Enterprise ~

Pricing

Open Source >



> T1036

sts	5	(Actions	₩ Wiki	① Security	<u></u> ✓ Ir	nsights				
i	atomi	c-re	d-team /	atomics / T	1552.003 / T1	552.00	3.md ┌☐				•••
		Atom	nic Red Tea	am doc genei	r at Generated	l docs fr	om job=generate-d	. 819934c ·	2 years ago	His	tory
	Pre	view	Code	Blame	44 lines (21 l	.oc) • :	1.7 KB		Raw	<u>+</u>	:=
	٦	Г15	552.0	003 - 1	Bash H	isto	ory				

Notifications

Q

Y Fork 2.8k

Sign in

Sign up

Star 9.7k

Description from ATT&CK

Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

Atomic Tests

Atomic Test #1 - Search Through Bash History

Atomic Test #1 - Search Through Bash History

Search through bash history for specifice commands we want to capture

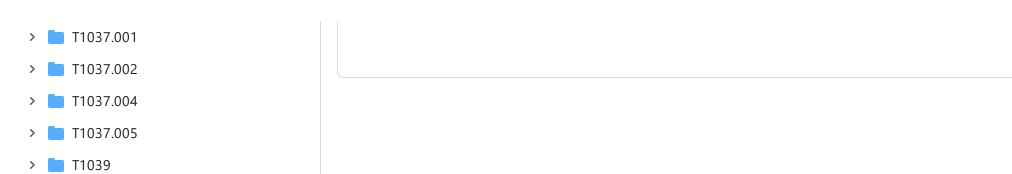
Supported Platforms: Linux, macOS

auto_generated_guid: 3cfde62b-7c33-4b26-a61e-755d6131c8ce

Inputs:

Name	Description	Туре	Default Value	
output_file	Path where captured results will be placed	Path	~/loot.txt	
bash_history_grep_args	grep arguments that filter out specific commands we want to capture	Path	-e '-p ' -e 'pass' - e 'ssh'	
bash_history_filename	Path of the bash history file to capture	Path	~/.bash_history	

Attack Commands: Run with sh!



> T1040