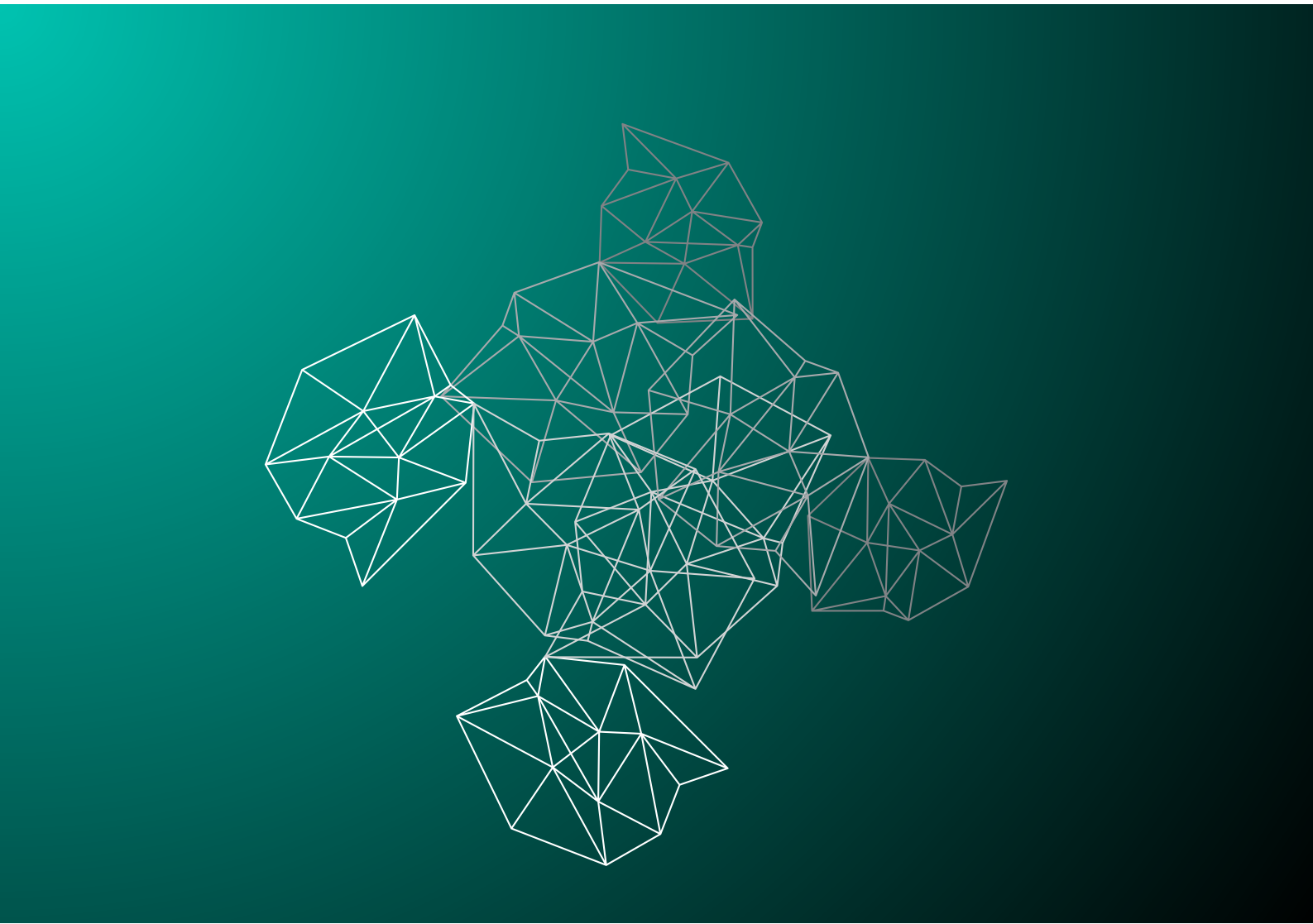
22 FEBBRAIO 2024

REPORT - EPICODE

S5L4

PRESENTED BY

Alessandro Marasca



NESSUS - Vulnerability Assessment

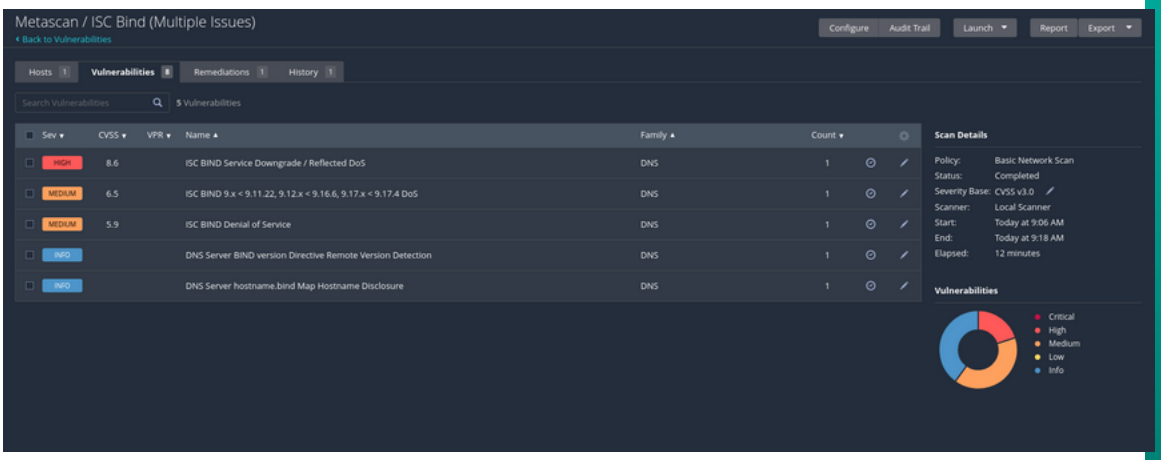
Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

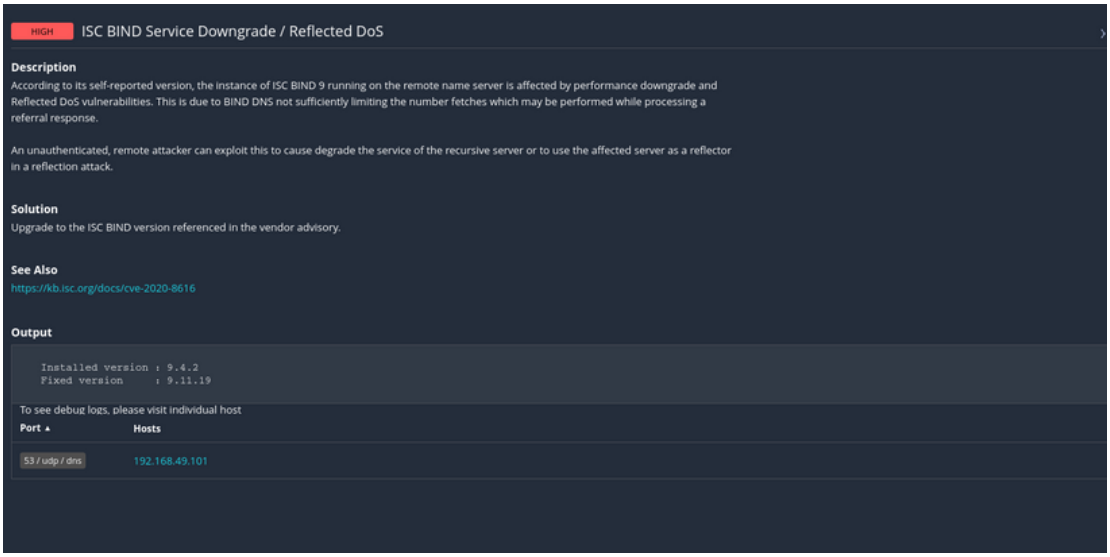
- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.

- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

VULNERABILITÀ



HIGH



SOLUTION

Upgrade to the ISC BIND version referenced in the vendor advisory.

SEE ALSO

https://kb.isc.org/docs/cve-2020-8616

MEDIUM

SOLUTION

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

SEE ALSO

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Hosts 1 | **Vulnerabilities 8** | Remediations 1 | History 1

MEDIUM ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

See Also

https://kb.isc.org/docs/cve-2020-8622

Output

```
Installed version : 9.4.2
Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

To see debug logs, please visit individual host

Port ▲	Hosts
53 / udp / dns	192.168.49.101

MEDIUM 2

SOLUTION

Upgrade to the patched release most closely related to your current version of BIND.

SEE ALSO

https://kb.isc.org/docs/cve-2020-8617

Metascan / Plugin #136808

‹ Back to Vulnerability Group

Hosts 1 | **Vulnerabilities 8** | Remediations 1 | History 1

MEDIUM ISC BIND Denial of Service

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to the patched release most closely related to your current version of BIND.

See Also

https://kb.isc.org/docs/cve-2020-8617

Output

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

To see debug logs, please visit individual host

Port ▲	Hosts
53 / udp / dns	192.168.49.101

INFO

Metascan / Plugin #35371

‹ Back to Vulnerability Group

Hosts 1 | **Vulnerabilities 8** | Remediations 1 | History 1

INFO DNS Server hostname.bind Map Hostname Disclosure

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Output

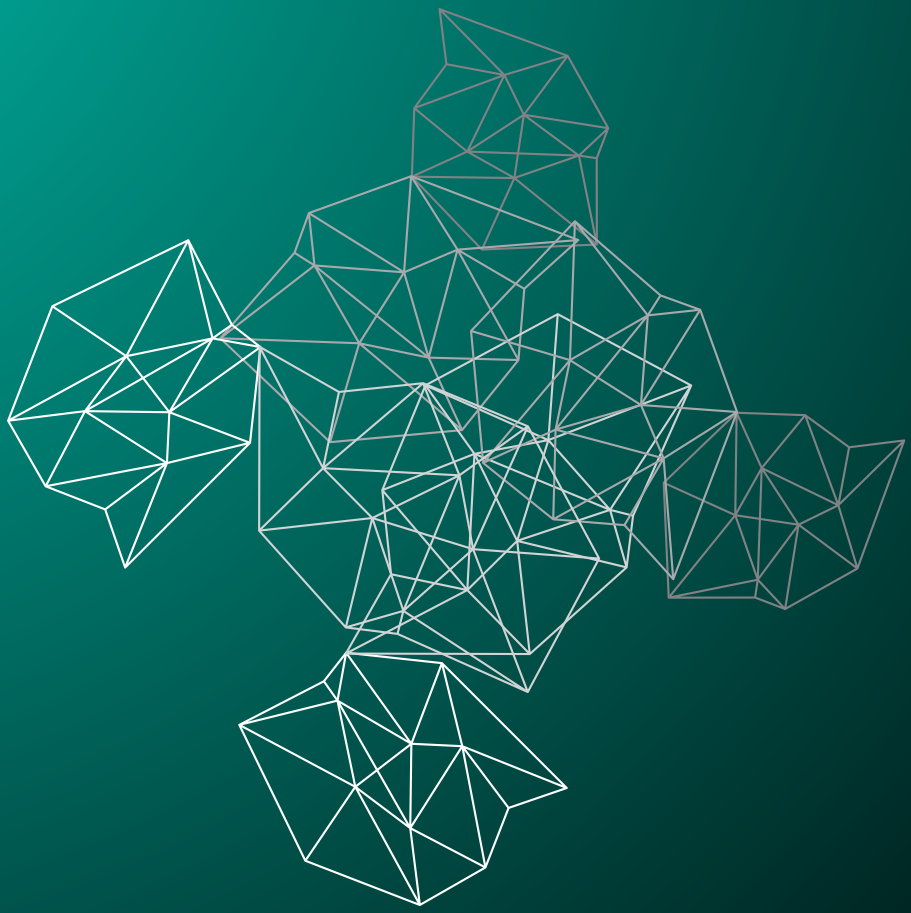
```
The remote host name is :

metasploitable
```

To see debug logs, please visit individual host

Port ▲	Hosts
53 / udp / dns	192.168.49.101

SOLUTION

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.



Alessandro Marasca

Epicode

S5L4 - CS0124

22 FEBBRAIO 2024