

# 방화벽 관리 및 침입기록 분석방법

NCSC-TR050016



국가사이버안전센터  
National Cyber Security Center

## 1. 가

가 ) 가 (

가 가

가 , 가

( , , , )

가 , 가

Email , ,

in/out , ,

, ,

2.

WEB·FTP·E-Mail

가

: , ,  
 : IP  
 : IP  
 : IP  
 : 가 TCP UDP  
 : 가

15가

1)

connect()

srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=[PORTGROUP], action=any
------------------------------------------------------------------------

dstport      PORTGROUP      5

. PORTGROUP .

## NCSC-TR050016 :

PORTGROUP= {21/tcp, 23/tcp, 79/tcp, 110/tcp, 111/tcp, 135/tcp, 135/udp, 161/udp, 512/tcp, 513/tcp, 514/tcp, 1433/tcp, 1433/udp, 1434/tcp, 1434/udp, 32771/tcp, 32771/udp}

(port scan)

- ◆ id=firewall time="2004-02-28 19:37:24" fw=firew4 pri=6 proto=21/TCP src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:39:24" fw=firew4 pri=6 proto=23/TCP src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:41:24" fw=firew4 pri=6 proto=135/UDP src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:43:24" fw=firew4 pri=6 proto=161/UDP src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:44:24" fw=firew4 pri=6 proto=513/TCP

## 2) Service Enumeration

DSTPORT 가	IP SRCIP가 , 5	DSTIP
--------------	---------------------	-------

(service enumeration)

- ◆ id=firewall time="2004-02-28 19:37:24" fw=firew4 pri=6 proto=21/TCP src=192.168.777.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:39:24" fw=firew4 pri=6 proto=21/TCP src=192.168.777.250 dst=158.216.666.2 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:41:24" fw=firew4 pri=6 proto=21/TCP src=192.168.777.250 dst=158.216.666.3 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:43:25" fw=firew4 pri=6 proto=21/TCP src=192.168.777.250 dst=158.216.666.4 sent=2592 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:44:25" fw=firew4 pri=6 proto=21/TCP src=192.168.777.250 dst=158.216.666.5 sent=2592 msg="ALLOW SESSION"

## NCSC-TR050016 :

### 3) MS FrontPage Server Extension Buffer Overflow

MS fp30reg.dll Buffer Overflow

가 80, 9999가

- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=80, action=any
- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=9999, action=any

(fpreg30.dll )

- ◆ id=firewall time="2004-02-28 19:31:24" fw=firew4 pri=6 proto=80/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 19:31:26" fw=firew4 pri=6 proto=9999/TCP src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

### 4) MS Messenger Heap Overflow

Overflow

MS03-

043

- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=135, action=any
- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=9191, action=any

(MS03-043 )

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 roto=135/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:32" fw=firew4 pri=6 roto=9191/TCP src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

### 5) LSASS.DLL RPC Buffer Overflow

MS04-011 가 Isasrv.dll Buffer Overflow

가

Houseofdabus

## NCSC-TR050016 :

- |                                                                     |
|---------------------------------------------------------------------|
| ◆ srcip=SRCPORT, srcport=any, dstip=DSTIP, dstport=445, action=any  |
| ◆ srcip=SRCPORT, srcport=any, dstip=DSTIP, dstport=4444, action=any |

(lsass.dll )

- |                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ◆ id=firewall time="2004-02-28 19:37:24" fw=firew4 pri=6 roto=445/TCP<br>src=192.168.777.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"  |
| ◆ id=firewall time="2004-02-28 19:37:27" fw=firew4 pri=6 roto=4444/TCP<br>src=192.168.777.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION" |

### 6) IPswitch IMAIL LDAP

IPswitch IMAIL Buffer Overflow

THC

- |                                                                    |
|--------------------------------------------------------------------|
| ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=389, action=any   |
| ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=31337, action=any |

(THC Exploit)

- |                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ◆ id=firewall time="2004-02-28 19:31:24" fw=firew4 pri=6 proto=389/TCP<br>src=192.168.777.250 dst=158.216.666.1 sent=2592 msg="DENY SESSION"  |
| ◆ id=firewall time="2004-02-28 19:31:26" fw=firew4 pri=6 roto=31337/TCP<br>src=192.168.777.250 dst=158.216.666.1 sent=2592 msg="DENY SESSION" |

### 7) Windows XP/2000 Return into Libc

RPCSS Buffer Overflow

- |                                                                   |
|-------------------------------------------------------------------|
| ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=135, action=any  |
| ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=7175, action=any |

## NCSC-TR050016 :

(Ins1der Exploit)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=135/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:32" fw=firew4 pri=6 proto=7175/TCP src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

### 8) Windows Workstation Service WKSSVC Libc

Windows Workstation Service Buffer Overflow

Snooq Exploit

가

- ◆ srcip=SRCIP, srcport=SRCPORT, dstip=DSTIP, dstport=24876, action=any
- ◆ srcip=DSTIP, srcport=any, dstip=SRCIP, dstport=SRCPORT, action=any

### 9) MSMQ Heap Overflow

Buffer Overflow

. DaveK exploit가

- ◆ srcip=any, srcport=1356, dstip=any, dstport=2101, action=any

### 10) ProFTPD ASCII File Remote Root Exploit

ProFTPD가 ASCII

Buffer Overflow

) Bkbll Exploit

- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=21, action=any
- ◆ srcip=DSTIP, srcport=20, dstip=SRCIP, dstport=34568, action=any

## NCSC-TR050016 :

### 11) Splaris /bin/login Remote Root Exploit

Solaris /bin/login Buffer Overflow가  
가 . morgan exploit telnet  
. 2  
.

- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=23, action=any
- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=2001, action=any

#### (Morgan Exploit)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=23/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:32" fw=firew4 pri=6 proto=2001/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

### 12) WFTPD STAT Command Remote Exploit

WFTPD Buffer Overflow

- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=21, action=any
- ◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=19800, action=any

#### (OYXin Exploit)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=21/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:32" fw=firew4 pri=6 proto=19800/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

### 13) Phatbot/Agobot/Gaobot

Phatbot, Agobot, Gaobot. SRCIPrk  
DSTIP PORTGROUP dstport  
1 가 .

## NCSC-TR050016 :

◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=[PORTGROUP], action=any

PORTGROUP= {80/tcp, 135/tcp, 139/tcp, 445/tcp, 3127/tcp, 6129/tcp}

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=139/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:32" fw=firew4 pri=6 proto=80/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"
- ◆ id=firewall time="2004-02-28 13:31:33" fw=firew4 pri=6 proto=445/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"
- ◆ id=firewall time="2004-02-28 13:31:33" fw=firew4 pri=6 proto=135/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"
- ◆ id=firewall time="2004-02-28 13:31:34" fw=firew4 pri=6 proto=3127/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=52 msg="DENY SESSION"

Phatbot, Agobot, Gaobot.

가

- ◆ id=firewall time="2004-02-28 13:31:24"5 fw=firew4 pri=6 proto=4387/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=328msg="ALLOW SESSION"

### 14) Dameware Probe

Dameware가

- ◆ srcip=any, srcport=220, dstip=any, dstport=21, action=any

(Dameware)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=21/TCP  
src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"

15) Doomejuice

Doomejuice가  
SRCIP가 DSTIP PORTGROUP dstport  
1 , PORTGROUP 가

◆ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=[PORTGROUP], action=any

PORTGROUP= {3127/tcp, 3128/tcp, NOT 1080/tcp}

(Doomejuice worm)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=3127/TCP src=192.168.777.250 dst=158.216.666.1 sent=328msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:25" fw=firew4 pri=6 proto=3128/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"

"Deadhat.B Worm Activity"  
1080/tcp가

(Dameware.B worm)

- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=3127/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=3127/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:24" fw=firew4 pri=6 proto=3127/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:25" fw=firew4 pri=6 proto=3128/TCP src=192.168.777.250 dst=158.216.666.1 sent=328 msg="ALLOW SESSION"
- ◆ id=firewall time="2004-02-28 13:31:25" fw=firew4 pri=6 proto=1080/TCP src=192.168.777.250 dst=158.216.666.1 sent=328msg="ALLOW SESSION"

3

	Listen		
LovGate.Z	6000	445	Mail, , password, P2P
Bagle.Z	1234(relay)	-	Mail
Bagle.Y	1234(relay)	-	Mail
Revacc	Reverse Telnet	-	Mail, mms.exe(45,056) (C: \ (WINDIR) \ system, C: \ (WINDIR) \ system32)
LovGate.Y	6000	445	Mail, , password, P2P
Sdbot.RZ	-	80, 135, 445, 6667	, password: MS03-001(445), MS03-007(80), MS03- 026(135) / 6667 IRC
Korgo.P	-	445, 80	6667 : MS04-011(445)/ /
Sdbot.FO	-	445, 6667	6667 : MS04-011(445)/ IRC
Peep2	Reverse Telnet	-	Mail, Explorer.exe(81,920), Service.exe(45,056) (C: \ (WINDIR) \ system, C: \ (WINDIR) \ system32)
Rbot.AF	-	80, 135, 445, 6667	, password: MS03-001(445), MS03-007(80), MS03- 026(135), MS04-011(445) / 6667 IRC
Gaobot.AQS	-	80, 135, 445, 6667	, password: MS03-007(80), MS03-026(135), MS04- 011(445) / 6667 IRC
Korgo.F	113, 3067, Random	445, 6667	6667 : MS04-011(445)/ IRC

## NCSC-TR050016 :

Listen			
Peep	Reverse Telne	-	Mail, Explorer.exe(81,920) (C: \ (WINDIR) \ system, C: \ (WINDIR) \ system32), systray.exe (C: \ (WINDIR))
Korgo.B	113,2041,3067	445, 6667	6667 : MS04-011(445)/ IRC
Korgo.A	113,2041,3067	445, 6667	6667 : MS04-011(445)/ IRC
Gaobot.ALU	-	80, 135, 445	, password: MS03-007(80), MS03-026(135), MS03- 049(445), MS04-011(445)
Bobax.D	HTTP(Random), SMTP(Random)	5000	: MS04-011(445)/ XP
Bobax.C			
Bobax.B			
Bobax.A			
Kibuv.B	7955(FTP),420	80,135,44 5,2745,55 54,6667(I RC)	: MS03-007(80), MS01-059(135), MS03-026(135), MS04-011(445), Bagle/Win32.Weird
Kibuv.A	9604(FTP),420, Random(Shell)	135,445	: MS03-026(135), MS04-011(445)
Dabber.A	69,8967(temp),9 898(Shell)	5554,9898	가 FTP
Gaobot.AJD	-	80,135,44 5,1080,14 34(U),300 0-5000	, password,Bagle/MyDoom/Optix
Sasser.F	5554(FTP),9996 (Shell)	445, 9996	
Sasser.E	1023(FTP),1022 (Shell)	445, 1022	(LSASS, MS04-11), 128
Sasser.D	5554(FTP),9996	445, 9996	

## NCSC-TR050016 :

	Listen		
Sasser.C	(Shell)		
Sasser.B			
Sasser.A			
Cycle.A	69(TFTP),RRandom(Shell)	445	(LSASS, MS04 - 11)
Welchia.C	-	80,135,13 9,445	(MS/03- 007,026,039), '04.6.1
Netsky.*	-	-	Mail, a.php
Bagle.*	2745, 2556, 81, 2535, 6777	-	Mail, P2P
MyDoom	3127,3198	-	Mail,P2P
Doomjuice	-	3127	MyDoom
Lovegate	10168,20168	-	Mail
Nimda.A	69	80,137 - 139,445	Mail, , IIS
Code_Red	-	80	( .ida , MS01 - 33)

### 4.

- ⊕ Firelogd :
- ⊕ Fwanalog : Unix Linux
- ⊕ XP Firewall Reporter: XP
- ⊕ ZoneLog Analyzer : ZoneAlam
- ⊕ Web Trends :Check Point, Cisco, MS ISA Server

5.

	가?(Single, HA, FLB )
	FWLB 가?
	1 , 2 가 가?
	가?(ESM, telnet, ssh, http(s))
	NMS/ESM 가?
	Console , 가?
	CPU 가?
	ID/Password 가?
	Rule 가? ( , )
	Rule 가 가?
Rule	IP Address, , Rule 가?
	Rule Performance 가?
	Rule 가?
IP	IP 가?
	가?
Inbound	Inbound 가?
Outbound	Outbound 가?
	ftp, ssh, telnet 가?
	ICMP, finger 가?
	Source Routing 가?
	Broadcast(Netbios, IDENT ) 가?
	가?
	가 가?
(DoS )	Trinoo Ddos 가?

NCSC-TR050016 :

	SYN flooding Dos 가?
	Nimda 가?
	port scanning 가?
	bypass 가?
Rule Update	Rule update 가?
	, , Source Address, Destination Address, 가?
	가?
	가?
	가?
	Rule 가?
( )	가?
S/W	S/W 가?
	가( )
	가 가?

6.

가가 “Security is management”  
가 .

NCSC-TR050016 :

,  
 .  
 가?  
 가?  
 가?  
 HTTP, SMTP, FTP, TELNET  
 가?  
 , ~ 11 .  
 11 . 가  
 .  
 Top 5 IP . IP  
 .  
 Top 10 IP  
 Top 10  
 0~5 . OS  
 .  
 0.0.0.0 IP  
 21/ FTP, 23/Telnet, 110/POP3, and 143/Imap  
 .  
 111/RPC Bind . 111/RPC Bind  
 가  
 ICMP 0 8

## NCSC-TR050016 :

. (ICMP types 0: icmp icmp , ICMP types 8:  
icmp )  
ICMP 5 9  
"Man in the middle"  
가 가 . (ICMP types 5: (Redirect  
message), ICMP types 9: router advertisement)  
ICMP type 12  
. (ICMP types 12: )  
33434~335600 Unix Trace  
Route

IP

IP .