Bolortuya Gombojav

CYBERSECURITY

VULNURABILITY

# Scan Results Summary

* **Host**: 172.20.10.4
* **Open Ports**:
  1. **Port 5000**: Running **UPnP**
  2. **Port 7000**: Running **AFS3 Fileserver**
* **Scan Duration**: 1.76 seconds
* **Network**: Subnet 172.20.10.0/28

## Analysis

**Port 5000 (UPnP)**

* **Description**: UPnP is a protocol used for device discovery and communication in a network. It is commonly used by smart devices to connect and configure themselves automatically.
* **Risks**:
  + UPnP has a history of vulnerabilities, such as allowing unauthorized devices to access internal networks.
  + Attackers could exploit UPnP to expose private data or enable further attacks.
* **Recommendation**:
  + Disable UPnP if it is not required.
  + Use a firewall to block external access to this port.

**Port 7000 (AFS3 Fileserver)**

* **Description**: This port is associated with AFS (Andrew File System), which is used for distributed file systems and remote file access.
* **Risks**:
  + If misconfigured, it could expose sensitive files to unauthorized users.
  + Outdated versions of AFS3 could be vulnerable to exploits.
* **Recommendation**:
  + Ensure the file server is updated with the latest security patches.
  + Restrict access to this port using access control lists (ACLs) or firewalls.
  + Disable this service if it is unnecessary.

# 1. Introduction:

In this section, you’ll briefly introduce the purpose of the scan and its scope.

* **Purpose**: The objective of this vulnerability scan is to identify active hosts on the network, discover open ports, and detect any vulnerabilities that may expose the network or connected devices to potential threats.
* **Scope**: The scan focused on a subnet (172.20.10.0/28) with at least two connected devices to gather data for analysis.

## 2. Methodology:

This section explains how you conducted the scan and why you chose those methods.

* **Initial Scan**: Used nmap -sn <subnet> to perform a ping scan and identify active hosts.
* **Detailed Scan**: Performed nmap -sV -O --script vuln <subnet> to probe for open ports, running services, and potential vulnerabilities.
* **Results Export**: The results were saved as a text file (nmap -oN results.txt) for reference and documentation.

## 3. Findings:

Here, you'll summarize the scan results, focusing on key findings.

* **Host**: 172.20.10.4
* **Open Ports**:
  + **Port 5000 (UPnP)**: A device communication protocol used for automatic device discovery. Known for vulnerabilities, could allow unauthorized access.
  + **Port 7000 (AFS3 Fileserver)**: Associated with file-sharing services. Outdated versions may expose sensitive data if not properly secured.
* **Scan Duration**: 1.76 seconds
* **Network**: Subnet 172.20.10.0/28

## 4. Analysis:

This section dives deeper into the vulnerabilities discovered and their implications.

* **Port 5000 (UPnP)**:
  + **Risk**: UPnP allows devices to automatically discover and configure themselves, which can expose the network to unauthorized devices or potential attacks.
  + **Implication**: Attackers may exploit this to access sensitive data or manipulate devices.
* **Port 7000 (AFS3 Fileserver)**:
  + **Risk**: If misconfigured or outdated, AFS3 may allow unauthorized access to files or be vulnerable to known exploits.
  + **Implication**: Exposing sensitive files to unauthorized users increases the risk of data breaches.

## 5. Action Plan:

Provide specific recommendations to mitigate the identified vulnerabilities.

* **Port 5000 (UPnP)**:
  + Disable UPnP if it’s not necessary.
  + Use a firewall to block external access to this port.
* **Port 7000 (AFS3 Fileserver)**:
  + Ensure the AFS service is updated to address known vulnerabilities.
  + Restrict access to this port through ACLs or a firewall.
  + If the service is not needed, consider disabling it entirely.

## 6. Layman’s Explanation:

For non-technical stakeholders, explain the findings and recommendations in simple terms.

* "Two open ports were detected during the scan. The first one (Port 5000) is used for automatic device communication, and the second one (Port 7000) is for file sharing. These open ports could allow attackers to access the network or sensitive files. It’s recommended to disable unnecessary services and ensure that any software running on these ports is up to date. These actions will help protect the network and sensitive information from potential risks."

## Conclusion:

Wrap up the report with a summary of what was found and the next steps.

* A summary of the key findings, the risks associated with the open ports, and a reminder of the actions that need to be taken to mitigate those risks.