Using An Open Source Intrusion Detection System To Detect And Protect From Insider Attacks

• Shabbir Bashir, SANS GSEC

shabbirbashir1@yahoo.com
**Intrusion Detection System**

- Detect Intrusions.
- What is an Intrusion?
- Two types of IDS.
- Host based or Network based.
- HIDS or NIDS
- Examples of host based IDS
- Examples of Network based IDS
HOW AN IDS WORKS

DEVELOPER NETWORK

IDS CONSOLE

HR NETWORK

Internet

IDS Sensor

FIREWALL

DMZ Server Farm

FIREWALL

IDS Sensor
What is Snort ...

Snort is an open source real time network Intrusion detection system that uses rules and signatures to check malicious traffic on a network segment and triggers alerts and various forms of logging.

Snort holds an inherent advantage over closed source IDSs, in that the IDS itself can be tailored and customized for each individual deployment to a level not possible for closed source competitors.
Like most IDS, snort works on rules or signatures.

All network traffic is passed through a rule set.

All packets are decoded and parsed.

If a packet matches a rule, one of many actions can be taken.

Actions: Log, Alert, block, or all of the above.
Rules are stored as plain text files, can be self written or downloaded from snort’s website and are read by snort upon startup.
Almost 2000 default rules which are categorized in simple text files named to reflect the types of attacks they detect.

Rules are updated on a regular basis by snort developers and users to detect new exploits and worm-like activity.

Custom snort rules can be created to detect insider attacks and violations of a company’s acceptable use policy.
A simple Snort Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 79 (msg:"FINGER version query";
flow:to_server,established; content:"version";
classtype:attempted-recon; sid:1541; rev:4;)
```

- **Rule Header**: Alert, Protocol, Source IP, Source port, Dest IP, Dest port.
- **Rule Options**: message, flow, content, classtype, sid and rev
Defining an Acceptable use policy.

An AUP "defines acceptable use of equipment, computing services and the appropriate employee security measures to protect the organization’s corporate resources and proprietary information."

A list of prohibited activities should be included in the acceptable use policy.
What's an AUP? (Cont…)

- Port scanning of internal or external hosts for vulnerabilities.
- Launching a denial of service attack against a internal or external host.
- Setting up unauthorized wireless access points.
- Setting up unauthorized services such as web, DHCP and DNS servers.
- Surfing the Internet for potentially offensive sites.
- Attempting to log in to a host by using another users network credentials.
Who is an Insider

- Users, business partners, contractors and vendors that are allowed to use network and computing resources.
- Example of resources are file and print services, Intranet web server and mail servers.
Insider threats

- Using legitimate access to do illegitimate activities on the network. For example…….
- Installing Web Servers
- DHCP Servers
- IRC chat servers
- Probing Internal and External hosts for operating system and application level vulnerabilities.
Insider threats (Cont....)

- Stealing confidential HR, R&D or finance data.
- Selling it on the Internet or to competitors.
- Disgruntle Employees.
- Plain mischief purposes, “Look, I can hack the server!”
Types of Attack or Misuse Detected in the Last 12 Months (by percent)
The Network administrator at XVZ Corporation receives a call on a Friday afternoon.

Users on a remote segment are losing their network connectivity.

Upon further investigation, it appears there is an unknown DHCP server on the network.

This DHCP server is assigning non-standard IP addresses, gateway and DNS information to hosts causing loss of connectivity.
If there was a snort sensor monitoring that segment of the network, this could have been triggered an alert long before a large number of users lost connectivity.
Snort rule to detect rouge dhcp servers.

```plaintext
alert udp !$DHCP_SERVERS 67 -> any 68 (msg: "Rogue DHCP server...");
```
Using snort to detect an internal hacker/cracker

Imagine your work place, around 9:00 PM.
How many people are around?
Jack, the programmer is at his desk tapping away.
Just another hard working employee working late trying to meet dead lines, right?
Using snort to detect an internal hacker/cracker (Cont …)

Think again!
Jack is scanning your internal file servers for vulnerabilities.

He is scanning all servers to see what services are open.

But the servers are behind a firewall, and port scans are not allowed so we are protected, right?
Using snort to detect an internal hacker/cracker (Cont …)

Where do you think Jack is?

You guessed it....

Inside your network!
A Typical Network

INTERNET

ISP ROUTER

FIREWALL

SWITCH

Network Segment

FILE SERVER

JACK
Google Search for Exploit code!

SecuriTeam.com™ (RPC Overflow Exploit Code)
Title, 27/7/2003. RPC Overflow Exploit Code. Summary. The Microsoft
RPC overflow (http://www.securiteam.com/windowsrtfocus/5SP0C20AKG ... www.securiteam.com/exploits/5YP0R2AAKU.html - 32k - Cached - Similar pages

SecuriTeam.com™ (Windows RPC DCOM Long Filename Heap Overflow ...
... Exploit: */ http://www.xfocus.net/tools/200309/MS03-039-exp.c ... 0x1000]; int i, iTYPE;
printf("MS03-039 RPC DCOM long filename heap buffer overflow exp \n ... www.securiteam.com/exploits/5WP0B20B5C.html - 25k - Cached - Similar pages
[ More results from www.securiteam.com ]

Securiteam: [EXPL] RPC Overflow Exploit Code
... [EXPL] RPC Overflow Exploit Code. ... - - - - - - . RPC Overflow Exploit Code -----
SUMMARY. ...
www.derkeiler.com/Mailing-Lists/ Securiteam/2003-07/0113.html - 33k - Cached - Similar pages

Securiteam: [NEWS] Oracle Exprec Buffer Overflow
... 2055118;i - - - - - - Oracle Exproc Buffer Overflow
Here it is, compile and run!

RPC Overflow Exploit Code

Summary
The Microsoft RPC overflow (http://www.securiteam.com/windowsntfocus/SSP0C20AKG.html) can be exploited remotely, allowing an attacker to execute arbitrary code. The following exploit code can be used to test your system for the mentioned vulnerability.

Details
/*
 DCOM RPC Overflow Discovered by LSD
 -> http://www.lsd.pl.net/files/get?WORKSTATION\WIN32\dcom

 Based on FleshSky/Benjurry's Code
 -> http:\/\/www.xfocus.org\documents/2003072.html

 Written by H D Moore <hmd [at] mctasploit.com>
 -> http://www.mctasploit.com/

 - Usage: ./dcom <Target ID> <Target IP>
 - Targets:
   - 0 Windows 2000 SP0 (english)
   - 1 Windows 2000 SP1 (english)
   - 2 Windows 2000 SP2 (english)
   - 3 Windows 2000 SP3 (english)
   - 4 Windows 2000 SP4 (english)
“Full Disclosure”

How many of you are aware of “Full-Disclosure” Mailing list?
Using snort to detect an internal hacker/cracker (Cont …)

If there was a snort sensor monitoring that segment of the network, this could have been triggered an alert long before Jack had a chance to exploit internal file and print servers for his benefits.
Port 3333 and 4444 traffic

Counterpane: Security Alerts: Microsoft RPC DCOM Remote Shell Vulnerability - Avant Browser

Address: http://www.counterpane.com/alert-v20030601-001.html

Counterpane and Network Associates Announce Strategic Partnership

Counterpane's Enterprise Protection Suite Draws Continued Customer Momentum in Third Quarter

vulnerability. Full details on the Microsoft security alert can be found at the following links:


Counterpane strongly urges you to block access to RPC ports at your network border through either router access lists or via your firewall. If access to ports 135, 139, and 445 via the network are not business critical, block this access.

Counterpane research has seen positive indicators of an exploit active in the wild. This tool is capable of causing Denial of Service attacks and installing backdoor access programs to the affected system. Additionally, independent research indicates that the application of the MS03-026 security patch does NOT solve the problem in all systems, meaning that even after the application of the patch, certain systems are still vulnerable. Regardless, it is important to apply all vendor supplied patches as soon as possible to reduce exposure.

Over the last two days the SOC has seen an elevated level of Windows RPC and NetBIOS traffic on ports 135 and 445. This is likely due to heavy scanning for vulnerable systems. We have also seen increased levels of scanning for ports 3333 and 4444, two of the ports that the exploit tool is known to install its backdoor program on. We will continue to track access to these questionable ports.

In order to assess your exposure to this vulnerability, eEye
Snort rules to detect RPC/DCOM attacks

```plaintext
? alert tcp any 4444 -> any any (msg:"ATTACK-RESPONSE successful DCom RPC System Shell Exploit Response"; flow:from_server,established; content:"|3a 5c 57 49 4e 44 4f 57 53 5c 73 79 73 74 65|"; classtype:successful-admin;)

? alert tcp any 3333 -> any any (msg:"ATTACK-RESPONSE successful DCom RPC System Shell Exploit Response"; flow:from_server,established; content:"|3a 5c 57 49 4e 44 4f 57 53 5c 73 79 73 74 65|"; classtype:successful-admin;)
```
What is a honey token?

"A honey pot is an information system resource whose value lies in unauthorized or illicit use of that resource."

A resource which no one should use.

Examples of honey token are ............
Using Honey tokens and snort to detect employee abuse of privilege access (Cont.....)

- A bogus medical record called "John F. Kennedy" inserted in a database at a hospital.
- If an intruder/attacker/insider is looking at records, this one will stick out and make them curious.
- If the words "John F Kennedy" appear in a data packet on a network segment that a snort sensor is monitoring, it will trigger an alert.
This method can be used to detect insiders accessing information they shouldn’t.

Create a document in your Human Resources network share and call it Exec-Bonuses.doc, make a snort rule to alert on traffic that has this ASCII content in it, “Exec-Bonuses.doc”.

If an insider is misusing his/her access and scanning for docs that look interesting, they will be identified.
Protecting critical Assets

Call-Center

SNORT SENSOR

IDS CONSOLE

FIREWALL

SNORT SENSOR

HUMAN RESOURCES

INTERNAL NETWORK

Research and Development

SNORT SENSOR

MARKETING
Guess which one of these files is a honey-token?
Snort rule to detect a honey token.

```snort
alert ip any any -> any any
   (msg:"HoneytokenAccess--Potential Unauthorized Activity";content:"Exec-Bounses.doc");
```
An Ideal IDS Implementation
But IDS are expensive!

- They are, don’t buy them!
- Use a combination of snort and acid on apache and redhat.
- All of them are FREE! to use.
A snort sensor
ACID

- Analysis Console for Intrusion Detection.
- Html based front end to Snort.
- Open Source. (FREE)
- Alert management.
- Query-builder and search interface
- Chart and statistics generation.
- Packet viewer (decoder)
ACID
Main screen

Snort Analysis Console for Intrusion Databases

Time window: [2000-07-29 10:05:05] - [2000-08-05 14:09:40]

- # of Sensors: 2
- Unique Alerts: 3
- Total Number of Alerts: 11962
  - Source IP addresses: 480
  - Dest. IP addresses: 26

Traffic Profile by Protocol:
- TCP (19%)
- UDP (74%)
- ICMP (7%)

Search

Snapshot

- Alert Listing
- Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
- Graph Alert detection time

ACID v0.9.2 (by Roman Danyliv as part of the AirCERT project)
ACID
Searching by arrival time and IP Address
ACID
Full Packet Decode
### ACID Alert Listing

**Alert Listing: 15 Last Alerts**

*Queried DB on: Wed September 24, 2003 17:17:18*

**Meta Criteria:** any

**IP Criteria:** any

**Layer 4 Criteria:** none

**Payload Criteria:** any

**Displaying 15 Last Alerts**

<table>
<thead>
<tr>
<th>Signature</th>
<th>Classification</th>
<th>Total #</th>
<th>Sensor #</th>
<th>Src. Addr.</th>
<th>Dest. Addr.</th>
<th>First</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>[cve][icat][cve][icat][cve][icat][snort] SNMP public</td>
<td>attempted-recon</td>
<td>154883</td>
<td>1</td>
<td>16</td>
<td>15</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[arachNIDS][snort] ICMP L3retriever Ping</td>
<td>attempted-recon</td>
<td>277552</td>
<td>1</td>
<td>244</td>
<td>195</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[arachNIDS][snort] ICMP PING CyberKit 2.2 Windows</td>
<td>misc-activity</td>
<td>77622</td>
<td>1</td>
<td>1818</td>
<td>287</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[arachNIDS][cve][icat][snort] DNS zone transfer TCP</td>
<td>attempted-recon</td>
<td>4415</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[snort] ICMP PING speedera</td>
<td>misc-activity</td>
<td>4721</td>
<td>1</td>
<td>74</td>
<td>2</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[arachNIDS][cve][icat][bugtraq][snort] NETBIOS NT NULL session</td>
<td>attempted-recon</td>
<td>3922</td>
<td>1</td>
<td>20</td>
<td>13</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[snort] ICMP Destination Unreachable (Communication with Destination Host is Administratively Prohibited)</td>
<td>misc-activity</td>
<td>1274</td>
<td>1</td>
<td>68</td>
<td>11</td>
<td>2003-08-27</td>
<td>2003-09-07</td>
</tr>
<tr>
<td>[cve][icat][bugtraq][arachNIDS][snort] WEB-IIS iSAPI .ida attempt</td>
<td>web-application-attack</td>
<td>81</td>
<td>1</td>
<td>48</td>
<td>7</td>
<td>2003-08-27</td>
<td>2003-08-27</td>
</tr>
<tr>
<td>url[cve][icat][snort] SMTP From comment overflow attempt</td>
<td>attempted-admin</td>
<td>110</td>
<td>1</td>
<td>9</td>
<td>3</td>
<td>2003-08-27</td>
<td>2003-08-27</td>
</tr>
<tr>
<td>[snort] WEB-IIS cmd.exe access</td>
<td>web-application-attack</td>
<td>333</td>
<td>1</td>
<td>76</td>
<td>7</td>
<td>2003-08-27</td>
<td>2003-08-27</td>
</tr>
<tr>
<td>[cve][icat][snort] WEB-IIS unicode directory traversal</td>
<td>web-application-attack</td>
<td>43</td>
<td>1</td>
<td>26</td>
<td>7</td>
<td>2003-08-27</td>
<td>2003-08-27</td>
</tr>
</tbody>
</table>
Some Tips for protection against insider attacks.

- Do not use a single shared logon account for multiple employees.
- When temporary employees leave, disable their user accounts on your computer systems immediately!
- In your corporate security policy, explain that all use of corporate computers and networks is subject to monitoring.
- Utilize the principle of least privileges.
- Activate logging and intrusion-detection systems on sensitive internal computers and network.
While companies often spend a great deal of time and money preventing attacks from outsiders, many ignore these threats from the malicious insider.

With the economy sputtering and layoffs mounting, a large segment of many companies’ employee population is in a disgruntled state.

As companies cut back on full-time employees, the use of temporary workers is increasing. This environment represents a dangerous mix from a security perspective.
My other Papers

- www.shabbir.mine.nu/Intro_to_tcpdump.pdf
- http://cert.uni-stuttgart.de/archive/intrusions/2004/01/msg00039.html
Questions ?
References

- www.sans.org
- www.giac.org/GCIA.php
- www.incidents.org
- http://www.securityfocus.com/infocus/1520
- http://www.securityfocus.com/infocus/1558
- www.snort.org
- www.dshield.org