

REDTEAMSIMMER

The UI You've Always Wanted for Atomic Red Team

A Web Based Adversary Emulation Platform
and Atomic Red Team Test Orchestration.

ABHIJITH "ABX" B R

Founder of Adversary Village
Director at BreachSimRange

DEFCON
SINGAPORE
Demo Labs | 28-30 April 2026



<https://breachsimrange.io>

\$whoami

ABHIJITH “ABX” B R

- Hacker, offensive cyber security specialist, security researcher, red team consultant, trainer and public speaker with over a decade of experience.
- Founder and Director at **BreachSimRange.io**
- Founder of **Adversary Village** at DEF CON, Las Vegas.
- Organizer of Bsides Kerala and AdversaryCon.
- Formerly worked with Envestnet, Inc., Nissan Motor Corporation, EY.
- Spoken at DEF CON, RSA Conference, BSides Las Vegas/San Francisco/Tampa/Delhi, Hack Space Con, Nullcon, cocon and many.
- <https://tacticaladversary.io/blog> research blog

<https://breachsimrange.io>



ABHIJITH “ABX” B R
Connect with me!



Abhijith B R

Building BreachSimRange | Founder
of Adversary Village | Offensive Cybe...



THE ~~A~~ TEAM RED



<https://breachsimrange.io>

*image credits goes to respective owners.





Guardians of the Galaxy!
Security operations team!

What is Adversary Emulation?

- Emulate the adversary by using the same documented TTPs
- Must understand the known adversaries and threat groups
- Plan adversary emulation based on cyber threat intelligence
- Must know how to effectively emulate TTPs [Technical capability]

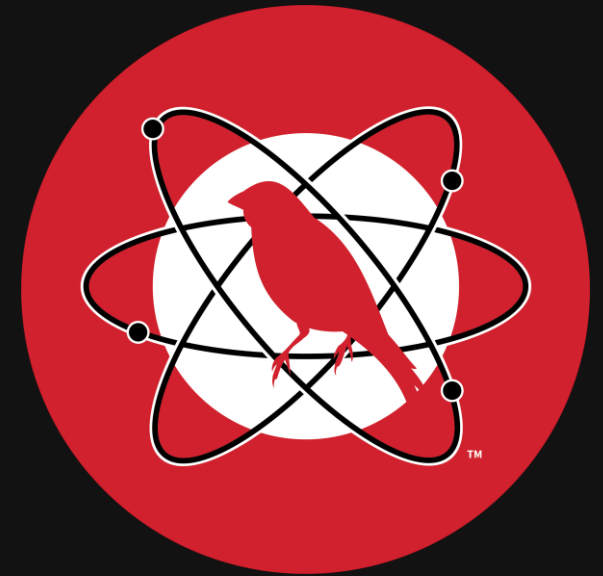
Atomic Red Team

Atomic Red Team™ is a library of tests mapped to the MITRE ATT&CK® framework.

Security teams can use Atomic Red Team to quickly, portably, and reproducibly test their environments.

URLs:

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



RedTeamSimmer - Core Features

- MITRE ATT&CK navigation by tactic, technique, and sub-technique
- Automatic prerequisite handling. parses YAML, checks, installs, re-verifies, then runs
- Live streaming output with stdout, stderr, and agent messages, toggleable
- rule correlation with Sigma, Splunk, Elastic, all local and offline
- Dashboard with ATT&CK heatmap, tactic coverage charts, and operations history

Pre-built Emulation Plans

- APT28 (Fancy Bear)
- APT29 (Cozy Bear)
- APT3 (Gothic Panda)
- APT41 (Wicked Panda)
- FIN7 (Carbanak)
- Lazarus Group
- Wizard Spider



Emulation Plans

<https://bre>

[Wicked Panda | APT41 | BARIUM]

- A state sponsored threat actor whose goals include cyber espionage and financial gain, active since at least 2007
- Also known as BARIUM, Winnti, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly
- APT41 compromised and gained various levels of access to at least 14 organizations worldwide.
- The group's targets include government and private organizations based in the **India, US, Taiwan, Thailand, China, Hong Kong, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei, and UK.**

<https://breachsimrange.io>



APT 41 - MITRE ATT&CK Navigator

APT41 (G0096) X +

Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 10 techniques Execution 14 techniques Persistence 20 techniques Privilege Escalation 14 techniques Defense Evasion 44 techniques

Active Scanning (2/3) Vulnerability Scanning Wordlist Scanning

Gather Victim Host Information (0/4)

Gather Victim Identity Information (0/3)

Gather Victim Network Information (0/5)

Gather Victim Org Information (0/4)

Phishing for Information (0/4)

Search Closed Sources (0/2)

Search Open Technical Databases (1/5)

Search Open Websites/Domains (1/3)

Search Victim-Owned Website

Scanning IP Blocks

Acquire Access

Botnet

DNS Server

Domains

Malvertising

Server

Serverless

Virtual Private Server

Web Services

Cloud Accounts

Email Accounts

Social Media Accounts

Compromise Infrastructure (0/5)

Develop Capabilities (0/4)

Establish Accounts (0/3)

CDNs

Digital Certificates

DNS/Passive DNS

Scan Databases

WHOIS

Code Repositories

Search Engines

Social Media

Stage Capabilities (0/5)

Content Injection

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (1/4)

Replication Through Removable Media

Supply Chain Compromise (1/3)

Trusted Relationship

Code Signing Certificates

Digital Certificates

Malware

Tool

Vulnerabilities

Spearphishing Attachment

Spearphishing Link

Spearphishing via Service

Spearphishing Voice

Compromise Hardware Supply Chain

Compromise Software Dependencies and Development Tools

Compromise Software Supply Chain

Cloud Administration Command

Command and Scripting Interpreter (4/11)

Container Administration Command

Deploy Container

Exploitation for Client Execution

Inter-Process Communication (0/1)

Native API

Scheduled Task/Job (1/5)

Serverless Execution

AppleScript

AutoHotKey & AutoIT

Cloud API

JavaScript

Lua

Network Device CLI

PowerShell

Python

Unix Shell

Visual Basic

Windows Command Shell

Account Manipulation (1/7)

BITS Jobs

Boot or Logon Autostart Execution (1/14)

Boot or Logon Initialization Scripts (0/5)

Browser Extensions

Compromise Host Software Binary

Additional Cloud Credentials

Additional Cloud Roles

Additional Container Cluster Roles

Additional Email Delegate Permissions

Additional Local or Domain Groups

Device Registration

SSH Authorized Keys

Active Setup

Authentication Package

Kernel Modules and Extensions

Login Items

LSASS Driver

Port Monitors

Print Processors

Re-opened Applications

Registry Run Keys / Startup Folder

Security Support Provider

Shortcut Modification

Time Providers

Winlogon Helper DLL

XDG Autostart Entries

Abuse Elevation Control Mechanism (0/5)

Access Token Manipulation (0/5)

Account Manipulation (1/7)

Boot or Logon Autostart Execution (1/14)

Boot or Logon Initialization

Additional Cloud Credentials

Additional Cloud Roles

Additional Container Cluster Roles

Additional Email Delegate Permissions

Additional Local or Domain Groups

Device Registration

SSH Authorized Keys

Active Setup

Authentication Package

Kernel Modules and Extensions

Login Items

LSASS Driver

Port Monitors

Print Processors

Re-opened Applications

Security Support Provider

Shortcut Modification

Time Providers

Winlogon Helper DLL

XDG Autostart Entries

Abuse Elevation Control Mechanism (0/5)

Access Token Manipulation (0/5)

BITS Jobs

Build Image on Host

Debugger Evasion

Deobfuscate/Decode Files or Information

Deploy Container

Direct Volume Access

Domain or Tenant Policy Modification (1/2)

Execution Guardrails (1/2)

Exploitation for Defense Evasion

File and Directory Permissions Modification (0/2)

Hide Artifacts (0/12)

Group Policy Modification

Trust Modification

Environmental Keying

Mutual Exclusion

AppDomainManager

COR_PROFILER

DLL Search Order Hijacking

DLL Side-Loading

Dylib Hijacking

Dynamic Linker Hijacking

Executable Installer File Permissions Weak

KernelCallbarkTable

Hijack Execution Flow (0/1)

Service

Agent

Daemon

Service

<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0096%2FG0096-enterprise-layer.json>

<https://breachsimrange.io>

Try RedTeamSimmer Today

Try RedTeamSimmer today and support the project.

We welcome contributions of all kinds - code, documentation, bug reports, feature ideas, or testing.

GitHub Repository:

- <https://github.com/BreachSimRange/RedTeamSimmer>

- [📁 DASHBOARD](#)
- [👤 AGENT MANAGEMENT](#)
- [>_ TECHNIQUE EXECUTION](#)
- [🕒 EMULATION PLANS](#)
- [📂 OPERATIONS](#)
- [🕒 TASK HISTORY](#)
- [📁 FILE DROP](#)
- [⚙️ CONFIGURATION](#)
- [📄 ABOUT](#)
- [➡️ LOGOUT](#)

ADVERSARY EMULATION PLANS

🔄 REFRESH

NOTE: EMULATION PLANS ARE LOADED FROM JSON FILES IN THE `emulation_plans/` FOLDER. ADD VALIDATED APT PLAN FILES TO THIS FOLDER AND REFRESH TO SEE THEM HERE.



60007 | UNKNOWN

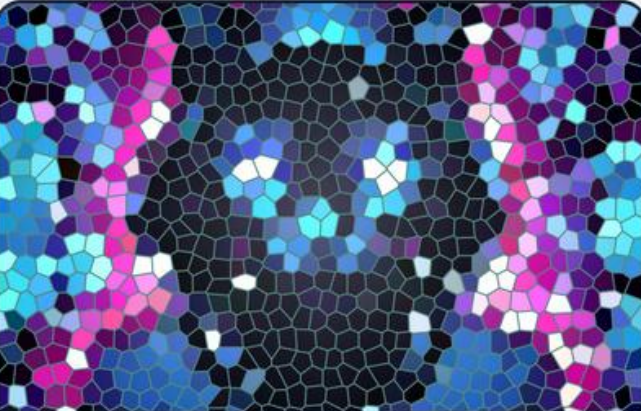
APT28 (FANCY BEAR)

APT28, FANCY BEAR, FOREST BLIZZARD

88 TESTS

0 TECHNIQUES

0% COVERAGE



60022 | CHINA MINISTRY OF STATE SECURITY (MSS)

APT3 (GOTHIC PANDA)

APT3, GOTHIC PANDA, PIRPI

41 TESTS

44 TECHNIQUES

93% COVERAGE



60096 | CHINA MINISTRY OF STATE SECURITY (MSS)

APT41 (WICKED PANDA)

APT41, WICKED PANDA, BRASS TYPHOON

83 TESTS

95 TECHNIQUES

80% COVERAGE



Try RedTeamSimmer Today

REDTEAMSIMMER

A COOL UI FOR ATOMIC RED TEAM!



DASHBOARD



AGENT MANAGEMENT



TECHNIQUE EXECUTION



EMULATION PLANS



OPERATIONS



TASK HISTORY



FILE DROP



CONFIGURATION



ABOUT



LOGOUT

☐ ATOMIC TEST #7: SEND NTLM HASH WITH RPC TEST CONNECTION

POWERSHELL

T1003.001 T1003.001 OS CREDENTIAL DUMPING: LSASS MEMORY

14 TESTS

☒ ATOMIC TEST #1: DUMP LSASS.EXE MEMORY USING PROCDUMP

COMMAND_PROMPT

☒ ATOMIC TEST #2: DUMP LSASS.EXE MEMORY USING COMSVCS.DLL

POWERSHELL

☐ ATOMIC TEST #3: DUMP LSASS.EXE MEMORY USING DIRECT SYSTEM CALLS AND API UNHOOKING

COMMAND_PROMPT

☒ ATOMIC TEST #4: DUMP LSASS.EXE MEMORY USING NANODUMP

COMMAND_PROMPT

☐ ATOMIC TEST #5: DUMP LSASS.EXE MEMORY USING WINDOWS TASK MANAGER

MANUAL

☐ ATOMIC TEST #6: OFFLINE CREDENTIAL THEFT WITH MIMIKATZ

COMMAND_PROMPT

☐ ATOMIC TEST #7: LSASS READ WITH PYPYKATZ

COMMAND_PROMPT

☒ ATOMIC TEST #8: DUMP LSASS.EXE MEMORY USING OUT-MINIDUMP.PS1

POWERSHELL

☐ ATOMIC TEST #9: CREATE MINI DUMP OF LSASS.EXE USING PROCDUMP

COMMAND_PROMPT

☒ ATOMIC TEST #10: POWERSHELL MIMIKATZ

POWERSHELL

☐ ATOMIC TEST #11: DUMP LSASS WITH CREATEDUMP.EXE FROM .NET V5

POWERSHELL

☐ ATOMIC TEST #12: DUMP LSASS.EXE USING IMPORTED MICROSOFT DLLS

POWERSHELL

☐ ATOMIC TEST #13: DUMP LSASS.EXE USING LOLBIN RDRLEAKDIAG.EXE

POWERSHELL

☐ ATOMIC TEST #14: DUMP LSASS.EXE MEMORY THROUGH SILENT PROCESS EXIT

COMMAND_PROMPT

T1003.002 T1003.002 OS CREDENTIAL DUMPING: SECURITY ACCOUNT MANAGER

8 TESTS

☐ ATOMIC TEST #1: REGISTRY DUMP OF SAM, CREDS, AND SECRETS

COMMAND_PROMPT

☐ ATOMIC TEST #4: POWERDUMP HASHES AND USERNAMES FROM REGISTRY

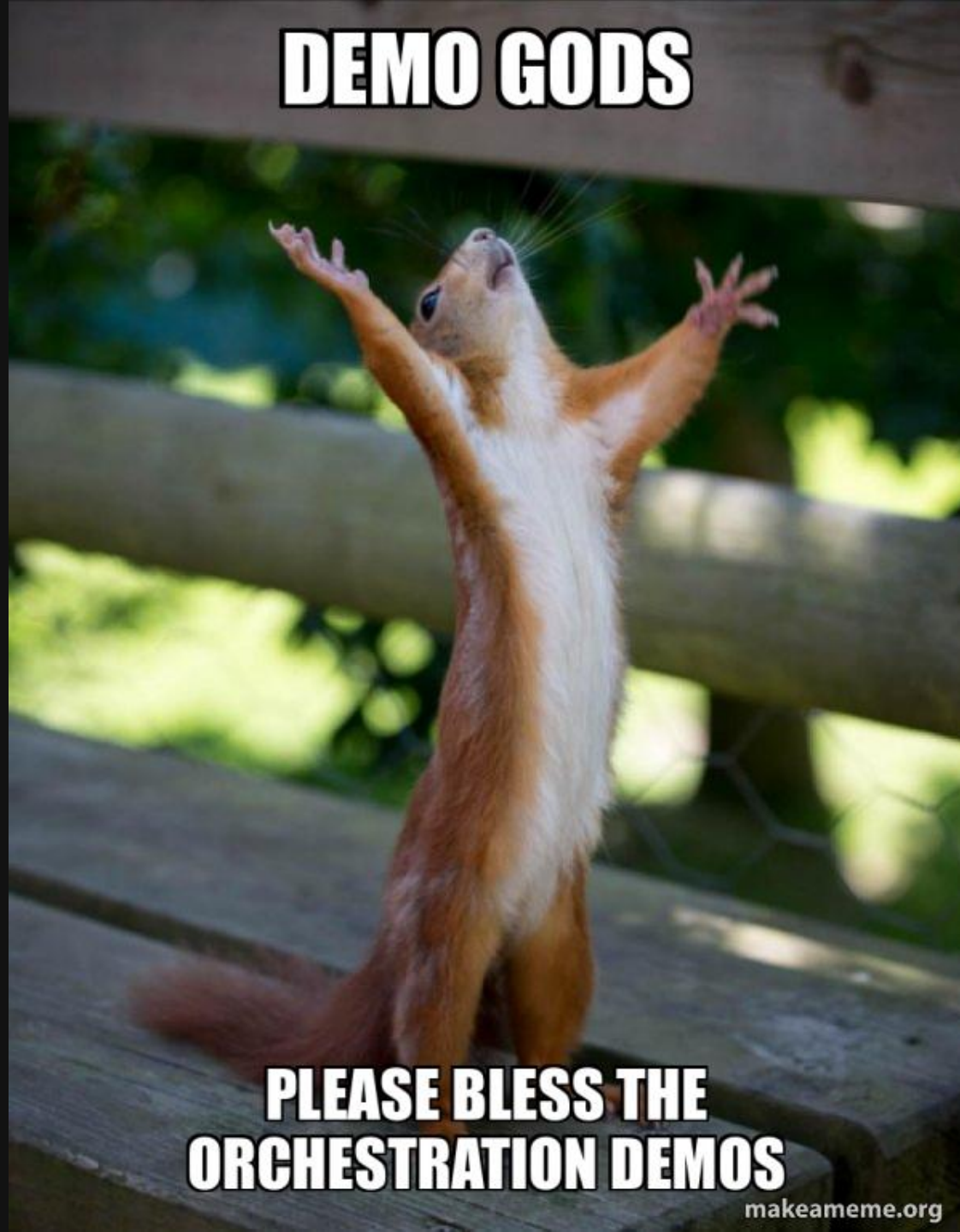
POWERSHELL

☐ ATOMIC TEST #5: DUMP VOLUME SHADOW COPY HIVES WITH CERTUTIL

COMMAND_PROMPT

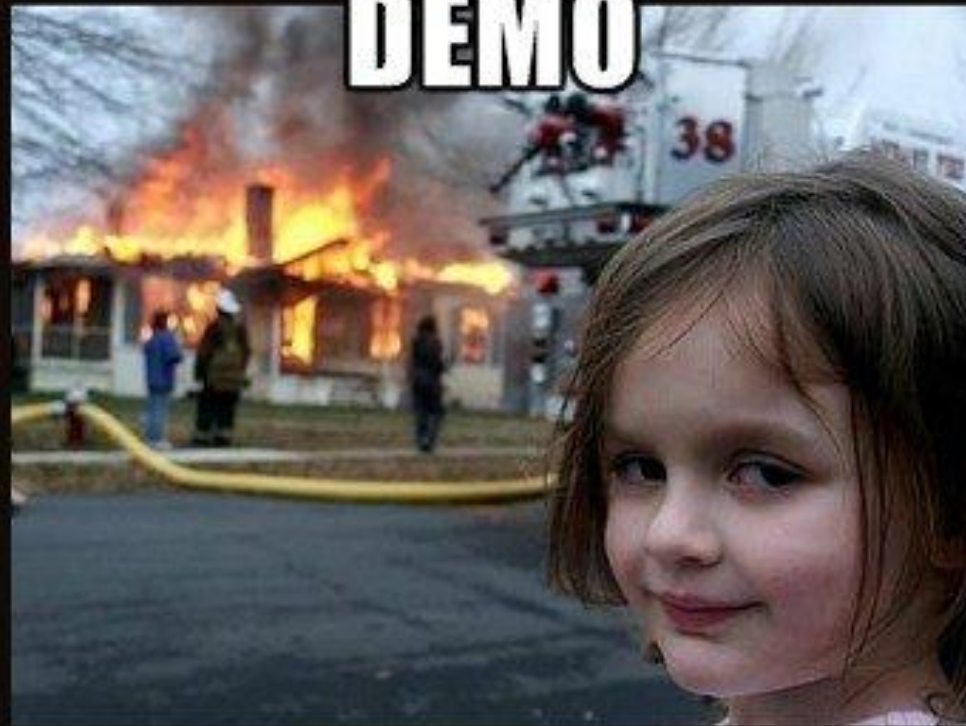
Try RedTeamSimmer Today

DEMO GODS



**PLEASE BLESS THE
ORCHESTRATION DEMOS**

**TIME FOR A LIVE
DEMO**



WHAT COULD GO WRONG?

memegenerator.net

I LOVE QUESTIONS

**QUESTIONS ARE MY
FAVORITE**

Keep in touch



<https://breachsimrange.io>



BLOG: <https://tacticaladversary.io/blog>



<https://x.com/abhijithbr>



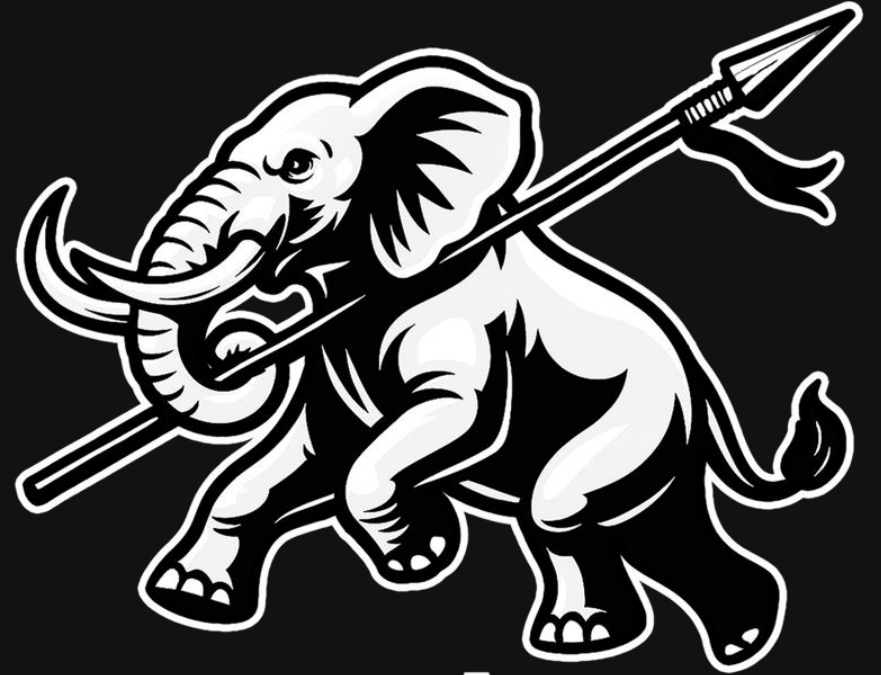
[linkedin.com/in-abhijith-b-r](https://www.linkedin.com/in-abhijith-b-r)



Abx#1337

<https://breachsimrange.io>

Thank You!



breachsimrange