

# DESIGNING PLAYBOOKS WITH PURPLE TEAM APPROACH

SANS Purple Team Summit 2021

# whoami



Semanur Guneyusu

- ❑ 3+ cyber security experience
- ❑ SOC Analyst and Team Leader
- ❑ Designing MSSP - SOC Services
- ❑ Beginner for purple teaming

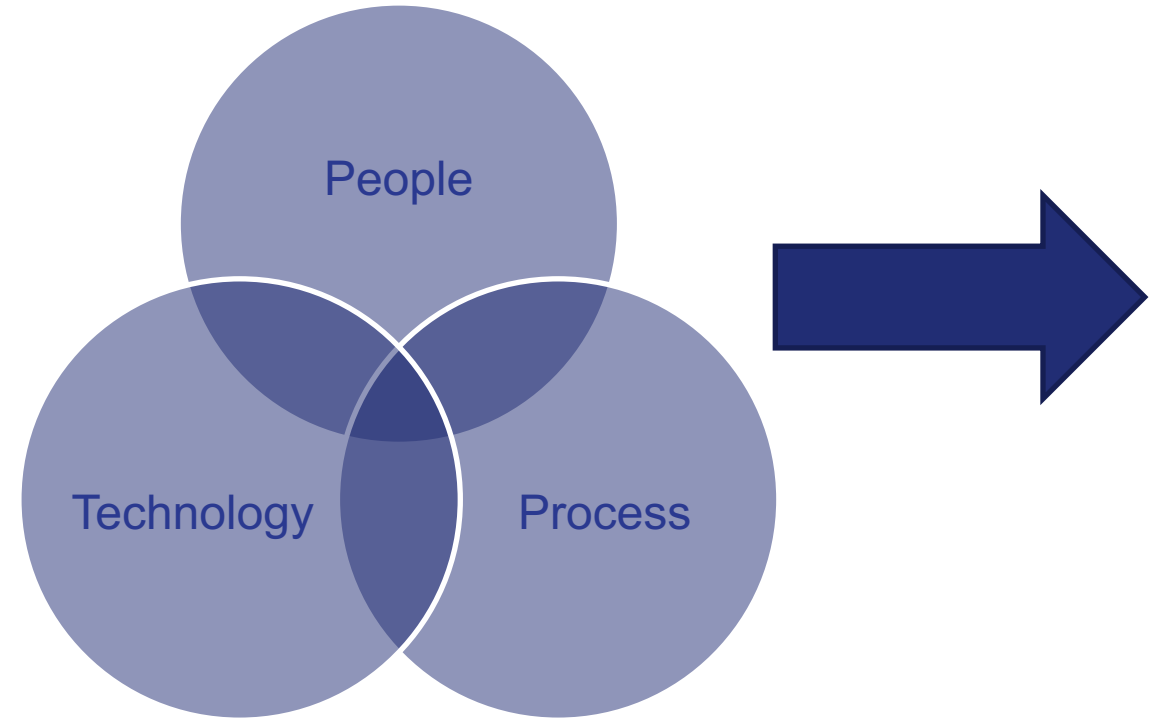
 [semanurtg](#)

# Agenda

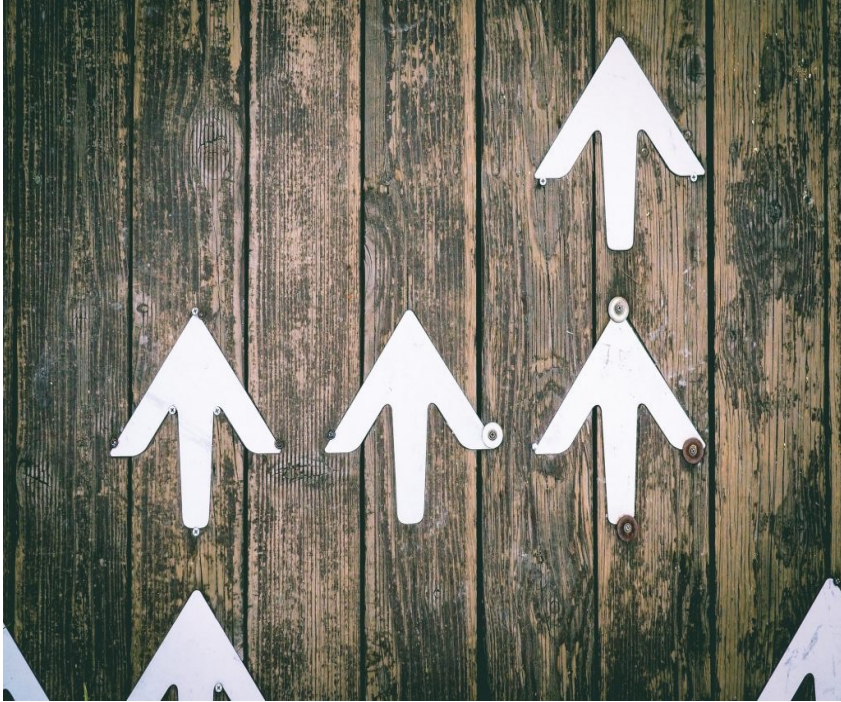
- The **5W1H** of Purple Teaming in SOC
- Requirements / Tools
- Take Advantage of Playbooks
- Demo Time



# 5W1H – Where ?



# 5W1H – Why ?



## Goals:

- Self - Assessment
- Improvement
- Learning & Teaching

# 5W1H – What ?

Purple Teaming



## 5W1H – When ?

Continuous

On Demand



# 5W1H – Who ?

Threat Hunters

SOC Analysts

Incident Responders

Red Teamers

...

...





## 5W1H – How ?

1. Plan scope
2. Decide the tools and requirements
3. Determine the methodology
4. Establish roles and responsibilities

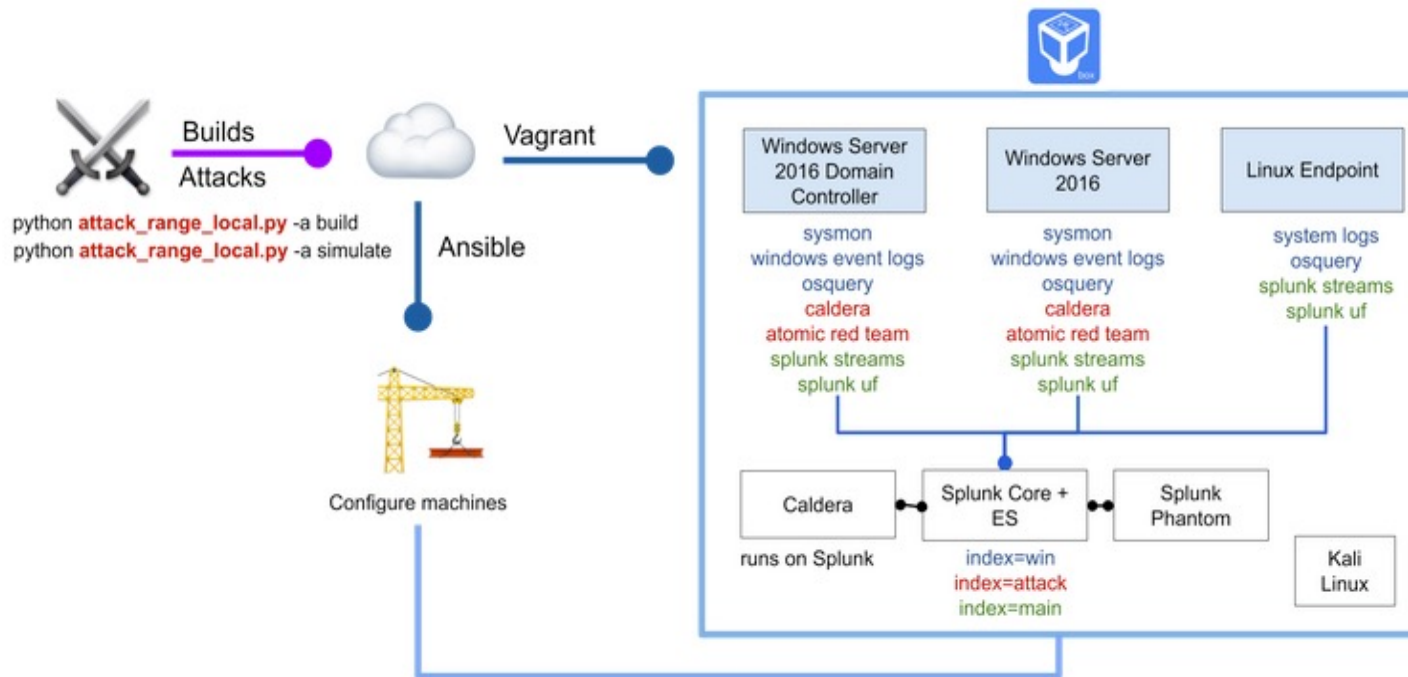


# Requirements / Tools

- Data Sources
- Attack Simulation Tools
- Dedicated Blue and Red team
- Time
- Tracking Process
- Threat Intelligence



# Attack Range Local



*“SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. ... SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.”*



# Benefits of Designing Playbooks

- Standardized workflow for analysts
- Automated repeatable actions
- Enriched incident response procedure

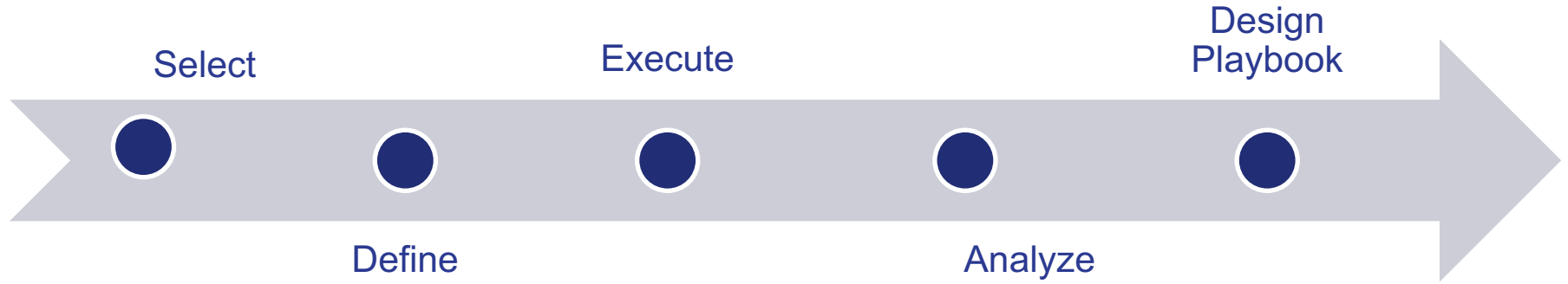


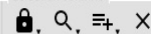
# Key Points

- Threat Intelligence
- Testing
- Tracking
- Documentation
- Team



# Timeline





Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 26 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
II Active Scanning (0/2)	II Obtain Capabilities (1/6)	II Exploit Public-Facing Application	II Command and Scripting Interpreter (5/8)	II Scheduled Task/Job (1/6)	II Process Injection (2/11)	II Obfuscated Files or Information (6/5)	II OS Credential Dumping (5/8)	II System Information Discovery	II Remote Services (5/6)	II Archive Collected Data (2/3)	II Ingress Tool Transfer	II Exfiltration Over Web Service (0/2)	II Service Stop
II Gather Victim Host Information (0/4)	Code Signing Certificates	II Phishing (3/3)	PowerShell	Scheduled Task	Process Hollowing	Software Packing	LSASS Memory	File and Directory Discovery	Remote Desktop Protocol	Archive via Utility	II Encrypted Channel (1/2)	II Exfiltration to Cloud Storage	II Inhibit System Recovery
II Gather Victim Identity Information (0/3)	Digital Certificates	Spearphishing Attachment	Windows Command Shell	At (Linux)	Thread Execution Hijacking	Binary Padding	NTDS	Query Registry	SMB/Windows Admin Shares	Archive via Library	Asymmetric Cryptography	II Exfiltration to Code Repository	II System Shutdown/Reboot
II Gather Victim Network Information (0/6)	Exploits	Spearphishing Link	Visual Basic	Cron	Asynchronous Procedure Call	Compile After Delivery	/etc/passwd and /etc/shadow	II System Network Configuration Discovery (0/1)	SSH	Archive via Custom Method	Symmetric Cryptography	II Automated Exfiltration (0/1)	II Data Manipulation (1/3)
II Gather Victim Org Information (0/4)	Malware	Spearphishing via Service	JavaScript	Launchd	Dynamic-link Library Injection	Indicator Removal from Tools	DCSync	Internet Connection Discovery	Distributed Component Object Model	Input Capture (1/4)	Non-Application Layer Protocol	II Data Transfer Size Limits	II Stored Data Manipulation
II Phishing for Information (0/3)	Tool	External Remote Services	Python	System Timers	Extra Window Memory Injection	II Indicator Removal on Host (4/6)	Security Account Manager	II Virtualization/Sandbox Evasion (1/3)	Windows Remote Management	Keylogging	II Application Layer Protocol (4/4)	II Exfiltration Over Alternative Protocol (0/3)	II Runtime Data Manipulation
II Search Closed Sources (0/2)	II Acquire Infrastructure (1/6)	II Valid Accounts (0/4)	Network Device CLI	II Server Software Component (1/3)	Portable Executable Injection	File Deletion	Cached Domain Credentials	System Checks	Internal Spearphishing	Web Portal Capture	Protocol Tunneling	II Exfiltration Over Physical Medium (0/1)	II External Defacement
II Search Open Technical Databases (0/5)	Virtual Private Server	Trusted Relationship	II System Services (1/2)	Web Shell	Proc Memory	Timestamp	LSA Secrets	Time Based Evasion	Remote Service Session Hijacking (1/2)	Data from Information Repositories (1/2)	Multi-hop Proxy	II Defacement (1/2)	II Internal Defacement
II Search Open Websites/Domains (0/2)	Botnet	Drive-by Compromise	Service Execution	SQL Stored Procedures	Process Doppelganging	Clear Windows Event Logs	Proc Filesystem	User Activity Based Checks	RDP Hijacking	Sharepoint	Domain Fronting	II Scheduled Transfer	II Data Destruction
II Search Victim-Owned Websites	DNS Server	Hardware Additions	Launchctl	Transport Agent	Ptrace System Calls	Network Share Connection Removal	II Brute Force (2/4)	Process Discovery	SSH Hijacking	Confluence	External Proxy	II Transfer Data to Cloud Account	II Disk Wipe (0/2)
	Server	Replication Through Removable Media	II Scheduled Task/Job (1/6)	Account Manipulation (0/4)	VDSO Hijacking	Clear Command History	Password Spraying	Software Discovery (0/1)	Replication Through Removable Media	Email Collection (1/3)	Internal Proxy	II Data Obfuscation (0/3)	II Endpoint Denial of Service (0/4)
	Web Services	II Supply Chain Compromise (1/3)	II User Execution (2/3)	Create or Modify System Process (1/4)	Clear Linux or Mac System Logs	Clear Linux or Mac System Logs	Password Guessing	Security Software Discovery	Use Alternate Authentication Material (2/4)	Email Forwarding Rule	Dynamic Resolution (1/3)	II Domain Generation Algorithms	II Firmware Corruption
	II Compromise Infrastructure (0/6)	II Compromise Software Supply Chain	Malicious Link	Windows Service	Scheduled Task/Job (1/6)	Subvert Trust Controls (1/6)	Credential Stuffing	System Owner/User Discovery	Pass the Hash	Remote Email Collection	DNS Calculation	II Fast Flux DNS	
	II Develop Capabilities (1/4)	Malicious File	Malicious Image	Launch Agent	Create or Modify System Process (1/4)	Code Signing	Input Capture (1/4)	Domain Trust Discovery	Pass the Ticket	Screen Capture	Non-Standard		
	Digital Certificates	Exploitation for Client Execution	Windows Management Instrumentation	Launch Daemon	Windows Service	Code Signing Policy Modification	Keylogging	System Network Connections Discovery	Application Access Token	Audio Capture			
	Code Signing Certificates	Compromise Hardware Supply Chain	Native API	Systemd Service	Launch Agent	Gatekeeper Bypass	Credential API Hooking	System Service Discovery	Web Session Cookie	Data from Cloud Storage Object			
	Exploits	Compromise Software Dependencies and Development Tools	II Inter-Process Communication (0/2)	Valid Accounts (0/4)	Systemd Service	Install Root Certificate	GUI Input Capture	Account Discovery (2/4)	Exploitation of				
	Malware	II Compromise Accounts (0/2)	Shared Modules	Create Account (2/3)	II Valid Accounts (0/4)	Mark-of-the-Web Bypass	Web Portal Capture	Cloud Account					
	II Establish Accounts (0/2)		Software Deployment Tools	Domain Account	II Access Token Manipulation (1/5)	SIP and Trust Provider Hijacking	Process Injection (2/11)	Email Account					
			Local Account	Local Account	Token Impersonation/Theft	Process Hollowing		Local Account					
			Cloud Account	Cloud Account	Create Process with								



Persistence, Privilege Escalation

## T1543.003 **Create or Modify System Process: Windows Service**

Discovery

T1018      **Remote System Discovery**



ID: T1543.003

Sub-technique of: [T1543](#)

- ① Tactics: Persistence, Privilege Escalation
- ① Platforms: Windows
- ① Effective Permissions: Administrator, SYSTEM
- ① Data Sources: [Command](#): Command Execution, [Process](#): OS API Execution, [Process](#): Process Creation, [Service](#): Service Creation, [Service](#): Service Modification, [Windows Registry](#): Windows Registry Key Creation, [Windows Registry](#): Windows Registry Key Modification
- ① CAPEC ID: [CAPEC-478](#), [CAPEC-550](#), [CAPEC-551](#)

Contributors: Matthew Demaske, Adaptforward; Pedro Harrison; Travis Smith, Tripwire

Version: 1.1

Created: 17 January 2020

Last Modified: 16 September 2020



ID: T1018

Sub-techniques: No sub-techniques

- ① **Tactic:** Discovery
- ① **Platforms:** Linux, Windows, macOS
- ① **Permissions Required:** Administrator, SYSTEM, User
- ① **Data Sources:** **Command:** Command Execution, **File:** File Access, **Network Traffic:** Network Connection Creation, **Process:** Process Creation
- ① **CAPEC ID:** [CAPEC-292](#)

**Contributors:** Daniel Stepanic, Elastic; RedHuntLabs, @redhuntlabs

**Version:** 3.1

**Created:** 31 May 2017

**Last Modified:** 13 April 2021



# DEMO TIME



(venv) Semanur@STG attack\_range\_local %python attack\_range\_local.py -a simulate -st T1543.003 -t attack-range-win10

starting program loaded for B1 battle droid

```
| | Z _ ' ^ .  
| | / O ' - . :  
| - . | |  
| o ( o )  
| | | \ \ . = = , _  
| | | ( o ) = = : : '  
` ` T " "  
  O  
  |\  
  | |\  
  O O  
  | | / /  
  | | / /  
  . ' = = ,
```

attack\_range is using config at path attack\_range\_local.conf  
2021-05-18 12:33:20,953 - INFO - attack\_range - INIT - attack\_range v1

PLAY [all] \*\*\*\*\*

TASK [atomic\_red\_team : Enable strong dotnet crypto] \*\*\*\*\*

ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Microsoft\NetFramework\v4.0.30319)  
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Wow6432Node\Microsoft\NetFramework\v4.0.30319)

TASK [atomic\_red\_team : Check installed providers] \*\*\*\*\*

ok: [10.0.1.17]

TASK [atomic\_red\_team : Install NuGet Provider] \*\*\*\*\*

skipping: [10.0.1.17]

TASK [atomic\_red\_team : Install Atomic Red Team] \*\*\*\*\*

changed: [10.0.1.17]

TASK [atomic\_red\_team : set\_fact] \*\*\*\*\*

ok: [10.0.1.17]

TASK [atomic\_red\_team : include\_tasks] \*\*\*\*\*

included: /Users/Semanur/Documents/GitHub/attack\_range\_local/ansible/roles/atomic\_red\_team/tasks/run\_art\_test.yml for 10.0.1.17

TASK [atomic\_red\_team : set\_fact] \*\*\*\*\*

ok: [10.0.1.17]

TASK [atomic\_red\_team : debug] \*\*\*\*\*

ok: [10.0.1.17] => {  
 "technique": "T1543.003"  
}

TASK [atomic\_red\_team : Get requirements for Atomic Red Team Technique] \*\*\*\*\*

changed: [10.0.1.17]

TASK [atomic\_red\_team : Run specified Atomic Red Team Technique] \*\*\*\*\*

changed: [10.0.1.17]

```
(venv) Semanur@STG attack_range_local % python attack_range_local.py -a simulate -st T1018 -t attack-range-win10
```

```
starting program loaded for B1 battle droid
```

```
  ||/_'\
  ||/O'\-.:
  |-.||
  |o(o)
  |||\ \ .==.-
  |||(o) ==:.'
  _|T  ""
  |O
  ||\
  ||\
  O()
  ||//
  ||//
  _|'\=.
```

```
attack_range is using config at path attack_range_local.conf
```

```
2021-05-18 13:12:36,187 - INFO - attack_range - INIT - attack_range v1
```

```
PLAY [all] *****
```

```
TASK [atomic_red_team : Enable strong dotnet crypto] *****
```

```
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Microsoft\NetFramework\v4.0.30319)
```

```
ok: [10.0.1.17] => (item=HKLM:\SOFTWARE\Wow6432Node\Microsoft\NetFramework\v4.0.30319)
```

```
TASK [atomic_red_team : Check installed providers] *****
```

```
ok: [10.0.1.17]
```

```
TASK [atomic_red_team : Install NuGet Provider] *****
```

```
skipping: [10.0.1.17]
```

```
TASK [atomic_red_team : Install Atomic Red Team] *****
```

```
changed: [10.0.1.17]
```

```
TASK [atomic_red_team : set_fact] *****
```

```
ok: [10.0.1.17]
```

```
TASK [atomic_red_team : include_tasks] *****
```

```
included: /Users/Semanur/Documents/GitHub/attack_range_local/ansible/roles/atomic_red_team/tasks/run_art_test.yml for 10.0.1.17
```

```
TASK [atomic_red_team : set_fact] *****
```

```
ok: [10.0.1.17]
```

```
TASK [atomic_red_team : debug] *****
```

```
ok: [10.0.1.17] => {
  "technique": "T1018"
}
```

```
TASK [atomic_red_team : Get requirements for Atomic Red Team Technique] *****
```

```
changed: [10.0.1.17]
```

```
TASK [atomic_red_team : Run specified Atomic Red Team Technique] *****
```

```
changed: [10.0.1.17]
```

# T1543.003

2-Service Installation CMD	win10	Windows Service Windows Service	<a href="https://attack.mitre.org/techniques/T1543/003">https://attack.mitre.org/techniques/T1543/003</a> <a href="https://attack.mitre.org/techniques/T1543/003">https://attack.mitre.org/techniques/T1543/003</a>	TA0003 TA0004	T1543.003	Service Installation CMD	win10\vagrant
1-Modify Fax service to run PowerShell	win10	Windows Service Windows Service	<a href="https://attack.mitre.org/techniques/T1543/003">https://attack.mitre.org/techniques/T1543/003</a> <a href="https://attack.mitre.org/techniques/T1543/003">https://attack.mitre.org/techniques/T1543/003</a>	TA0003 TA0004	T1543.003	Modify Fax service to run PowerShell	win10\vagrant

## Executed simulations

atomic_test ↕	Hostname ↕	mitre_id ^
1-Remote System Discovery - net	win10	T1018 - Remote System Discovery
3-Remote System Discovery - nltest	win10	T1018 - Remote System Discovery
2-Remote System Discovery - net group Domain Computers	win10	T1018 - Remote System Discovery
5-Remote System Discovery - arp	win10	T1018 - Remote System Discovery
4-Remote System Discovery - ping sweep	win10	T1018 - Remote System Discovery

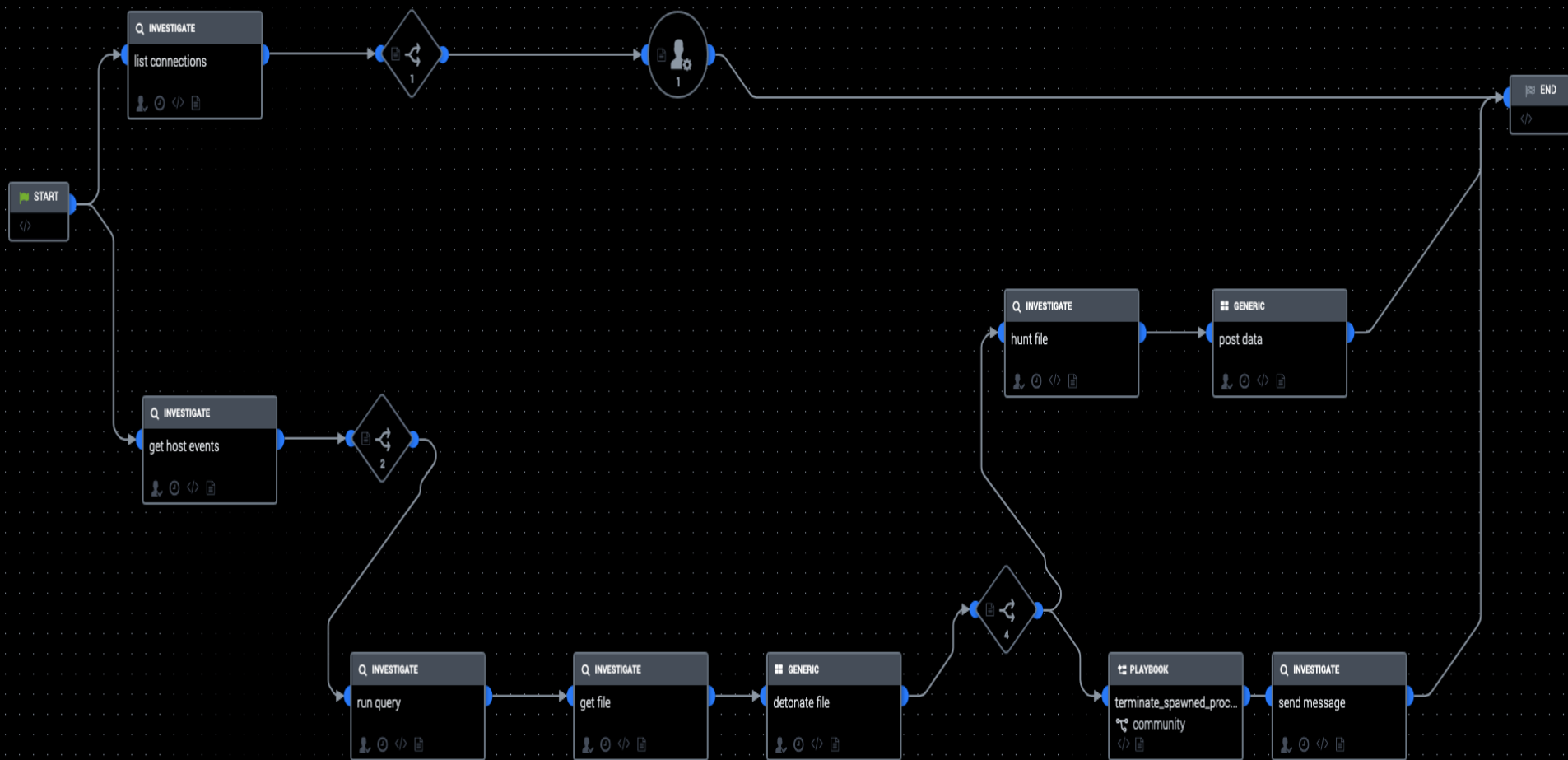
# T1543.003

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	host ▼	win-client-7637484	▼
	<input checked="" type="checkbox"/>	source ▼	XmlWinEventLog:Security	▼
	<input checked="" type="checkbox"/>	sourcetype ▼	XmlWinEventLog	▼
Event	<input type="checkbox"/>	Caller_Domain ▼	WIN10	▼
	<input type="checkbox"/>	Caller_User_Name ▼	vagrant	▼
	<input type="checkbox"/>	Channel ▼	Security	▼
	<input type="checkbox"/>	CommandLine ▼	sc config Fax binPath= "C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe -noexit -c \"write-host 'T1543.003 Test'\""	▼
	<input type="checkbox"/>	Computer ▼	win10	▼



# T1018

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	host ▼	win-client-7637484	▼
	<input checked="" type="checkbox"/>	source ▼	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	▼
	<input checked="" type="checkbox"/>	sourcetype ▼	xmlwineventlog	▼
Event	<input type="checkbox"/>	Channel ▼	Microsoft-Windows-Sysmon/Operational	▼
	<input type="checkbox"/>	CommandLine ▼	"C:\Windows\system32\cmd.exe" /c "nltest.exe /dclist:domain.local"	▼
	<input type="checkbox"/>	Company ▼	Microsoft Corporation	▼
	<input type="checkbox"/>	Computer ▼	win10	▼



# Resources

1. [https://github.com/splunk/attack\\_range\\_local](https://github.com/splunk/attack_range_local)
2. <https://github.com/rabobank-cdc/DeTTECT/tree/master/threat-actor-data/ATT%26CK-Navigator-layers/20210413-FireEye-Mandiant>
3. <https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar>





# Q & A

 [semanurtg](#)