목차

보안점검

- https://www.cisecurity.org/ Center for Internet Security

- NIST 800-53 (National Institute of Standards and Technology) 미국 국립표준기술 연구소
- STIG (Security Technical Implementation Guides) 미국 국방부 보안 표준 가이드
- DISA (Defence Information Systems Agency) 미국 국방정보 시스템
- USGCB (United States Government Configuration Baseline) 미국 연방 기관 보안 표준
- PCI-DSS (Payment Card Industry Data Security Standard) 신용카드/결제기관 데이터 보안 표준
- CJIS (Criminal Justice Information Services) FBI형사 사법 정보 서비스 보안 정책
- ANSSI DAT-NT28 - The National Cybersecurity Agency of France 프랑스 사이버 보안 정책 (이후 Central Directorate for Network and Information Security (DCSSI))로 명칭 변경
- ACSC (Australian Cyber Security Centre) Essential Eight 호주 사이버 보안 센터
- HIPAA (Health Insurance Portability and Accountability Act) 건강보험정보시스템

국내 보안 점검 가이드

- 인터넷 진흥원 기술안내서 가이드
- 보안취약점 점검
- Apache HTTPD 보안취약점 점검
- WAS 보안 취약점 점검

웹 보안성 점검

- https://www.ssllabs.com/
- https://www.immuniweb.com/

국가별 IP 대역 및 차단

국가별 IP대역 데이터를 다운로드 받을수 있는곳

- https://www.ipdeny.com/ipblocks/
- https://www.maxmind.com/en/geolite2/ **회원가입해야만 다운로드 가능**
- https://한국인터넷정보센터.한국/destFile/ipv4.csv
- http://www.ip2nation.com/

firewalld 를 이용하여 중국IP 차단 스크립트

```
#!/bin/bash
IP=$(curl https://www.ipdeny.com/ipblocks/data/countries/cn.zone)


for target in ${IP[*]}
do
        firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source
```

```
address='$target' drop"
done

firewall-cmd --reload
```

굉장이 많은 아이피 대역이 존재하기 때문에 시간이 매우 오래걸린다는것을 감안해야 한다.

OpenSCAP

홈페이지:http://open-scap.org

- OpenSCAP
- https://www.open-scap.org/security-policies/choosing-policy/ openSCAP 에서 지원하는 정책목록

OpenVAS

홈페이지 : http://openvas.org

OpenVAS는 포괄적이고 강력한 취약성 검색 및 취약성 관리 솔루션을 제공하는 여러 서비스 및 도구의 프레임 워크입니다. 프레임 워크는 Greenbone Networks 의 상용 취약성 관리 솔루션의 일부로 2009 년부터 개발이 오픈 소스 커뮤니티에 기여합니다.

실제 보안 스캐너에는 정기적으로 업데이트되는 네트워크 취약성 테스트 (NVT) 피드가 5 만 개가 넘습니다.

모든 OpenVAS 제품은 자유 소프트웨어입니다. 대부분의 구성 요소는 GNU General Public License (GNU GPL)에 따라 라이센스가 부여됩니다.

- OpenVAS

Lynis

홈페이지 : https://cisofy.com/lynis/

Lynis는 Linux, macOS 또는 Unix 기반 운영 체제를 실행하는 시스템에 대한 전투 테스트를 거친 보안 도구입니다. 시스템의 광범위한 상태 검사를 수행하여 시스템 강화 및 적합성 테스트를 지원합니다. 이 프로젝트는 GPL 라이센스 가있는 오픈 소스 소프트웨어이며 2007 년부터 제공됩니다.

OSSEC

홈페이지 : http://www.ossec.net/

OSSEC은 확장 가능한 다중 플랫폼의 오픈 소스 호스트 기반 침입 탐지 시스템 (HIDS)입니다. 로그 분석,

파일 무결성 검사, Windows 레지스트리 모니터링, 중앙 집중식 정책 실행, 루트킷 탐지, 실시간 경고 및 활성 응답을 통합하는 강력한 상관 관계 및 분석 엔진을 가지고 있습니다. Linux, OpenBSD, FreeBSD, MacOS, Solaris 및 Windows에서 동작합니다..