# LDAP-Server hamster.panzer 192.168.56.100

**Owner**: Smooth Beans GmbH
**Reviewer**: Max Mustermann
**Contributors**: Michael Herz, Andy Salewski, David Westmeyer
**Date Generated**: Wed Oct 09 2024

*OWASP Threat Dragon*

# Executive Summary

## High level system description

Systemübersicht:
Diese Virtuelle Maschine (VM) läuft auf Ununtu-Biotic und wird in VirtualBox gehostet. Diese Maschine dienst als administrativer Domain-Controller für die Smooth Beans GmbH mit dem Domain-Namen "hamster.panzer" mit der IP-Adresse 192.168.56.100. Die VM stellt zentrale Dienste wie LDAP und SSH bereit und legt besonderen Wert auf Sicherheit durch den Einsatz verschiedener Schutzmechanismen. Zukünftige Integationen umfassen ein Wazuh SIEM, einen Webserver, Client-Geräte sowie einen dezidierten Backup-Server.

System-Spezifikationen:
- Host-Plattform: VirtualBox VM
- Betriebssystem: Ubuntu-Biotic
- RAM: 4698 MB
- CPU: 2 Kerne

Dienste:

1. LDAP-Dienste:

Bereitstellung von Verzeichnisdiensten für die Administratordomäne 'hamster.panzer'. Dazu gehören Benutzer-Authentifizierung, Autorisierung und zentrale Verzeichnisverwaltung.

2. Remote-Zugriffsdienst für die sichere Administration der VM und der LDAP-Dienste.

Sicherheitsfunktionen:

- ClamAV & ClamAV-Daemon:
Bieten Echtzeitschutz und geplante Virenscans, zur Maleware Detektion um die Systemintegrität zu gewährleisten.

- Snort:
Ein Netzwerk  Intrusion-Detection system, welches den Netzwerkwerkverkehr analysiert und bei potentiell schädlichen Aktivitäten Alarm schlägt.

- Suricata:
Ein Netzwerk-Sicherheitsmonitoring-Tool, welches Eindringversuche erkennen  und verhinden, sowie das Netzwerk überwachen kann. Suricata ist ein Intrusion Detection und Intrusion Prevention System.

- Fail2Ban:
Schützt den LDAP-Server vor Brute-Force-Angriffen, indem es Anmeldeversuche überwacht und verdächtige IP-Adressen blockiert.

-rkhunter:
Zur Detektion von Rootkits, Backdoors und lokalen Exploits, zur gewährleistung der Sicherheit und der Integrität des Systems.

- UFW (Uncomplicated Firewall):
 Eine Firewall-Oberfläche für iptabels, welche den Zugriff auf bestimmte Dienste einschränkt und sichere Kommunikation sicherstellt.

- AppArmor:
Ein Mandatory  Access Control (MAC)-Framework, welches Anwendungen innerhalb spezifischer Sicherheitsprofile beschränkt und so das Risoko bei einer eventuellen Kompromittierung minimiert.

Backup-Strategie:

- BorgBackup:
Die VM nutzt neben den Snapshots auch BorgBackup für effiziente, duplizierte Systemdaten. Dies stellt eine zuverlässige Datenwiederherstellung und den Schutz vor Datenverlust sicher.

Netzwerkkonfiguration:

- IP-Adresse: 192.168.56.100
Der virtuelle LADP-Server wurde mit einem Virtualbox typischen NAT-Netzwerkadpter für Updates und der Installation von Software sowie einem statischen Host-Only Netzwerkadapter zur Integration in das Unternehmens-Netzwerk konfiguriert. Dies gewährleistet einen verlässlichen Zugriff auf den Server aus dem internen Netzwerk bei gleichzeitiger gewährleistung der Verbindung in das Internet für Notwendige Updates.

- Domain-Name: "hamster.panzer"
Die Smooth Beans GmbH verwendet diesen einzigartigen Domain-Namen für die Verwaltung sowie die LDAP-Verzeichnisdiesnte.

Trust Boundarys:
Trust Boundaries sind in der IT-Sicherheit die Grenzlinien zwischen verschiedenen Systemen, Komponenten oder Zonen, die unterschiedliche Vertrauensniveaus haben. Diese Grenzen trennen Bereiche, in denen unterschiedliche Sicherheitsanforderungen gelten, z. B. ein internes Netzwerk und das Internet.

Innerhalb eines Trust Boundaries wird davon ausgegangen, dass alle Komponenten ein gewisses Vertrauensniveau teilen, während bei Interaktionen über diese Grenze hinweg zusätzliche Sicherheitsmaßnahmen (wie Authentifizierung, Verschlüsselung oder Firewalls) notwendig sind. In dem Netzwerk des  Unternehmens "Smooth Beans GmbH" welches eigens für dieses Projekt entworfen wurde, wurden von uns mehrere Trust Boundarys definiert, welche nun kurz erläutert werden.

Trust Boundary: LDAP-Administratoren:
Die LDAP-Administratoren benötigen zur effektiven Administration der Admin-Domäne weitreichende Zugriffsberechtigungen, aus diesem Grund umfasst die Trust Boundary "LDAP-Administratoren das gesamte Netzwerk. Nur die Mitglieder dieser Gruppe haben Zugriff und Zugang zu allen Ressourcen, sowie die nötigen Bechtigungen Änderungen und Konfigurationen vorzunehmen.

Trust Boundary: Benutzer/ Clients:
Mitglieder dieser Gruppe haben lediglich Zugriff auf die Ressourcen welche für ihre Arbeit unerlässlich und Notwendig sind, dies umfasst den Zugriff auf LDAP-Dienste sowie den SSH-Dienst. Sie können keine Änderungen an den System- oder Softwarekonfigurationen vornehmen und erhalten keinen Zugriff auf essentielle Prozesse und Stores wie Log-Dateien oder Backup-Prozesse.

Trust-Boundary: Internes Netzwerk:
Dies umfasst alle innerhalb des Firmen-Netzwerks, diese Grenze dienst der Abgrenzung zum Externen Netzwerk (Internet) Zugriff auf Ressourcen des Internen Netzwerks sind nur durch erfolgreiche Authentifizierung über den VPN-Server und die LDAP-Dienst möglich.

Trust Boundary: Backup-Speicher:
Auf diese Grenze haben lediglich die Administratoren Zugriff. In dieser Zone werden die Backup-Daten erstellt, gespeichert und im Notfall abgerufen.

Trust Boundary: extern:
Diese überschneidet sich mit der Demilitarisierten Zone. Die Firewall verhindert den unbefugten Zugriff durch unautorisierte Personen. Externe Entitäten ohne Zugriff auf das Interne Netzwerk haben lediglich Zugang zu den für sie zugänglichen ressourcen des Webservers, auf welchem sich auch der Webshop des Unternehmens befindet.

DMZ-Demilitarisierte Zone:
Eine DMZ (Demilitarisierte Zone) ist ein Sicherheitskonzept in Netzwerken, das einen Bereich zwischen einem internen, vertrauenswürdigen Netzwerk und dem unsicheren Internet schafft. Die DMZ enthält in der Regel öffentlich zugängliche Server (wie Web- oder E-Mail-Server), während der direkte Zugriff auf das interne Netzwerk eingeschränkt wird.

Das Ziel der DMZ ist es, kritische interne Systeme zu schützen, indem man sicherstellt, dass Angriffe auf öffentlich zugängliche Dienste nicht direkt ins interne Netzwerk gelangen. Der Datenverkehr in und aus der DMZ wird meist durch Firewalls und zusätzliche Sicherheitsrichtlinien kontrolliert.

Zukünftige Integration (Außerhalb des aktuellen Umfangs):

- Wazuh-Agent:
Der Wazuh-Agent wird installiert, um die Integration mit dem Wazuh SIEM zu ermöglichen, welches alle relevanten Log-Dateien gebündelt auswertet wodurch die Sicherheitsüberwachung und Ereignisskorrelation bietet.

- Webserver:
Der Webserver mit dem Online-Shop der Smooth Beans GmbH wird in die Domäne intigriet.

- Backup-Server:
Dieses System wird mit einem dezidierten Backup-Server synchronisiert, um das Backup-Management zu gewährleisten.

- Clients:
Verschiedene Clients (Desktop/Notebooks) werden in der Zukunft über den LDAP-Server authentifiziert, dies zentralisiert das Benutzer-Management ebenso wie die Sicherheit des Netzwerks.
Alle Log-Dateien werden verschlüsselt und schreibgeschützt gelagert, um unbefugten Zugriff zu verhindern. Der SSH-Dienst wird per RSA-Key geschützt.

Die Out-of-Scope Elemente sind in dem STRIDE-Diagramm entsprechend dargestellt und dienen dort zur Orientierung, sie werden deshalb nicht spezifisch analysiert und bewertet. Begründung:

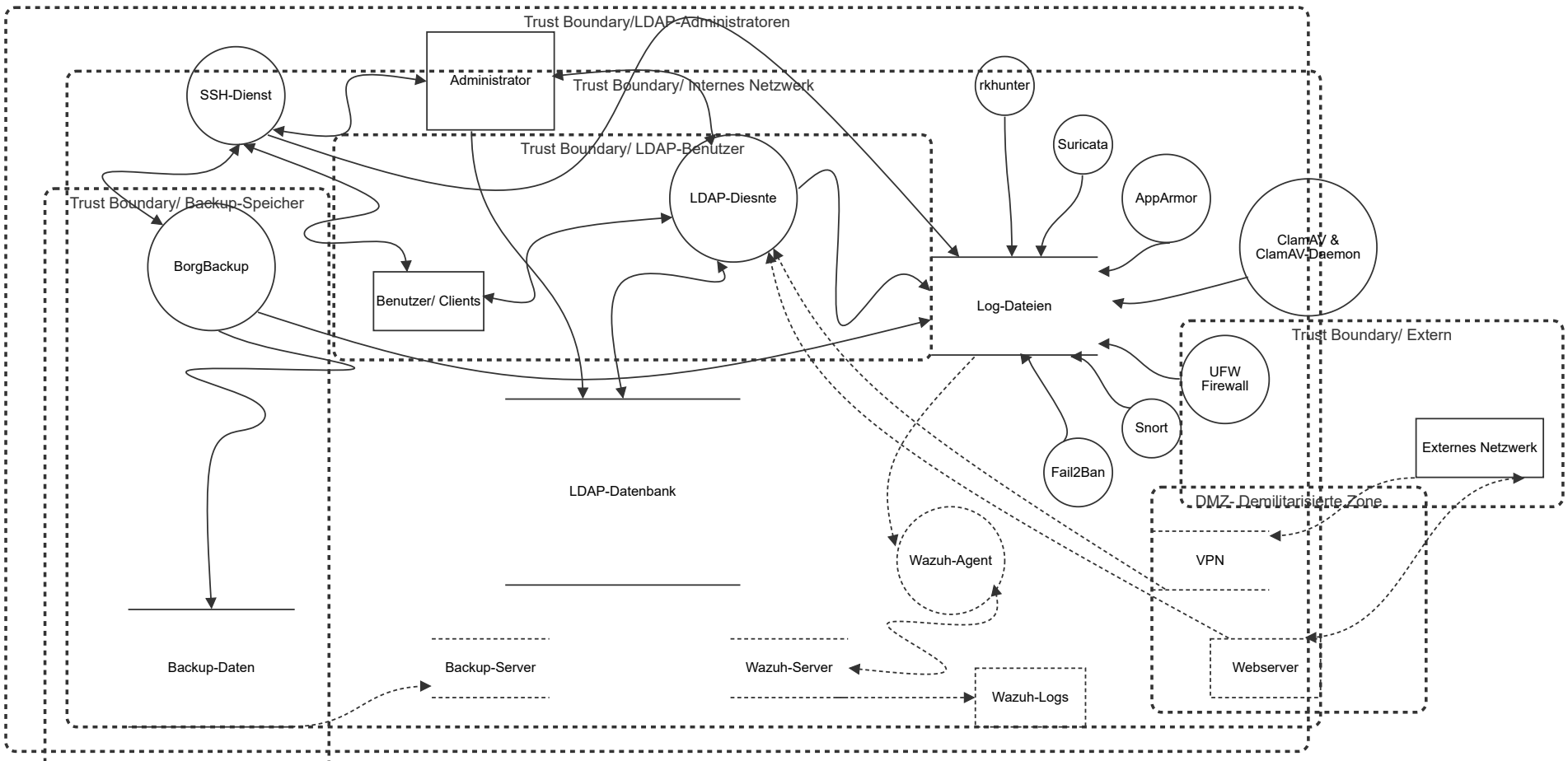
Diese Elemente wurden noch nicht der Domäne hinzugefügt wurden, weshalb sämtliche potentielle Bedrohungen welche auf diese Komponenten zutreffend sind, als nicht Mitiegiert bewertet werden müssen, dies bedarf keiner gesonderten Ausweisung in der nachfolgenden Analyse. eine Anpassung bzw. Erweiterung dieses Modells sollte Zeitnah nach deren Impementierung erfolgen, um den Schutz des LDAP-Servers und des Netzwerkes weiterhin zu gewährleisten.

Der VPN-Server, die Verwendung von Passwortmanagern, eine sichere Passwort-Policy werden als gegeben betrachtet. Auch der Einsatz von MFA (Multi-Faktor-Authentifizierung) wird als gegeben betrachtet.

# Summary

| | |
|---|---|
| **Total Threats** | 83 |
| **Total Mitigated** | 83 |
| **Not Mitigated** | 0 |
| **Open / High Priority** | 0 |
| **Open / Medium Priority** | 0 |
| **Open / Low Priority** | 0 |
| **Open / Unknown Priority** | 0 |

# New STRIDE diagram



# New STRIDE diagram

## Snort (Process)

Überwacht Netzwekverkehr auf verdächtige Aktivitäten.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 15 | New STRIDE threat | Tampering | Medium | Mitigated | 6 | Angreifer könnten die Snort Konfiguration ändern oder die Protokolle manipulieren. | Regelmäßige Integrationsprüfungen der Konfigurationsdateien. |
| 16 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten Snort mit übermäßgem Datenverkehr überlasten. | Kapazitätsplanung und Ressourcenüberwachung. |

## ClamAV-Daemon (Process)

Echtzeit- und Gepannte Scnas des Systems auf Maleware.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 12 | New STRIDE threat | Tampering | High | Mitigated | 7 | Maleware könnte die Virenidentifikationsdateien modifizieren, | Regelmäßige Updates und Integritätsprüfungen. |
| 13 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung des Scanner-Services durch zu viele Anfragen. | Ressourcenüberwachung, Limitierungen. |
| 14 | New STRIDE threat | Elevation of privilege | Medium | Mitigated | 6 | Angreifer könnten Administrative Berechtigungen auf dem System erhalten. | Eingeschränkte Benutzerechte, regelmäßige Sicherheitsaudits. |

## Log-Dateien (Store)

Speichern Protokolle für sicherheitsrelevante Ereignisse.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 31 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation der Log-Dateien zur Spurenverwischung. | Unveränderliche /Schreibgeschütze= Log-Server, regelmäßige Integritätsprüfungen. |
| 32 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Unbefugte könnten Zugriff auf sensible Informationen in den Log-Dateien erlangen. | Zugriffskontrollen und Datenverschlüsselung. |

## LDAP-Datenbank (Store)

Speichert LDAP-Informatonen und Berechtigen

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 28 | New STRIDE threat | Tampering | High | Mitigated | 8 | Unbefugte Änderungen an den gespeicherten Daten in der Datenbank. | Zugriffskontrollen, regelmäßige Backups und Integritätsprüfungen. |
| 29 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Sensible Daten der LDAP-Datenbank könnten offen gelegt werden. | Datenverschlüsselung und Zugriffskontrollen. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 30 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten die Verfügbarkeit der Datenbank beeinträchtigen. | Überwachung und Ressourcenmanagement. |

# Suricata (Process)

Netzwerküberwachung und tiefergehende Analyse.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 17 | New STRIDE threat | Tampering | Medium | Mitigated | 6 | Unbefugte Änderungen an den Regeln könnten vorgenommen werden. | Schutzeinstellungen für Konfigurationsdateien, regelmäßige Überprüfungen. |
| 18 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten den Netzwerkverkehr so beeinflussen, dass Suricata funktionsunfähig wird. | Lastenausgleich und redundante Systeme. |

# Fail2Ban (Process)

Verhindert Brute-Force-Angriffe durch IP-Sperrung.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 19 | New STRIDE threat | Denial of service | Medium | Mitigated | 5 | Angreifer könnten Brute-Force-Angriffe versuchen um Sperrung zu umgehen. | Überwachung und Anpassung der Sperregeln, Nutzung von Ratelimits. |

# rkhunter (Process)

Überprüfung des Systems auf Rootkits.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 20 | New STRIDE threat | Tampering | Medium | Mitigated | 6 | Angreifer könnten die rkhuter-Konfigurationsdateien ändern oder die Scans manipulieren. | Integriätsprüfunegn der Kofigurationsdaten, Logging aktivieren. |
| 21 | New STRIDE threat | Denial of service | Medium | Mitigated | 5 | Überlastung des rkhunter services durch zu viele Anfragen. | Regelmäßige Wartung und Überwachung der Systemressourcen. |

# UFW
# Firewall (Process)

Steuert und filteret Netzwerkzugriffe.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 22 | New STRIDE threat | Tampering | Medium | Mitigated | 6 | Änderung der bestehenden Firewallregeln durch Unbefugte, um Zugang zu erlangen. | Zugriffsbeschränkungen- und Kontrollen für Firewall-Konfiguration, Logging aktivieren. |
| 23 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung der Firewall durch übermäßiges Verbindeungsaufkommen. | Überwachung und Begrenzung der Verbindungen. |

# AppArmor (Process)

Beschränkt den Zugriff auf Systemdienste.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 24 | New STRIDE threat | Tampering | Medium | Mitigated | 6 | Manipulation der AppArmor-Profile durch unbefugte zur Erlangung von Zugriffsberechtigungen. | Regelmäßige Überprüfungen sowie Audits der profile. |
| 25 | New STRIDE threat | Elevation of privilege | High | Mitigated | 7 | Angeriferkönnte die Rechte bestimmter Prozesse erhöhen. | Strikte Zuweisung von Rechten und Rollenkontrolle. |

# Data Flow (Data Flow)

Bideirektionaler Datenfluss zwischen der LDAP-Datenbank und den LDAP-Diensten.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|

# Data Flow (Data Flow)

Bidirektionaler Datenfluss zwischen SSH-Dienst und Benutzern/Clients

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 43 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation der SSH-Verbindung, um unberechtigten Zugang zu erhalten oder Befehle auszuführen. | SSH mit modernen Verschlüsselungsalgorithmen wie AES oder RSA. |
| 44 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Sensible Daten könnten duch unsichere SSH-Verbindung offengelegt werden. | Eindatz von sicheren Verschlüsselungsprotokollen wie AES oder RSA. |
| 45 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung des SSH-Dienstes durch Brute-Force-Angriffe oder zu viele Verbindungsanfragen. | Fail2Ban, UFW-Konfiguration, Rate-Limeting. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von den LDAP-Diensten zu den Log-Dateien

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 48 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation der Logs, um LDAP-Aktionen zu verbergen oder zu fälschen. | Logs auf Remote-Server speichern, regelmäßige Integritätschecks. |
| 49 | New STRIDE threat | Information disclosure | Medium | Mitigated | 6 | Sensible Informationen aus LDAP-Anfragen könnten die Log-Dateien offengelegt werden. | Verschlüsselung der Logs, Zugriffskontrollen. |

# Data Flow (Data Flow)

Unidirektionaler Datenfluss von dem BorgBackup-Prozess zu den Backup Daten

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 50 | New STRIDE threat | Tampering | High | Mitigated | 8 | Unbefugte könnten Backup-Daten könnten Backup-Daten oder löschen. | Verschlüsslung und regelmäßige Überprüfung der Backup-Integrität. |
| 51 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Backup-Daten könnten sensible Informationen enthalten, welche offengelegt werden könnten. | Verschlüsselung der Backup-Daten, Zugriffskontrollen. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 52 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung des Backup-Dienstes, um den Sicherungsprozess zu verhindern oder zu verlangsamen. | Ressourcenmanagement, Rate-Limiting. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss des BorgBackup-Prozesses zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 53 | New STRIDE threat | Tampering | High | Mitigated | 7 | Unbefugte Änderungen der Logs, um Aktionen zu verschleiern oder zu fälschen. | Log-Signierung auf unveränderlichen Systemen. |
| 54 | New STRIDE threat | Information disclosure | Medium | Mitigated | 6 | Sensible Informationen könnten in Log-Dateien des Backup-Prozesses offengelegt werden. | Verschlüsselung und Zugriffskontrollen. |

# Data Flow (Data Flow)

Bidirektional Datenfluss zwischen SSH-Dienst und Administrator.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 55 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation der SSH-Sitzung durch den Administrator oder Angreifer, um unautorisierte Befehle auszuführen. | Nutzung von MFA, SSH mit modernen Verschlüsslungsmethoden. |
| 56 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Abfangen von sensiblen Informationen, z.B. Anmeldedaten oder Befehle, durch unsichere SSH-Kommunikation. | Sichere Protokolle vie AES oder SSH zur Verschlüsselung. |
| 58 | New STRIDE threat | Tampering | Medium | Mitigated | 7 | Überlastung des SSH-Dienstes durch übermäßige Anfragen oder Brute-Force-Angriffe. | Fail2Ban, UFW-Konfiguration, Ressourcenmanagement. |

# Data Flow (Data Flow)

Unidirektionaler Datenfluss vom Administrator zur LDAP-Datenbank.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 59 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation der LDAP-Datenbank durch unbefugte Änderungen, um z.B. Verzeichnisdaten oder Berechtigungen zu ändern. | Zugriffskontrollen , regelmäßige Backupsund Integritätsprüfungen. |
| 60 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Sensible Daten in der LDAP-Datenbank könnten offengelegt werden, z.B. durch ungesicherte Zugriffe des Administrators. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 61 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten durch übermäßige Anfragen oder gezielte Angriffe auf den Administrator die LDAP-Datenbank lahmlegen. | Überwachung und Ressourcenmanagement. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von dem SSH-Dienst zu den Log Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 46 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation der Log-Dateien, um Aktionen zu verschleiern oder falsche Informationen zu erzeugen. | Unveränderliche Log-Server, Signierung der Logs. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 47 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Unbefugter Zugriff auf Log-Dateien und Einsicht in sensible Informationen. | Verschlüsselung der Logs, Zugriffsbeschränkungen. |

# Data Flow (Data Flow)

Bidirektionaller Datenfluss zwischen dem Administrator und den LDAP-Diensten.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 62 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation der Informationen, die von den LDAP-Diensten an den Administrator übermittelt werden. | Integritätsschutz durch Verschlüsselung und Protokollierung. |
| 63 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Der Administrator-Account könnte auf vertrauliche LDAP-Daten zugreifen. | Zugriffsrichtlinien, Datenverschlüsselung. |
| 64 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Durch unzureichend gesicherte LDAP-Dienstes könnte der Administrator den Zugriff auf Verwaltungsfunktionen verlieren. | Überwachung und Schutz der Dienste vor Überlastungen |

# Data Flow (Data Flow)

Bidirektionaller Datenfluss zwischen den Benutzern/Clients und den LDAP-Diensten.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 39 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulation von LDAP-Anfragen durch Man-in-the-Middle Angriffe. | TLS-Verschlüsselung, sichere Verbindungsprotokolle. |
| 41 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Manipulation von LDAP-Daten könnten durch unsichere Kommunikation mit dem Client abgefangen werden. | TLS- oder SSL Verschlüsselung für die Datenübertragung. |
| 42 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung der LDAP-Dienste durch zu viele Anfragen. | Implementierung von Rate-Limitierung und Ressourcenüberwachung. |

# Data Flow (Data Flow)

Bidirektionaler Datenflus zwischen SSH-Dienst und dem BorgBackup-Prozess.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 65 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation der Backups der Backups über eine kompromitiere SSH-Verbindung, um die Daten zu verändern oder zu löschen. | SSH mit starker Verschlüsselung, MFA für SSH-Zugänge, Zugriffskontrollen. |
| 66 | New STRIDE threat | Tampering | High | Mitigated | 7 | Manipulierte Daten könnten vom Backup-Prozess an den SSH-Dienst übermittelt werden, was zu falschen oder beschädigten Backups führt. | Datenintegritätsprüfungen, Verschlüsselung und Protokiolierung. |
| 68 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Der Backup-Prozess könnte sensible Daten an den SSH-Dienst weitergeben, die dann unsachmenäß geschützt oder offengelegt werden. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 69 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Ein Überlastungsangriff auf den Backup-Prozess könnte die Backups lahmlegen und die Wiederherstellung von Systemdaten behindern. | Ressourcenüberwachung und-management,  Schutz vor Überlstungen. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von ClamAV und ClamAV-Daemon zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 70 | New STRIDE threat | Tampering | High | Mitigated | 8 | Ein Angreifer könnte versuchen, die Log-Einträge von ClamAV zu manipulieren, um die Erkennung von Maleware zu behindern. | Unveränderliche Log-Server, Zugriffskontrollen. |
| 71 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Sensible Informationen über erkannte Bedrohungen könnten in Log-Dateien ungeschützt sein un von unbefugten Nutzern abgerufen werden. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 72 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Übermäßige Log-Einträge könnten die Systemressourcen überlasten und die Leistung von ClamAV beeinträchtigen. | Regelmäßige Überprüfungen und Ressourcenmanagement. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von Snort zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 73 | New STRIDE threat | Tampering | High | Mitigated | 8 | Angreifer könnten versuchen, Snort-Log Dateien zu manipulieren, um Sicherheitsverletzungen zu verbergen. | Unveränderliche Log-Server, regelmäßige Überprüfungen. |
| 74 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Sensible Informationen über Netzwerkverkehr und erkannte Angriffe könnten in Log-Dateien offengelegt werden. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 75 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten versuchen, Snort zu überlasten, was zu einem Verlust an Protokollierungsfunktionen führen könnte. | Ressourcenmanagemt und Überwachung. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von Suricata zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 76 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation der von Suricata erzeugten Logs durch Angreifer, um Sicherheitsereignisse zu verbergen. | Unveränderliche Log-Server, regelmäßige Integritätsprüfungen. |
| 77 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Sensible Informationen über erkannte Angriffe könnten in Log-Dateien sichtbar sein. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 78 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung durch zu viele Log-Einträge könnte die Effizienz von Suricata beeinträchtigen. | Ressourcenmanagement und Überwachung. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von rkhunter zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 79 | New STRIDE threat | Tampering | High | Mitigated | 8 | Ein Angreifer könnte versuchen, die von RkHunter erstellten Log-Dateien zu manipulieren, um Hinweise auf Rootkits oder Backdoor-Prozesse zu verbergen. | Unveränderliche Log-Server, regelmäßige Integritätsprüfungen. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 80 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Log-Dateien könnten sensible Informationen über das System enthalten, welche Angreiffern unbefugten Zugriff ermöglichen. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 81 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Hohe Log-Generierung könnte die Systemressourcen beanspruchen und den Betrieb von RkHunter beeinträchtigen. | Überwachung und Ressourcenmanagement. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von AppArmor zu den LogDateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 82 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation von AppArmor-Log-Dateien um Sicherheitsverletzungen oder Fehlkonfiguration zu verbergen. | Unveränderliche Log-Server, Zugriffskontrollen. |
| 83 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Log-Dateien könnten vertrauliche Informationen über die Sicherheitsrichtlinien und die Systemkonfiguration enthalten. | Datenverschlüsselung und Zugriffsbeschränkungen |
| 84 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angriffe könnten darauf abzielen, die Protokollierungsressourcen von AppArmor zu überlasten, was zu einem Verlust der Sichtbarkeit führen kann. | Ressourcenmanagement und Überwachung |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von der UFW-Firewall zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 85 | New STRIDE threat | Tampering | High | Mitigated | 8 | Ein Angreifer könnte versuchen, die von UFW generierten Log-Einträge zu manipulieren, um unbefugte Zugriffsversuche zu verschleiern. | Unveränderliche Log-Server, regelmäßige Integritätsprüfungen |
| 86 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Unbefugte könnten Zugang zu Log-Dateien erhalten, die sensible Informationen über Netzwerkverbindungen enthalten. | Datenverschlüsselung und Zugriffsbeschränkunge |
| 87 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten versuchen, UFW mit einer Flut von Verbindungsversuchen zu überlasten, was zu einer Unterbrechung der Protokollierung führen könnte. | Ressourcenmanagement und Überwachung. |

# Data Flow (Data Flow)

Unidirektionaller Datenfluss von Fail2Ban zu den Log-Dateien.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 88 | New STRIDE threat | Tampering | High | Mitigated | 8 | Manipulation der von Fail2Ban erstellten Log-Einträge durch einen Angreifer, um wiederholte Angriffsversuche zu verbergen. | Unveränderliche Log-Server, regelmäßige Integritätsprüfungen. |
| 89 | New STRIDE threat | Information disclosure | High | Mitigated | 7 | Informationen über blockierte IPs oder Sicherheitsereignisse könnten in Log-Dateien ungeschützt sein. | Datenverschlüsselung und Zugriffsbeschränkungen. |
| 90 | New STRIDE threat | Denial of service | High | Mitigated | 6 | Angreifer könnten versuchen, die Protokollierung von Fail2Ban zu überlasten, wodurch wichtige sicherheitsrelevante Ereignisse verloren gehen könnten. | Ressourcenmanagement und Überwachung. |

# LDAP-Diesnte (Process)

Verarbeitet Authentifizieungs- und Verzeichnisanfragen.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 3 | New STRIDE threat | Spoofing | High | Mitigated | 8 | Angreifer könnten sich als legitime Benutzer ausgeben. | Provide remediation for this threat or a reason if status is N/ANutzung von sicheren Passwörtern, MFA, TLS-Verschlüsselung. |
| 4 | New STRIDE threat | Tampering | High | Mitigated | 8 | Unbefugte Änderungen an LDAP-Daten könnten vorgenommen werden. | Berechtigungen und Zugriffsrechte beschränken, Integritätsprüfungen. |
| 6 | New STRIDE threat | Repudiation | High | Mitigated | 7 | Benutzer könnte Aktionen leugnen, welche er am LDAP-Dienst durchgeführt hat. | Umfassendes Logging, Benutzerkontenaktivitäten protokollieren. |
| 7 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Sensible Daten im LDAP könnten offen gelegt werden. | Provide remediation for this threat or a reason if status is N/AZugriffskontrollen, Datenverschlüsselung, Anonymisierung. |

# SSH-Dienst (Process)

Ermöglicht Remote-Verwaltung über gesicherte Kanäle.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 8 | New STRIDE threat | Spoofing | High | Mitigated | 8 | Angreifer könnten sich als Administrator ausgeben und Zugriff erhalten. | Nutzung von Public-Key Authentifizierung und MFA. |
| 9 | New STRIDE threat | Tampering | Medium | Mitigated | 7 | Daten könnten während der Übertragung modifiziert werden. | SSH mit starken Verschlüsslungskomponenten konfigurieren. |
| 10 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Angreifer könnten den SSH-Dienst durch Flooding angreifen. | Fail2Ban für IP-Sperrung, Rate Limiting. |
| 11 | New STRIDE threat | Elevation of privilege | High | Mitigated | 7 | Angrifer könnten unbefugte Administrative Berechtigungen erlangen. | Minimize Privileges, strenge Zugriffssteuerung. |

# BorgBackup (Process)

Führt Backups durch und überprüft deren Integrität.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 26 | New STRIDE threat | Tampering | High | Mitigated | 7 | Angreifer könnten Backup-Daten verfälschen oder löschen. | Verschlüsselung der Backups, regelmäßge Integritätsprüfungen. |
| 27 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Übermäßige Anfragen könnten den BAckup-Dienst überlasten. | Ressourcenmanagement und Limits für Anfragen. |

# Backup-Daten (Store)

Gespeicerte Backups der Systemdaten.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 33 | New STRIDE threat | Tampering | High | Mitigated | 8 | Unbefugte könnten Backups verändern oder löschen. | Verschlüsselung und regelmäßige Überprüfungen der Backup-Integrität. |

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 34 | New STRIDE threat | Denial of service | Medium | Mitigated | 6 | Überlastung des BAckup-Dienstes durch übermäßige Anfragen. | Ressourcenmanagement und Limits für Anfragen. |
| 35 | New STRIDE threat | Information disclosure | High | Mitigated | 8 | Offenlegung sensibler in den Backup-Daten gespeicherter Informationen. | Datenverschlüsselung und Zugriffskontrollen. |

# Administrator (Actor)

Verwalter des LDAP-Dienstes und des Systems.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 36 | New STRIDE threat | Spoofing | High | Mitigated | 8 | Impersonitation des Administrators und unbefugter Zugriff. | Nutzung von MFA, sichere einzigartige Passwörter, Überwachung des Zugriffs. |

# Benutzer/ Clients (Actor)

Externe benutzer, welche die LDAP-Dienste nutzen.

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|
| 38 | New STRIDE threat | Spoofing | High | Mitigated | 7 | Angreifer könnten sich als legitime Benutzer ausgeben. | Sichere einzigartige Passwörter, MFA, Zugriffskontrollen. |

# Externes Netzwerk (Actor)

Alle Endgeräte und personen außerhhalb des loklaen Netzwerks

| Number | Title | Type | Priority | Status | Score | Description | Mitigations |
|---|---|---|---|---|---|---|---|