리눅스 커널 루트킷 점검 가이드

문서버전	작성/수정일	설명	비고
v1.0	2025.12.11	초기버전(최초공개)	-
v1.0-rev1	2025.12.12	누락된 파일시스템 추가: BTRFS	점검가이드 미표기(스크립트(v1.0)에서는 지원 O)

📢 **주의사항**
본 가이드는 레드햇 기반 리눅스 시스템에서 '리눅스 커널 루트킷' 탐지를 지원하기 위한 스크립트를 포함하고 있습니다. 다만, **시스템 별 환경 차이(커널 버전, 보안 설정, 서비스 구성 등)로 인해 해당 명령어나 스크립트 실행 시, 시스템에 예기치 않은 동작 또는 오류가 발생**할 수 있습니다.
따라서 **실행 전 ▲사내 보안 정책 위반 여부, ▲시스템 영향 가능성 등을 반드시 확인**해 주시기 바라며, 실행으로 인해 **발생하는 모든 결과 및 책임은 사용자 본인에게 있음**을 안내 드립니다.

📌 **스크립트 실행 및 진단방법**

⚠️ **시스템 요구사항**

- 운영체제(유닉스 계열은 지원하지 않음)
  - 레드햇 계열 리눅스 (Red Hat Enterprise Linux, CentOS 등)
- 파일시스템: XFS, EXT2, EXT3, EXT4, BTRFS

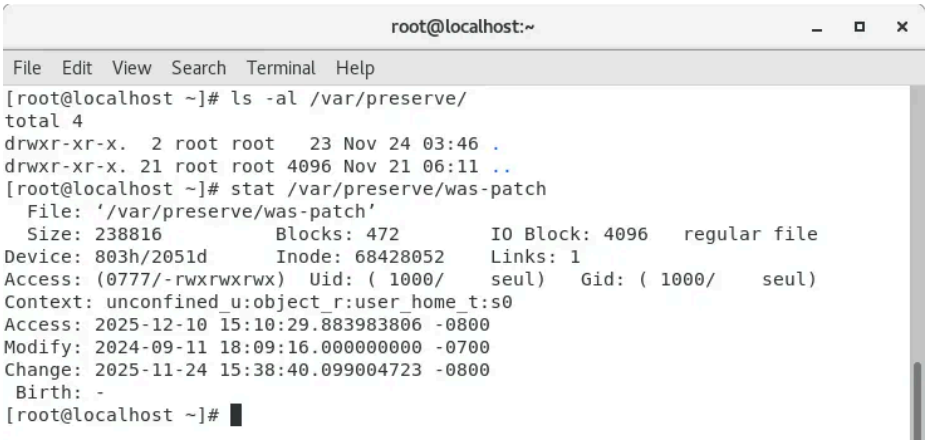
```
# 관리자(root) 권한 및 스크립트 실행권한 부여 필요
./rootkit_detect_scanner_v1.0.sh
# POSIX의 경우 POSIX 호환 스크립트(rootkit_detect_scanner_posix_v1.0.sh) 실행
```

(정상메시지 😀) [OK] No Hidden Entry | Rootkit Not Found | Backdoor Not Found
(비정상메시지 😈) [ALERT] Hidden Entry Found! | Suspicious Rootkit Found! | Backdoor Found!
비정상메시지의 경우 출력된 악성(의심)파일 대상 추가 점검 필요

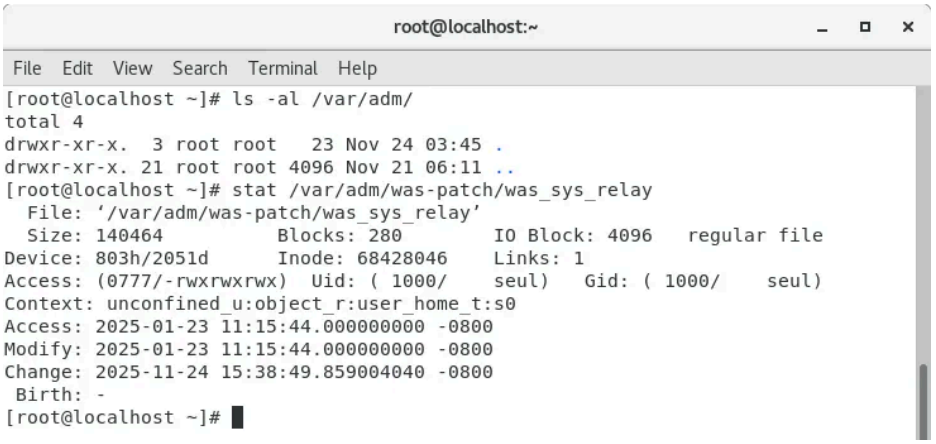
점검 배경 및 감염증상

최근 리눅스 커널 루트킷 및 함께 사용되는 백도어 악성코드의 유행에 따라 점검할 수 있는 스크립트를 개발 및 배포

- **감염증상**
  1. 루트킷(was-patch) 은닉



2. 백도어(was_sys_relay) 은닉



점검 스크립트 동작절차

1. 부팅/서비스 디렉토리 설정(`/etc/systemd/system/`, `/etc/init.d/`, `/etc/rc2.d/`, `/etc/rc3.d/`, `/etc/rc5.d/`)

> 💡 사내 정책상 자동실행경로가 추가로 존재하면 스크립트 수정 후 실행 권장

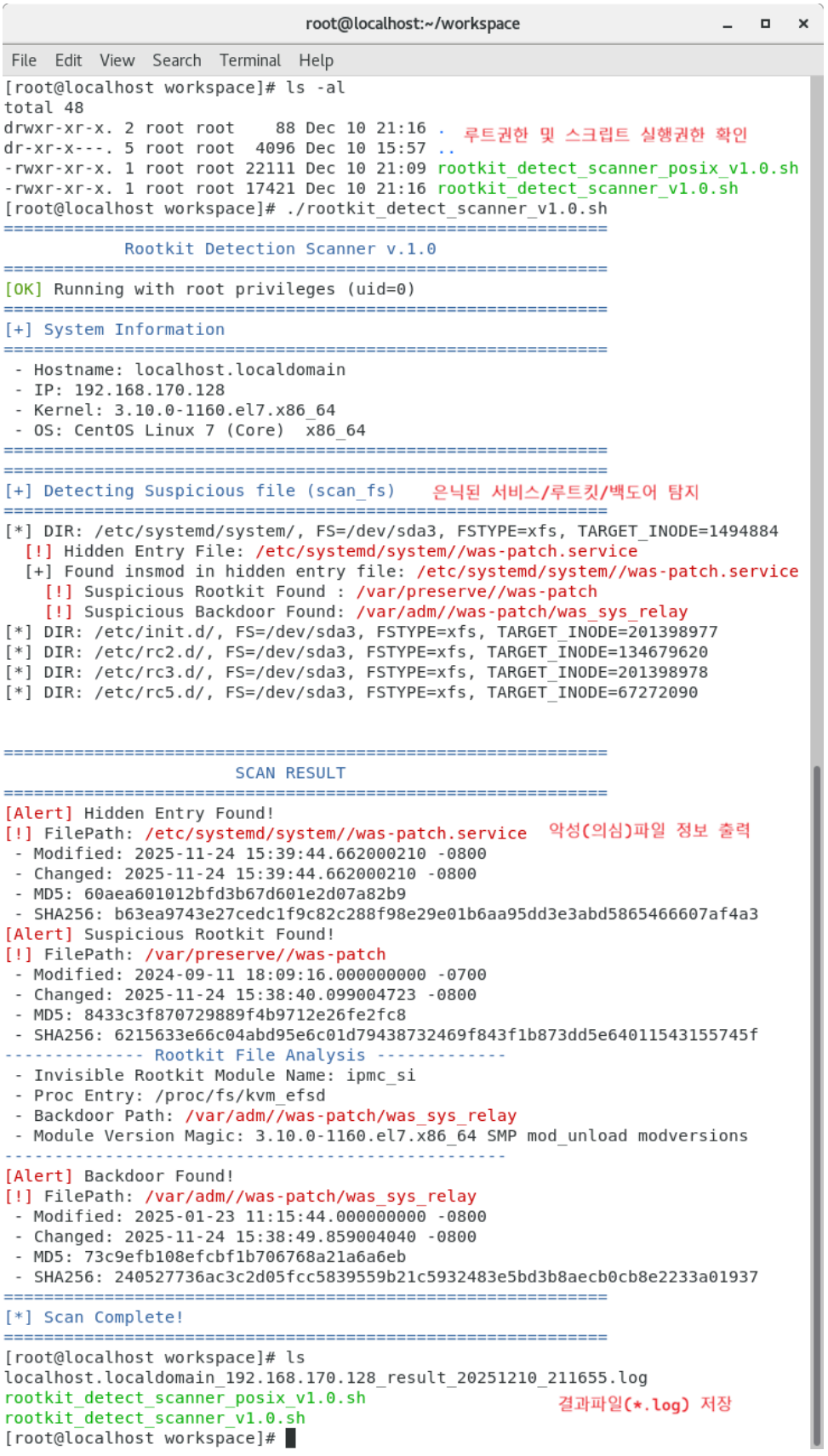
> 현재 유포되고 있는 루트킷은 지속성 유지를 위하여 시스템 부팅시 자동으로 실행되도록 구성되기 때문에 부팅/서비스 스크립트 점검을 통해 악성코드를 탐지하도록 개발

2. 부팅/서비스 디렉토리에 대한 아이노드를 확인하고, 연결된 데이터블록을 조회→ **은닉된 스크립트 포함**

> 💡 **아이노드(inode)와 데이터블록(data block)이란?**
> **아이노드** : 파일타입, 권한, 크기 등 파일에 대한 메타데이터와 데이터의 실제 저장 위치를 가지고 있는 구조체
> **데이터블록** : 디스크 상 실제 파일이 저장되어 있는 공간

3. 리눅스 명령어(`ls`)를 통해 유저 스페이스에서 확인되는 디렉토리 내 파일목록 조회 → **은닉된 스크립트 미포함**
4. 동작절차 2와 3의 차집합을 도출, 은닉된 부팅/서비스 스크립트 존재 확인
5. 스크립트 파일 내 정의되어 있는 루트킷 악성코드 파일경로 확인
6. 루트킷 악성코드 내 문자열을 추출하여 백도어 악성코드 파일경로 확인
7. 탐지된 악성코드(루트킷, 백도어) 실행 시점 및 해시, 프로세스 정보 출력

실행결과


root@localhost:~/workspace
File Edit View Search Terminal Help
[root@localhost workspace]# ls -al
total 48
drwxr-xr-x. 2 root root   88 Dec 10 21:16 .
dr-xr-x---. 5 root root 4096 Dec 10 15:57 ..
-rwxr-xr-x. 1 root root 22111 Dec 10 21:09 rootkit_detect_scanner_posix_v1.0.sh
-rwxr-xr-x. 1 root root 17421 Dec 10 21:16 rootkit_detect_scanner_v1.0.sh
[root@localhost workspace]# ./rootkit_detect_scanner_v1.0.sh
Rootkit Detection Scanner v.1.0
[OK] Running with root privileges (uid=0)
[+] System Information
- Hostname: localhost.localdomain
- IP: 192.168.170.128
- Kernel: 3.10.0-1160.el7.x86_64
- OS: CentOS Linux 7 (Core) x86_64
[+] Detecting Suspicious file (scan_fs)
[*] DIR: /etc/systemd/system/, FS=/dev/sda3, FSTYPE=xfs, TARGET_INODE=1494884
[!] Hidden Entry File: /etc/systemd/system//was-patch.service
[+] Found insmod in hidden entry file: /etc/systemd/system//was-patch.service
[!] Suspicious Rootkit Found : /var/preserve//was-patch
[!] Suspicious Backdoor Found: /var/adm//was-patch/was_sys_relay
[*] DIR: /etc/init.d/, FS=/dev/sda3, FSTYPE=xfs, TARGET_INODE=201398977
[*] DIR: /etc/rc2.d/, FS=/dev/sda3, FSTYPE=xfs, TARGET_INODE=134679620
[*] DIR: /etc/rc3.d/, FS=/dev/sda3, FSTYPE=xfs, TARGET_INODE=201398978
[*] DIR: /etc/rc5.d/, FS=/dev/sda3, FSTYPE=xfs, TARGET_INODE=67272090
SCAN RESULT
[Alert] Hidden Entry Found!
[!] FilePath: /etc/systemd/system//was-patch.service
- Modified: 2025-11-24 15:39:44.662000210 -0800
- Changed: 2025-11-24 15:39:44.662000210 -0800
- MD5: 60aea601012bfd3b67d601e2d07a82b9
- SHA256: b63ea9743e27cedc1f9c82c288f98e29e01b6aa95dd3e3abd5865466607af4a3
[Alert] Suspicious Rootkit Found!
[!] FilePath: /var/preserve//was-patch
- Modified: 2024-09-11 18:09:16.000000000 -0700
- Changed: 2025-11-24 15:38:40.099004723 -0800
- MD5: 8433c3f870729889f4b9712e26fe2fc8
- SHA256: 6215633e66c04abd95e6c01d79438732469f843f1b873dd5e64011543155745f
Rootkit File Analysis
- Invisible Rootkit Module Name: ipmc_si
- Proc Entry: /proc/fs/kvm_efsd
- Backdoor Path: /var/adm//was-patch/was_sys_relay
- Module Version Magic: 3.10.0-1160.el7.x86_64 SMP mod_unload modversions
[Alert] Backdoor Found!
[!] FilePath: /var/adm//was-patch/was_sys_relay
- Modified: 2025-01-23 11:15:44.000000000 -0800
- Changed: 2025-11-24 15:38:49.859004040 -0800
- MD5: 73c9efb108efcbf1b706768a21a6a6eb
- SHA256: 240527736ac3c2d05fcc5839559b21c5932483e5bd3b8aecb0cb8e2233a01937
[*] Scan Complete!
[root@localhost workspace]# ls
localhost.localdomain_192.168.170.128_result_20251210_211655.log
rootkit_detect_scanner_posix_v1.0.sh
rootkit_detect_scanner_v1.0.sh
[root@localhost workspace]#
루트권한 및 스크립트 실행권한 확인
은닉된 서비스/루트킷/백도어 탐지
악성(의심)파일 정보 출력
결과파일(*.log) 저장