



FIST Conference 2003 - September Edition



Router and Routing Protocol Attacks

Balwant Rathore, CISSP

balwant@mahindrabt.com

Moderator, PenTest Group

<http://groups.yahoo.com/group/PenTest>

Consultant, Mahindra British Telecom Ltd.



Router and Routing Protocol Attacks



Overview of Routing Protocols

Router Security Common Issues

Routing Protocol Attacks

Cisco Discovery Protocol (CDP) Attacks

Autonomous System Scanning

Routing Information Protocol (RIP) Attacks

Open Shortest Path First (OSPF) Attacks

Border Gateway Protocol (BGP) Attacks



Introduction

What is routing Protocol

Protocols that are used by routers

To communicate with each other

**To determine appropriate path over which data
can be transmitted**

To make dynamic adjustment to its conditions

Many improvements on host security

**Core technology still uses unauthenticated
services**



Router security common issues



Miss-configurations

IP Packet Handling bugs

SNMP communitystring

Weak password or weak password encryption

DoS because of malformed packets

Above mentioned attacks are commonly known

If attacked with routing protocol impact is very high

Any NIDS can detect most of them



Safeguard



Up to date patching

Strong SNMP community string

Strong encryption

Proper ingress/egress implementation

Proper management implementation

Encrypted Sessions

Strong Passwords

Run on Non standard ports

Route Filtering



Routing Protocol Attacks



Cisco Discovery Protocol (CDP) Attacks

Autonomous System Scanning

Routing Information Protocol (RIP) Attack

Open Shortest Path First (OSPF) Attacks

Border Gateway Protocol (BGP) Attacks



Cisco Discovery Protocol (CDP) overview



Layer 2 Protocol

Used to find out Cisco devices

Protocol is not routed

**Sent periodically to multicast address
[01:00:0C:CC:CC:CC]**

So limited only for local segment

The default period is 60 second

Implemented in every Cisco device



Cisco Discovery Protocol (CDP) overview



Contain information about sending router/s

Host Name

Connected Port

Running Platform

Version

show cdp neighbors [*type number*] [detail]



Cisco Discovery Protocol (CDP) Attack



Phenoelit IRPAS

Download from <http://www.phenoelit.de/irpas/download.html>

This suit contains interesting tools `cdp`, `igrp`, `irdp`, `irdpresponder`, `ass`, `hsrp`



Cisco Discovery Protocol (CDP) Attack



IRPAS CDP

Operates in two modes: Flood and Spoof

Flood mode

Send garbage cdp messages

IOS 11.1.(1) was rebooted after sending long device ID

Later version store the messages and fill the memory

While debugging these message most IOS will reboot



Cisco Discovery Protocol (CDP) Attack



Smart way to perform this attack

Run two processes of IRPAS CDP

Send 1480 kb message to fill up the major part of memory

Send another message to fill length of 10 octet

Spoof mode

Targeted for social engineering or to confuse administrator

You can give proof of concept



Safeguards



Disable CDP if not required

no cdp run: disables CDP globally

no cdp enable: disables CDP on an interface (interface command)

Highly recommended to disable at Border Routers/Switches etc...



Autonomous System Scanning



Used to find AS of routers

IRPAS's ASS supports IRDP, IGRP, EIGRP, RIPv1, RIPv2, CDP, HSRP and OSPF

Operates in Active and Passive mode

Passive mode: Listens to routing protocol packets

Active mode: Discover routers asking for information

You can scan range of AS\$

Spoofed IP can be used



Routing Information Protocol (RIP v1) Overview



Routing Decisions are based on number of hops

Works only within a AS

Supports only 15 hops

Not good for large networks

RIP v1 communicates only it's own information

RIP v1 has no authentication.

Can't carry subnet mask so applies default subnet mask.



Routing Information Protocol (RIP v2) Overview



It can communicate other router information

RIP v2 supports authentication upto 16 char password

It can carry subnet information.

Doors are open to attackers by providing authentication in clear text.



Routing Information Protocol (RIP) Attack



Identify RIP Router by performing a Scan `nmap -v -sU -p 520`

Determine Routing Table

If you are on same physical segment, sniff it

If remote: `rprobe + sniff`

Add a route using `srip` to redirect traffic to your system

Now you know where to send it.



Safeguards



Disable RIP use OSPF, security is always better

Restrict TCP/UDP 520 packets at border router



Open Shortest Path First (OSPF) Attack



OSPF is a Dynamic Link State Routing Protocol

Keeps map of entire network and choose shortest path

Update neighbors using LSAs messages

**Hello packets are generated every 10 second and sent to
224.0.0.5**

Uses protocol type 89



Open Shortest Path First (OSPF) Attack



Identify target: scan for proto 89

JiNao team has identified four ospf attacks

<http://152.45.4.41/projects/JiNao/JiNao.html>

Max Age attack

Sequence++ attack

Max Sequence attack

Bogus LSA attack



Open Shortest Path First (OSPF) Attack



nemiss-ospf can be used to perform ospf attacks

Tuff to use coz of the complexity of OSPF

Good for skilled N/W admin

Some time doesn't work properly



Safeguards



Do not use Dynamic Routing on hosts wherever not required

Implement MD5 authentication

You need to deal with key expiration, changeover and coordination across routers



Border Gateway Protocol (BGP) overview



Allows interdomain routing between two ASs

Guarantees the loop-free exchange

Only routing protocol which works on TCP (179)

Routing information is exchanged after connection establishment.



Border Gateway Protocol (BGP) Attacks



Large network backbone gives special attention on it's security

Medium size networks are easier target

Packet Injection Vulnerabilities are specially dangerous coz flapping penalties



Border Gateway Protocol (BGP) Attacks



Identify BGP Router

It has many problem same as TCP

SYN Flood

Sequence number prediction

DOS

Possible advertisement of bad routes



Further Readings



Router Exploits www.antonline.com

<http://anticode.antonline.com/download.php?dcategory=roi>
=

<http://www.packetninja.net/>.

<http://www.phenoelit.de/irpas/>

RIP Spoofing <http://www.technotronic.com/horizon/ripar.txt>.



Questions ?





Thank you for you time !