Cyber Operations

Unit 11 - Domain Token Stealing

# Lab 09 - Meterpreter and Persistence

You will need your Kali VM or a desktop that can run the tools shown below (meterpreter, netcat, netstat). You will also need a target Windos XP machine as well as a Windows domain controller VM. Be extremely careful in running these scans, it is your responsibility to remain passive and to only access systems you are authorized to do so.

### **Meterpreter Post Modules**

Gain a Meterpreter shell on the Windows XP target, then, find a post exploitation module that interests you, and get it to successfully run. Take a screenshot of the results of the module and explain in five sentences or less what the module is and why it’s useful.

### **Impersonating a Domain Admin**

When you have a Meterpreter shell directly on the XP, steal the domain tokens. If you do not see any domain tokens, log into XP directly as a domain user and try again.

Once you have stolen the domain token, load up the **incognito** module and impersonate one of the domain admin tokens. Drop to a shell and run **whoami.exe**. Take a screenshot.

From the command line, add yourself your own domain admin account, and then add that new account to the domain admins group. Take a screenshot of both commands.

### **NC Listener**

If you have not done so already, upload the **nc.exe** binary to the XP host.

Use the meterpreter execute command to launch nc.exe on the remote host. This command should ensure that NC stays open after a user disconnects, be bound to port **12345**, and spawn **cmd.exe** when connected to.

Verify that the port has opened using **netstat**.

From a new Kali terminal window, connect to the remote victim with **netcat** and take a screenshot.

### **Generate a new NC .exe**

Use the **payload/windows/exec** module in Metasploit to generate a new executable for netcat. It should have the following parameters:

* Listen even after disconnect
* Bound to port 12121
* Spawn cmd.exe when called

Take a screenshot of the generate of the new .exe.

## What to submit

Create a PDF document containing the screenshots required in the lab. The document should include your name and only the screenshots requested.