ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Response

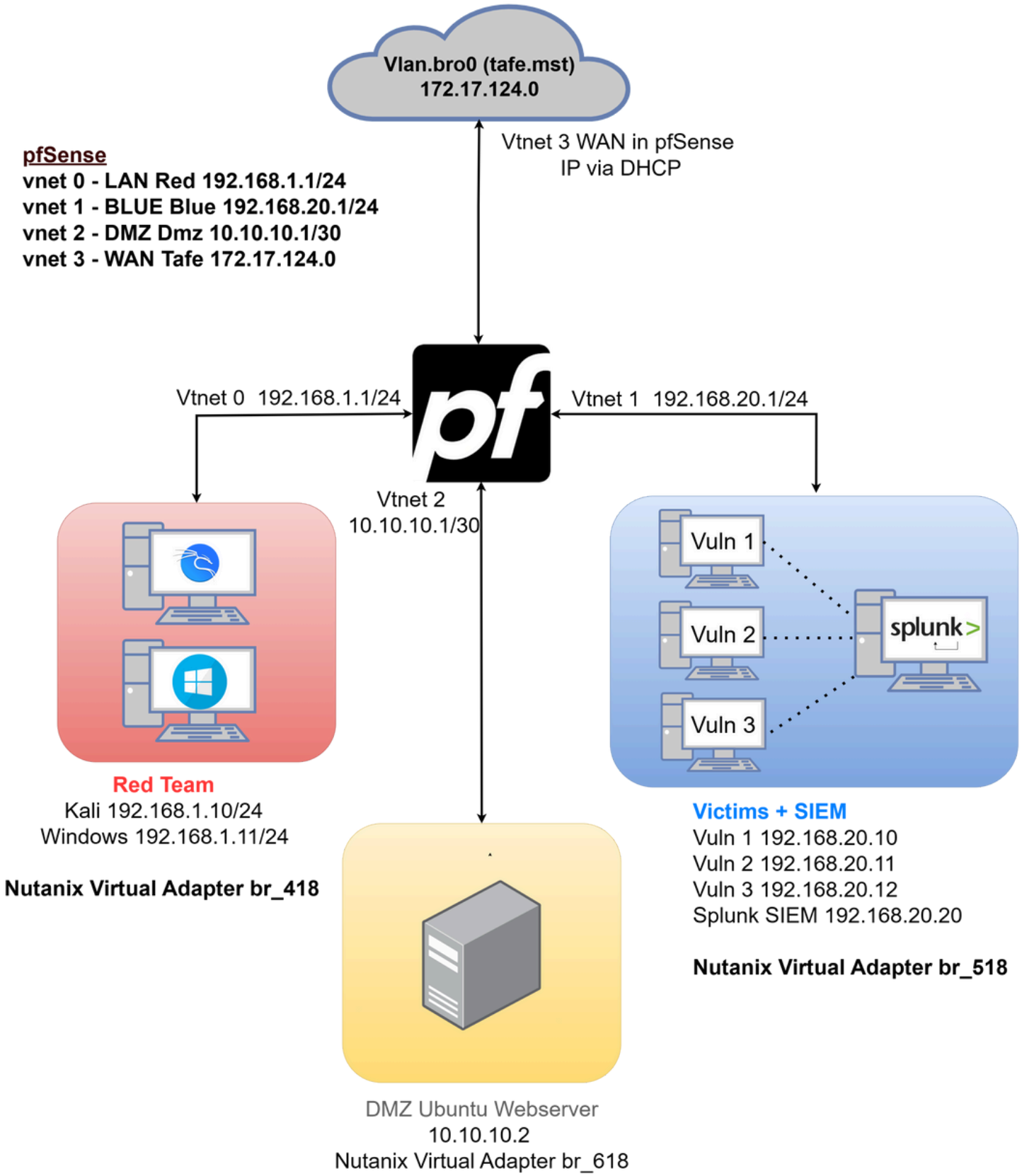
PURPLE TEAM PLAYBOOK

Phishing | Data Exfiltration | Ransomware | Privilege Escalation

WWW.ALPHA7RESPONSE.COM

TABLE OF CONTENTS

NETWORK TOPOLOGY



INTRODUCTION, PURPOSE & SCOPE

Introduction
This Purple Team Playbook provides a structured approach for monitoring and assessing the Red Team/Blue Team IRTx. The goal is to improve security posture by leveraging offensive (Red Team) tactics and defensive (Blue Team) monitoring and response mechanisms.

Purpose
Ensure the Red Team (offensive) and Blue Team (defensive) collaborate effectively to identify and close gaps, improve detection, and streamline response processes.

Scope
Ensures IRTx runs in accordance with the Rules of Engagement, covers pre-exercise coordination, in-exercise monitoring, and post-exercise reporting for the phishing and credential harvesting scenario detailed in the Red Team Runbook.

ROLES AND RESPONSIBILITIES

Purple Team Representative:
• Provide a bridge between Red and Blue Teams, ensuring immediate feedback and coordinated improvements.
• Validate that relevant events are captured in SIEM alerts and logs.
• Track how quickly the Blue Team detects, investigates, and contains the threats.
• Use real-time feedback to adjust Red Team tactics and Blue Team defenses during the exercise.

Red Team Representative: Explains tactics, techniques, and procedures to the Purple Team.

Blue Team Representative: Provides real-time feedback on logs, alerts, and investigations.

Name	Project Role	Project Responsibilities
Adam Baguley	Virtual Environment Lead Red Team Lead	Management and maintenance of technical aspects of Nutanix virtual network environment and providing technical direction to red and blue team co-ordination. Technical lead for red team IRTx activities.
Rachel Willmann	Project Manager Red Team	Management of project within approved constraints, scope, quality, time and budget. Ensure quality and delivery of requirements and outcomes. Contributes to development of red team IRTx activities.
Pavli Fuxova	Communication Lead Blue Team Lead	Outlines and maintains communication channels and methods to be utilised throughout project. Technical lead role for establishing and maintaining blue team IRTx activities.
Mariann Nygaard	Project Status Lead Blue Team	Management of project status, timelines and overall project status. Contributes to blue team IRTx activities.

RULES OF ENGAGEMENT

Exercise Scope:
• All activities must be conducted within the designated virtual environment – Nutanix.
• No real-world systems, networks, or users should be affected by the exercise.
• Pre-approved tools and attack vectors only with no unapproved exploits, malware, or persistent backdoors.

Ethical & Legal Considerations:
• Not permitted to access other users Nutanix.
• All participants must adhere to ethical hacking principles and legal frameworks.
• No real-world personal data should be collected, used, or compromised.

Communication & Coordination:
• Blue Team Playbook provided one week before IRTx.
• Playbook must include enough information to get in (Network Map, IP address range, Email address).
• Purple Team oversees the exercise, ensuring adherence to rules and resolving disputes.
• Out-of-scope incidents or rule violations must be reported immediately to the Purple Team/ Sponsor.
• Post-exercise, all compromised systems should be restored to a known-good state.
• Attack within the defined scenario using agreed-upon tactics (e.g., phishing, privilege escalation, windows enumeration, linux enumeration, MITM, XSS, SQL injection, ransomware, router base attacks, Wi-Fi attacks).
• Defend using only the security tools and configurations available in the environment.
• Monitor and log all activities to identify and respond to threats.
• Contain, eradicate, and recover from Red Team activities following incident response protocols.
• Submit feedback detailing detections, mitigations, and lessons learned.

IRTX ATTACK SCENARIO - MITRE ATT&CK

Phase 1 – Initial Access, Command & Control, Persistence
Goal: Establish a foothold on the victim machine using phishing and remote access tools.

Reconnaissance → Weaponization → Delivery → Exploitation → Installation → C2 → Actions on Objectives

Tactic	MITRE ATT&CK Technique ID	Technique
Inital Access	T1566.002	Phishing email delivering a disguised malware payload (RightPointV3.exe)
Execution	T1204.002	User execution: Malicious file. Victim downloads and runs the payload, establishing an HTTP-based reverse shell
Command & Control	T1071.001	Application Layer Protocol: Web Protocols (HTTP to GitHub) Attacker communicates via a fake GitHub repository, sending commands and receiving output undetected.
Persistence	T1547.001	Registry Run Keys / Startup Folder Malware is configured to run at startup, maintaining access.
Exfiltration	T1567.002	Exfiltration Over Web Service (GitHub exfiltration folder) Victim system is probed for sensitive files, which are exfiltrated via the attackers GitHub account.

Phase 2 – Ransomware Deployment
Goal: Execute ransomware to simulate business impact.

Follows Recon → Weaponization → Delivery → Exploitation → Installation → Actions on Objectives

Tactic	MITRE ATT&CK Technique ID	Technique
Initial Acess	T1566.002	Social engineering tactics identify newly hired, vulnerable staff.
Execution	T1059.003	Windows Command Shell: The ransomware encrypts files in the user's Documents and Pictures folders.
Privilege Escalation	T1055	Process Injection (if ransomware injects into processes)
Impact	T1486	Data Encrypted for Impact (Ransomware) A ransom note is displayed; decryption is contingent on fake "payment".
Defence Evasion	T1027	Obfuscated Files or Information

Phase 3 - Credential Cracking, Privilege Escalation, Data Exfiltration
Goal: Gain privileged access and extract data from the web server.

Lateral movement → Root access → Exfiltration

Tactic	MITRE ATT&CK Technique ID	Technique
Credential Access	T1110.001	Brute Force: Password Guessing (Hydra over SSH) on Ubuntu Server.
Lateral Movement	T1021.004	Remote Services: SSH
Privilege Escalation	T1078	Valid Accounts (gained via brute force or account creation)
Persistence	T1136.001	Create Account: Local Account (root backdoor)
Exfiltration	T1041	Exfiltration Over C2 Channel (SCP over SSH), all files from /var folder are exfiltrated
Defence Evasion	T1070.004	Indicator Removal: File Deletion (e.g., registry, users)

Evaluation Checklist:

Phase 1: Initial Access, Command & Control, Persistence

Checklist	Item to Validate	Notes/Feedback
☐	Was the phishing email delivered and received by the target system?	
☐	Did the victim execute the `RightPointUpdate.exe` file?	
☐	Was a reverse shell successfully established via HTTP?	
☐	Was persistence successfully installed?	
☐	Was any data exfiltrated (`secrets.txt`) visible on the GitHub exfiltration page?	
☐	Splunk captures the executable being run?	
☐	Splunk detects the ‘echo’ command when a file is written to desktop?	
☐	Splunk detects file exfiltration (port 80)?	
☐	Splunk detects ‘persistence’ function being run?	

Phase 2: Ransonware Deployment

Checklist	Item to Validate	Notes/Feedback
☐	Was the ransomware payload delivered successfully?	
☐	Were files in the `Documents` and `Pictures` folders encrypted as intended?	
☐	Was the ransom note generated and visible on the desktop?	
☐	Was the decryption simulation process confirmed by purple team?	
☐	Were any detection mechanisms triggered during this phase (unusual file access)?	
☐	Was ransomware behavior logged or captured by endpoint monitoring tools?	
☐	Splunk detects ransomware being download with ‘curl’?	
☐	Splunk detects bulk file being encrypted?	

Phase 3: Credential Access, Lateral Movement & Data Exfiltration

Checklist	Item to Validate	Notes/Feedback
☐	Did the attacker successfully brute-force SSH credentials using Hydra?	
☐	Was the SSH login to the Ubuntu server successful using compromised credentials?	
☐	Was a new backdoor/root user (`backdoor`) created on the system?	
☐	Did the attacker access and exfiltrate `/var` or other sensitive directories?	
☐	Were SSH login attempts or account creation events logged on the server?	
☐	Did any host-based or network-based detections trigger during lateral movement?	

Overall Observations:

Checklist	Item to Validate	Notes/Feedback
☐	Was the attack timeline followed accurately from all runbooks?	
☐	Were there any deviations or enhancements worth documenting for future tests?	
☐	Were red team indicators successfully detected at any stage?	
☐	Was the fake GitHub infrastructure functioning?	
☐	Are there recommendations for improving detection, response, or hardening?	

WWW.ALPHA7RESPONSE.COM