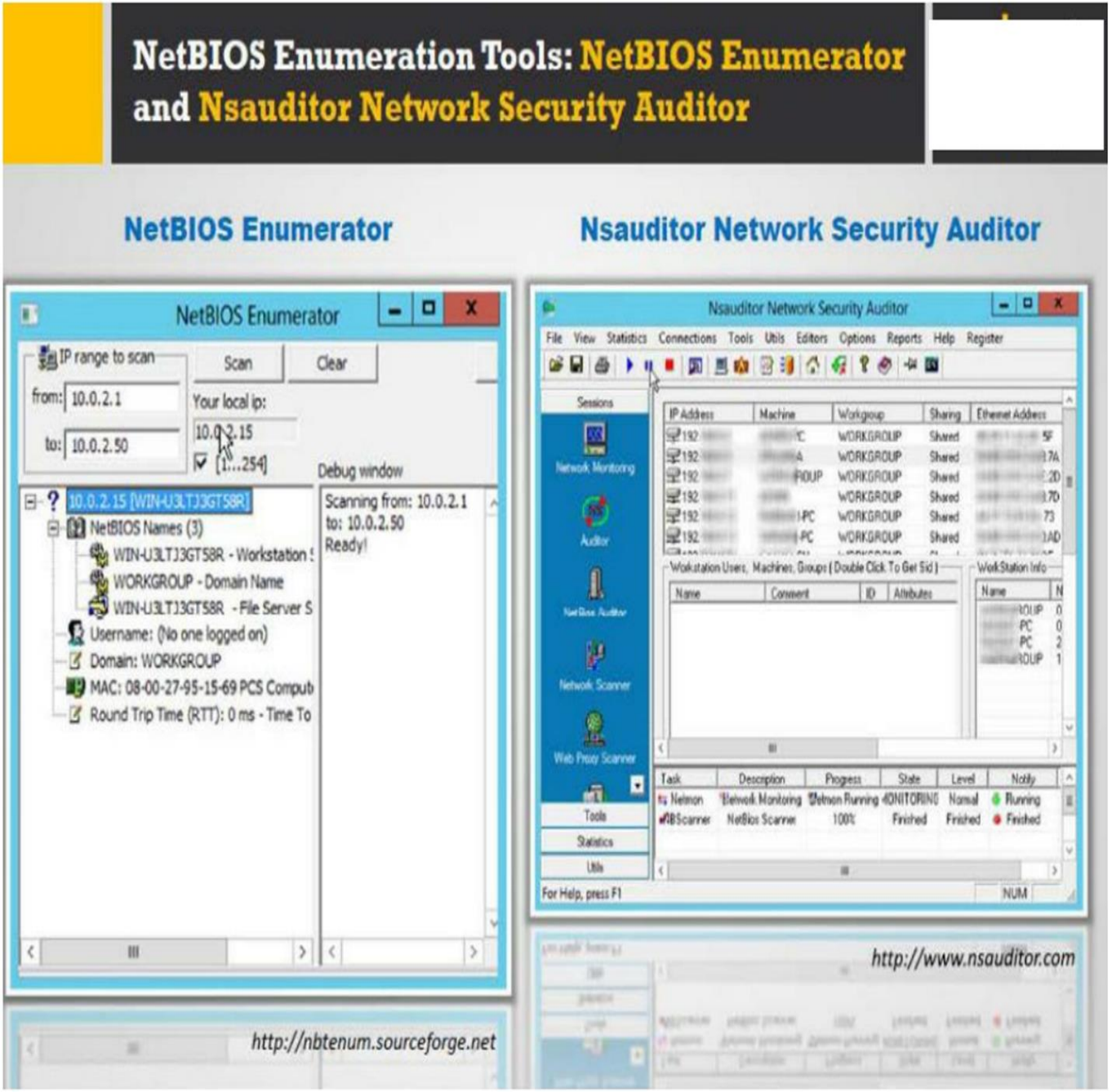

# NetBIOS Enumeration Tool: Winfingerprint

Winfingerprint determines OS, **enumerate users**, **groups**, **shares**, **SIDs**, **transports**, **sessions**, **services**, service pack and hotfix level, date and time, disks, and open TCP and UDP ports




**LinkedIn** : https://www.linkedin.com/in/mohamed-elsayaad

**GitHub** : https://github.com/0xDos




**netbios from kali**

nbtscan -v -s : 192.168.3.0/24

note:
00U is workstation
00G is domain name

20U is file server service

nbtscan -rv 192.168.159.12

**Using nmap in enumeration**

nmap --script smb-os-discovery 192.168.3.12
nmap --script smb-enum-users 192.168.3.129