

## Installing NetBIOS Enumerator.

NetBIOS is an acronym that stands for Network Basic Input Output System. It enables computer communication over a LAN and the sharing of files and printers. TCP/IP network devices are identified using NetBIOS names (Windows). It must be network-unique and limited to 16 characters, with 15 reserved for the device name and the 16th reserved for identifying the type of service running or name record type.

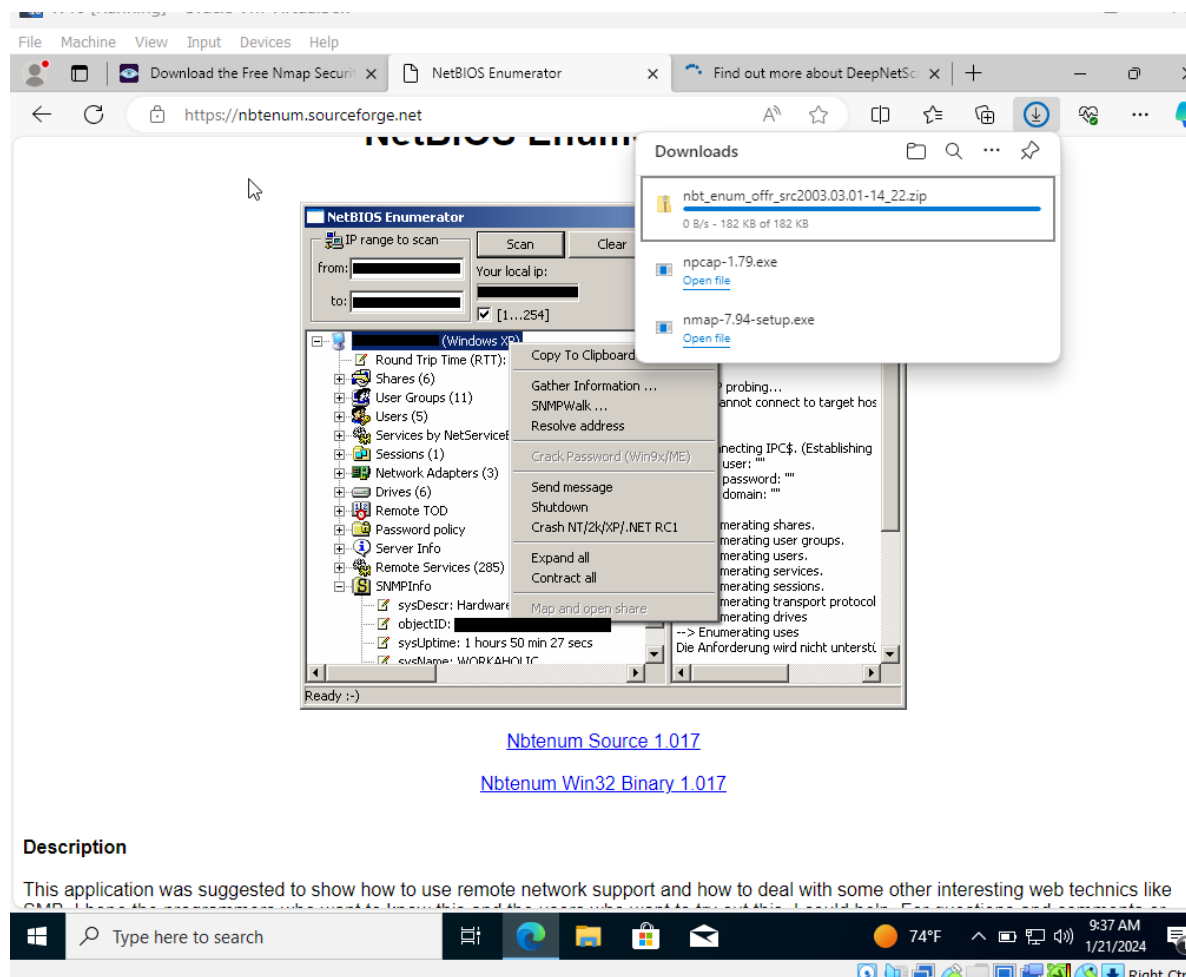
## Uses of NetBIOS Enumeration:

An attacker who discovers a Windows OS with port 139 open can investigate what resources are accessible or viewable on the remote system. To enumerate the NetBIOS names, the remote system must have file and printer sharing enabled. Depending on the availability of shares, NetBIOS enumeration may allow an attacker to read or write to the remote computer system or launch a (Dos).

## NetBIOS Enumeration Tools:

NetBIOS's enumeration tools explore and scan the network for security loopholes or flaws in networked systems within a given range of IP addresses and computer lists. In addition, these tools list the operating system, users, password policies, groups, service packs and hotfixes, services, NetBIOS shares, discs, transmits, sessions, SIDs and security event logs.

Reference: <https://www.geeksforgeeks.org/what-is-netbios-enumeration/>



## Installing Active Directory Explorer

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. You can use AD Explorer to easily navigate an AD database, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that you can save and re-execute.

AD Explorer also includes the ability to save snapshots of an AD database for off-line viewing and comparisons. When you load a saved snapshot, you can navigate and explore it as you would a live database. If you have two snapshots of an AD database you can use AD Explorer's comparison functionality to see what objects, attributes and security permissions changed between them.

**Note: installed the software in Windows 10 Added to the Domain. Checked the following: Computers, Users, Domain Zones, Forests.**

File Machine View Input Devices Help

Active Directory Explorer - Sysinternals: www.sysinternals.com [192.168.32.3 [om.code.academy.om]]

File Edit Favorites Search Compare History Help

Path: CN=Computers,DC=code,DC=academy,DC=om,192.168.32.3 [om.code.academy.om]

Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	Computers
description	DirectoryString	1	Default container for upgraded computer accounts
distinguishedName	DN	1	CN=Computers,DC=code,DC=academy,DC=om
dSCorePropagationData	GeneralizedTime	5	1/21/2024 12:36:02 PM; 1/21/2024 12:34:40 PM; 1/21/2024 10:02:52 AM; 1/15/2024 10:00:44 PM; 7/14/1601 3:53:56 PM
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
name	DirectoryString	1	Computers
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPLOCRRRCWDWO;;;DA)(OA;;CCDC;bf967a86-0de6-11d0-a285-00aa003049e2;;AO)(O...
objectCategory	DN	1	CN=Container,CN=Schema,CN=Configuration,DC=code,DC=academy,DC=om
objectClass	OID	2	top;container
objectGUID	OctetString	1	{92255CBF-3309-4793-A2E1-7D6A5707B9CF}
showInAdvancedViewO...	Boolean	1	FALSE
systemFlags	Integer	1	-1946157056
uSNCChanged	Integer8	1	0x161D
uSNCreated	Integer8	1	0x161D
whenChanged	GeneralizedTime	1	1/15/2024 9:59:05 PM
whenCreated	GeneralizedTime	1	1/15/2024 9:59:05 PM



Path: CN=Reem Al Marzooqi,CN=Users,DC=code,DC=academy,DC=om,192.168.32.3 [om.code.academy.om]

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
badPasswordTime	Integer8	1	1/21/2024 9:35:42 PM
badPwdCount	Integer	1	0
cn	DirectoryString	1	Reem Al Marzooqi
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Reem Al Marzooqi
distinguishedName	DN	1	CN=Reem Al Marzooqi,CN=Users,DC=code,DC=academy,DC=om
dSCorePropagationData	GeneralizedTime	3	1/21/2024 12:36:04 PM; 1/21/2024 10:02:52 AM; 1/1/1601 12:04:21 AM
givenName	DirectoryString	1	Reem
instanceType	Integer	1	4
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	1/22/2024 8:50:08 AM
lastLogonTimestamp	Integer8	1	1/15/2024 11:59:45 PM
logonCount	Integer	1	13
name	DirectoryString	1	Reem Al Marzooqi
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;RS)(OA;;RP;5f202010-79a5-11d0-9020-00c04fc2d4cf;RS)(OA;;bc0ac240-79a9-11d0-9020-00c04f...
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=code,DC=academy,DC=om
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{05FF7CD0-953A-4588-81F5-8BE3B1569EB4}
objectSid	Sid	1	S-1-5-21-1490393355-2737541710-1442272815-1106
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	1/16/2024 12:00:29 AM
sAMAccountName	DirectoryString	1	reemalmarzooqi
sAMAccountType	Integer	1	805306368
sn	DirectoryString	1	Al Marzooqi
userAccountControl	Integer	1	512
userPrincipalName	DirectoryString	1	reemalmarzooqi@code.academy.om
uSNChanged	Integer8	1	0x3233
uSNCreated	Integer8	1	0x321D
whenChanged	GeneralizedTime	1	1/16/2024 12:00:29 AM
whenCreated	GeneralizedTime	1	1/15/2024 11:10:10 PM

CN=Reem Al Marzooqi,CN=Users,DC=code,DC=academy,DC=om,192.168.32.3 [om.code.academy.om]

Path: DC=DomainDnsZones,DC=code,DC=academy,DC=om,192.168.32.3 [om.code.academy.om]

Attribute	Syntax	Count	Value(s)
dc	DirectoryString	1	DomainDnsZones
description	DirectoryString	1	Microsoft DNS Directory
distinguishedName	DN	1	DC=DomainDnsZones,DC=code,DC=academy,DC=om
dSA_Signature	OctetString	1	1 0 0 0 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 110 152 208 251 95 124 113 70 144 81 203 30 235 216 123 79
dSCorePropagationData	GeneralizedTime	2	1/21/2024 12:36:04 PM; 1/1/1601 12:00:04 AM
instanceType	Integer	1	13
msDs-masteredBy	DN	1	CN=NTDS Settings,CN=OM,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=code,DC=academy,DC=om
msDS-NCType	Integer	1	0
name	DirectoryString	1	DomainDnsZones
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e...
objectCategory	DN	1	CN=Domain-DNS,CN=Schema,CN=Configuration,DC=code,DC=academy,DC=om
objectClass	OID	3	top;domain;domainDNS
objectGUID	OctetString	1	{94D93B74-943E-4F72-830A-033D50E758B4}
uSNChanged	Integer8	1	0x3211
uSNCreated	Integer8	1	0x313A
wellKnownObjects	ORName	4	98 39 240 175 31 194 65 13 142 59 177 6 21 187 91 15, CN=NTDS Quotas,DC=DomainDnsZones,DC=code,DC=academy,DC=om;47 186 193 135 10 222 17 21...
whenChanged	GeneralizedTime	1	1/15/2024 11:00:53 PM
whenCreated	GeneralizedTime	1	1/15/2024 10:09:33 PM

Path: DC=ForestDnsZones,DC=code,DC=academy,DC=om,192.168.32.3 [om.code.academy.om]

Attribute	Syntax	Count	Value(s)
dc	DirectoryString	1	ForestDnsZones
description	DirectoryString	1	Microsoft DNS Directory
distinguishedName	DN	1	DC=ForestDnsZones,DC=code,DC=academy,DC=om
dSA_Signature	OctetString	1	1 0 0 0 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 110 152 208 251 95 124 113 70 144 81 203 30 235 216 123 79
dSCorePropagationData	GeneralizedTime	2	1/21/2024 12:36:04 PM; 1/1/1601 12:00:04 AM
instanceType	Integer	1	13
msDs-masteredBy	DN	1	CN=NTDS Settings,CN=OM,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=code,DC=academy,DC=om
msDS-NCType	Integer	1	0
name	DirectoryString	1	ForestDnsZones
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;CIIO;RP;4c164200-20c0-11d0-a768-00aa006e...
objectCategory	DN	1	CN=Domain-DNS,CN=Schema,CN=Configuration,DC=code,DC=academy,DC=om
objectClass	OID	3	top;domain;domainDNS
objectGUID	OctetString	1	{2C48DC7E-4AA9-499C-B08B-879BC00F3C8E}
uSNChanged	Integer8	1	0x3212
uSNCreated	Integer8	1	0x3150
wellKnownObjects	ORName	4	98 39 240 175 31 194 65 13 142 59 177 6 21 187 91 15, CN=NTDS Quotas,DC=ForestDnsZones,DC=code,DC=academy,DC=om;47 186 193 135 10 222 17 210 ...
whenChanged	GeneralizedTime	1	1/15/2024 11:00:53 PM
whenCreated	GeneralizedTime	1	1/15/2024 10:09:33 PM