```
::Start of recon
@echo off
setlocal enabledelayedexpansion
set LOG=auto_pentest.txt
echo Recon started at: %date% %time% >> %LOG%
echo Recon started at: %date% %time%
echo . >> %LOG%

echo IP Configuration >> %LOG%
ipconfig /all >> %LOG%
echo . >> %LOG%

echo ARP Table >> %LOG%
arp -a >> %LOG%
echo . >> %LOG%

echo Routing Table >> %LOG%
route print >> %LOG%
echo . >> %LOG%

echo DNS Info >> %LOG%
hostname >> %LOG%
nslookup %computername% >> %LOG%
echo . >> %LOG%

echo Ping Sweep >> %LOG%
for /l %%i in (1,1,254) do (
   ping -n 1 -w 300 192.168.0.%%i | find "Reply from" >> !LOG!
)
echo . >> %LOG%

echo Recon complete. Output saved to %LOG%
Pause
echo . >> %LOG%

::Start of vulnerability scan

echo Checking for pending Windows Updates... >> %LOG%
powershell -command "Get-WindowsUpdate | Out-String" >> %LOG% 2>&1
if %ERRORLEVEL% EQU 0 (
   echo     Windows Update check completed. >> %LOG%
) else (
   echo     WARNING: Could not retrieve Windows Update information. >> %LOG%
)
```

```
echo . >> %LOG%


echo Checking Windows Defender status... >> %LOG%
powershell -Command "Get-MpComputerStatus | Select-Object AMServiceEnabled,
RealTimeProtectionEnabled, AntivirusEnabled" >> %LOG%
echo . >> %LOG%

echo Checking for SMBv1... >> %LOG%
dism /online /Get-Features | findstr /i "SMB1Protocol" >> %LOG%
echo . >> %LOG%

echo Checking Windows Firewall status... >> %LOG%
netsh advfirewall show allprofiles | findstr /i "State" >> %LOG%
echo . >> %LOG%

echo Checking for listening network ports... >> %LOG%
netstat -an | find "LISTENING" >> %LOG%
echo . >> %LOG%

echo Checking for local users with blank passwords... >> %LOG%
powershell -Command "Get-LocalUser | Where-Object { $_.PasswordRequired -eq $false } |
ForEach-Object { '    WARNING: User ' + $_.Name + ' has no password set!' }" >> %LOG%

echo . >> %LOG%
echo        Scan Completed >> %LOG%
echo. >> %LOG%
Pause

::Start of Enumeration
echo Starting enumeration >> %LOG%
echo . >> %LOG%
echo Checking local administrators... >> %LOG%
powershell -Command "Get-LocalGroupMember -Group 'Administrators' | Out-String" >>
%LOG%
echo. >> %LOG%

echo Enumerating installed software... >> %LOG%
powershell -Command "Get-ItemProperty
HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object
DisplayName, DisplayVersion | Format-Table -AutoSize | Out-String" >> %LOG%
echo. >> %LOG%
```

```
echo Checking for auto-logon credentials... >> %LOG%
powershell -Command "Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon' | Select-Object DefaultUserName, DefaultPassword,
AutoAdminLogon | Out-String" >> %LOG%
echo. >> %LOG%

echo Listing running services... >> %LOG%
powershell -Command "Get-Service | Where-Object {$_.Status -eq 'Running'} | Select-Object
DisplayName, Status | Format-Table -AutoSize | Out-String" >> %LOG%
echo. >> %LOG%

echo . >> %LOG%
echo        Enumeration Completed >> %LOG%
echo. >> %LOG%
Pause
```