MOBIA is a business technology integrator with over thirty years of experience and 500+ employees across Canada and USA. Our talented bench of technical engineers and trusted advisors deliver process improvements and business transformations within our core pillars of Cloud, Infrastructure, Software Development, Cybersecurity and Broadband & Wireless Services.

Our inside-out approach allows us to understand business challenges from deep within the organization, mapping the impact as it ripples outward. This insight enables us to create future-proof solutions that maximize results and repeatedly exceed our client's expectations.

Adversary Simulation Workshop

Lab Guide:
Lateral Movement

Objective:

Simulate a two stage attack with lateral movement. Initial stage will follow Lab 9:

STEP 1: Initial attack launched via Word Doc as unprivileged user
STEP 2: Resultant process adds persistence via scheduled task
STEP 3: Perform discovery (local service exploits)
STEP 4: Use discovery to escalate privileges to SYSTEM
STEP 5: Create new local account

One additional step we'll add to the Lab 9 is to not only create a new local account but also dump lsass for exfiltration and hash cracking.

STEP 6 - In this exercise we won't cover the exfiltration or hash cracking, we'll assume those steps were successful and we now have the local administrator password. With the local administrator password we want to achieve the following:

STEP 7 – Create a remote scheduled task on a secondary server
STEP 8 – Run Step 2 – 5 above

Instructions:

First we want to build a Stage 1 execution plan as an atomic test:

- STEP 1: T1566.001 Initial attack launched via Word Doc as unprivileged user
- STEP 2: T1053.005 Resultant process adds persistence via scheduled task
- STEP 3: T1082 or T1007 Perform discovery (local service exploits)
- STEP 4: T1574.009 or T1574.010 Use discovery to escalate privileges to SYSTEM
- STEP 5: T1078.003 Create new local account

A prerequisite for this lab is to ensure there's a vulnerable service (user write permissions to service home directory) we can exploit.

The setup for this services can be found in this reportsitory:
https://github.com/mobia-security-services/adversarysimulationworkshop

Run the create_service.ps1 script as administrator on your machine:

```
Iex (iwr https://raw.githubusercontent.com/mobia-security-services/adversarysimulationworkshop/main/create_services.ps1)
```

Check that you now have both the directory c:\kdservice and the service kdservice on your machine:

Name	Description	Status	Startup Type	Log On As
KDService			Automatic	Local Syste...
KtmRm for Distributed Tran...	Coordinates...		Manual (Trig...	Network S...
Language Experience Service	Provides inf...		Manual	Local Syste...
Link-Layer Topology Discov...	Creates a N...		Manual	Local Service
Local Profile Assistant Service	This service ...		Manual (Trig...	Local Service
Local Session Manager	Core Windo...	Running	Automatic	Local Syste...
MessagingService_1b5af5	Service sup...		Manual (Trig...	Local Syste...
Microsoft (R) Diagnostics H...	Diagnostics ...		Manual	Local Syste...
Microsoft Account Sign-in ...	Enables use...		Manual (Trig...	Local Syste...
Microsoft App-V Client	Manages A...		Disabled	Local Syste...
Microsoft Defender Antiviru...	Helps guard...	Running	Manual	Local Service
Microsoft Defender Antiviru...	Helps prote...	Running	Automatic	Local Syste...
Microsoft Edge Elevation Se...	Keeps Micr...		Manual	Local Syste...
Microsoft Edge Update Serv...	Keeps your ...		Automatic (...	Local Syste...
Microsoft Edge Update Serv...	Keeps your ...		Manual	Local Syste...
Microsoft iSCSI Initiator Ser...	Manages In...		Manual	Local Syste...
Microsoft Keyboard Filter	Controls ke...		Disabled	Local Syste...
Microsoft Office Click-to-R...	Manages re...	Running	Automatic	Local Syste...

This PC > Windows 10 (C:)

Name	Date modified	Type	Size
AtomicRedTeam	4/14/2021 2:43 PM	File folder	
KDService	4/14/2021 5:49 PM	File folder	
PerfLogs	12/7/2019 9:14 AM	File folder	
Program Files	4/13/2021 8:18 AM	File folder	
Program Files (x86)	4/13/2021 6:39 AM	File folder	

Now that we have our service ready to be exploited we can build our emulation yaml. For this emulation yaml use the custom atomics folder you created in Lab 10 (C:\AtomicRedTeam\myatomics).

We are going to abuse the atomic redteam tool a little. It's purpose is to run singular reversable test aligned to mitre. In our case we're going to pull everything we want into a single test. Let's get started:

You can use your original MyTest atomic and yaml file from Lan 10 for this exercise.

The low-level steps required to achieve this lab are not included in this lab but your instructor will walk you through a possible solution. There are no truly right answers here, use what you've learned to build this threat actor emulation plan.

Important! Let's start off as the unprivileged user. Do you best not to cheat ☺

Step 1: T1566.001 Initial attack launched via Word Doc as unprivileged user

Copy and paste the technique info from the original file into your mytest.yaml. Keep track of custom input names, those will be important (duplicate names for different uses could be a real problem).

Step 2: T1053.005 Resultant process adds persistence via scheduled task

An example of scripted persistence is located in the workshop repo:
https://github.com/mobia-security-services/adversarysimulationworkshop

The script persist_discovery.ps1 demonstrates both the creation of the scheduled task and the vulnerable service discovery. Read over the example, even if you don't understand it you should be able to use other powershell execution example and copy and paste.

Step 3: : T1082 or T1007 Perform discovery (local service exploits)

This step is covered in the powershell example above but feel free to experiment with the existing examples.

STEP 4: T1574.009 or T1574.010 Use discovery to escalate privileges to SYSTEM

Now that we have our service discovery complete there should be a file $env:APPDATA\services.txt that captures the misconfiguration of KDService.

The privilege escalation and LSASS dump are all wrapped into an example script escalate_create_user.ps1 in the workshop repo:
https://github.com/mobia-security-services/adversarysimulationworkshop

Same as step to use powershell to examples to copy and paste from the example script.

STEP 5: T1078.003 Create new local account

This is covered in the script from Step 4 but again feel free to use the existing atomic test.

STEP 7 – Create a remote scheduled task on a secondary server

After step 5 we assume we were able to gain administrator password via lsass dump. Now we want to create a remote scheduled task. Use T1053.005 Scheduled Task.

End of Lab