Team 10.2

Practice Website Nessus Scan report

1. DNS Server Spoofed Request Amplification DDoS

Synopsis:

The remote DNS server could be used in a distributed denial of service attack.

Description:

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution:

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor:

Medium

CVSS v3 Base Score:

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

2. DNS Server Recursive Query Cache Poisoning Weakness

Synopsis:

The remote name server allows recursive queries to be performed by the host running nessusd.

Description:

It is possible to query the remote name server for third-party names.

If this is your internal nameserver, then the attack vector may be limited to employees or guest access if allowed.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third party names (such as www.nessus.org).

This allows attackers to perform cache poisoning attacks against this nameserver.

If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

Solution:

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf.

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command.

Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }'

If you are using another name server, consult its documentation.

Risk Factor:

Medium

CVSS v2.0 Base Score:

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

3. DNS Server Detection

Synopsis:

A DNS server is listening on the remote host.

Description:

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Solution:

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor:

None

CVSS v3.0 Base Score:

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

4.Nessus SYN scanner

Synopsis:

It is possible to determine which TCP ports are open.

Description:

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution:

Protect your target with an IP filter.

Risk Factor:

None

5. ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating timebased authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)