THREAT SIMULATION
OF THE MOMENT

NEW

Linux Insider

common threat

BLACKNOISE

PLATFORM

BlackNoise is the first European breach & attack simulation platform, and aims to assess, evaluate & improve your Cyber capabilities in real conditions.

THREAT SCENARIOS

The platform includes comprehensive presets for threat scenarios (APT, ransomware, wiper, data leak, etc.) and over 1,000 security events, with continuous updates.

>_ ABOUT LINUX INSIDER THREAT

A thorough simulation using common technical actions across attack phases with various techniques from MITRE ATT&CK to assess overall detection capabilities (network and system discovery, lateral movement, defense evasion, credential access, persistence...). This scenario assesses an organization's ability to detect and respond to opportunistic attacks by trusted insiders (such as employees or contractors) or attackers having compromised a resource from the Internet and attempting to spread across the internal network.

>_ WHY PLAY THIS SIMULATION ?

Active threat

This scenario is vital for simulating insider threats targeting Linux systems, focusing on techniques like service discovery (SSH, SMB, databases), brute-force attacks, and credential theft. It reflects real-world tactics used to escalate privileges, establish persistence, and evade detection. With the rise of insider threats, this exercise strengthens an organization's ability to detect lateral movement, secure critical services, and respond swiftly to sophisticated attacks.

Demonstrate Compliance

RGPD ☐ NIS 2 ☑ DORA ☑

Risk assessment

Espionage ☐ Destruction ☐ Data breach & leak ☑

Insider ☑ External attack ☐

Security solution assessed

☑ EDR	☑ NDR	☑ EPP
☐ HONEY POT	☐ FW / PROXY	☐ DLP / DLD
☑ SYSTEM LOGS	☐ ID/PS	☑ SIEM

SIMULATION DETAILS

>_ COMPOSITION

1 high severity events

22 low severity events

>_ TARGETS

Network, Windows, Linux, MacOs

AWS, MS Azure, Google Cloud

>_ ATTACK SCOPE

MITRE ATT&CK matrix

>_ RULES ASSOCIATED

Suricata Rules

Sigma Rules

>_ TECHNICAL DETAILS OF BLACKNOISE SIMULATION

To address this kind of threat, you must validate your capabilities to detect technical adversary behaviors in a short time frame, and validate the effectiveness of your investigation & reaction strategy. For this simulation, BlackNoise will execute the following actions :

- Remote System Discovery: ICMP Scan
- Network Service Discovery: SSH Furtive TCP Scan
- Network Service Discovery: SMB TCP SYN Scan
- Network Service Discovery: Database TCP Connect Scan
- Network Service Discovery: File Share TCP Connect Scan
- Network Service Discovery: Web TCP Connect Scan
- Network Service Discovery: Top 100 Ports TCP Connect Scan
- Brute Force: FTP password guessing
- Brute Force: SSH password guessing
- Brute Force: SMB password guessing
- Session Creation: SSH Password Authentication
- Session Creation: SSH Key Authentication
- System Information Discovery
- System Service Discovery
- Process Discovery
- System Network Configuration Discovery
- Account Discovery: Local Account
- Unsecured Credentials: Credentials in files
- Unsecured Credentials: Private Keys
- Masquerading: Rename sh binary
- Create Account: Local Account
- Account Manipulation: Add Account to Privileged Group
- Indicator Removal: Clear Linux System Logs

>_ STRENGTHEN YOUR DETECTION CAPABILITIES

To effectively tackle this threat model, BlackNoise strongly recommends implementing the following actions:

- Deploy Intrusion Detection Systems (IDS) like Snort or Suricata to detect ICMP scans, stealthy TCP scans (SSH, SMB), and abnormal service probing.
- Restrict access to essential services (SSH, SMB, FTP, databases) using IP whitelisting, firewalls, and default-deny policies for unused ports and services.
- Implement rate-limiting, account lockout mechanisms, and tools like Fail2Ban to block IPs after multiple failed login attempts on SSH, SMB, and FTP.
- Enforce SSH key authentication only, disable password-based login, and use strong cryptographic algorithms for SSH keys. Rotate keys periodically.
- Monitor entries in the main log files such as `/var/log/syslog`, `/var/log/messages`, `/var/log/dmesg`, `/var/log/auth.log`, `/var/log/secure`, `/var/log/cron`, `/var/log/systemd/journal`, `/var/log/audit/audit.log`, `/var/log/nginx`, `/var/log/apache2`, `/var/log/mysql/error.log`.
- Enforce least-privilege access by ensuring users only have the necessary permissions and auditing privileged group memberships.
- Implement FIM to detect changes to critical binaries (e.g., `sh`), system logs, and configuration files. Audit log deletion attempts.
- Use centralized logging solutions (e.g., ELK Stack, rsyslog, syslog-ng) with immutable logs to detect log tampering and maintain a reliable audit trail for incident response.

For additional technical recommendations, visit the BlackNoise platform or [contact us](#) for more information.

CONTACT
contact@blacknoise.co

BLACKNOISE
NEVER TRUST. ALWAYS CHECK.