

Intrusion Detection Systems and Vulnerability Assessment

Thorsten Fischer
<t.fischer@rhul.ac.uk>

Revision : 1.6

March 22, 2004

1 Basic questions

One

foo.

- find targets

- evaluate the target, collect data and choose attack vector most likely to succeed

- do it!

foo.

Two

foo.

- software-based scans (internal net)

- web-based scans (external)

- pen test

foo.

Three

foo.

Four

foo.

Five

foo.

- network-based: look at packets and streams

- host-based: look at log files

foo.

Six

foo.

- nice built-in denial of service feature

foo.

Seven

foo.

2 Intermediate questions

Eight

foo.

Nine

foo.

Ten*foo.*

If the TCP stack is really stupid enough not to throw this type of packet away, this packet might lead to the host sending back an *SYNACK* packet to itself, then responding with a *ACK* packet to itself, establishing a TCP connection to itself which will most likely time out after a period of time. Lots of this type of packets could lead to a denial of service attack.

But the TCP stack should dump packets which have their source and destination address set to the address of the host; it should do the same with packets that come in on the network interface and have the IP address of the host as a source address; and finally, it should ignore *SYNACK* packets that it has not sent the corresponding *SYN* packet to before.

foo: look up LEAD attack.

Eleven*foo.***Twelve***foo.***Thirteen***foo.***Fourteen***foo.***Fifteen***foo.***Sixteen***foo.*

- cheap (there are free ones)
- it must perform (they do)
- it must scale (oh, really?)

- must produce reasonable output (that can be understood or processed to produce something understandable)

- should have a positive security record (so it does not get itself hacked into)

- easy to setup, configure and maintain

- signatures should be updated by the makers in a timely and comprehensive manner

*foo.***Seventeen***foo.***3 Advanced questions****Eighteen***foo.***Nineteen***foo.*

The way an attacker might detect the presence of an intrusion detection system on a network is similar to the way an administrator of a network might find out about any type of sniffer on the network.

A common technique is to send out artificially created packets that originate from faked source addresses which are not present within the network. When an IDS (or a sniffer) finds that packet, it might be configured in a way to resolve the name of the IP address. So if the attacker suddenly sees DNS traffic on the network regarding the IP address he faked, then obviously someone must have intercepted that packet.

*foo.***Twenty***foo.***Twenty-One***foo.***Twenty-Two***foo.*

Twenty-Three

foo.

References

Contents

1	Basic questions	1
2	Intermediate questions	1
3	Advanced questions	2