mvelazc0 / **PurpleSharp** Public

Notifications Fork 110 Star 774

master Go to file Code

mvelazc0 Update README.md 6a2fc9b · last year 161 Commits

PurpleSharp	update mitre navigator layer	last year
.gitignore	adding Costura.Fody	3 years ago
LICENSE	Update LICENSE	4 years ago
PurpleSharp.sln	Second commit	5 years ago
README.md	Update README.md	last year
azure-pipelines.yml	Update azure-pipelines.yml for Azure P...	last year

About

PurpleSharp is a C# adversary simulation tool that executes adversary techniques with the purpose of generating attack telemetry in monitored Windows environments

purple-team adversary-simulation detection-engineering controls-validation

Readme
BSD-3-Clause license
Activity
774 stars
30 watching
110 forks
Report repository

Releases 4

BlackHat Arsenal 2021 Latest
on Sep 18, 2021

+ 3 releases

Packages

No packages published

Languages

● C# 100.0%

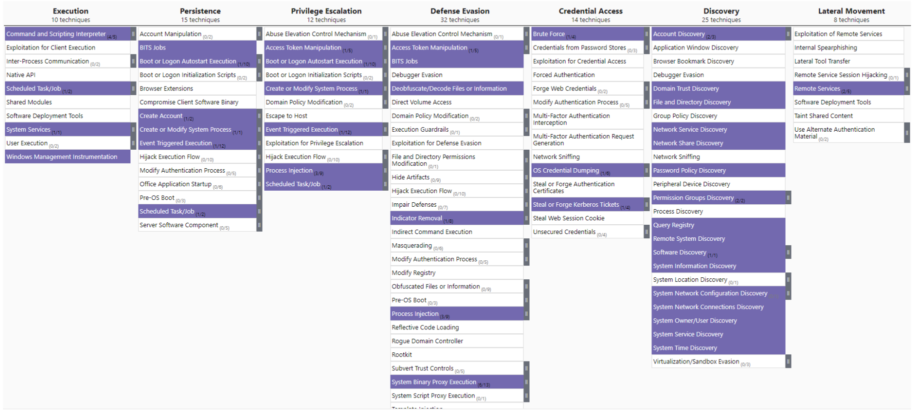
README BSD-3-Clause license

PurpleSharp

Open Threat Research Community | Black Hat Arsenal USA 2021 | Black Hat Arsenal Asia 2023

Defending enterprise networks against attackers continues to present a difficult challenge for blue teams. Prevention has fallen short; improving detection & response capabilities has proven to be a step in the right direction. However, without the telemetry produced by adversary behavior, building new and testing existing detection capabilities will be constrained.

PurpleSharp is an open source adversary simulation tool written in C# that executes adversary techniques within Windows Active Directory environments. The resulting telemetry can be leveraged to measure and improve the efficacy of a detection engineering program. PurpleSharp leverages the MITRE ATT&CK Framework and executes different techniques across the attack life cycle: execution, persistence, privilege escalation, credential access, lateral movement, etc. It currently supports 47 unique ATT&CK techniques.



Execution 10 techniques	Persistence 15 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 8 techniques
Command and Scripting Interpreter (4/5)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/1)	Abuse Elevation Control Mechanism (0/1)	Brute Force (1/4)	Account Discovery (2/3)	Exploitation of Remote Services
Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing
Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (1/10)	Boot or Logon Autostart Execution (1/10)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Native API	Boot or Logon Initialization Scripts (0/2)	Boot or Logon Initialization Scripts (0/2)	Debugger Evasion	Forced Authentication	Debugger Evasion	Remote Service Session Hijacking (0/1)
Scheduled Task/Job (1/2)	Browser Extensions	Create or Modify System Process (1/1)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Domain Trust Discovery	Remote Services (2/5)
Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Direct Volume Access	Modify Authentication Process (0/5)	File and Directory Discovery	Software Deployment Tools
Software Deployment Tools	Create Account (1/2)	Escape to Host	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Group Policy Discovery	Taint Shared Content
System Services (1/1)	Create or Modify System Process (1/1)	Event Triggered Execution (1/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Network Service Discovery	Use Alternate Authentication Material (0/2)
User Execution (0/2)	Event Triggered Execution (1/12)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Network Share Discovery	
Windows Management Instrumentation	Hijack Execution Flow (0/10)	Hijack Execution Flow (0/10)	File and Directory Permissions Modification (0/1)	OS Credential Dumping (1/6)	Network Sniffing	
	Modify Authentication Process (0/5)	Process Injection (3/9)	Hide Artifacts (0/9)	Steal or Forge Authentication Certificates	Password Policy Discovery	
	Office Application Startup (0/6)	Scheduled Task/Job (1/2)	Hijack Execution Flow (0/10)	Steal or Forge Kerberos Tickets (1/4)	Peripheral Device Discovery	
	Pre-OS Boot (0/3)		Impair Defenses (0/7)	Steal Web Session Cookie	Permission Groups Discovery (2/2)	
	Scheduled Task/Job (1/2)		Indicator Removal (1/8)	Unsecured Credentials (0/4)	Process Discovery	
	Server Software Component (0/5)		Indirect Command Execution		Query Registry	
			Masquerading (0/6)		Remote System Discovery	
			Modify Authentication Process (0/5)		Software Discovery (1/1)	
			Modify Registry		System Information Discovery	
			Obfuscated Files or Information (0/9)		System Location Discovery (0/1)	
			Pre-OS Boot (0/3)		System Network Configuration Discovery (0/1)	
			Process Injection (3/9)		System Network Connections Discovery	
			Reflective Code Loading		System Owner/User Discovery	
			Rogue Domain Controller		System Service Discovery	
			Rootkit		System Time Discovery	
			Subvert Trust Controls (0/5)		Virtualization/Sandbox Evasion (0/3)	
			System Binary Proxy Execution (6/13)			
			System Script Proxy Execution (0/1)			

PurpleSharp was first presented at Derbycon IX on September 2019.

An updated version was released on August 6th 2020 as part of BlackHat Arsenal 2020. The latest version was released on August 2021 as part of BlackHat Arsenal 2021

Visit the Demos section to see PurpleSharp in action.

Goals / Use Cases

The attack telemetry produced by simulating techniques with PurpleSharp aids research & detection teams in:

- Building new detecttion analytics
- Testing existing detection analytics
- Validating detection resiliency
- Identifying gaps in visibility
- Identifing issues with event logging pipeline

Quick Start Guide

Build from Source

PurpleSharp can be built with Visual Studio Community 2019 or 2020.

Download Latest Release

Download the latest release binary ready to be used to execute TTP simulations.

.NET Framework 4.5 is required.

Simulate

The PurpleSharp assembly is all you need to start simulating attacks.

For simulation ideas, check out the Active Directory Purple Team Playbook, a repository of ready-to-use JSON playbooks for PurpleSharp.

Documentation

https://www.purplesharp.com/

Authors

- **Mauricio Velazco** - @mvelazco

Acknowledgments

The community is a great source of ideas and feedback. Thank you all.

- Olaf Hartong
- Roberto Rodriguez
- Matt Graeber

- Jonny Johnson