A green chameleon logo

Description automatically generated

XMAS SCAN

TEAM PROJECT-A 374

​​

**TABLE OF CONTENTS**

1-SUMMARY……………………………………………………………………………………..

2-INTRODUCTION……………………………………………………………………………..

3- TOOLS USED………………………………………………………………………………..

4-SCOPE OF TESTING………………………………………………………………………….

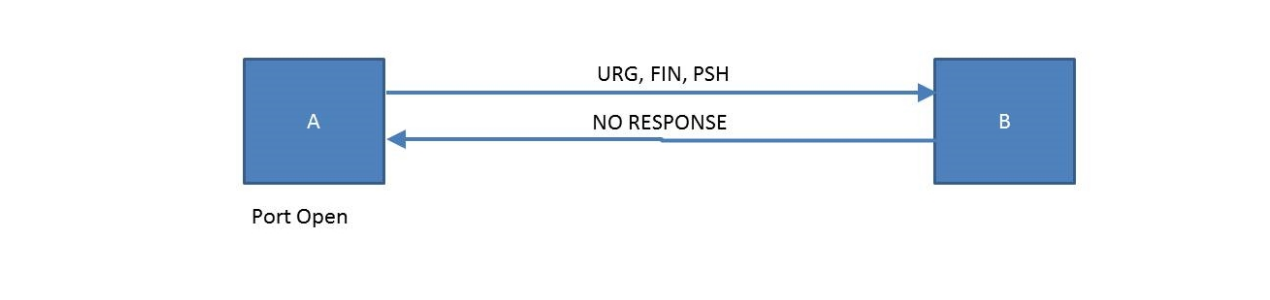
5-RESULTS…………………………………………………………………………………………

6-CONCLUSIONS……………………………………………………………………………….

7-REFERENCES……………………………………………………………………………………

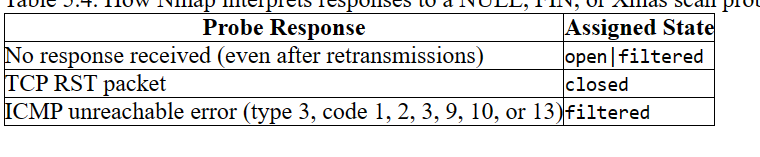
**EXECUTIVE SUMMARY**

In this scan, the **ACK**, **SYN**, **URG**, **RST**, and **FIN** flags are all set at once on the same packet. The issue with this is that since all the flags are set, the target system may have difficulties in interpreting the packets it has received. The following diagram shows this process:



**INTRODUCTION**

This scan uses a loophole with the TCP RFC to differentiate between open and closed ports. So in other words, the Xmas scan in order to identify listening ports on a targeted system will send a specific packet. If the port is open on the target system then the packets will be ignored. The key advantage to these scan types is that they can sneak through certain non-stateful firewalls and packet filtering routers. Such firewalls try to prevent incoming TCP connections (while allowing outbound ones) by blocking any TCP packets with the SYN bit set and ACK cleared. This configuration is common enough that the Linux iptables firewall command offers a special --syn option to implement it. The NULL, FIN, and Xmas scans clear the SYN bit and thus fly right through those rules.



**TOOLS USED**

Nmap (Network Mapper): A powerful open-source tool for network discovery and security auditing.

OpenVAS (Open Vulnerability Assessment System): An open-source vulnerability scanner used to execute remote security checks against your systems.

Nessus: A widely used vulnerability scanner that can identify vulnerabilities, misconfigurations, and other security issues.

Wireshark: A network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network.

Burp Suite: An integrated platform for performing security testing of web applications.

Metasploit: An advanced open-source penetration testing framework that helps security researchers, penetration testers, and IDS/IPS developers.

Aircrack-ng: A suite of tools for assessing Wi-Fi network security.

**SCOPE OF TESTING**

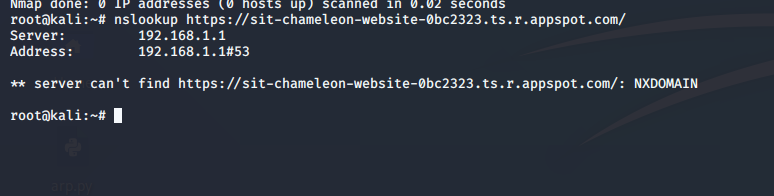
Define Objectives: Clearly outline the objectives of the security scan. Are you looking for vulnerabilities in a specific network, web application, or system? Are you assessing the overall security posture or focusing on a particular area?

Identify Assets: Determine the assets that are within the scope of the scan. This could include network devices, servers, applications, databases, and other components. Understanding the assets helps in focusing the scan on relevant targets.

Authorization: Obtain proper authorization from the owners or administrators of the systems being scanned. Unauthorized scanning is illegal and can lead to serious consequences.

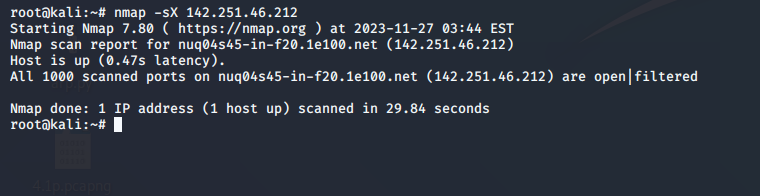
Legal and Regulatory Compliance: Ensure that the security scan complies with relevant laws and regulations. Different industries and regions may have specific requirements regarding security assessments and data protection.

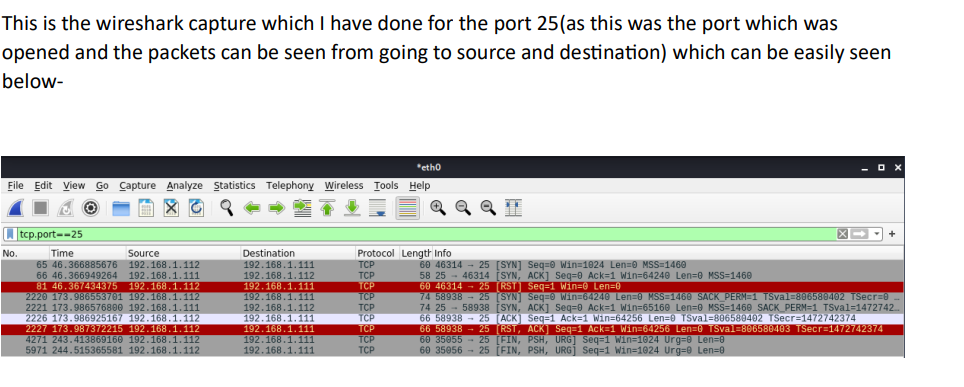
**RESULTS**



A screenshot of a computer

Description automatically generated





This is the XMAS SCAN I have done with he chameleon website and it can be seen easily that all the ports (1000) are opened.

**CONCLUSION**

Findings: Summarize the vulnerabilities, weaknesses, and security issues identified during the scan.

Risk Assessment: Evaluate the risks associated with the identified vulnerabilities, considering factors such as potential impact and likelihood of exploitation.

Recommendations: Provide recommendations for mitigating or remedying the identified vulnerabilities. This may include applying patches, reconfiguring systems, or implementing additional security measures.

Documentation: Ensure that all findings, assessments, and recommendations are thoroughly documented. This documentation is essential for future reference, auditing, and compliance purposes.

**REFERENCES**

1-https://www.plixer.com/blog/understanding-xmas-scans/

2-TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX) | Nmap Network Scanning

3-https://subscription.packtpub.com/book/security/9781788995177/4/ch04lvl1sec39/xmas-scans