**Nwachukwu Edumanichukwu**

**CYBR 445 - Advanced Incident Detection and Response**

**Module 8-1 Lab – Testing with Atomic Red Team and Caldera**

Professor Chelsie Thompson

July 6, 2023

**What is the first command suggested for Discovery - T1615 Group Policy Discovery?**

**gpresult /z – Displaying group policy information via gpresult**

**What is the name of the compiler used in the first Atomic Test for Execution - T1106 Native API?**

**C#**

**How many tests are available for the Credential Access - T1003.001 OS Credential Dumping: LSASS Memory test?**

**There are 12 Tests.**

**List 5 different tools/programs used in the Credential Access - T1003.001 OS Credential Dumping: LSASS Memory test.**

**NanoDump, Mimikatz, ProcDump, Dumpert, PowerShell**

**Paste a screenshot of your alert window below showing all four of the alerts:**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Pick three abilities and describe them below. You can click on the ability to get more information about how it is set up in Caldera.**

* **Name: AWS-Scan for Anonymous Access to S3.**
* **Tactic: Collection**
* **Technique ID: T1530**
* **This ability tests for anonymous access to AWS S3 buckets and dumps all the files to a local folder.**
* **Name: Account-type Admin Enumerator.**
* **Tactic: discovery**
* **Technique ID: T1069.002**
* **This ability uses PowerView to query the Active Directory server to determine remote admins.**
* **Name: Activate Windows NoDesktop Group Policy Feature**
* **Tactic: defense-evasion**
* **Technique ID: T1112**
* **Modifies the registry of the currently logged in user using reg.exe via cmd console to hide all icons on Desktop Group Policy.**

**List the 8 abilities associated with the Check Adversary below:**

**Advanced Thief (collection, exfiltration)**

**Advanced Thief via DropBox (collection, exfiltration)**

**Advanced Thief via FTP (collection, exfiltration)**

**Advanced Thief via GitHub Gist (collection, exfiltration)**

**Alice 2.0 (discovery, credential-access, lateral-movement, execution)**

**Check (discovery)**

**Enumerator (collection, discovery)**

**Nosy Neighbor (defense-evasion, discovery, impact)**

**Paste screenshots of the View Command and View Output for the following:**

* **View Processes**

**A black screen with white text

Description automatically generated**

**A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**

* **Network Interface Configuration**

**A black rectangular object with a black stripe

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**

* **List Directory**

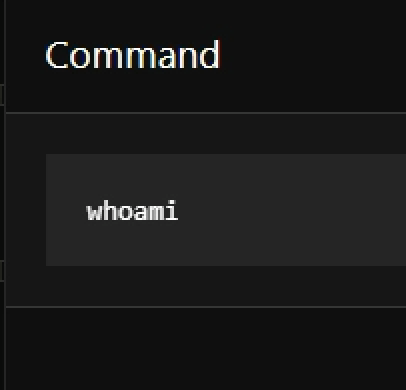
**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

* **Current User**



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Which is the Sandcat/Caldera agent running as?**

**Caldera2 -ryminq**

**A screenshot of a computer

Description automatically generated**