# RALAYALA SEEMA UNIVERSITY KURNOOL SRI SANKARS DEGREE COLLEGE IN KURNOOL

R somanath
Bsc micro biology
21367008008

# PROJCET TITLE:UNDERSTANDING NESSUS THREAT EXPLORING AND INFORMATION

- **Team ID :** LTVIP2024TMID14115
- **Team Size :5**
- **Team Leader :** Repakula Somanath
- **Team member :** Maddela Jeevan Kumar
- **Team member :** Masapogu Greswari
- **Team member :** S Anwar Basha
- **Team member :** Syed Ashafaq Ali
- college: sri sankars degree college kurnool

# INDEX

# UNDERSTANDING FOR THREAT FOR EXPLORING AND NESSUS INFORMATION REPORT

And nessus vulnerabilities

# INTRODUCTION FOR CYBER THREAT AND VULNERABLILTIE SCANNING

- Understanding a Nessus report is a key aspect of cybersecurity, especially in threat analysis and mitigation. Nessus is a widely used vulnerability assessment tool that scans systems and networks for potential vulnerabilities and generates detailed reports. Here's a basic introduction to cyber security for threat understanding using Nessus reports:
- **Understanding Vulnerabilities**: A vulnerability is a weakness or flaw in a system that can be exploited by attackers to compromise the security of the system. Nessus scans identify these vulnerabilities by probing various aspects of the system, such as open ports, software versions, configurations, etc.
- **Interpreting Nessus Reports**: Nessus generates reports that detail the vulnerabilities found during the scan. These reports typically include information such as the severity of the vulnerability, affected systems, description of the vulnerability, and potential impact if exploited.
- **Severity Levels**: Vulnerabilities are often categorized into severity levels such as critical, high, medium, and low. Critical vulnerabilities pose the most significant risk and should be addressed immediately, while low-severity vulnerabilities may not pose an immediate threat but should still be remediated to reduce overall risk.

# DNS INFORMATION GATHERING TO TARGET:IBOMMA WEBSITE

Jump to: A Records AAAA Records CNAME Records MX Records NS Records PTR Records SRV Records SOA Records TXT Records CAA Records DS Records DNSKEY Records

## A

| Type | Domain Name | TTL | Address |
|---|---|---|---|
| A | ott.ibomma.party/telugu-movies/ | 300 | 104.21.67.23 \| Check IP Blacklist<br>**Owner:** CloudFlare Inc. \| WHOIS \| AS13335 |
| A | ott.ibomma.party/telugu-movies/ | 300 | 172.67.211.144 \| Check IP Blacklist<br>**Owner:** CloudFlare Inc. \| WHOIS \| AS13335 |

## AAAA

| Type | Domain Name | TTL | Address |
|---|---|---|---|
| AAAA | ott.ibomma.party/telugu-movies/ | 300 | 2606:4700:3033::6815:4317<br>**Owner:** CloudFlare Inc. \| WHOIS \| |
| AAAA | ott.ibomma.party/telugu-movies/ | 300 | 2606:4700:3030::ac43:d390<br>**Owner:** CloudFlare Inc. \| WHOIS \| |

# PLANING FOR PREPARATION

- **Nessus Vulnerability Assessment Project Plan**
- 1. Project Initiation
- **Objective Definition**: Clearly define the objectives of the Nessus vulnerability assessment project. Example: "To identify and remediate vulnerabilities in the organization's internal network infrastructure to improve overall security posture."
- **Scope Identification**: Define the scope of the project, including the systems, networks, and assets to be assessed. Example: "The assessment will cover all servers, workstations, and networking devices within the internal network.“
- 2.Resource Allocation
- **Team Formation**: Identify the project team members responsible for conducting the Nessus scans, analyzing the results, and implementing remediation actions. Example: Security Analyst, Network Administrator, System Administrator.
- **Timeframe**: Determine the project timeline, including milestones and deadlines for each phase of the assessment. Example: "The project will be completed within four weeks, with Nessus scans conducted in the first two weeks and remediation activities carried out in the subsequent two weeks."

# BASIC SCANING BEYOND OVER VIEW NESSUS SCANNING TOOLS

- 3.Pre-Scan Preparation
- **Nessus Installation**: Install and configure the Nessus vulnerability scanner according to organizational requirements and best practices.
- **Scan Policy Configuration**: Define and configure scan policies in Nessus based on the project scope and objectives. Customize scan settings to minimize impact on production systems while maximizing vulnerability coverage.
- 4.Initial Scan
- **Scan Execution**: Perform an initial Nessus scan of the target environment to identify vulnerabilities, misconfigurations, and potential security issues.
- **Scan Analysis**: Analyze the results of the Nessus scan to prioritize vulnerabilities based on severity ratings, potential impact, and exploitability.
- 5.Remediation Planning
- **Vulnerability Prioritization**: Prioritize vulnerabilities for remediation based on risk factors and organizational priorities. Develop a remediation plan outlining specific actions for addressing each identified vulnerability.

# BASIC SCAN FOR REPORT MY IP ADDRESS




## My Basic Network Scan

Report generated by Nessus™ Tue, 02 Apr 2024 00:08:24 EDT

# VULNERABILITIES TO HOST SERVICE FOR BASIC SCAN

**Vulnerabilities by Host**

# HOST DISCOVERY FOR VULNERABILITIES

TABLE OF CONTENTS

# THESE REPORT FOR ANALYSIS FOR MY IP ADDRESS

**192.168.186.2**

| 0 | 0 | 2 | 0 | 11 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities — Total: 13

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| MEDIUM | 6.5 | 4.9 | 50686 | IP Forwarding Enabled |
| MEDIUM | 5.3 | - | 12217 | DNS Server Cache Snooping Remote Information Disclosure |
| INFO | N/A | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | 11002 | DNS Server Detection |
| INFO | N/A | - | 35371 | DNS Server hostname.bind Map Hostname Disclosure |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 35716 | Ethernet Card Manufacturer Detection |
| INFO | N/A | - | 86420 | Ethernet MAC Addresses |
| INFO | N/A | - | 11219 | Nessus SYN scanner |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 10287 | Traceroute Information |
| INFO | N/A | - | 20094 | VMware Virtual Machine Detection |

* indicates the v3.0 score was not available; the v2.0 score is shown

# WEBAPP FOR MY IP ADDRESS SOURCE




## webapp

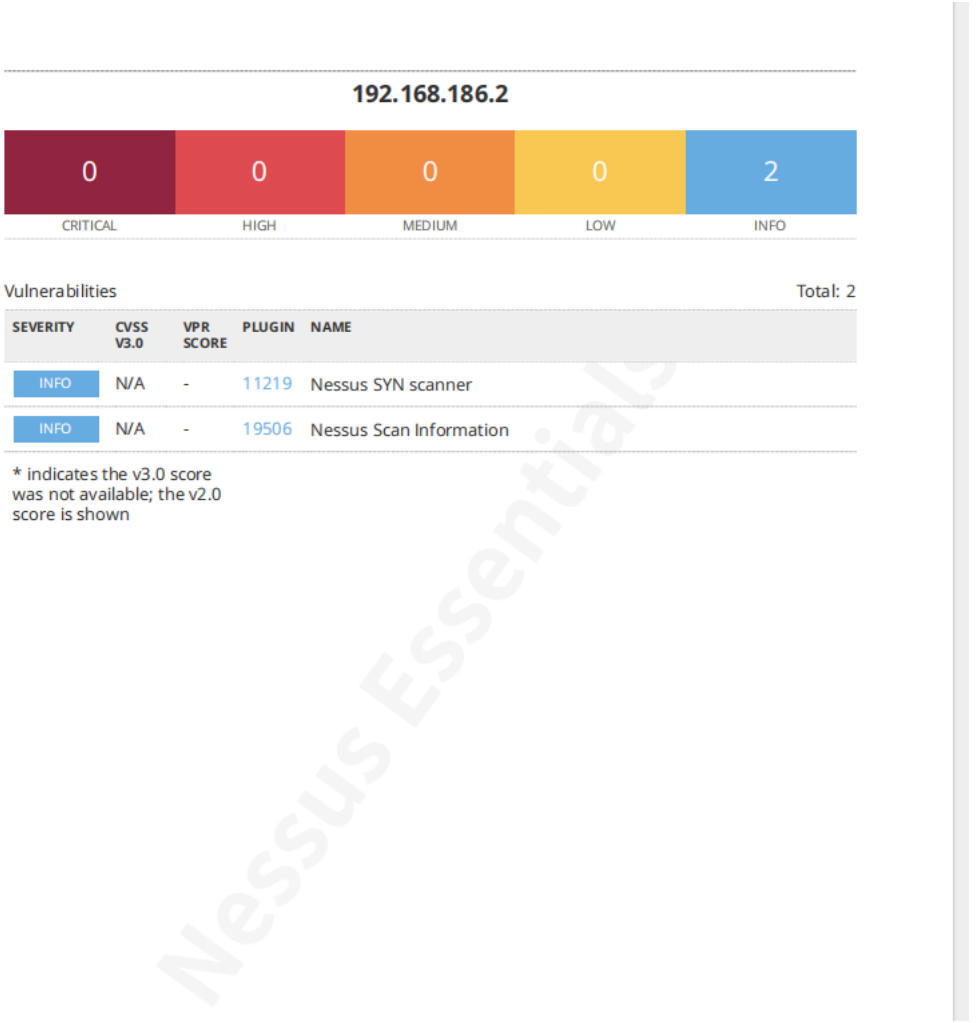
Report generated by Nessus™ Tue, 02 Apr 2024 01:33:26 EDT

# THE VULNERABILITIES FOR RESOURCE COMMONLY SCANING

TABLE OF CONTENTS

**Vulnerabilities by Host**

# SCANER FOR WEB APP SOURCE



192.168.186.2

| 0 | 0 | 0 | 0 | 2 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Vulnerabilities Total: 2

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| INFO | N/A | - | 11219 | Nessus SYN scanner |
| INFO | N/A | - | 19506 | Nessus Scan Information |

* indicates the v3.0 score was not available; the v2.0 score is shown

# DNS LOOK UP INFORMATION TO GATHERING FOR SOURCE INTO MY IP ADDRESS

WHOIS Lookup ( 172.17.0.1 )

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange:       172.16.0.0 - 172.31.255.255
CIDR:           172.16.0.0/12
NetName:        PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-172-16-0-0-1
Parent:         NET172 (NET-172-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to
a home gateway, and are automatically configured in hundreds of millions of devices.  They are only intended for use within a private context  and traffic
that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.  The traffic from these addresses
does not come from ICANN or IANA.  We are not the source of activity you may see on logs or in e-mail records.  Please refer to
http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC
1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/172.16.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
```

# THESE ARE MORE DETAILS ANALYSIS DNS LOOK UP OR IP ADDRESS

```
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

# THESE ARE COMMON ONLY MY IP ADDRESS

## IP2Location

| | |
|---|---|
| IP: | 172.17.0.1 |
| Country: | N/A |
| State: | N/A |
| City: | N/A |
| Latitude: | N/A |
| Longitude: | N/A |
| ISP: | N/A |

IP Location Services by: IP2Location

Updated: April 01 2024


## IPInfo.io

| | |
|---|---|
| IP: | 172.17.0.1 |
| Country: | N/A |
| State: | N/A |
| City: | N/A |
| Latitude: | N/A |
| Longitude: | N/A |
| ISP: | N/A |
| Proxy: | No |

# NESSUS SCANNING KEY POINTS

- **Vulnerability Detection**: Nessus scans networks, systems, and applications to identify vulnerabilities that could be exploited by attackers.
- **Comprehensive Coverage**: It supports various platforms and technologies, including Windows, Linux, Unix, network devices, databases, web servers, and more.
- **Customizable Scans**: Users can configure scans based on their specific requirements, including target selection, scan type (e.g., full, credentialed, web application), and scan frequency.
- **Reporting**: Nessus generates detailed reports outlining discovered vulnerabilities, severity levels, and remediation recommendations. These reports help organizations prioritize and address security issues effectively.
- **Integration**: It can integrate with other security tools and platforms, such as SIEM (Security Information and Event Management) systems and ticketing systems, to streamline vulnerability management processes.

# NESSUS FOR DOMAIN AND REPORT

- Nessus is a popular vulnerability scanner used to identify security issues in networks and systems.
- Once you've run a scan with Nessus, you can generate a report detailing the vulnerabilities it found, along with recommendations for remediation.
- Ibomma report for analysis in their website in complete process submit