IDS IMPLEMENTATION WITH MIKROTIK

BY: ANTONIUS DUTY SUSILO

MUM (MIKROTIK USER MEETING)
VIETNAM
2017
PROFILE

• Antonius Duty Susilo
• Email dutymlg@gmail.com
• Master degree of Information Technology in ITB (Institute Teknologi Bandung) Indonesia
• Teacher in SMK Telkom Malang and Lecturer in University
• Trainer Mikrotik (belajarmikrotik.com) and Consultant Mikrotik
• Cisco Networking Academy Program and Oracle Academy Instructor and Oracle WDP (Workforce Development Program) Instructor
SMK TELKOM MALANG

SMK TELKOM Malang was founded in 1992 to become the first Vocational High School in Indonesia to organize the Vocational Education in Telecommunication Engineering specializing in informatics engineering program (www.smktelkom-mlg.sch.id)

SMK Telkom Malang is under the auspices of Telkom Education Foundation or Yayasan Pendidikan Telkom (YPT) Bandung (www.ypt.or.id)
The Study Program:

**Computer and Networks Engineering**
Students will be able to create Computer Technicians and Network Engineer

**Software Engineering**
Students will be educated in software development and programming
SECURING ROUTER

• THE MAIN IDEA TO SECURED THE ROUTER IS BY MINIMIZING THE INTRUSION

• SECURITY MEANS COMPLEXITY
NETWORK INTRUSION TYPES

• NETWORK INTRUSION IS A SERIOUS SECURITY RISK THAT COULD RESULT IN NOT ONLY THE TEMPORAL DENIAL, BUT ALSO IN TOTAL REFUSAL OF NETWORK SERVICE

• WE CAN POINT OUT 5 MAJOR NETWORK INTRUSION TYPES:
  • PING FLOOD
  • PORT SCAN
  • DOS ATTACK
  • DDOS ATTACK
  • UNAUTHORIZED ACCESS TO THE ROUTER

• ALL IDS IS IMPLEMENTED IN INPUT OR OUTPUT CHAIN
PING FLOOD

• PING FLOOD USUALLY CONSIST FROM VOLUMES OF RANDOM ICMP MESSAGES

• WITH “LIMIT” CONDITION IT IS POSSIBLE TO BOUND THE RULE MATCH RATE TO A GIVEN LIMIT

• THIS CONDITION IS OFTEN USED WITH ACTION “LOG”
LIMIT (FOR PING-FLOOD)

• MAKE A RULE TO LIMIT ICMP PROTOCOL TO 2 PACKET / SECOND AND BURSTABLE TO 2 OTHER PACKET
LIMIT (FOR PING-FLOOD)

- MAKE ANOTHER RULE TO BLOCK OTHER THAN THOSE TRAFFIC BEFORE (2 PPS BURSTABLE TO 2 OTHER PPS)
LIMIT (FOR PING-FLOOD)

• TRY TO PING SEVERAL TIMES (MORE THAN 2)

Accept Counter (if less than or equal to 2 pps)

Drop counter (more than 2 pps or 4 pps)
ICMP MESSAGE TYPES

• TYPICAL IP ROUTER USES ONLY FIVE TYPES OF ICMP MESSAGES (TYPE:CODE)
  • FOR PING - MESSAGES 0:0 AND 8:0
  • FOR TRACEROUTE – MESSAGES 11:0 AND 3:3
  • FOR PATH MTU DISCOVERY – MESSAGE 3:4
• OTHER TYPES OF ICMP MESSAGES SHOULD BE BLOCKED
**ICMP MESSAGE RULE EXAMPLE**

<table>
<thead>
<tr>
<th>New Firewall Rule</th>
<th>General</th>
<th>Advanced</th>
<th>Extra</th>
<th>Action</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chain:</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Src. Address:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dst. Address:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol:</td>
<td></td>
<td>icmp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Src. Port:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dst. Port:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TCP Flags**

**ICMP Options**

- **ICMP Type:** 0 (echo reply)
- **ICMP Code:**
ICMP FLOOD

- MAKE THE NEW CHAIN – ICMP
  - ACCEPT 5 NECESSARY ICMP MESSAGES
  - SET MATCH RATE TO 3 PPS WITH 5 PACKET BURST POSSIBILITY
  - DROP ALL OTHER ICMP PACKETS
ICMP FLOOD

New Firewall CHAIN

- ACCEPT all ICMP Type and Code defined earlier
- DROP other ICMP type and code
ICMP FLOOD

• MOVE ALL ICMP PACKETS TO ICMP CHAIN
  • CREATE AN ACTION “JUMP” RULE IN THE CHAIN INPUT
  • PLACE IT ACCORDINGLY
  • CREATE AN ACTION “JUMP” RULE IN THE CHAIN FORWARD
  • PLACE IT ACCORDINGLY
PORT KNOCKING

• PORT KNOCKING IS A METHOD OF EXTERNALLY OPENING PORTS ON A FIREWALL BY GENERATING A CONNECTION ATTEMPT ON A SET OF PRE-SPECIFIC CLOSED PORT

• THE PRIMARY PURPOSE OF PORT KNOCKING IS TO PREVENT AN ATTACKER FROM CONNECTING TO AN OPEN PORT AND GET A BRUTE-FORCE ON THE USERNAME/PASSWORD

• THE PORT "KNOCK" ITSELF IS SIMILAR TO A SECRET HANDSHAKE AND CAN CONSIST OF ANY NUMBER OF TCP, UDP, OR EVEN SOMETIMES ICMP AND OTHER PROTOCOL PACKETS TO NUMBERED PORTS ON THE DESTINATION MACHINE
PORT KNOCKING SCHEME

1. Send a connection to TCP-1234
2. The router store requester IP for an amount of time
3. Send a connection to TCP-4321
4. The router checked if the IP is the same IP with the first connection (TCP-1234)
5. If the IP is the same and the time between 1st attempt and 2nd, then the requester IP will be allowed to access the router
PORT KNOCKING IN MIKROTIK

• THE STEP OF APPLYING PORT KNOCKING IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  • TRAP A CONNECTION TO TCP PORT 1234 AND PUT THE SRC-ADDRESS TO AN ADDRESS-LIST TEMPORARY FOR 10S
  • TRAP A CONNECTION TO TCP PORT 4321 AND CHECKED WHETHER THE SRC-ADDRESS IS ALREADY AT ADDRESS-LIST TEMPORARY. IF SO PUT THE SRC-ADDRESS TO AN ADDRESS-LIST SECURED
  • ALLOW ACCESS FROM SRC-ADDRESS-LIST SECURED
  • DROP OTHER CONNECTION
PORT KNOCKING

• TRAP TCP(1234) AND PUT THE SOURCE ADDRESS TO ADDRESS-LIST TEMPORARY FOR 10 SECONDS
PORT KNOCKING

- TRAP TCP(4321) AND SRC-ADDRESS IS IN TEMPORARY. PUT IT TO ADDRESS-LIST SECURED
PORT KNOCKING

• ALLOW ACCESS FROM SRC-ADDRESS-LIST SECURED
PORT KNOCKING

- DROP ANOTHER TRAFFIC
- ALL THE RULE VIEW

At the end, DROP ALL
PORT KNOCKING

Usage:

knock [options] <host> <port[:proto]> [ proto]

Options:
- -udp: make all ports hits use
- -verbose: be verbose
- -version: display version
- -h: -help: this help

Example:

knock 192.168.46.1254 1234

C:\knock>
PORT KNOCKING

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=
Reply from 192.168.46.254: bytes=

Interfaces

Firewall

Filter Rules  NAT  Mangle  Service P

Name  Address
D  secured  192.168.46.1

-u, --udp  make all ports hits use
-u, --verbose  be verbose
-U, --version  display version
-h, --help  this help

example: knock myserver.example.com 123:tcp 45

C:\knock> knock 192.168.46.254 1234
C:\knock> knock 192.168.46.254 4321
C:\knock>
PORT KNOCKING

• TRY TO CHANGE THE PORT
• MAKE IT A SEQUENCE OF 3 PORTS OR MORE
  • USE TEMPORARY-X AS THE TEMPORARY LIST FOR MORE THAN 2 PORTS USED
PORT SCAN

• PORT SCAN IS A METHOD OF INTRUSION WHERE THE OUTSIDER WILL SCAN THE ROUTER’S PORT TO FIND ONE OR MORE OPEN PORT THAT THEY CAN USE TO PENETRATE THE ROUTER

• THERE ARE 2 KIND OF PORT, WHICH ARE:
  • LOW PORT (OR WELL-KNOW-PORT) WHICH USUALLY USE BY MANY PROGRAMS TO IDENTIFY THEMSELVES. THIS PORT RANGE IS FROM 0 – 1023
  • HIGH PORT WHICH ARE USED RARELY AS AN APPLICATION. THE PORT RANGE IS FROM 1024 - 65535
PORT SCAN DETECT

• MIKROTIK CAN DETECT PORT SCAN BY PSD OPTION IN ADVANCED TAB AT THE FIREWALL

• PSD IS POSSIBLE ONLY FOR TCP PROTOCOL

• LOW PORTS
  • FROM 0 TO 1023

• HIGH PORTS
  • FROM 1024 TO 65535
PORT SCAN DETECT STEP-BY-STEP

• THE STEP OF APPLYING PSD IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  • DROP A CONNECTION FROM SRC-ADDRESS BLACK-LIST
  • TRAP A CONNECTION THAT TRY TO DO A PSD AND PUT THE SRC-ADDRESS TO ADDRESS-LIST BLACK-LIST
  • NOTE : DO NOT CHANGE THE ORDER OF THE RULES ABOVE
PORT SCAN

• DROP A CONNECTION FROM SRC-ADDRESS BLACK-LIST
PORT SCAN DETECT

• TRAP A CONNECTION THAT TRY TO SCAN AND PUT THE SRC-ADDRESS TO ADDRESS-LIST BLACK-LIST
PORT SCAN DETECT

• TRY TO CHANGE THE OPTIONS (LOW PORT WEIGHT, HIGH PORT WEIGHT, AND WEIGHT THRESHOLD)

• INSTEAD OF USING DROP AT THE FIRST RULE, YOU CAN ALSO USE TARPIT (TCP TRAFFIC ONLY). FIGURED OUT THE DIFFERENCE
DOS ATTACKS

- **Main Target for DOS Attacks is Consumption of Resources**, such as CPU time or bandwidth, so the standard services will get denial of service (DOS).

- Usually router is flooded with TCP/SYN (connection request) packets, causing the server to respond with a TCP/SYN-ACK packet, and waiting for a TCP/ACK packet.

- Mostly DOS attackers are virus infected customers.
<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Port</th>
<th>Protocol</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.0.1</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.3</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.3</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.4</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.4</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.5</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.5</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.6</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.6</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.8</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.8</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.10</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.10</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.11</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.11</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.12</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.12</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.13</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.13</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.14</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.14</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.16</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.16</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.17</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.17</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.18</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
<tr>
<td>10.17.0.18</td>
<td>1.1.1.110</td>
<td>80</td>
<td>TCP</td>
<td>syn sent</td>
</tr>
</tbody>
</table>
DOS ATTACK PROTECTION

• All IP’s with more than 10 connections to the router should be considered as DOS attackers

• With every dropped TCP connection we will allow attacker to create new connection

• We should implement DOS protection into 2 steps:
  • Detection - creating a list of DOS attackers on the basis of connection-limit
  • Suppression – applying restrictions to the detected DOS attackers
DOS ATTACK DETECTION
DOS ATTACK SUPPRESSION

• TO STOP THE ATTACKER FROM CREATING NEW CONNECTIONS, WE WILL USE ACTION “TARPIT”

• WE MUST PLACE THIS RULE BEFORE THE DETECTION RULE OR ELSE ADDRESS-LIST ENTRY WILL REWRITE ALL THE TIME
CONNECTION LIMIT

- CONNECTION LIMIT LIMITS THE PACKET PER SECOND (PPS) RATE ON A PER DESTINATION IP OR PER DESTINATION PORT BASE.
- AS OPPOSED TO THE LIMIT MATCH, EVERY DESTINATION IP ADDRESS / DESTINATION PORT HAS IT'S OWN LIMIT.
- CONNECTION LIMIT ONLY EFFECT THE TCP TRAFFIC.
CONNECTION LIMIT

• LIMIT THE NUMBER OF ACTIVE CONNECTIONS TO 5 PER SINGLE IP ADDRESS FOR TELNET SESSION TO THE ROUTER

• THINK ABOUT THE VARIOUS EFFECTS OF THE RULE ABOVE
CONNECTION LIMIT

• THE STEP OF MAINTAINING DOS ATTACK IN MIKROTIK (EVERYTHING IS APPLIED IN INPUT CHAIN)
  • TARPIT A CONNECTION FROM SRC-ADDRESS BLACK-LIST
  • CREATE A RULE TO ALLOW ONLY 5 SIMULTANEOUS CONNECTION FROM A /32 IP, OTHERWISE ADD THE SRC-ADDRESS TO A BLACK-LIST ADDRESS-LIST

• NOTE: TARPIT AND CONNECTION-LIMIT ONLY VALID FOR TCP PACKET
CONNECTION LIMIT

• TARPIT A CONNECTION WITH SRC-ADDRESS BLACK-LIST
CONNECTION LIMIT

- CREATE A RULE TO ALLOW ONLY 5 SIMULTANEOUS CONNECTION FROM A /32 IP, OTHERWISE ADD THE SRC-ADDRESS TO A BLACK-LIST ADDRESS-LIST
CONNECTION LIMIT

• TRY TO MAKE A TELNET OR WEB ACCESS CONNECTION TO YOUR ROUTER AS MUCH AS POSSIBLE

• SEE WHAT IS HAPPENED
  • IT WILL SHOW UP DIFFERENCES ON THE 6TH TELNET/WEB SESSION
DDoS Attacks

- A Distributed Denial of Service Attack is very similar to DOS Attack only it occurs from multiple compromised systems.

- Only thing that could help is “TCP SYN Cookie” option in Conntrack system.
BRUTE FORCE ATTACK

- BRUTE FORCE IS AN ATTEMPT TO CONNECTING TO A ROUTER WITH RANDOM USERNAME/PASSWORD
BRUTE FORCE DETECTION

- The idea to detect brute force is by detecting an unsuccessfully login attempt from the outsider.
- We can detect an unsuccessfully login attempt by checking the response from router to outsider.
- For FTP connection, all unsuccessfully login attempt will return to outsider with a text contains “530 login incorrect”.
BRUTE FORCE DETECTION

• BRUTE FORCE ATTEMPTS ALWAYS GENERATED BY A MACHINE, THUS IT WILL REPEATED SIMULTANEOUSLY

• UNSUCCESSFUL LOGIN FOR ONE OR TWO TIMES CANNOT CONSIDER TO BE A BRUTE FORCE ATTEMPT
DETECTING A BRUTE FORCE

• THE STEP TO DETECTING A BRUTE FORCE ATTACK IN MIKROTIK (CREATED IN OUTPUT-CHAIN)
  • ADD A RULE TO ALLOW AN UNSUCCESSFUL ATTEMPT WITH 1 CONNECTION PER MINUTE (BURST IT TO 5 CONNECTION) BASED ON DESTINATION-ADDRESS
  • ADD A RULE TO PUT A DESTINATION-ADDRESS THAT HAS MORE THAN 1 CONNECTION PER MINUTE (HAS BEEN KICKED-OUT FROM THE RULE BEFORE) INTO AN ADDRESS-LIST NAMED BLACKLIST
DROP THE BRUTE FORCE IP

• THE STEP TO BLOCKING A BRUTE FORCE ATTACK IN MIKROTIK (AFTER THE BRUTE FORCER IP HAS BEEN REVEALED)
  • IN INPUT CHAIN, ADD A RULE TO DROP PACKET FROM SRC-ADDRESS BLACKLIST
DESTINATION LIMIT

- ADD A RULE TO ACCEPT AN UNSUCCESSFUL ATTEMPT WITH 1 CONNECTION PER MINUTE (BURST IT TO 5 CONNECTION) BASED ON DESTINATION-ADDRESS
DESTINATION LIMIT

• ADD A RULE TO PUT A DESTINATION-ADDRESS THAT HAS MORE THAN 1 CONNECTION PER MINUTE (HAS BEEN KICKED-OUT FROM THE RULE BEFORE) INTO AN ADDRESS-LIST NAMED BLACKLIST
THANK YOU