network vulnerabilities assesment

MOULI DUTTA

Mitigation plan for Network Vulnerabilities

### **Operational environment:**

The random Ip addresses were taken for network vulnerabilities and analyzed thoroughly using NESSUS tool.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *RISKS* | *DESCRIPTION* | *LIKELIHOOD* | *SEVERITY* | *PRIORITY* |
| - DNS Server Spoofed Request Amplification DDoS | . 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 | *3* | *2* | *6* |
| DNS Server Cache Snooping Remote Information Disclosure | The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. | *2* | *2* | *4* |
| - DNS Server Recursive Query Cache Poisoning Weakness | It is possible to query the remote name server for third-party names | *2* | *1* | *2* |

**Risk(s):** A potential risk to the organization's information systems and data.

**Description:** A vulnerability that might lead to a security incident.

**Likelihood:** Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there is a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.

**Severity:** Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.

**Priority:** How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

The used IP addresses are :

* 198.162.1.1
* 199.173.79.79
* 205.45.22.105
* ip61.ip-91-121-235.eu
* p78060-ipngnfx01marunouchi.tokyo.ocn.ne.jp
* static-181-143-195-194.une.net.co

the solution for the risks are following:

1. For the risk, DNS Server Spoofed Request Amplification DDoS as the it is high in level we need to Restrict access to the DNS server from public network or reconfigure it to reject such queries.
2. For the risk , DNS Server Cache Snooping Remote Information Disclosure , Contact the vendor of the DNS software for a fix is required as For instance, if an attacker was interested in whether the company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.
3. For the risk, DNS Server Recursive Query Cache Poisoning Weakness there are several solution we need to follow to resolve the problem .

Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If it is bind 8, we 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.

## Sample risk matrix

**Severity**

**Likelihood**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Low  1 | Moderate  2 | Catastrophic  3 |
| Certain  3 | 3 | 6 | 9 |
| Likely  2 | 2 | 4 | 6 |
| Rare  1 | 1 | 2 | 3 |

s