ATT&CK®

TuxCare
We Take Care of Linux

WHITEPAPER

The Impact of Live Patching on MITRE ATT&CK™ Classification Tasks

www.tuxcare.com

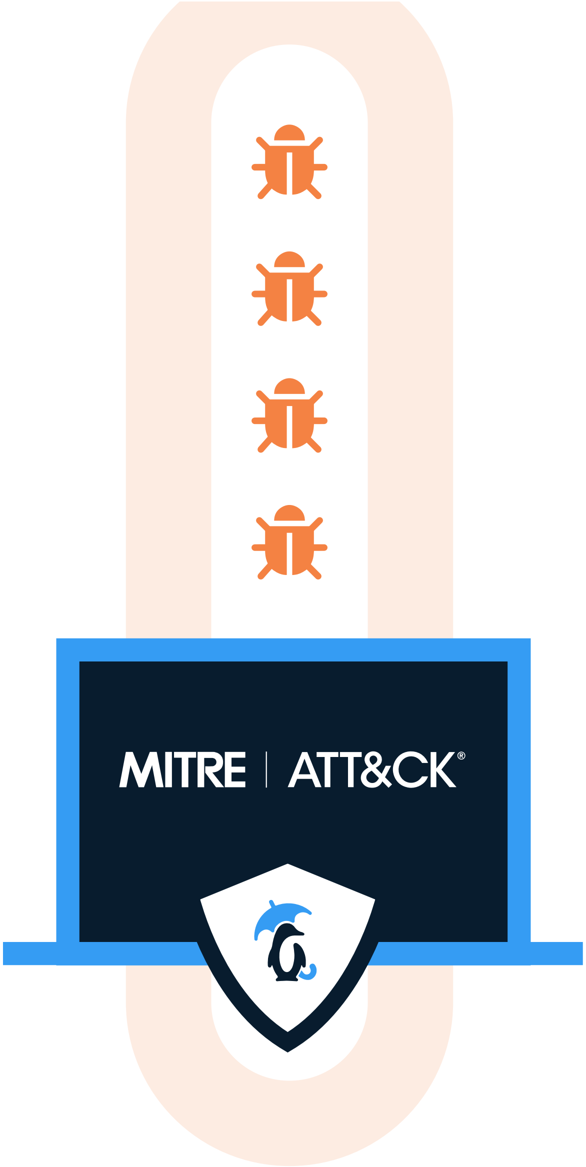
Summary

TuxCare's vulnerability patching technology enables organizations to deliver security updates without reboots or downtime on all popular enterprise Linux distributions as well as deliver patches to end-of-life operating systems long after their vendor-supported lifecycle has ended.

With many organizations using the MITRE ATT&CK™ framework to categorize the cyberattacks that target their systems, TuxCare commissioned this report to demonstrate how its vulnerability patching solutions greatly reduce the number of attacks that need to be categorized through this classification system.

By leveraging TuxCare's **KernelCare Enterprise** and **Endless Lifecycle Support** solutions, organizations can minimize how many tactics, threats, and procedures (TTPs) need to be identified in the first place – as these TuxCare solutions rapidly eliminate vulnerabilities before they become successful cybersecurity incidents.

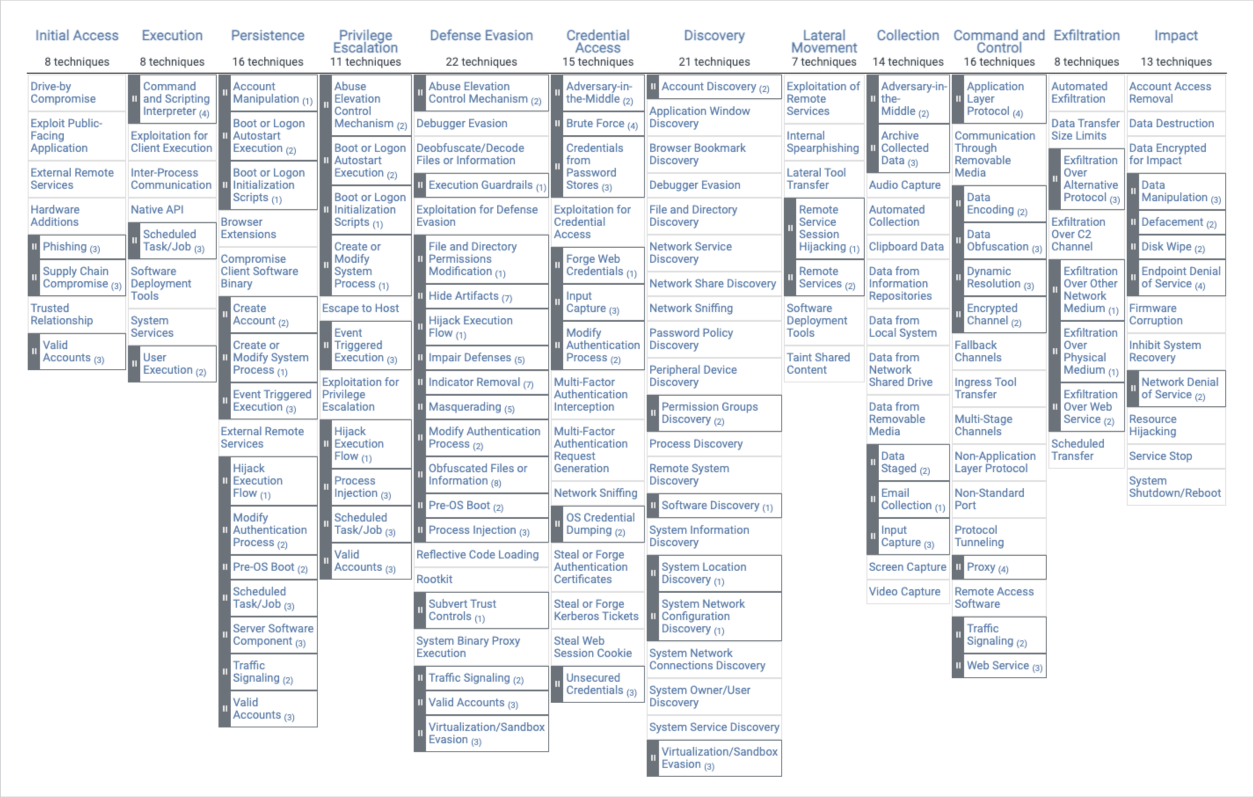
To demonstrate this, this report maps the various Linux OS kernel vulnerabilities identified through the MITRE ATT&CK framework before remediation with TuxCare patching solutions, helping to visualize the various TTPs discovered on the unpatched target machines. After the various patches have been applied, the target systems were found to be significantly more secure.



Report Objective

This report's primary objective is to understand how TuxCare's patching technology reduces vulnerability exposure and improves response times to emerging threats, contextualizing the success of this technology through the lens of the MITRE ATT&CK framework. In addition, this report seeks to provide insight into how such patching mechanisms deliver powerful adaptive control into a standardized security remediation strategy.

Report Scope



Initial Access
8 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (3)

Execution
8 techniques

- Command and Scripting Interpreter (4)
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job (3)
- Software Deployment Tools
- System Services
- User Execution (2)

Persistence
16 techniques

- Account Manipulation (1)
- Boot or Logon Autostart Execution (2)
- Boot or Logon Initialization Scripts (1)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (2)
- Create or Modify System Process (1)
- Event Triggered Execution (3)
- External Remote Services
- Hijack Execution Flow (1)
- Modify Authentication Process (2)
- Pre-OS Boot (2)
- Scheduled Task/Job (3)
- Server Software Component (3)
- Traffic Signaling (2)
- Valid Accounts (3)

Privilege Escalation
11 techniques

- Abuse Elevation Control Mechanism (2)
- Boot or Logon Autostart Execution (2)
- Boot or Logon Initialization Scripts (1)
- Create or Modify System Process (1)
- Escape to Host
- Event Triggered Execution (3)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1)
- Process Injection (3)
- Scheduled Task/Job (3)
- Valid Accounts (3)

Defense Evasion
22 techniques

- Abuse Elevation Control Mechanism (2)
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (1)
- Hide Artifacts (7)
- Hijack Execution Flow (1)
- Impair Defenses (5)
- Indicator Removal (7)
- Masquerading (5)
- Modify Authentication Process (2)
- Obfuscated Files or Information (8)
- Pre-OS Boot (2)
- Process Injection (3)
- Reflective Code Loading
- Rootkit
- Subvert Trust Controls (1)
- System Binary Proxy Execution
- Traffic Signaling (2)
- Valid Accounts (3)
- Virtualization/Sandbox Evasion (3)

Credential Access
15 techniques

- Adversary-in-the-Middle (2)
- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forge Web Credentials (1)
- Input Capture (3)
- Modify Authentication Process (2)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (2)
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials (3)

Discovery
21 techniques

- Account Discovery (2)
- Application Window Discovery
- Browser Bookmark Discovery
- Debugger Evasion
- File and Directory Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (2)
- Process Discovery
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
7 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (1)
- Remote Services (2)
- Software Deployment Tools
- Taint Shared Content

Collection
14 techniques

- Adversary-in-the-Middle (2)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (1)
- Input Capture (3)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
8 techniques

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to classify attacks better and assess an organization's risk. A cyberattack involves many stages and requires multiple methods to reach the desired outcome. MITRE ATT&CK uses the Tactics, Techniques, and Procedures (TTP) metric to measure the security telemetry data coming from XDR and SYSLOG.

The exercise contained within this report was executed on a controlled group of Linux systems, running a variety of standard enterprise Linux distributions, with aggregated log collection and processing through a security information event management (SIEM) platform. These machines provided vulnerability information before and after being protected with TuxCare's two vulnerability patching solutions: **KernelCare Enterprise** and **Endless Lifecycle Support.**

This report aims to illuminate whether, after processing the data from the TuxCare test machines through the LogRhythm-hosted SIEM platform, the MITRE ATT&CK portal gives SecOps and Threat Hunters insight into which TTPs have been most utilized in recent attacks against the four targeted hosts.

For this report, TuxCare collaborated with LinearStack, a LogRhythm and Palo Alto Networks-managed security service provider. The collaboration with different external organizations, with recognized merits in their fields of expertise, provides third-party validation that the findings correspond with actual measurable benefits from the deployed TuxCare solutions.

Testing Platform and Project Engagements

To support this report, TuxCare deployed four virtual machines (VMs) running Enterprise Linux distributions within a virtualized environment. To deploy vulnerability patches to these machines, one of two TuxCare solutions was installed:

KernelCare Enterprise

TuxCare’s flagship live patching solution, which applies vulnerability patches to the Linux kernel while it’s running in memory so that the host does not need to be rebooted to apply each patch.

Endless Lifecycle Support

TuxCare’s patching solution for end-of-life Linux distributions, which provides a repository of vulnerability patches for Linux distributions that have reached the end of their vendor-provided support lifecycle and no longer receive patches from the manufacturer.

The following VMs deployed for this report were designated with one Linux distribution and one TuxCare patching solution:

Ubuntu 16.04

Patching Solution:
TuxCare Endless Lifecycle Support

Ubuntu 20.04

Patching Solution:
TuxCare KernelCare Enterprise

CentOS 6.10

Patching Solution:
TuxCare Endless Lifecycle Support

CentOS 8.5

Patching Solution:
TuxCare KernelCare Enterprise

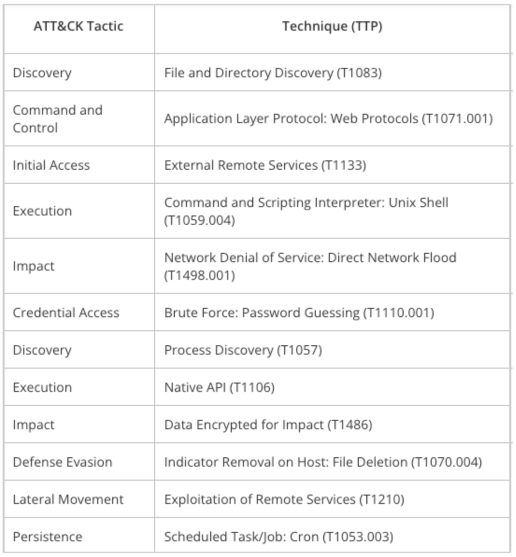
Understanding MITRE TTP and Mapping to Security Telemetry

The MITRE ATT&CK framework provides a broad matrix of tactics for analyzing threats to organizations. The framework is broken down into 12 attack vectors:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Within each attack vector, this framework assigns a TTP tag. The tag links the TTP to the MITRE database, which provides details including:

- The tag number
- Summary details around the TTP
- What OS the TTP impacts
- Procedure examples
- Mitigation
- Detection



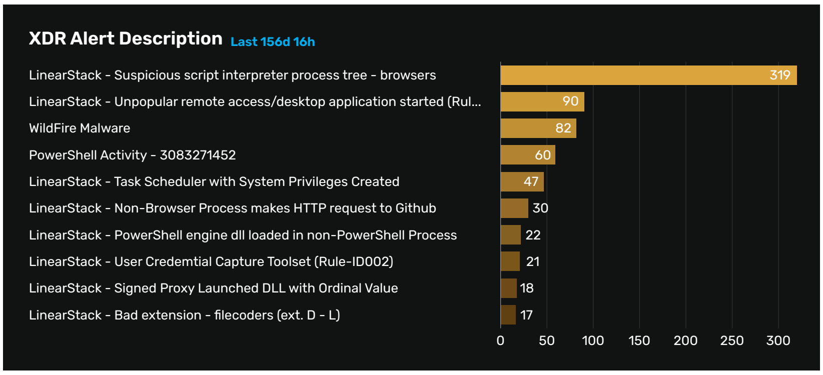
ATT&CK Tactic	Technique (TTP)
Discovery	File and Directory Discovery (T1083)
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)
Initial Access	External Remote Services (T1133)
Execution	Command and Scripting Interpreter: Unix Shell (T1059.004)
Impact	Network Denial of Service: Direct Network Flood (T1498.001)
Credential Access	Brute Force: Password Guessing (T1110.001)
Discovery	Process Discovery (T1057)
Execution	Native API (T1106)
Impact	Data Encrypted for Impact (T1486)
Defense Evasion	Indicator Removal on Host: File Deletion (T1070.004)
Lateral Movement	Exploitation of Remote Services (T1210)
Persistence	Scheduled Task/Job: Cron (T1053.003)

Methodology

LinearStack, an MSSP provider based in New Zealand, provided access to the SIEM platform and the MITRE ATT&CK portal for this report.

LinearStack is a Managed Security Service Provider (MSSP) for LogRhythm's Security Information Event Management (SIEM) and Palo Alto Networks CORTEX Extended Direction and Response (XDR) solution for endpoint security.

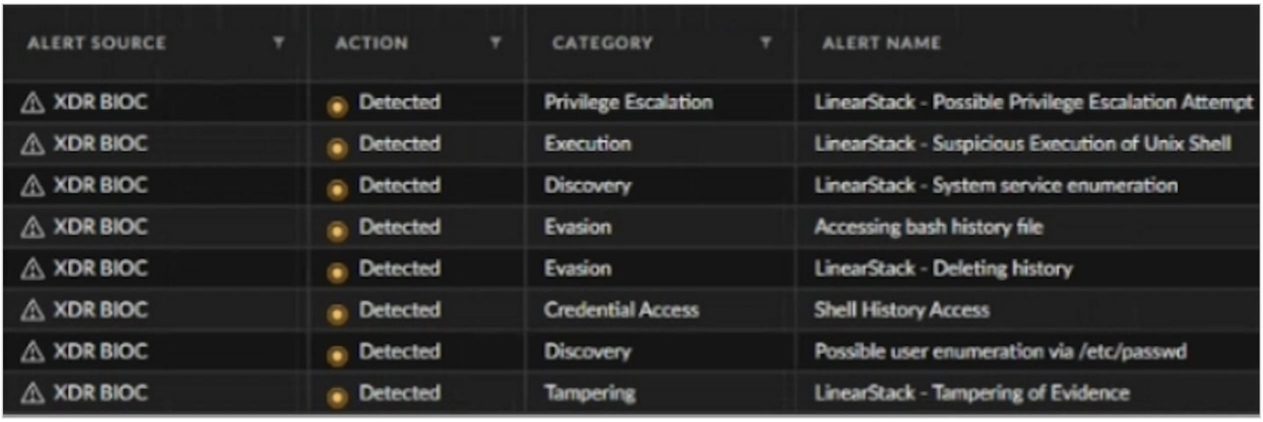
Both solutions were very helpful for this case study. The LogRhythm SIEM played a critical role in both SYSLOG collection and feeding the data into the MITRE portal. The Palo Alto Networks XDR client delivered more real-time security telemetry from the VM test machines into the LogRhythm SIEM Portal.



The LinearStack engineers, in cooperation with TuxCare cloud engineering, helped direct the SYSLOG and XDR telemetry from the four VMs into a hosted LogRhythm SIEM instance managed by LinearStack.

The pentesting, remediation, and risk-reporting data were captured in SYSLOG in real time with a Palo Alto CORTEX XDR client loaded onto the target VMs.

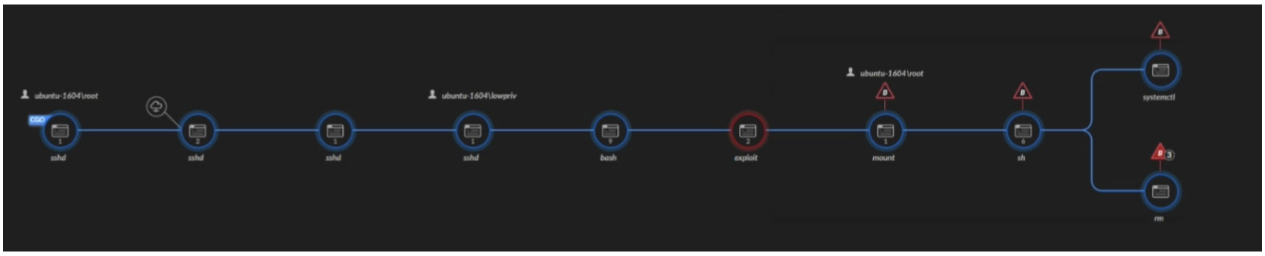
The security telemetry collected into the SIEM platform leveraged several built-in rules and policies, providing deep insight into the various attack methods and vulnerability exploits.



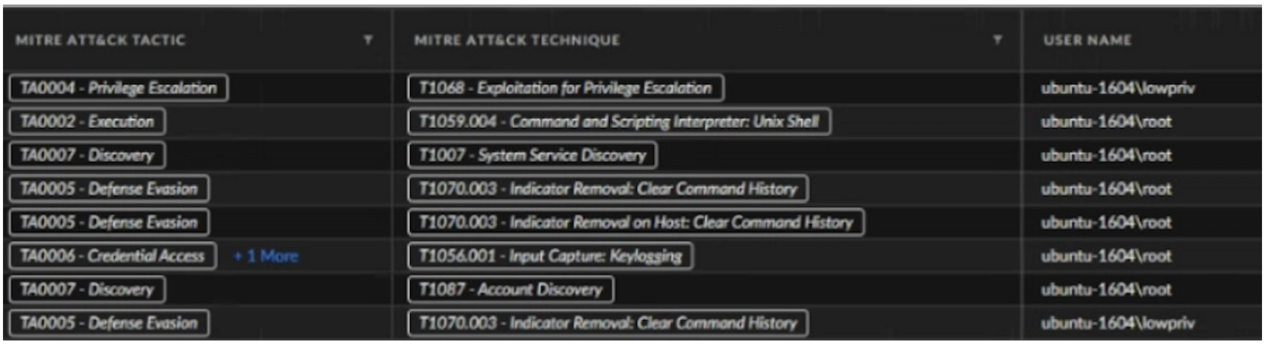
ALERT SOURCE	ACTION	CATEGORY	ALERT NAME
⚠ XDR BIOC	● Detected	Privilege Escalation	LinearStack - Possible Privilege Escalation Attempt
⚠ XDR BIOC	● Detected	Execution	LinearStack - Suspicious Execution of Unix Shell
⚠ XDR BIOC	● Detected	Discovery	LinearStack - System service enumeration
⚠ XDR BIOC	● Detected	Evasion	Accessing bash history file
⚠ XDR BIOC	● Detected	Evasion	LinearStack - Deleting history
⚠ XDR BIOC	● Detected	Credential Access	Shell History Access
⚠ XDR BIOC	● Detected	Discovery	Possible user enumeration via /etc/passwd
⚠ XDR BIOC	● Detected	Tampering	LinearStack - Tampering of Evidence

The LogRhythm SIEM helps categorize the attacks coming into the VMs, including the source of the security telemetry and details about the alert.

The SIEM captured this specific security attack telemetry in real time (red) from the Palo Alto CORTEX XDR agent:

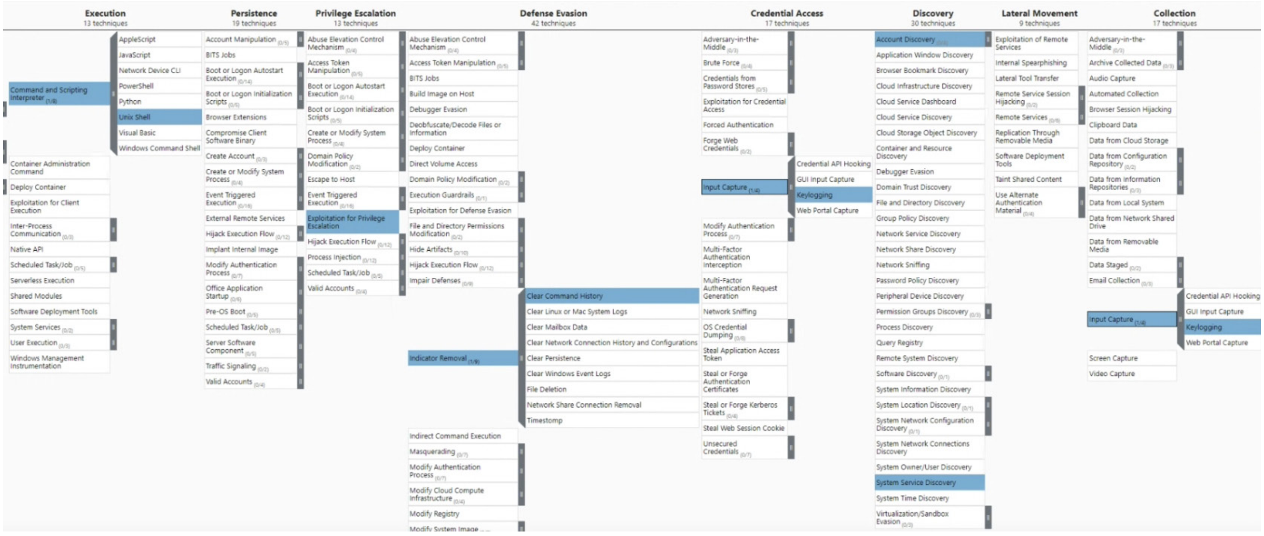


Along with displaying the real-time capture of the event, the LogRhythm SIEM also mapped the attack TTPs to the MITRE framework:



MITRE ATT&CK TACTIC	MITRE ATT&CK TECHNIQUE	USER NAME
TA0004 - Privilege Escalation	T1068 - Exploitation for Privilege Escalation	ubuntu-1604\lowpriv
TA0002 - Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell	ubuntu-1604\root
TA0007 - Discovery	T1007 - System Service Discovery	ubuntu-1604\root
TA0005 - Defense Evasion	T1070.003 - Indicator Removal: Clear Command History	ubuntu-1604\root
TA0005 - Defense Evasion	T1070.003 - Indicator Removal on Host: Clear Command History	ubuntu-1604\root
TA0006 - Credential Access + 1 More	T1056.001 - Input Capture: Keylogging	ubuntu-1604\root
TA0007 - Discovery	T1087 - Account Discovery	ubuntu-1604\root
TA0005 - Defense Evasion	T1070.003 - Indicator Removal: Clear Command History	ubuntu-1604\lowpriv

Once the TTPs were mapped within the SIEM instance, LinearStack SecOps teams activated the ATT&CK framework to see which TTPs were triggered during the pen testing and remediation sequence.



Execution
13 techniques

- Command and Scripting Interpreter (1/8)
  - AppleScript
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (0/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (0/12)
- Implant Internal Image
- Modify Authentication Process (0/7)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component (0/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (0/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (0/12)
- Impair Defenses (0/9)
- Indicator Removal (1/9)
  - Clear Command History
  - Clear Linux or Mac System Logs
  - Clear Mailbox Data
  - Clear Network Connection History and Configurations
  - Clear Persistence
  - Clear Windows Event Logs
  - File Deletion
  - Network Share Connection Removal
  - Timestomp
- Indirect Command Execution
- Masquerading (0/7)
- Modify Authentication Process (0/7)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
  - Credential API Hooking
  - GUI Input Capture
  - Keylogging
  - Web Portal Capture
- Modify Authentication Process (0/7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/7)

Discovery
30 techniques

- Account Discovery (1/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (1/4)
  - Credential API Hooking
  - GUI Input Capture
  - Keylogging
  - Web Portal Capture
- Screen Capture
- Video Capture

Success Factors for SecOps and Threat Hunters

By leveraging the MITRE ATT&CK portal, threat hunters and SecOps teams can see which Linux OS TTPs are used by hackers. In this exercise, the blue boxes (above) show actual threat data telemetry from the targeted TuxCare cloud VMs, based on data collected from both SYSLOG and the XDR client.

The threat hunters can analyze the blue boxes for further details about the attack and the severity level.

The MITRE Framework tracks several TTPs specific to the Linux OS kernel. Here is an example of a TTP that was identified:

ID:	T1547.006
Sub-technique of:	T1547
Tactics:	Persistence, Privilege Escalation
Platforms:	Linux, macOS
Permissions Required:	root

Hackers may alter the kernel to activate programs automatically on system startup. Loadable Kernel Modules (LKMs) are fragments of code that can be loaded and unloaded into the kernel. They augment the capacity of the kernel without having to restart the system. The device driver permits the kernel to communicate with machines connected to the system.

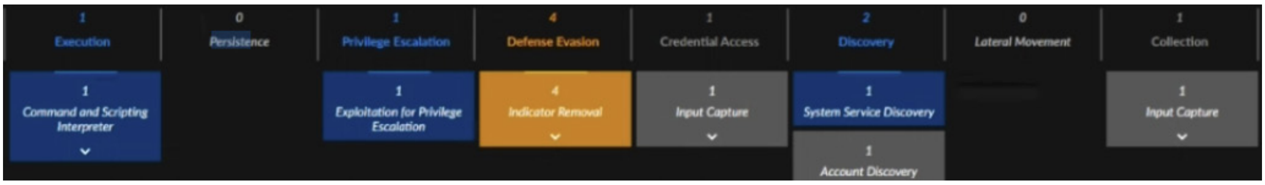
Malicious LKMs can form a kernel-mode Rootkit and gain the highest system privilege. Some of the common characteristics of these LKM Rootkits are hiding, masking selected files, processes, and network traffic, altering logs, providing allowed backdoors, and granting non-privileged users root access.

MITRE ATT&CK helps in understanding adversaries by quantifying and classifying their behavior. Various terminology and classification of particular techniques and methods provide a unified experience of threat actors and facilitate responses by providing a standard response framework and process for each TTP. A single classification system allows for identifying a threat's TTP to take a specific action.

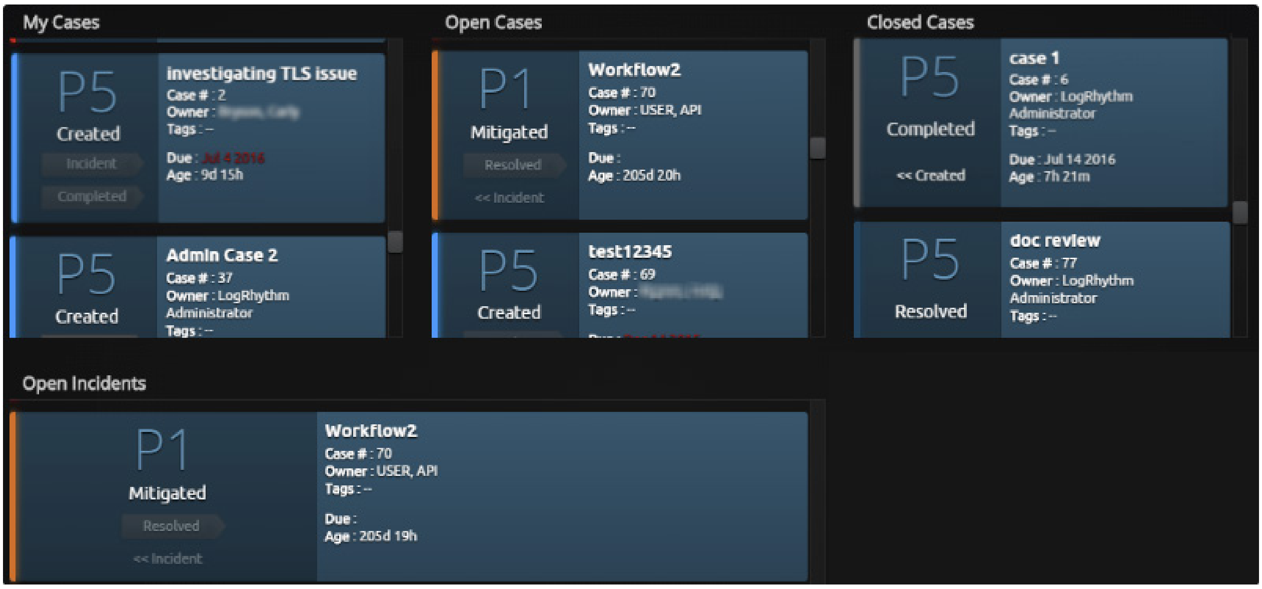
The Value of TuxCare Patching Solutions for Threat Hunting Using MITRE

With MITRE's detailed reporting of TTPs, threat hunters have the needed detail to understand the preferred channels of the attacks against their hosts. SecOps also sees this information to help determine a remediation strategy.

By enabling both **KernelCare** and **Endless Lifecycle Support** from TuxCare, SecOps teams can track these solutions' effectiveness with the LogRhythm SIEM and the MITRE ATT&CK Portal by capturing the decline in reported vulnerabilities once the TuxCare remediations became enabled across the target machines.



By clicking on the various boxes, SecOps and threat hunters can see specific details about the latest TTPs after either of TuxCare's solutions have been enabled.



My Cases

P5 Created
Incident
Completed
investigating TLS issue
Case # : 2
Owner : [redacted]
Tags : --
Due : Jul 4 2016
Age : 9d 15h

P5 Created
Admin Case 2
Case # : 37
Owner : LogRhythm Administrator
Tags : --

Open Cases

P1 Mitigated
Resolved
<< Incident
Workflow2
Case # : 70
Owner : USER, API
Tags : --
Due :
Age : 205d 20h

P5 Created
test12345
Case # : 69
Owner : [redacted]
Tags : --

Closed Cases

P5 Completed
<< Created
case 1
Case # : 6
Owner : LogRhythm Administrator
Tags : --
Due : Jul 14 2016
Age : 7h 21m

P5 Resolved
doc review
Case # : 77
Owner : LogRhythm Administrator
Tags : --

Open Incidents

P1 Mitigated
Resolved
<< Incident
Workflow2
Case # : 70
Owner : USER, API
Tags : --
Due :
Age : 205d 19h

LogRhythm's case handling portal can be shared with colleagues, who can build on forensic information and annotations to quicken threat detection and response. All action is traced as a part of the event history, showing the current status and an unalterable examination line. Accessibility can be obstructed for any individual to ensure secrecy. Case Management allows organizations to dramatically enhance the capability and productivity of their security operations and disaster response facilities.

Validation of Adaptive Controls With MITRE

Organizations deploy several adaptive controls to protect their digital assets from a TTP identified through the MITRE ATT&CK framework. MITRE is an excellent tool to validate adaptive security controls and their effectiveness.

Similar to seeing the success of TuxCare's patching technology, organizations can validate other controls, including email security, XDR, and cloud security, to ensure those tools protect the organization correctly.

Conclusion

The MITRE ATT&CK framework provides detailed information to help justify the funding for security mitigation by identifying the highest risk assets and what TTPs cybercriminals use. By accessing this valuable intel, organizations will have the needed data for the correct security adaptive control to remediate and reduce risk.

By running an exercise with four virtual machines with four common Linux operating systems and examining which TTPs they were successfully targeted with before and after arming these machines with TuxCare solutions, this report validated the effectiveness of TuxCare’s Linux patching technology.

With the results of this exercise as a benchmark, organizations that enable either T uxCare’s **KernelCare Enterprise** or **Endless Lifecycle Support** have a very strong likelihood of noticing a steep drop in – or complete elimination of – vulnerabilities in their Linux-based operating systems. In addition, using the MITRE portal and the SIEM solution from LogRhythm, organizations can measure the effectiveness of patching in the near term to help reduce the high-risk vulnerabilities embedded within their Linux OS kernels.

About TuxCare

TuxCare enables enterprises to shrink their vulnerability exposure, avoid patching-related downtime, and stay compliant with three popular Linux security solutions. **KernelCare Enterprise** automatically applies the latest vulnerability patches on all popular Linux distributions without reboots or downtime. **Endless Lifecycle Support** provides ongoing patches for several end-of-life Linux distributions, as well as PHP and Python software languages. AlmaCare is an enterprise-grade support service for AlmaLinux, providing automated security updates, rebootless patching, painless compliance, and more.

Learn More

About LINEARSTACK

Founded in 2013 with a strong focus on world-class cyber security services, LinearStack was built from the ground up in Auckland, New Zealand and now makes information security simple and accessible for all organizations. LinearStack is made up of a team of certified Cyber Defence Analysts, Threat Hunters, Incident Responders, CTI specialists, malware analysts, security architectures, and engineers with two geo-redundant operations centers across the globe.

Learn More