KITIR WHS 2기 프로젝트 NA팀 오픈소스 정리

작성자: 함준형

2024년 05월 23일 기준

* nDPI
* securityonion – 진행중
* arkime
* dpdk – 진행중
* bcc
* zeek
* suricata
* bpftool - 수정중
* XDP-Firewall
* xdp-tutorial – 진행중
* gpt-2
* BGP-Anycast-Tuner
* ELK Stack

목적: 논문(함준형, 강성원, 최홍석), 개발(함준형, 라민우, 김도현, 지도환, 임정훈) 각 담당팀들의 업무를 보다 수월하게 진행하고자 작성됨.

nDPI

* 설명: 네트워크 트래픽 분석 및 식별을 위한 오픈 소스 DPI 라이브러리.
* 기능 특징: 다양한 프로토콜 식별, 트래픽 분류, 애플리케이션 감지.
* 장단점:
  + 장점: 다양한 프로토콜과 애플리케이션 식별 지원.
  + 단점: 특정 환경에서 성능 문제가 발생할 수 있음.
* 설치 가이드: 프로젝트의 GitHub 페이지 또는 문서를 참조하여 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/nDPI/nDPI%20%ED%99%98%EA%B2%BD%20%EA%B5%AC%EC%84%B1%20%EA%B0%80%EC%9D%B4%EB%93%9C%EB%9D%BC%EC%9D%B8.md>

arkime

* 설명: 네트워크 트래픽 분석 및 패킷 캡처 도구.
* 기능 특징: 대규모 데이터 저장 및 검색, 시각화, 패킷 분석 및 필터링.
* 장단점:
  + 장점: 대규모 데이터 처리에 용이, 다양한 시각화 및 분석 기능 제공.
  + 단점: 설정 및 구성에 대한 학습 곡선이 가팔라 사용자에게는 복잡할 수 있음.
* 설치 가이드: [Arkime GitHub 페이지](https://github.com/arkime/arkime)의 설치 지침을 따라 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/Arkime/Arkime.md>

bcc

* 설명: BPF 컴파일러 컬렉션으로 시스템 및 네트워크 성능 모니터링을 위한 도구 모음.
* 기능 특징: BPF를 사용한 다양한 시스템 및 네트워크 추적 및 분석.
* 장단점:
  + 장점: 시스템 성능 모니터링에 우수, 유연한 BPF 프로그래밍 언어 사용.
  + 단점: 복잡한 BPF 코드 작성 및 디버깅에 대한 기술적 지식 요구.
* 설치 가이드: [BCC GitHub 페이지](https://github.com/iovisor/bcc)의 설치 지침을 따라 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/BCC/About_BCC.md>

Zeek

* 설명: 네트워크 보안 감시를 위한 프레임워크로, 네트워크 트래픽 분석에 초점.
* 기능 특징: 네트워크 트래픽 분석, 보안 이벤트 탐지, 프로토콜 분석.
* 장단점:
  + 장점: 강력한 프로토콜 분석 및 보안 이벤트 탐지 기능.
  + 단점: 초기 설정 및 규칙 작성이 복잡할 수 있음.
* 설치 가이드: [Zeek GitHub 페이지](https://github.com/zeek/zeek)의 설치 지침을 따라 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/zeek/1.%20About%20Zeek.md>

suricata

* 설명: 실시간으로 네트워크 트래픽을 검사하여 보안 이벤트를 감지하는 네트워크 보안 도구.
* 기능 특징: 이상 행위 탐지, 시그니처 기반 및 행위 기반 감지, 네트워크 인터페이스에서 패킷 캡처.
* 장단점:
  + 장점: 다양한 보안 이벤트 감지 기능, 높은 성능 및 신뢰성.
  + 단점: 초기 설정 및 세부적인 튜닝이 필요할 수 있음.
* 설치 가이드: [Suricata GitHub 페이지](https://github.com/OISF/suricata)의 설치 지침을 따라 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/Suricata/About%20and%20Setting%20Guide.md>

xdp-firewall

* 설명: eXpress Data Path를 사용하여 Linux 커널 수준에서 방화벽을 구현하는 프로젝트.
* 기능 특징: 네트워크 트래픽 필터링, XDP 프로그램 개발 및 적용.
* 장단점:
  + 장점: 네트워크 성능에 미치는 영향이 적은 고성능 방화벽 제공.
  + 단점: XDP 프로그래밍 및 커널 모듈 관리에 대한 기술적 지식 요구.
* 설치 가이드: 프로젝트의 GitHub 페이지 또는 문서를 참조하여 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/xdpfw/XDP%20FIREWALL.md>

gpt-2

* 설명: OpenAI가 개발한 대형 언어 모델로, 텍스트 생성 및 이해에 사용됨.
* 기능 특징: 자연어 이해, 텍스트 생성, 언어 모델 평가.
* 장단점:
  + 장점: 뛰어난 텍스트 생성 및 이해 능력.
  + 단점: 크기 및 자원 사용량이 큼.
* 설치 가이드: OpenAI의 공식 문서를 참조하여 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/GPT-2/setting_guide.md>

bgp-anycast-tuner

* 설명: BGP anycast 환경에서 라우팅 경로 최적화를 위한 도구.
* 기능 특징: BGP 라우팅 경로 분석, anycast 대상 선택 최적화.
* 장단점:
  + 장점: BGP anycast 네트워크의 성능을 향상시키는데 유용.
  + 단점: 설정 및 튜닝에 대한 이해가 필요.
* 설치 가이드: 프로젝트의 GitHub 페이지 또는 문서를 참조하여 설치.

<https://github.com/DDoSMitigation/main/tree/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/BGP-Anycast-Tuner>

ELK stack

* 설명: 로그 수집, 저장, 시각화를 구현
* 기능 특징: 실시간 로그 수집 및 분석, 데이터 시각화, 중앙 집중화된 로그 관리.
* 장단점:
  + 장점: 강력한 검색 및 분석 기능, 사용자 친화적인 대시보드 제공, 다양한 데이터 소스와의 통합 가능.
  + 단점: 초기 설정 및 구성 복잡성, 고성능을 위해 상당한 리소스 필요.
* 설치 가이드: 프로젝트의 GitHub 페이지 또는 문서를 참조하여 설치.

<https://github.com/DDoSMitigation/main/blob/main/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4/ELK%20stack/ELK%20stack%20install%20guideline.pdf>