# LAB-1: Security Attack & Detection

## Prerequisites:

1. vmware workstation pro
2. Windows Server 2016 os image/ova/ovf
3. Oracle Linux 9 os image/ova/ovf

## Lab preparation

1. Install vmware workstation pro
2. Open a virtual machine from ovf provided by the instructor.

## Attack simulation

1. Run the command below from a Windows Server PowerShell session. Ensure that you run this as an administrator each time a new PowerShell session is invoked.

```
Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
```

2. Run the attack simulation for brute force. First, get the prerequisites, if any.

```
Invoke-AtomicTest T1110.001 -GetPrereqs
```

3. Run the attack

```
Invoke-AtomicTest T1110.001
```

4. Run another attack simulation for registry key modification. First, get the prerequisites, if any.

```
Invoke-AtomicTest T1547.008 -GetPrereq
```

5. Run the attack

```
Invoke-AtomicTest T1547.008 -Force -Verbose
```

6. revert to the original state

```
Invoke-AtomicTest T1110.001 -Cleanup
Invoke-AtomicTest T1547.008 -Cleanup
```

## Attack detection

1. Log in to the Splunk Search Head from Oracle Linux or Windows VM.
   URL: https://192.168.200.50:8000
2. Go to Splunk app > search and reporting
3. Detect the alerts by the provided use case.

   For BruteForce

```
index=windows
| search EventCode=4625
| search NOT Account_Name=*$
| bin _time span=1m
| stats count as failed_attempts by Source_Network_Address, Account_Na
me, _time
| where failed_attempts >= 5
| table Source_Network_Address, Account_Name, failed_attempts, _time
| sort - failed_attempts
```

   For Registry modification

```
index=windows | search EventCode=4657
| rename Account_Name as User, ComputerName as Host, Object_Name as
Registry_Path, Object_Value_Name as Modified_Object
| where NOT match(User, "(?i)^(SYSTEM|LOCAL SERVICE|NETWORK SERV
ICE)$")
```

```
| where NOT match(User, ".*\\$$")
| table _time, User, Host, Registry_Path, Modified_Object, Process_Name
```

---