정보관리기술사 데일리 다이제스트

2026-11-12 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE LAW NW 정보보안	**N2SF 대응 접속검증·업무웹 격리 보안환경** 근거 국가정보원 국가 망 보안체계(N2SF) 가이드라인 · 망분리 대체 N2SF 보안통제 구현 사례 · etnews.com/20261111000410	N2SF · 망분리 대체 · 접속 검증 · 웹 격리
국제	OS SE 운영체제	**eBPF 루트킷의 커널모듈 없는 은닉 확산** 탐지 우회형 커널 확장 기능 악용 동향 · bleepingcomputer.com/news/security/ebpf-rootkits-why-underground-actors-are-taking-notice/	eBPF · 루트킷 · 커널 후킹 · 탐지 우회
공공·정책	LAW AI SE 법·규제	**AI 침해 위협 대응 개인정보 보호체계 정착** 근거 「개인정보 보호법」(AI 개인정보 침해 대응) · AI 개인정보 침해 대응 정책 방향 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12629	AI 침해 위협 · 개인정보 보호 · 민관 협력

2. 오늘의 토픽 — eBPF 루트킷(eBPF Rootkit)

OS SE | 출제 예상: **1교시**

2-1. 개념 및 정의

eBPF 프로그램을 악용해 커널 모듈 적재 없이 프로세스·네트워크 활동을 은닉하는 루트킷 기법. 탐지 회피와 커널 수준 지속성 확보 목적의 공격 방식.

2-2. 등장 배경

정상 관측·보안 도구의 기반 기술인 eBPF의 공격 전용 활용 확산. 모듈 서명·적재 감시 중심 전통 탐지 체계의 사각지대 노출.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
은닉 기법	시스템콜 후킹, 트레이스포인트, kprobe	커널 훅 지점 가로채기 기반 프로세스·파일 은닉
지속성 확보	BPF 맵, 프로그램 핀닝	bpffs 고정 기반 프로그램 상주와 C2 데이터 은닉
방어 통제	BPF 권한 제한, BPF LSM, 커널 락다운	비특권 BPF 차단과 적재 프로그램 감사

2-4. 시험·실무 관점

- [SE 연계] 커널 모듈 중심 탐지의 한계와 BPF 프로그램 적재 감사
- [OS 연계] eBPF 검증기(Verifier)의 안전성 보장 범위와 한계

답안 필수 키워드 — eBPF / 루트킷 / BPF 검증기 / BPF LSM / 커널 락다운