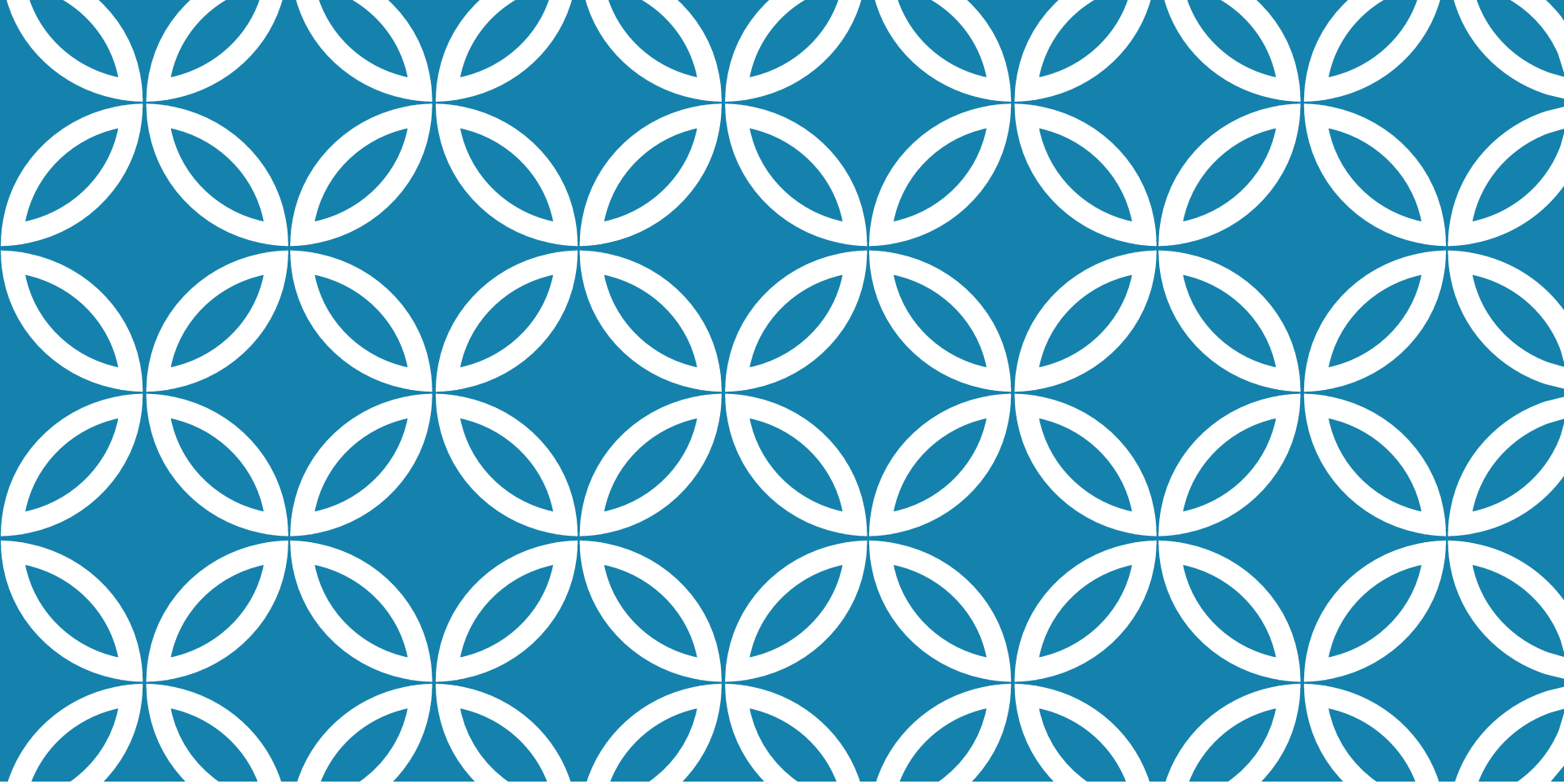


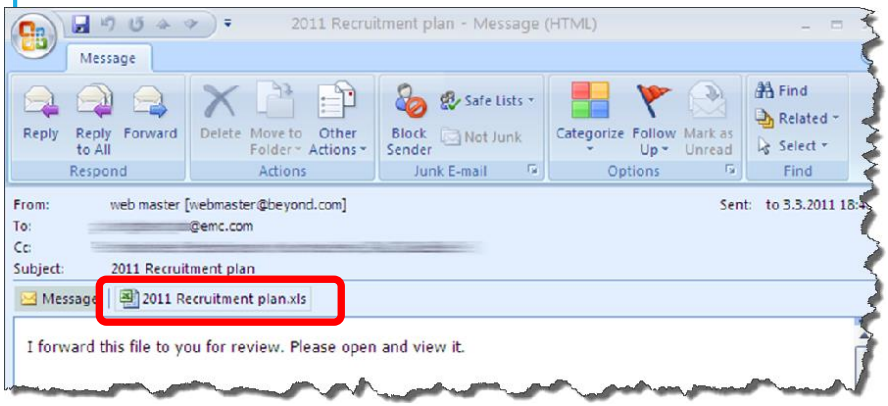
오픈소스 툴 활용으로 보안 200% 강화하기

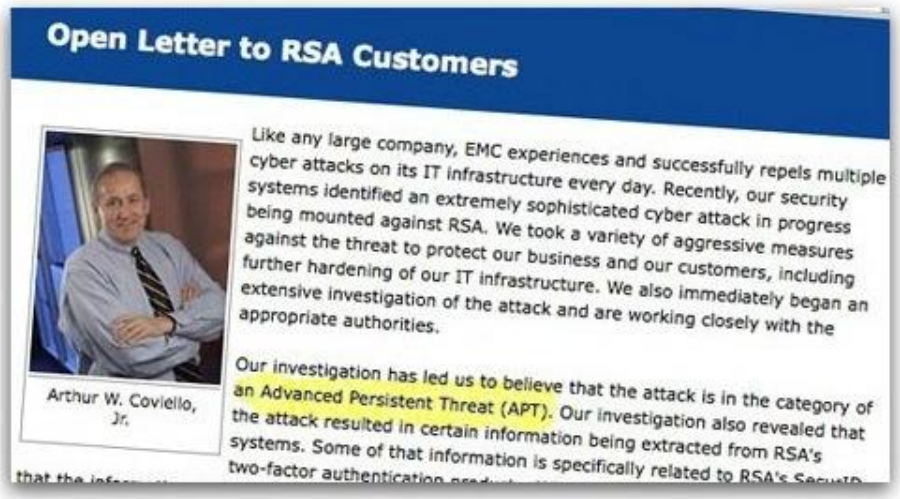
홍석범
(CDNetworks)

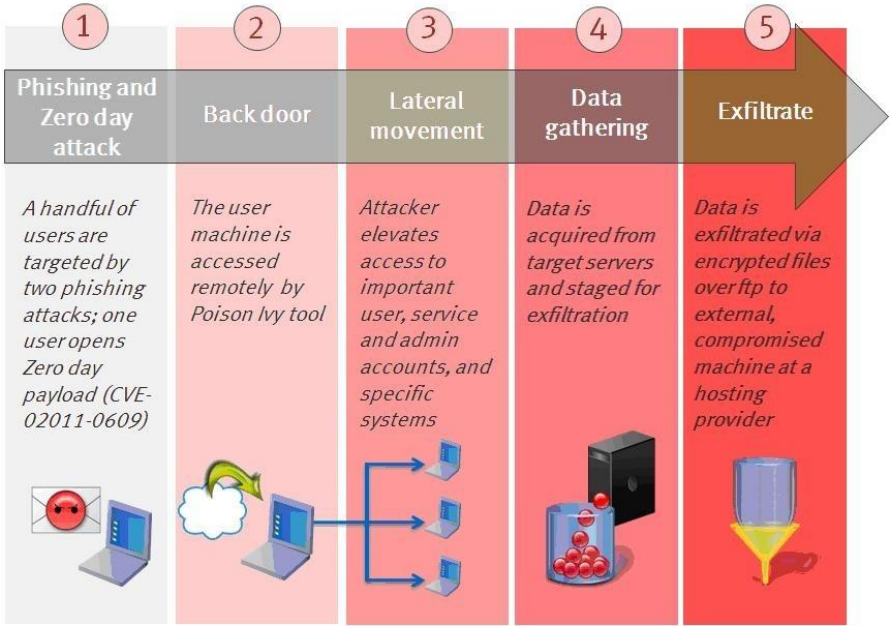
보안 사고 발생 …

- 공격자가 내부 직원에게 악성코드가 첨부된 메일 발송
- 해당 직원이 첨부 파일을 실행하여 자신의 PC 감염
- 공격자는 해당 PC의 원격 권한을 얻어 내부 네트워크를 스캔하여 결국 핵심 엔지니어의 PC까지 접근
- 해당 엔지니어의 PC를 통해 내부의 핵심 시스템에 접근하여 중요 정보 취득
- 이 사실이 외부에 공개되자 해당 기관은 전 고객들에게 사과문 게재와 함께 암호 등 고객 정보 변경 요청

타산지석…

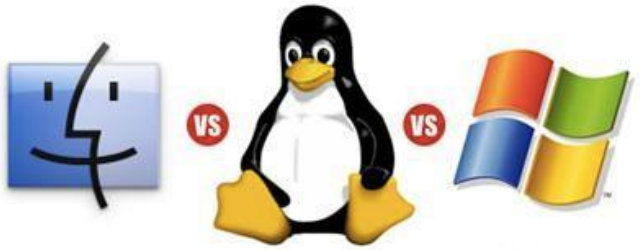




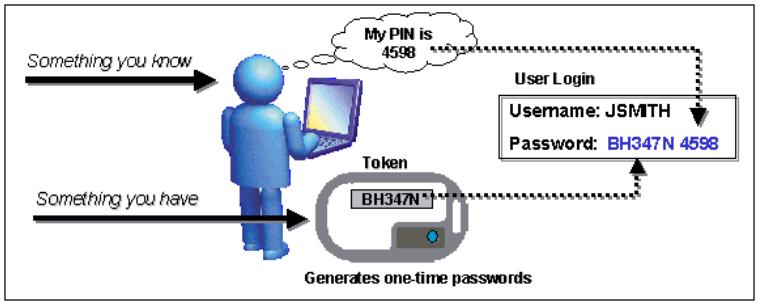


2011년 Adobe flash 0-day exploit 취약성을 이용한 2통의 메일(엑셀 파일) 전송
엑셀실행시 RAT(remote administration tool) 활성화 =>목표지점으로 접근

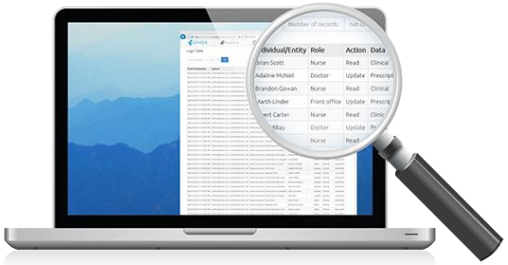
개선 사항



- 대부분의 악성코드는 MS 계열
기술조직은 모두 Linux,MAC을 기반OS로 사용
- 필요하다면 VM으로 Windows설치
Office(PPT등)만 사용



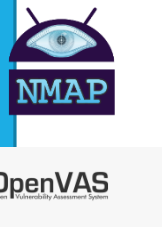
- Gateway등 주요 시스템 로그인에 도입
- 초기에 Google OTP 도입
=> 상용 migration 진행중



- 마지막 보루로서 SIEM을 이용,
침해사고의 Golden time(1주~2주) 활용

보안을 위한 요구사항들

우리가 사용하는 IP 대역에 어떤 포트(서비스,취약성)가 열려있지?



공격자에 의해 서버 설정이 변경되어도 자동으로 복구 될 수 없을까?

많은 서버에서 생겨나는 로그, 의미 있는 이벤트만 볼 수 없을까?

웹스캐너,웹 방화벽도 필요한데....

ID/PW로는 부족한데,2단계 인증은 어떻게 구현하지?

ISMS나 PCI등 Compliance도 통과해야 하는데, 표준보안 가이드 없나?

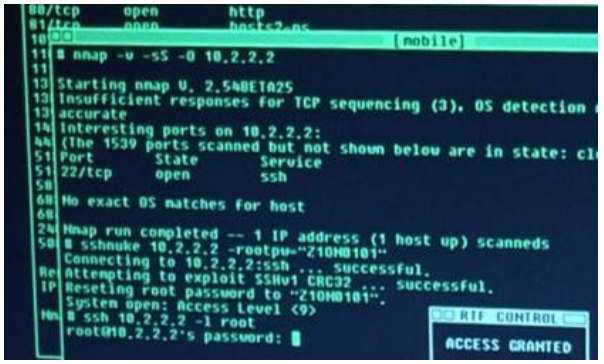
오픈소스툴을 활용해야 하는 이유

- 제품에 환경을 맞출 것인가? 환경에 제품을 맞출 것인가?
- 일년만 쓰고 버릴 것인가? 재활용할 것인가?
- 메뉴를 이해할 것인가? 작동 원리를 이해할 것인가?
- 횟수에 제한 없이 사용 필요
- 신뢰할 수 있다

요구조건에 맞는 툴 활용하기

우리가 사용하는 IP 대역에 어떤 포트(서비스,취약성)가 열려있지?

NMAP 활용



- 가장 대표적인 port scanner :: https://nmap.org
- Matrix등 13편의 영화에 출현(?)함
- 특정 포트, Application의 오픈 검색

$nmap -sV -P0 --open -p 22,3389,445 –iL ip_list -oG open_result

$ cat open_result | grep telnet
Host: 10.0.82.74 () Ports: 23/open/tcp//telnet//BSD-derived telnetd
Host: 10.0.85.139 () Ports: 23/open/tcp//telnet//Netscreen ScreenOS telnetd
Host: 10.0.90.66 () Ports: 23/open/tcp//telnet//Cisco router telnetd/
Host: 10.1.93.245 () Ports: 23/open/tcp//telnet//telnet (generic)/

$ cat open_result | grep SSH
Host: 10.19.150.195 Ports: 22/open/tcp//ssh//OpenSSH 4.3 (protocol 2.0)
Host: 10.19.89.10 Ports: 22/open/tcp//ssh//OpenSSH 3.9p1 (protocol 1.99)

-oG :: output with Grepable format

NMAP 활용

- NSE(Nmap Scripting Engine)를 활용, 확장된 기능 가능
  /usr/local/share/nmap/scripts 에 500여개 스크립트(+계속 증가)

auth : 인증과 관련된 스크립트, anonymous ftp 스캔등
discovery : 대상에 대한 깊이 있는 정보를 찾는 스크립트들
external : 외부의 자원(resources)을 활용한 스크립트들
intrusive : 대상에 대한 공격 시도를 하는 스크립트들
malware : 백도어나 악성코드(malware) 점검과 관련된 스크립트들
Vuln : 알려진 취약성을 점검하는 스크립트들

- nmap --script dns-recursion 192.168.1.0/24
- nmap --script ftp-anon 192.168.1.0/24
- nmap --script ftp-brute 192.168.1.0/24
- nmap -p 80 --script http-backup-finder www.example.com
  index.bak 나 index.html~ 등과 같은 백업 파일 검색

NMAP의 NSE 활용

- nmap -p80 --script http-google-malware <host>
  safe browsing을 이용, malware가 삽입되었는지 여부 점검

PORT STATE SERVICE
80/tcp open http
|_http-google-malware.nse: Host is known for distributing malware.

- nmap -p80 --script http-sql-injection www.example.com
- nmap -p80 --script http-slowloris www.example.com

- nmap --script http-virustotal

--script-args='apikey="xxxxxxx",http-virustotal.filename="/root/john-1.8.0.tar.gz"'
| http-virustotal:
| Permalink: https://www.virustotal.com/file/xxxxxx/analysis/1418142671/
| Scan date: 20xx-xx-09 16:31:11
| Results

name	result	date	version
AhnLab-V3	-	20xx1209	20xx.xx.10.00
ALYac	-	20xx1209	1.0.1.4
Comodo	UnclassifiedMalware	20xx1209	20312

.....

NMAP의 NSE 활용

- nmap -sV --script=mysql-brute.nse -p 3306 192.168.1.201

```
3306/tcp open mysql
| mysql-brute:
| Accounts
| root:root - Valid credentials
```

- nmap --script reverse-index 192.168.0.0/24

```
Post-scan script results:
| reverse-index:
|   22/tcp: 192.168.0.60
|   23/tcp: 192.168.0.100
|   80/tcp: 192.168.0.70
|   445/tcp: 192.168.0.1
|   53/udp: 192.168.0.105, 192.168.0.70, 192.168.0.60, 192.168.0.1
|_  5353/udp: 192.168.0.105, 192.168.0.70, 192.168.0.60, 192.168.0.1
```

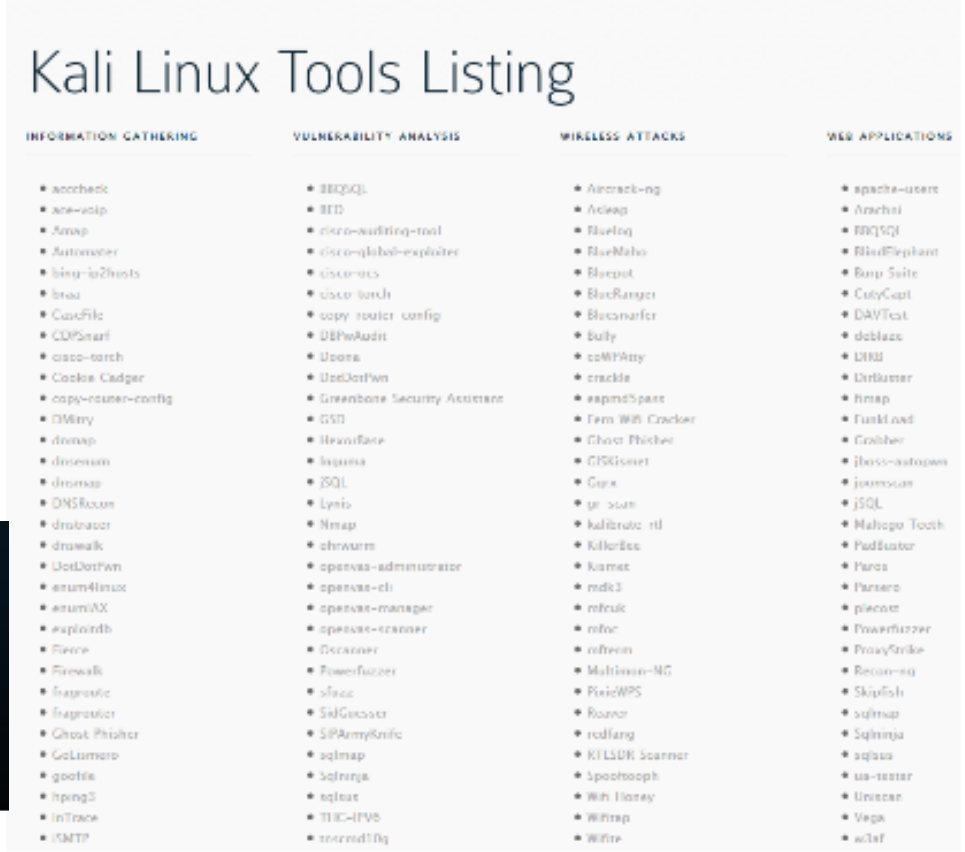
OPENVAS IN KALI

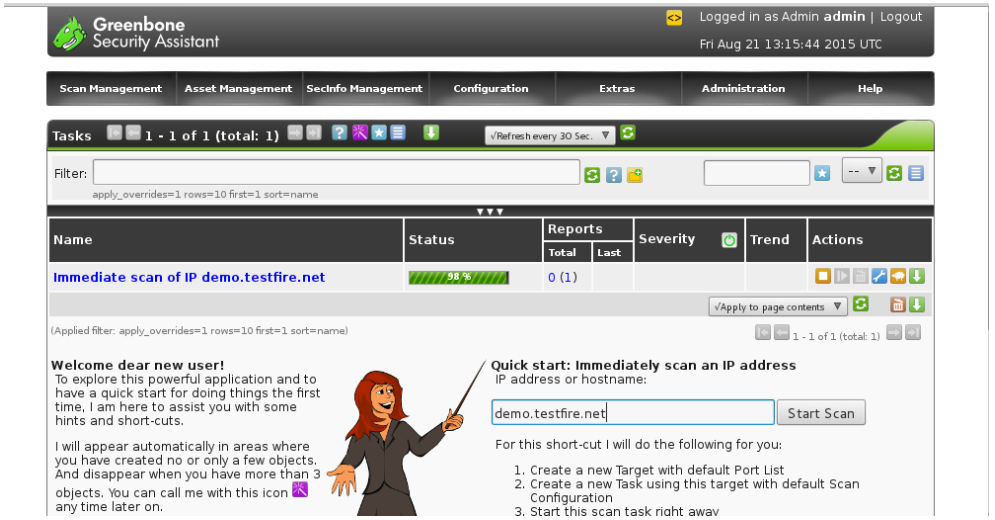
- http://tools.kali.org/tools-listing
- Openvas (http://openvas.org/)

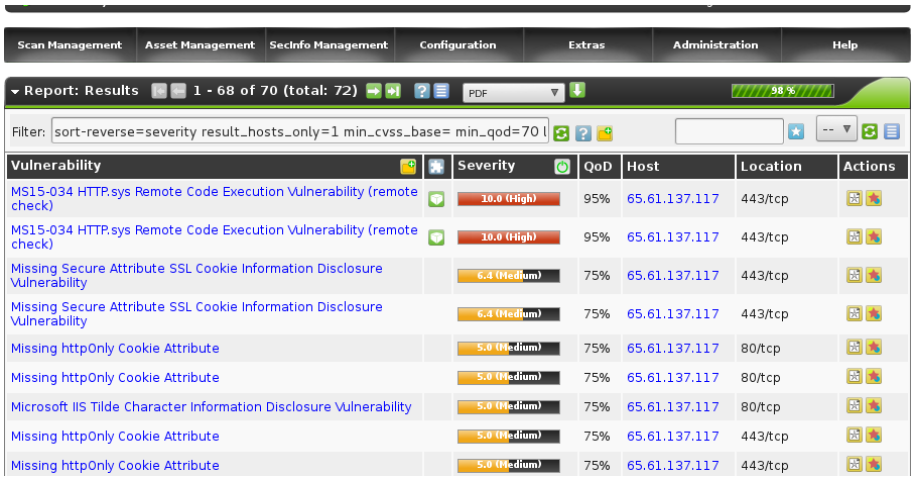
Nessus의 뒤를 잇는 취약성 점검솔루션
매우 복잡한 설치과정, Kali는 매우 쉬움

openvas-setup;
openvas-stop ; openvas-start

```
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2011.xml, file is older than last revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2012.xml, file is older than last revision
[i] Skipping /var/lib/openvas/cert-data/dfn-cert-2013.xml, file is older than last revision
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2014.xml
[i] Updating /var/lib/openvas/cert-data/dfn-cert-2015.xml
[i] Updating Max CVSS for CERT-Bund
[i] Updating Max CVSS for DFN-CERT
Rebuilding NVT cache... done.
root@kali:~# openvas-stop
Stopping OpenVas Services
root@kali:~# openvas-start
Starting OpenVas Services
root@kali:~# openvasmd --user=admin
root@kali:~# openvasmd --user=admin --new-password=admin1
root@kali:~#
```



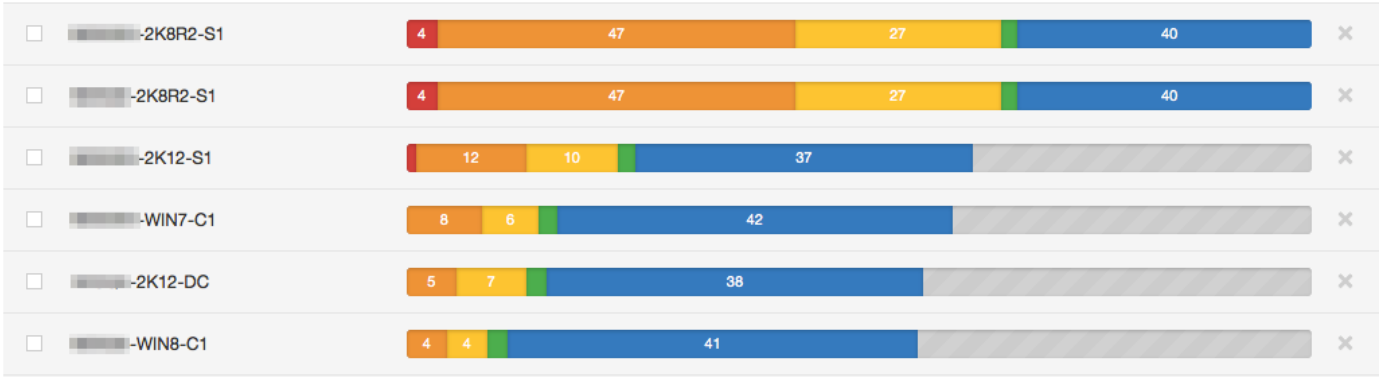


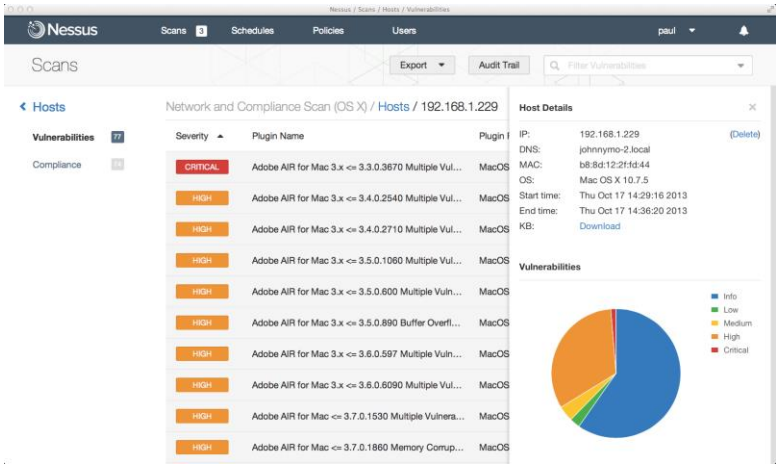


Remote file access	62 of 62	
SMTP problems	48 of 48	
SNMP	6 of 6	
Service detection	548 of 549	
Settings	12 of 12	
Slackware Local Security Checks	534 of 534	
Solaris Local Security Checks	898 of 898	
SuSE Local Security Checks	1553 of 1553	
Ubuntu Local Security Checks	2480 of 2480	
Useless services	13 of 13	
VMware Local Security Checks	39 of 39	
Web Servers	257 of 257	
Web application abuses	3410 of 3411	
Windows	145 of 145	
Windows : Microsoft Bulletins	887 of 887	
Total: 56	40291 of 40307 in selected families of 40307 in total	

NESSUS

https://www.tenable.com/products/nessus-home



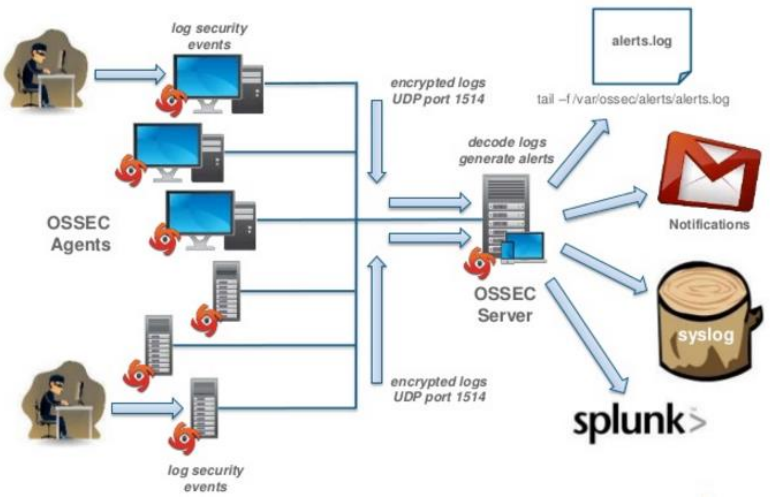


요구조건에 맞는 툴 활용하기

많은 서버에서 생겨나는 로그, 의미 있는 이벤트만 볼 수 없을까?

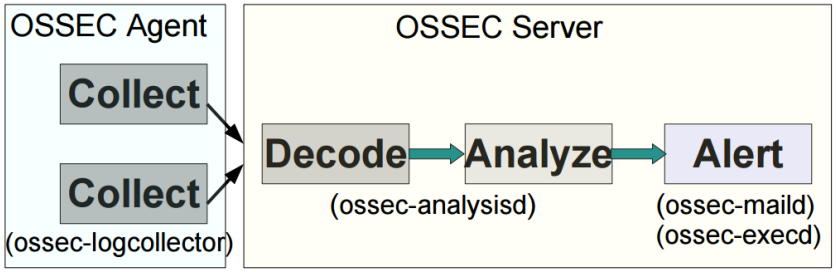
OSSEC :: OPEN SOURCE SECURITY

- 오픈소스 기반의 Host 기반 IDS/IPS(침입탐지시스템), 현재는 Trendmicro에서 인수하여 제공
- http://ossec.net/
- Log 분석, 파일무결성모니터링(FIM), 루트킷탐지, 실시간 탐지 및 차단
- agent 기반, agentless 모두 지원, log management 솔루션은 아님
- System(kernel, 내부 daemons등)의 visibility(가시성)를 제공함
- Server-agent 기반으로 각 서버에는 로그를 수집하는 agent만 설치하면 되므로 확장성이 용이
- 기본적으로 /var/ossec에 설치되고, 주 설정파일은 /var/ossec/etc/ossec.conf
- /var/ossec/rules/*.xml :: 룰 파일, snort처럼 오탐이 많지는 않음
- /var/ossec/logs/alert.log :: 알람 파일



OSSEC

- Log는 ossec 서버에서만 분석되며 agent는 로그를 보내기만 함



- 활용사례

```
<syscheck>
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories check_all="yes">/root/users.txt,/bsd,/root/db.html</directories>
  <ignore>/etc/passwd</ignore>
</syscheck>
```

⇒ 파일이나 디렉토리의 속성(md5,owner,permission등)이 변경시 알람함

```
<rule id="31103" level="6">
    <if_sid>31100,31108</if_sid>
    <url>=select%20|select+|insert%20|%20from%20|%20where%20|union%20|</url>
    <url>union+|where+|null,null|xp_cmdshell</url>
    <description>SQL injection attempt.</description>
    <group>attack,sql_injection,</group>
  </rule>
```

OSSEC 알람예

Received From: (www.example.com) 192.168.7.19->/var/log/secure
Rule: 5551 fired (level 10) -> "Multiple failed logins in a small period of time."
Src Location: CN,Guangdong,Guangzhou
Portion of the log(s):
www vsftpd: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp ruser=zhaolg rhost=61.144.79.245
=> **지속적인 ftp 접속 시도를 알람**

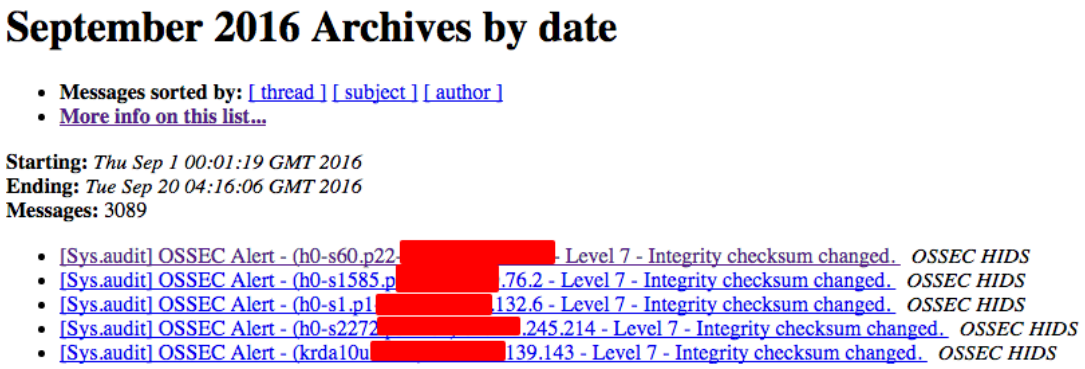
Received From: localhost->ossec-logcollector
Rule: 592 fired (level 8) -> "Log file size reduced."
Portion of the log(s):
ossec: File size reduced (inode remained): '/var/log/messages'.
⇒ **파일을 삭제하거나 로그의 특정 부분을 삭제시 알람**

Rule: 510 fired (level 7) -> " Host-based anomaly detection event (rootcheck). "
Portion of the log(s):
Process ' 17251 ' hidden from /proc. Possible kernel level rootkit.
=> **Hidden process 탐지**

OSSEC 알람예

-. level 0 : 가장 낮은 것으로 무시하거나 어떠한 액션도 취하지 않는다.
흔히 기존 룰에서 오탐이 발생하였을 때 알람이 발생하지 않도록 조정할 때 사용된다.
-. level 2: 보안과는 무관하게 시스템과 관련된 이벤트를 의미한다.
-. level 3 : 인증 성공
-. level 4 : 보안과는 무관하게 프로그램 설치나 시스템 에러등 이벤트
-. level 6 : 웜이나 바이러스 관련 이벤트이지만 심각도가 낮은 경우,
이를테면 리눅스 시스템인데 윈도우 관련 웜의 스캔인 경우
-. level 10 : 여러 번 암호인증에 실패하는 경우의 이벤트, 실제 공격이거나 암호를 잊었을 때 발생할 수 있다
-. level 12 : 시스템의 error나 warning 수준으로 공격과 관련된 이벤트일 수 있음
-. level 13 : buffer overflow등 비정상적인 공격 시도
-. level 14 : 여러개의 룰에서 이벤트가 발생하는 등 공격 발생시
-. level 15 : 공격이 성공하였을때의 경우로 즉각적인 대응이 필요함

```
<alerts>
<log_alert_level>1</log_alert_level>
<email_alert_level>7</email_alert_level>
</alerts>
```



September 2016 Archives by date

- **Messages sorted by:** [thread] [subject] [author]
- More info on this list...

Starting: *Thu Sep 1 00:01:19 GMT 2016*
Ending: *Tue Sep 20 04:16:06 GMT 2016*
Messages: 3089

- [Sys.audit] OSSEC Alert - (h0-s60.p22[redacted] - Level 7 - Integrity checksum changed. *OSSEC HIDS*
- [Sys.audit] OSSEC Alert - (h0-s1585.p[redacted].76.2 - Level 7 - Integrity checksum changed. *OSSEC HIDS*
- [Sys.audit] OSSEC Alert - (h0-s1.p1[redacted]132.6 - Level 7 - Integrity checksum changed. *OSSEC HIDS*
- [Sys.audit] OSSEC Alert - (h0-s2272[redacted].245.214 - Level 7 - Integrity checksum changed. *OSSEC HIDS*
- [Sys.audit] OSSEC Alert - (krda10u[redacted]139.143 - Level 7 - Integrity checksum changed. *OSSEC HIDS*

OSSEC AUTOMATIC RESPONSE

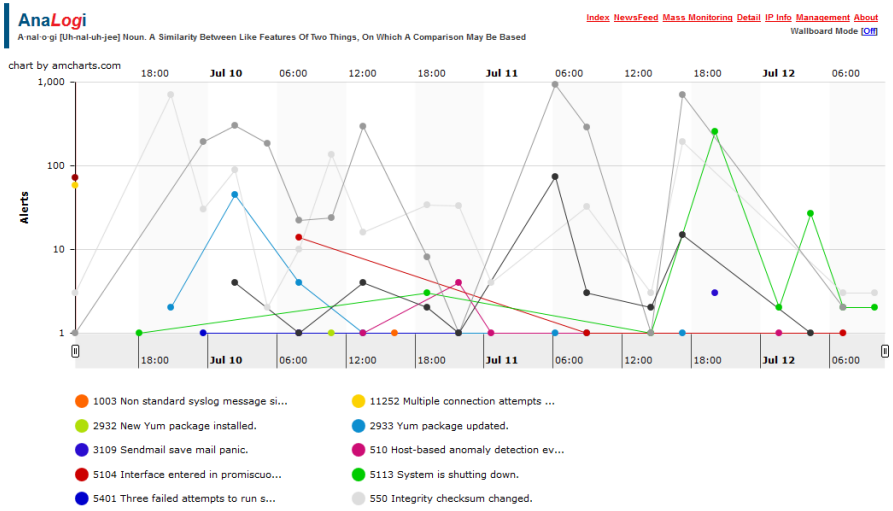
** Alert 1436711244.73713: - ossec,active_response,
2015 Jul 12 23:27:24 (www.server2.com) any->/var/ossec/logs/active-responses.log
Rule: 603 (level 3) -> 'Host Blocked by host-deny.sh Active Response'
Src IP: 192.168.0.2
Sun Jul 12 23:27:21 KST 2015 /var/ossec/active-response/bin/host-deny.sh add - 192.168.0.2 1436711242.71719 5720

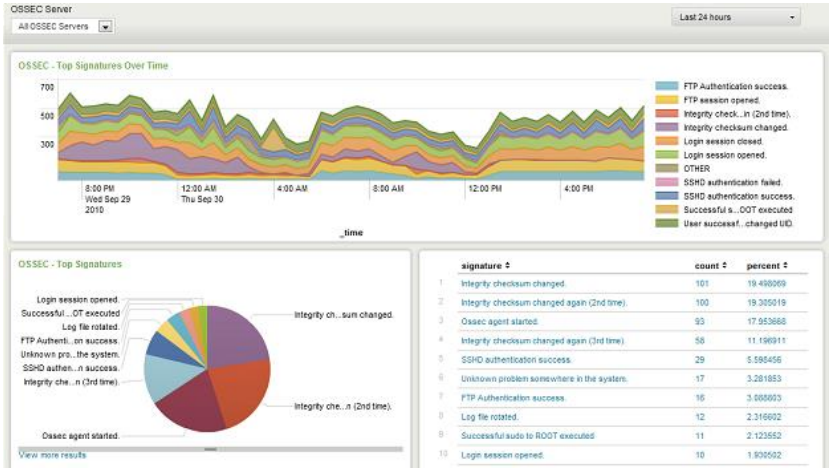
```
<command>
<name>host-deny</name>
<executable>host-deny.sh</executable>
<expect>srcip</expect>
<timeout_allowed>yes</timeout_allowed>
</command>
```

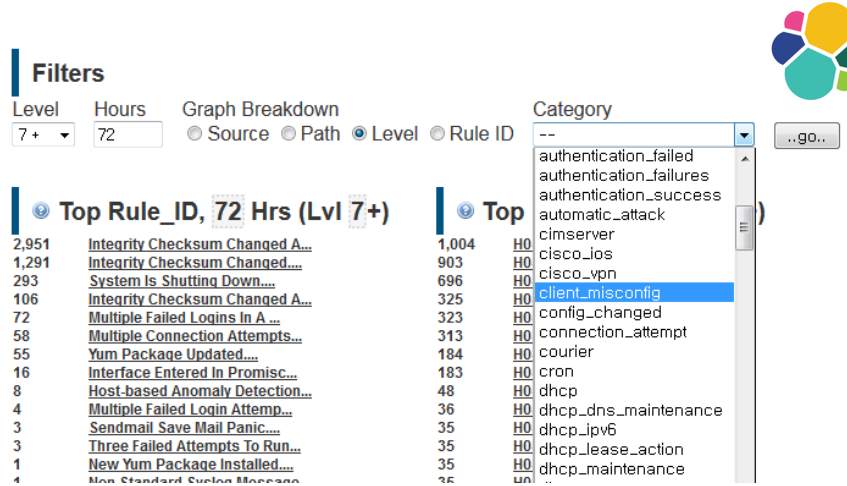
```
<active-response>
<command>host-deny</command>
<location>local</location>
<level>3</level>
<timeout>600</timeout>
</active-response>
```

OSSEC GUI

```
# SPLUNK 설정예
<syslog_output>
    <server>172.10.2.3</server>
    <port>10002</port>
</syslog_output>
```

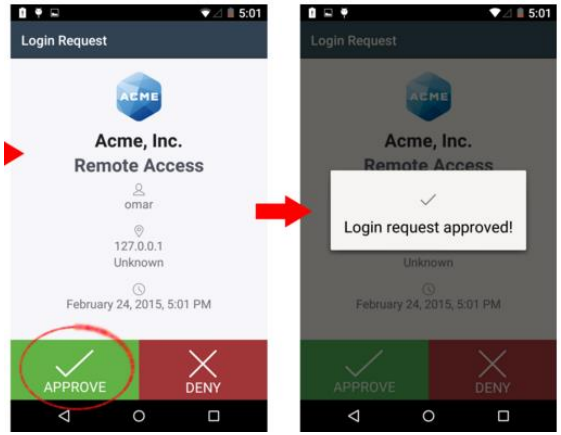






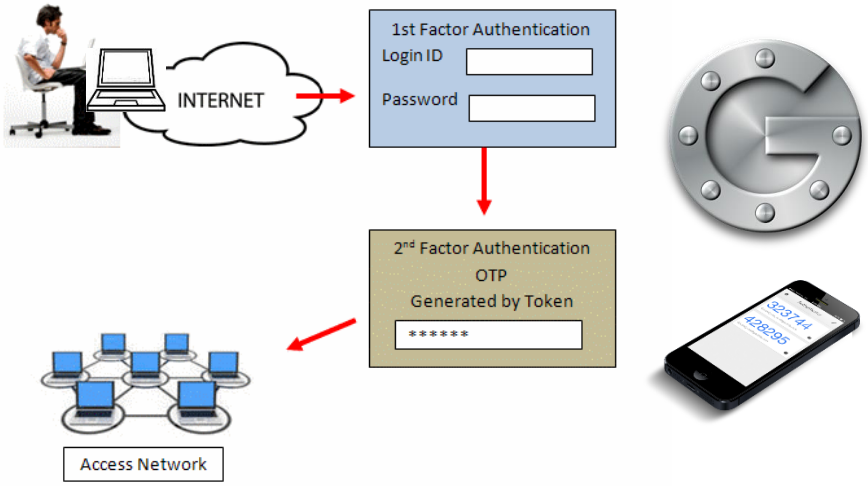
요구조건에 맞는 툴 활용하기

ID/PW로는 부족한데,2단계 인증은 어떻게 구현하지?



GOOGLE OTP

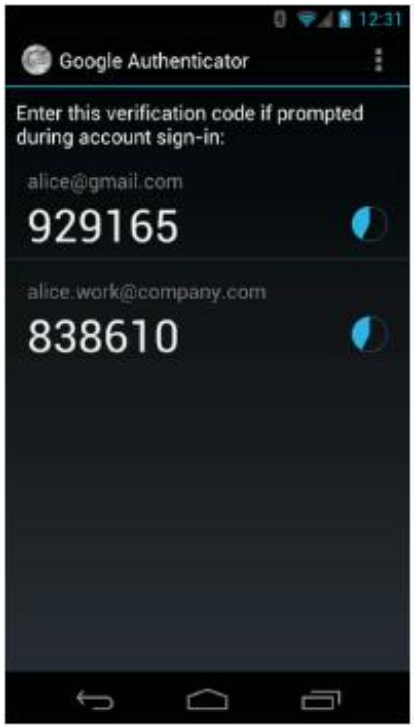
- Iphone, 안드로이드,윈도우폰 등 모든 device 지원
- OTP 코드는 30초간 유효, 30초마다 Random하게 변경됨
- T(Time based)OTP의 경우 WIFI/LTE연결이 되지 않아도 사용가능 (시간 동기화가 중요)
  별도의 인증 서버가 필요하지 않아 비용 투자가 없음
- Brute force 공격에 안전, ID/PW를 저장하는 사이트에도 안전
  IP등으로 ACL 설정이 불가한 서비스에도 유용함
- 사용하기 편리함



GOOGLE OTP :: SSH연동

- https://github.com/google/google-authenticator/wiki
- Git 또는 # yum install google-authenticator

이후 QR code를 볼 수 있도록 "# yum install qrencode" 로 설치
각 유저들은 각자 아래 명령어로 설정 초기화
$ google-authenticator
이후 .google_authenticator 라는 설정 파일이 생성됨



GOOGLE OTP :: SSH연동

이후 /etc/pam.d/sshd 파일에 아래 설정 추가하여 적용

```
auth       required pam_google_authenticator.so
```

/etc/ssh/sshd_config 파일에 아래 설정 추가

```
UsePAM yes
ChallengeResponseAuthentication yes
PasswordAuthentication yes
```

$ ssh antihong@192,168.11.4 -p22
Verification code: xxxxxx <== OTP코드
Password: <== 기존에 사용중인 password

응용예)

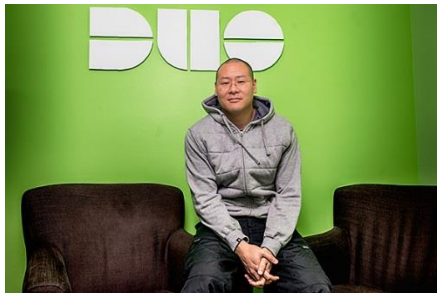
```
Match User somebody
AuthenticationMethods "publickey"
Match User "*,!somebody"
AuthenticationMethods "publickey,keyboard-interactive"
```

=> sombody는 Key로만 인증, 나머지는 Key와 OTP로 인증

다른 OTP 솔루션

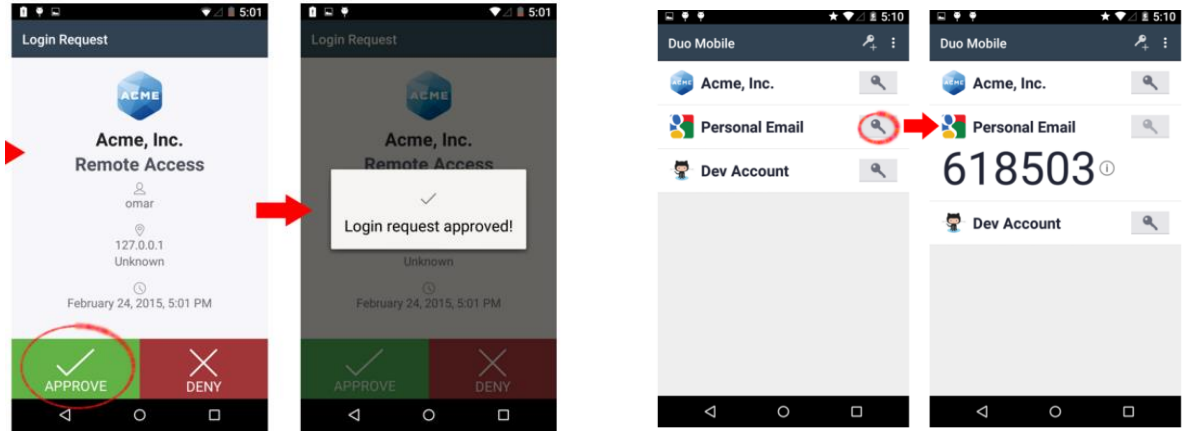
- **Google OTP의 단점**
- QR Code를 복사해 두면 OTP를 재사용(재생성)할 수 있음
- Browser plugin을 설치하여 사용할 수 있음
- OTP 사용에 대한 history 관리가 안 됨
- SSH외 RDP나 Web등 다른 Application 적용에 어려움
- 여러 Application을 사용할 경우 중앙 관리를 위해서는 별도 개발이 필요함
- FreeOTP :: https://fedorahosted.org/freeotp/

- **상용 OTP :: DUO OTP / AUTHY**
- 10개 계정까지는 Free로 사용 가능함, authy의 경우 인증수로 과금
- https://www.duosecurity.com/ CEO는 Dug Song(송덕준)으로 한국계
- SSH, RDP, VPN, WIKI, JIRA, OWA, WEB site등 대부분의 Application 을 지원함
- OTP 적용에 API를 이용하여 수십분 소요
- 기존 Free/Google OTP migration 가능함



유용한 기능들

- Push 기능, Passcode 입력(TOTP), SMS등 다양한 옵션 지원 가능



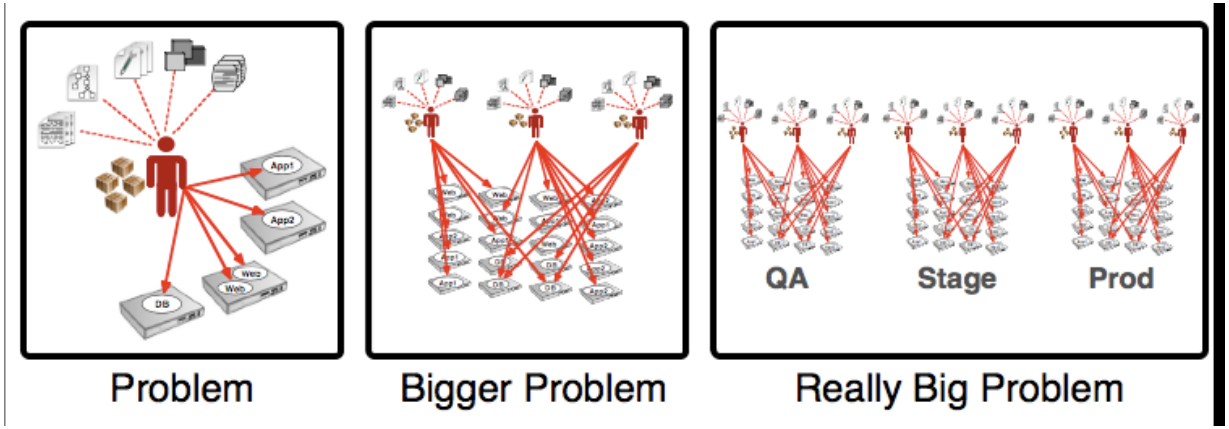
- Portal 을 통한 관리자의 관리(로그 모니터링)

Timestamp	User	Application	Event	Result	Access Device	Second Factor
Nov 14, 2015 9:43 AM	noc	KR WTG	Authentication	Access Granted User approved	10.40.217.101	Duo Push +82 10-2067-[redacted]
Nov 14, 2015 8:28 AM	junghyun.yoo	KR WTG	Authentication	Access Granted Valid passcode	10.40.222.86	Passcode +82 10-8940-[redacted]
Nov 14, 2015 7:26 AM	noc	KR WTG	Authentication	Access Granted Valid passcode	10.40.217.101	Passcode +82 10-2067-[redacted]
Nov 14, 2015 7:25 AM	noc	KR WTG	Authentication	Access Denied Invalid passcode	10.40.217.101	Passcode

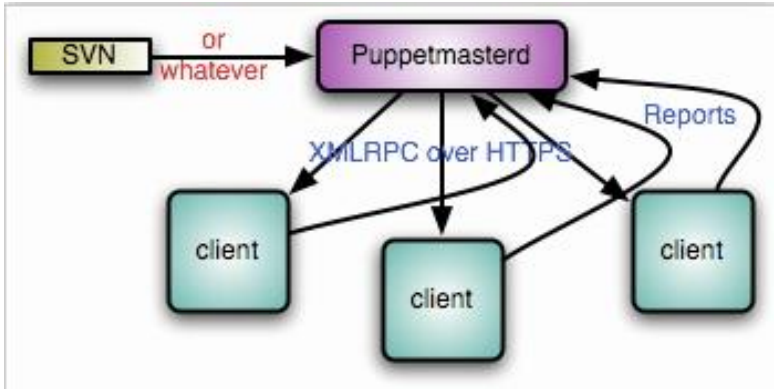
요구조건에 맞는 툴 활용하기

공격자에 의해 서버 설정이 변경되어도 자동으로 복구 될 수 없을까?

CONFIG MANAGEMENT TOOL 활용



- 수십~수백대의 서버를 어떻게 동일한 config로 유지할 것인가?
- 만약 누군가가 수작업으로 config를 수정할 수도 있을텐데, 이런 경우는 어떻게?
  공격자가 임의로 iptables에 특정IP를 허용하는 룰 추가?
- 설정을 변경했는데, 문제가 발생하면 어떻게? 롤백 가능? => 버전관리, wiki등..E-mail?
- 적은 인력으로 수천대를 어떻게 관리 할 것인가?
- history/sharing/consistency!!

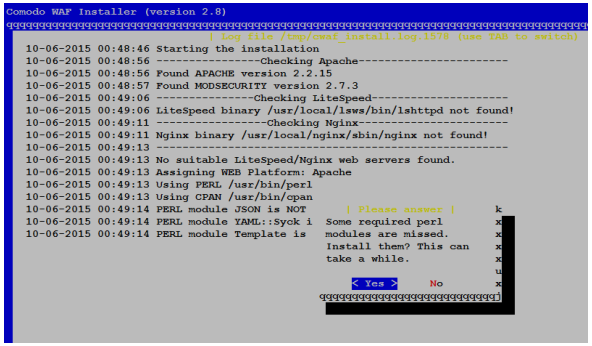


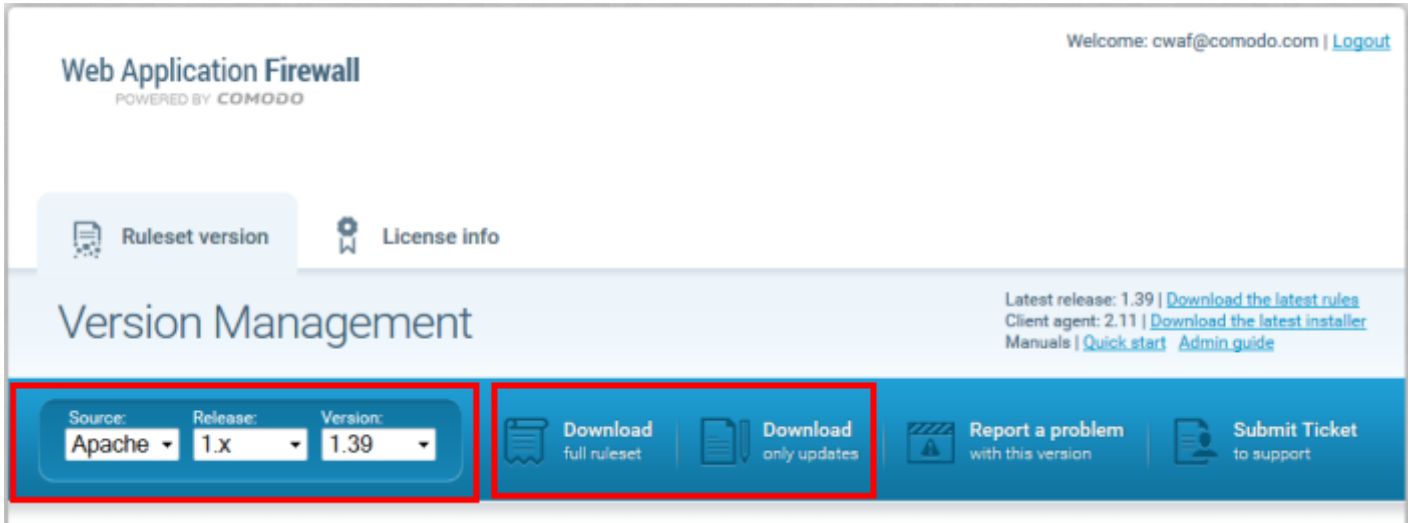
요구조건에 맞는 툴 활용하기

웹스캐너, 웹 방화벽도 필요한데....

COMODO FREE WAF.

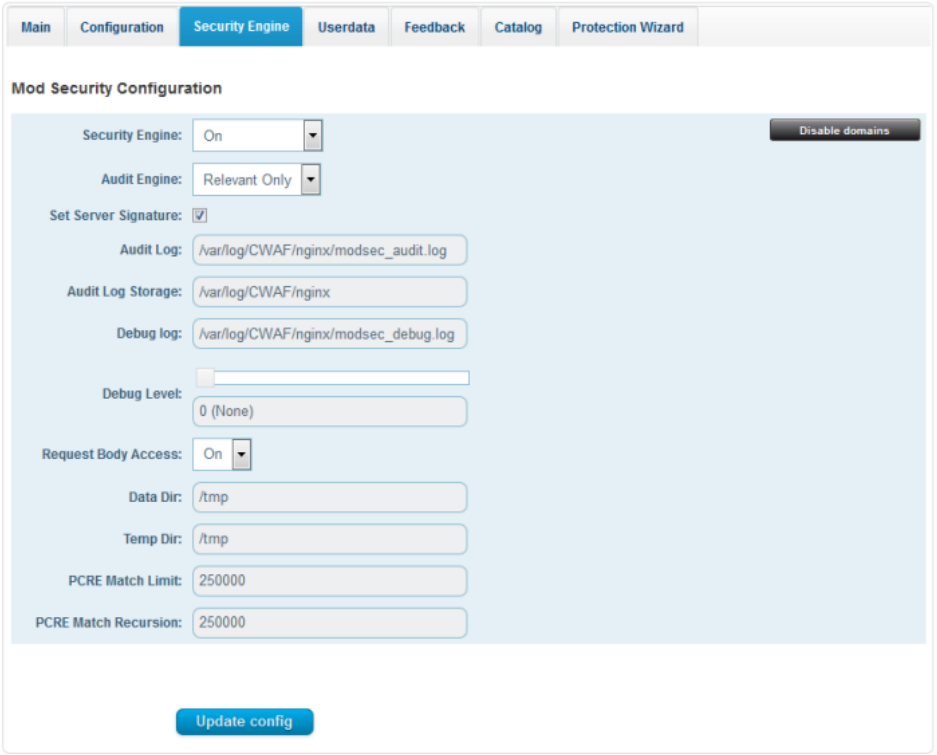
- Modsecurity 기반, Free로 제공
- Comodo에서 customizing 한 rule 제공
- Agent를 통해 룰 자동 업데이트 가능
- https://modsecurity.comodo.com/





COMODO WAF GUI 관리

- cPanel, Webmin, web hosting panel등 연동시 GUI로 룰 관리 가능함



NAXSI WAF

- Nginx 기반의 가벼운 WAF :: Nginx Anti XSS & SQL Injection.
- https://github.com/nbs-system/naxsi
- 기존 modsec의 문제점 해소 가능. 너무 많은 false positive, 너무 복잡함, performance 저하등
- Simple한 룰 활용, 일정 임계값에 이를 경우 action 수행

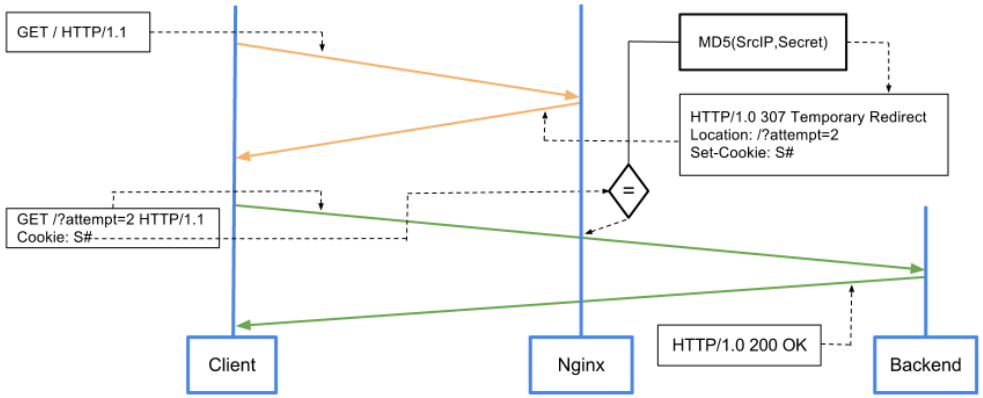
```
  GNU nano 2.3.1                                  File: naxsi.rules

LearningMode;
SecRulesEnabled;
#SecRulesDisabled;
DeniedUrl "/RequestDenied";

## Check & Blocking Rules
CheckRule "$SQL >= 8" BLOCK;
CheckRule "$RFI >= 8" BLOCK;
CheckRule "$TRAVERSAL >= 4" BLOCK;
CheckRule "$EVADE >= 4" BLOCK;
CheckRule "$XSS >= 8" BLOCK;
```

TESTCOOKIE TO FIGHT AGAINST BOT

- L7 DDoS를 차단하기 위한 가장 확실한 방법
- https://github.com/kyprizel/testcookie-nginx-module
- Bot 과 브라우저를 구분하기 위해
  30x + SetCookie 또는 200 + JS with SetCookie 등의 기술을 활용

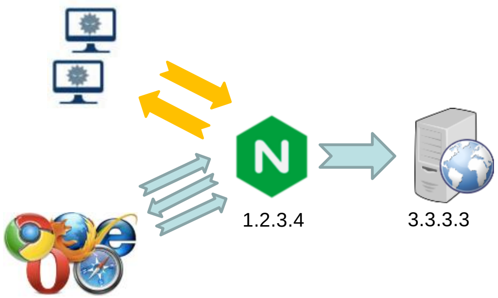


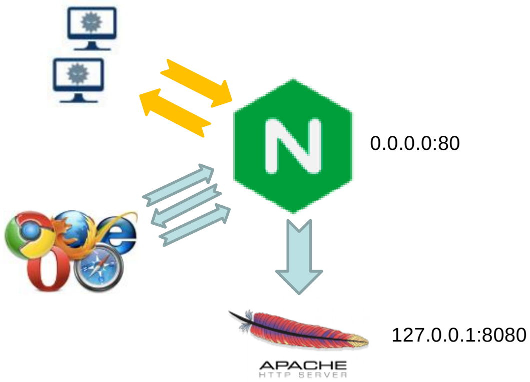

```
location / {
        testcookie on;
        testcookie_name LINUX;
        testcookie_session $remote_addr;
 }
```

```
Set-Cookie: LINUX=4ed8c4effbeededbf41aa98bd8d32e1d;
```

```
GET / HTTP/1.1.
Cookie:LINUX=4ed8c4effbeededbf41aa98bd8d32e1d;
```

TESTCOOKIE TO FIGHT AGAINST BOT

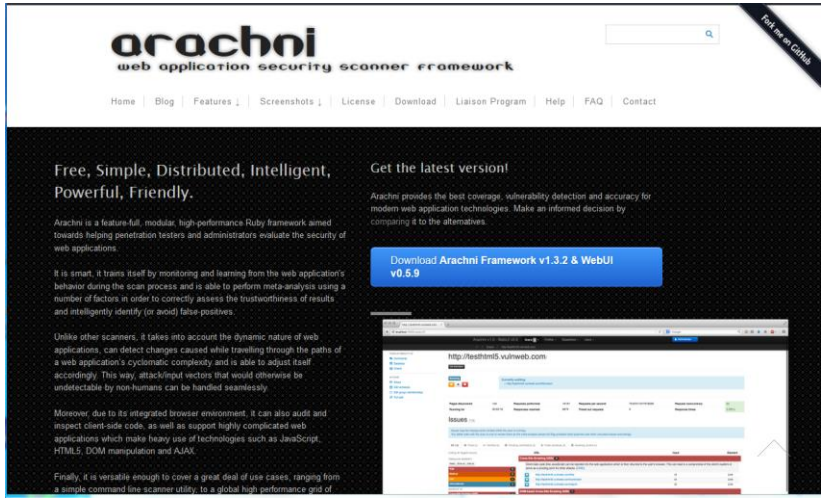




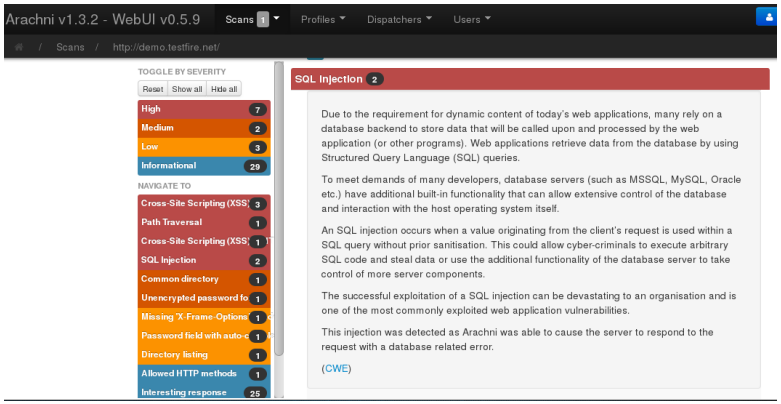
test.example.com
DNS Change from 3.3.3.3 => 1.2.3.4

```
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:46;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Googlebot/2.1; \ http://www.google.com/bot.html)
13:31:47;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:47;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:48;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:48;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:49;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:49;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:50;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:50;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:51;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:51;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:52;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:52;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:53;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:53;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:54;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:54;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:55;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
13:31:55;118.81.200.124;302;HTTP/1.1;http://www.ilotto6688.com/;GET;NOREFERER;Mozilla/5.0 (compatible; Baiduspider/2.0; \ http://www.baidu.com/search/spider.html)
```

ARACHNI, WEB SCANNER



http://www.arachni-scanner.com/



Rank	#	Logo	Vulnerability Scanner	Version	Vendor	WIVET Score
1			arachni	1.1	Tasos Laskos	96.00% Detection Rate
1			WebInspect	10.1.177.0	HP Application Security Center	96.00% Detection Rate
2			Acunetix WVS	9.0	Acunetix	94.00% Detection Rate
2			N-Stalker	X	N-Stalker	94.00% Detection Rate
2			NTOSpider	6.0	NT OBJECTives	94.00% Detection Rate
2			Syhunt Dynamic	5.0.0.7	Syhunt	94.00% Detection Rate
2			Tinfoil Security	X	Tinfoil Security	94.00% Detection Rate
3			Acunetix WVS Free Edition	8.0	Acunetix	92.00% Detection Rate
3			IBM AppScan	9.0.0.999 / 8.8.0.0	IBM Security Systems Division	92.00% Detection Rate
3			Netsparker	4.1.1.0	Netsparker Ltd	92.00% Detection Rate
3			QualysGuard WAS	2014-01-21	Qualys, Inc.	92.00% Detection Rate

http://sectoolmarket.com/wivet-score-unified-list.html

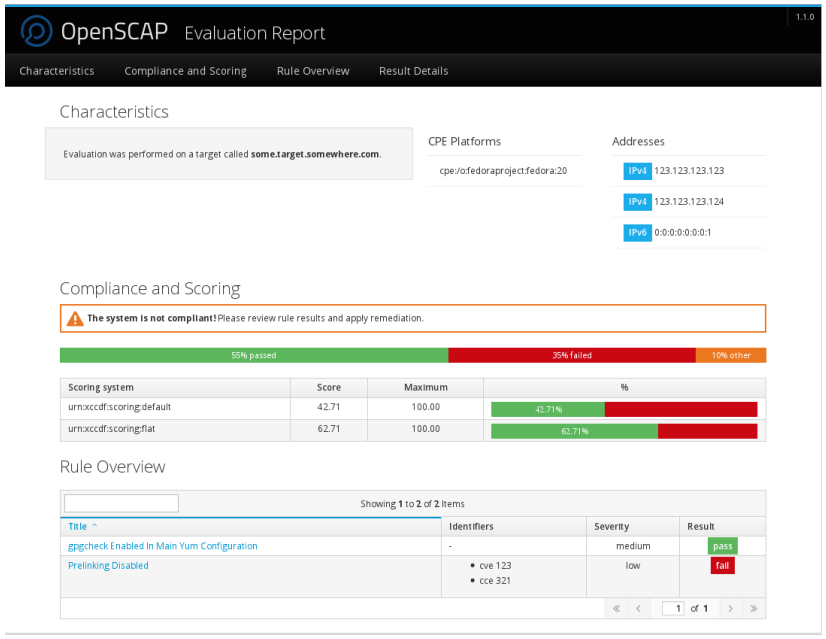
- Low false positive, finds lots of vulnerabilities
- Supports CLI as well as GUI
- Supports Beautiful Report

요구조건에 맞는 툴 활용하기

ISMS나 PCI등 Compliance도 통과해야 하는데, 표준보안 가이드 없나?

OPENSCAP 활용

- OpenSCAP(Security Content Automation Protocol) :: http://www.open-scap.org/
- OpenSCAP는 Open되어 있고 Free이며 매우 활발히 업데이트되고 있다.
- scan할 항목을 customize할 수 있어 환경에 따라 불필요한 항목은 제외하고 스캔할 수 있다.
- 유사한 프로젝트로 Lynis가 있음



OPENSCAP 활용

- yum -y install openscap openscap-utils scap-security-guide
- # oscap xccdf eval --profile stig-rhel6-server-upstream --results /tmp/oscap-results.xml --report /tmp/oscap-results.html --cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml

/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml

```
Title   Ensure Red Hat GPG Key Installed
Rule    ensure_redhat_gpgkey_installed
Ident   CCE-26506-6
Result  fail

Title   Ensure gpgcheck Enabled In Main Yum Configuration
Rule    ensure_gpgcheck_globally_activated
Ident   CCE-26709-6
Result  pass

Title   Ensure gpgcheck Enabled For All Yum Package Repositories
Rule    ensure_gpgcheck_never_disabled
Ident   CCE-26647-8
Result  pass

Title   Ensure Software Patches Installed
Rule    security_patches_up_to_date
Ident   CCE-27635-2
Result  notchecked

Title   Install AIDE
Rule    package_aide_installed
Ident   CCE-27024-9
Result  fail

Title   Configure Periodic Execution of AIDE
Rule    aide_periodic_cron_checking
Ident   CCE-27222-9
Result  pass
```

Title	Result
Ensure /tmp Located On Separate Partition	fail
Ensure /var Located On Separate Partition	fail
Ensure /var/log Located On Separate Partition	fail
Ensure /var/log/audit Located On Separate Partition	fail
Ensure /home Located On Separate Partition	pass
Encrypt Partitions	notchecked
Ensure Red Hat GPG Key Installed	fail
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Ensure Software Patches Installed	notchecked
Install AIDE	fail
Configure Periodic Execution of AIDE	pass
Verify and Correct File Permissions with RPM	fail
Verify File Hashes with RPM	pass
Install Intrusion Detection Software	notchecked
Install Virus Scanning Software	fail
Add noexec Option to Removable Media Partitions	pass
Disable Modprobe Loading of USB Storage Driver	fail
Disable the Automounter	pass
Verify User Who Owns shadow File	pass
Verify Group Who Owns shadow File	pass
Verify Permissions on shadow File	fail
Verify User Who Owns group File	pass
Verify Group Who Owns group File	pass
Verify Permissions on group File	pass
Verify User Who Owns gshadow File	pass
Verify Group Who Owns gshadow File	pass
Verify Permissions on gshadow File	pass
Verify User Who Owns passwd File	pass
Verify Group Who Owns passwd File	pass

OPENSCAP,LYNIS 활용

```
 --- Starting Remediation ---
Title   Ensure Red Hat GPG Key Installed
Rule    ensure_redhat_gpgkey_installed
Ident   CCE-26506-6
Result  error

Title   Disable Modprobe Loading of USB Storage Driver
Rule    kernel_module_usb-storage_disabled
Ident   CCE-27016-5
Result  fixed

Title   Verify Permissions on shadow File
Rule    file_permissions_etc_shadow
Ident   CCE-26992-8
Result  fixed

Title   Verify that All World-Writable Directories Have Sticky Bits Set
Rule    sticky_world_writable_dirs
Ident   CCE-26840-9
Result  fixed

Title   Set Daemon Umask
Rule    umask_for_daemons
Ident   CCE-27031-4
Result  fixed
```

```
Follow-up:
---------------------------
- Check the logfile for more details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data (Lynis Enterprise users)

================================================================================

Lynis security scan details:

Hardening index : 70 [###############       ]
Tests performed : 195
Plugins enabled : 0

Quick overview:
- Firewall [X] - Malware scanner [X]

Lynis Modules:
- Heuristics Check [NA] - Security Audit [V]
- Compliance Tests [X] - Vulnerability Scan [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat

================================================================================
```

--remediate option시 자동으로 fix

Lynis :: https://cisofy.com/lynis/

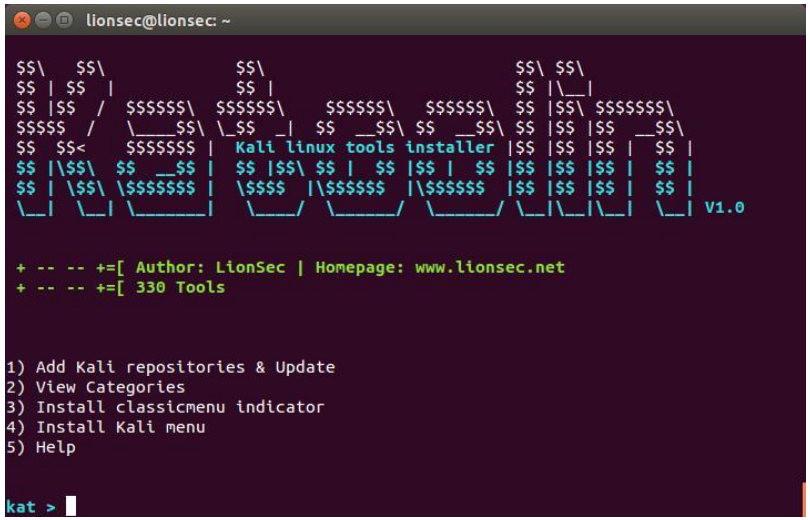
- Lynis는Linux,MacOS, unix에 대한 audit 지원

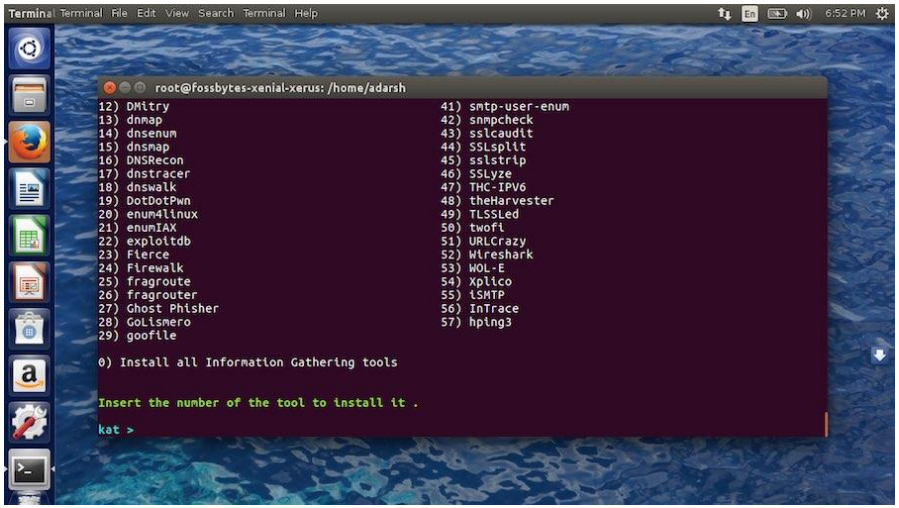
KALI LINUX

- https://www.exploit-db.com/ 의 offensive-security에서 운영하는 데비안 기반 배포판
- 이전에는 백트랙, 2013년 Kali라는 이름으로 바꾸어 배포(https://www.kali.org/)
- 정보수집, 취약성점검, 웹어플리케이션 분석, 패스워드 크랙, 무선해킹, 리버스엔지니어링, 스니핑 및 spoofing 툴, 포렌식, 리포팅툴등 다양한 분야별로 가장 대표적인 300여개의 프로그램들을 제공
- 복잡한 설치 과정 없이 즉시 사용 가능

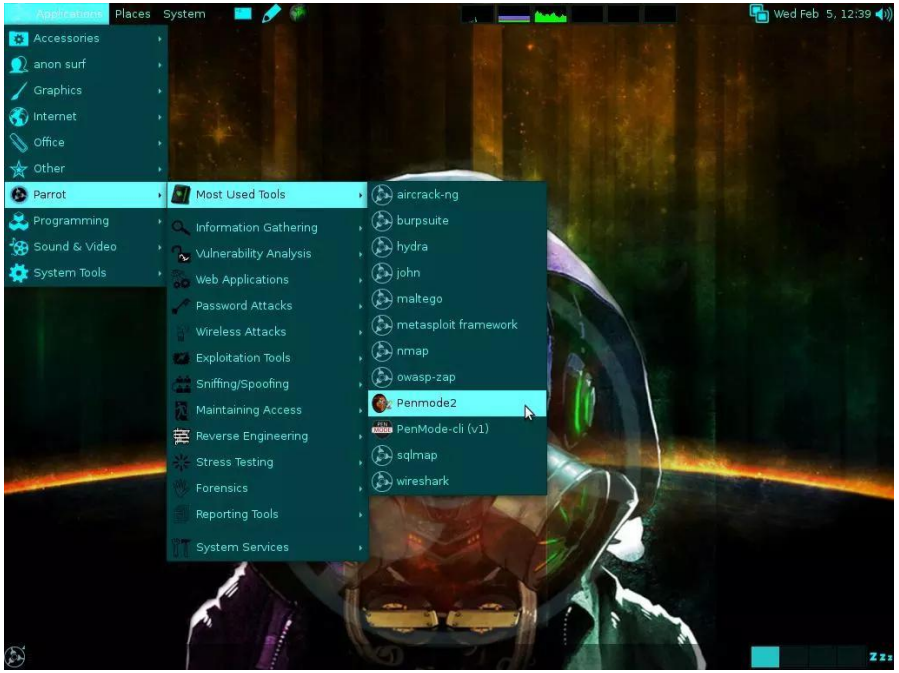
KALI TOOLS IN UBUNTU

- git clone https://github.com/LionSec/katoolin.git && cp katoolin/katoolin.py /usr/bin/katoolin



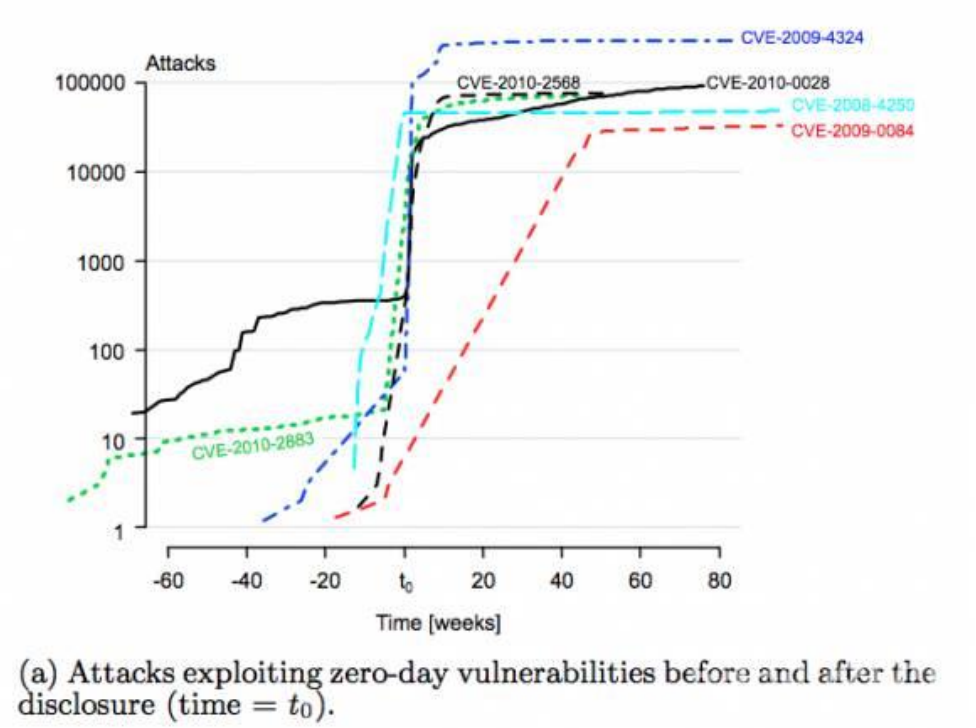


PENTEST를 위한 다른 배포판들



- Pentoo
- Parrot security OS
- LionSEC
- Samurai ……..

패치만 해도 안전?



(a) Attacks exploiting zero-day vulnerabilities before and after the disclosure (time = t_0).

- **패치로 80%의 위협은 제거할 수 있다.**
- **시스템에서는 아직도 알려지지 않은 취약성이 더 많을 수 있다.**
- **강력한 접근 통제는 보안의 기본이다.**
- **모든 Application의 실행권한은 최소한으로 유지한다.**

취약성 공개 전후 공격 발생 시간에 대한 통계 :: 적지 않은 공격이 CVE공개 전부터 수행됨

감사합니다.

antihong@gmail.com