Lab Manual: Windows Network Security Commands and Tools

Introduction

This lab manual focuses on Windows network security commands and tools available in the Command Prompt (CMD) that are used to monitor, troubleshoot, and secure Windows networks. Each section provides a brief introduction to the command or tool, followed by practical exercises to help you understand how to use it.

Lab Objectives

- Learn how to use various Windows CMD commands and tools to monitor and secure network traffic.
- Understand basic network troubleshooting techniques.
- Perform network configuration and security tasks.

Lab 1: Basic Network Commands

1.1 ipconfig

ipconfig is used to display and manage the IP configuration of a computer's network interfaces.

Exercise:

1. Open CMD as an Administrator.
2. Run the following command to view the network configuration:

```
ipconfig /all
```

   - This shows detailed information such as IP addresses, DNS servers, MAC addresses, etc.

Tasks:

- Identify the IP address of your network interface.
- Check whether DHCP is enabled or not.
- Find the MAC address of your computer.

1.2 ping

ping is used to test connectivity between devices on a network.

Exercise:

1. Use ping to check the connectivity between your machine and Google's DNS server:

   ```
   ping 8.8.8.8
   ```

2. To ping continuously, use:

   ```
   ping 8.8.8.8 -t
   ```

Tasks:

- Test connectivity to your default gateway.
- Test connectivity to an external IP address (e.g., www.google.com).

1.3 tracert

tracert (Trace Route) shows the path packets take to reach a specific IP address or hostname.

Exercise:

1. Use tracert to trace the route to Google's server:

   ```
   tracert www.google.com
   ```

Tasks:

- Analyze how many hops it takes to reach Google.
- Identify if there are any network issues in the path.

1.4 nslookup

nslookup is used for querying the DNS to obtain domain name or IP address mapping.

Exercise:

1. Use nslookup to find the IP address of a domain:

   ```
   nslookup www.microsoft.com
   ```

Tasks:

- Query DNS to find IP addresses of other websites.
- Change the default DNS server to 8.8.8.8 and check the resolution speed.

Lab 2: Network Configuration and Monitoring

2.1 netstat

netstat displays network statistics, including all active connections and listening ports.

Exercise:

1. View all active TCP connections:

   ```
   netstat -an
   ```

2. Check which applications are using specific network connections:

   ```
   netstat -b
   ```

Tasks:

- Identify all active TCP/UDP connections.
- List applications listening on open ports.

2.2 netsh

netsh is a powerful command-line scripting utility that allows you to display or modify the network configuration.

Exercise:

1. View the current network interface configuration:

   ```
   netsh interface ip show config
   ```

2. Change the IP address of a network adapter:

   ```
   netsh interface ip set address "Local Area Connection" static 192.168.1.100
   255.255.255.0 192.168.1.1
   ```

Tasks:

- View wireless network profiles on your machine:

  ```
  netsh wlan show profiles
  ```

2.3 route

route allows you to manipulate the routing table.

Exercise:

1. Display the current routing table:

   ```
   route print
   ```

2. Add a new static route:

   ```
   route add 10.0.0.0 mask 255.0.0.0 192.168.1.1
   ```

Tasks:

- View the system's routing table.
- Add and then delete a route.

Lab 3: Security Monitoring and Defense

3.1 net user

net user allows you to manage user accounts on the machine.

Exercise:

1. View all user accounts:

   ```
   net user
   ```

2. Create a new user account:

   ```
   net user JohnDoe Pa$$w0rd /add
   ```

3. Add the user to the Administrators group:

```
net localgroup Administrators JohnDoe /add
```

Tasks:

- Create and delete a user account.
- Change the password of an existing user.

3.2 net share

net share is used to create and manage shared folders on a network.

Exercise:

1. View all network shares:

```
net share
```

2. Create a new shared folder:

```
net share Documents=C:\Documents
```

Tasks:

- List all the shared folders on your system.
- Create a shared folder and test network access to it.

3.3 net session

net session lists or disconnects sessions with your local computer.

Exercise:

1. View all active sessions:

```
net session
```

Tasks:

- Identify all users connected to your machine over the network.

3.4 tasklist and taskkill

tasklist shows all running processes, while taskkill terminates them.

Exercise:

1. List all running processes:

```
tasklist
```

2. Kill a process using its PID:

```
taskkill /PID <PID> /F
```

Tasks:

- List all running processes and identify network-intensive ones.
- Use taskkill to stop a specific process.

Lab 4: Windows Firewall and Defender

4.1 netsh advfirewall

This command is used to configure Windows Firewall settings.

Exercise:

1. View the status of the Windows Firewall:

```
netsh advfirewall show allprofiles
```

2. Block a specific port (e.g., 8080):

```
netsh advfirewall firewall add rule name="Block Port 8080" protocol=TCP dir=in
localport=8080 action=block
```

Tasks:

- Block and unblock specific ports on your machine.
- View all firewall rules configured on your system.

4.2 MpCmdRun (Windows Defender)

MpCmdRun.exe is a command-line utility for Windows Defender Antivirus.

Exercise:

1. Run a quick scan using Windows Defender:

   ```
   "%ProgramFiles%\Windows Defender\MpCmdRun.exe" -Scan -ScanType 1
   ```

2. Update Defender’s definitions:

   ```
   "%ProgramFiles%\Windows Defender\MpCmdRun.exe" -SignatureUpdate
   ```

Tasks:

- Run different types of scans (quick, full).
- Update the Defender definitions and verify they are current.

Lab 5: Advanced Network Security

5.1 netdom

netdom is used for managing domains, trust relationships, and workstations in a domain.

Exercise:

1. Rename a computer:

   ```
   netdom renamecomputer %COMPUTERNAME% /newname:NewPCName /reboot
   ```

Tasks:

- Rename the machine and rejoin it to a domain.

5.2 sc

sc is a command to manage services on Windows.

Exercise:

1. Query the status of a service:

   ```
   sc query wuauserv
   ```

2. Stop a service:

   ```
   sc stop wuauserv
   ```

Tasks:

- Query, stop, and start a specific service.
- Investigate the status of security-related services (like Windows Defender).

Conclusion

This lab manual introduces essential CMD commands and tools for securing and troubleshooting Windows networks. Through these labs, you will be better equipped to monitor network activity, troubleshoot issues, and secure your systems against attacks.

Next Steps:

- Explore PowerShell for more advanced security tasks.
- Implement scheduled tasks and automated scripts for routine security audits.

LECTURER GOVERNMENT POLYTECHNIC KANPUR