Daryush

Ayman

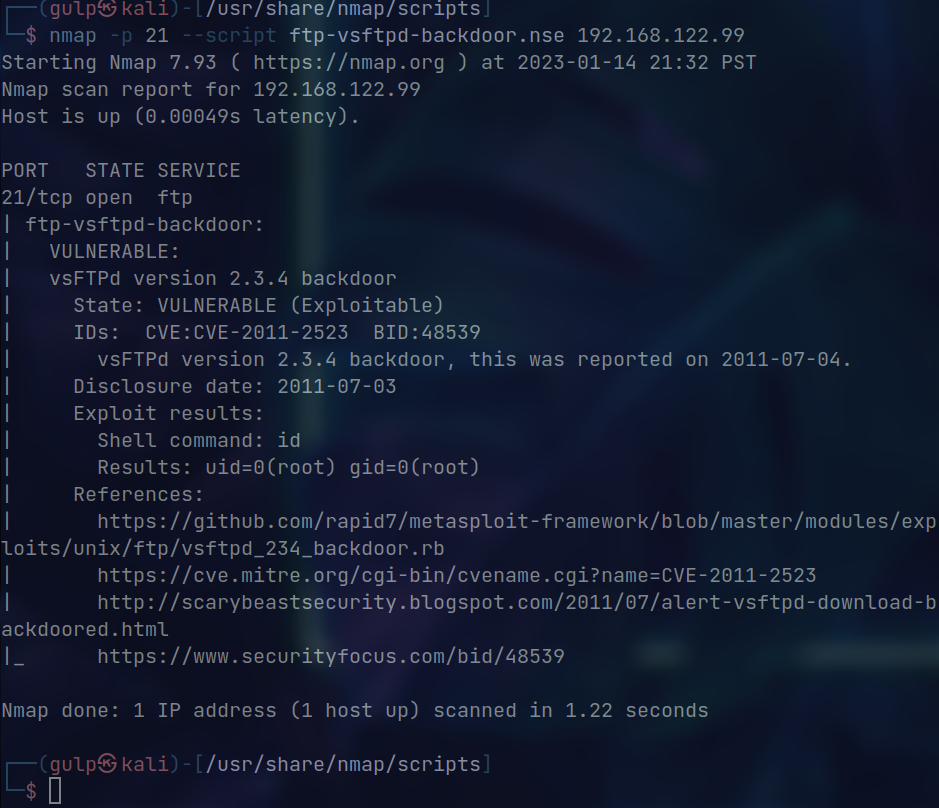
Part 1

1. -sn = ping scan - disable port scan

2. -sV = Probe open ports to determine service/version info

3. -A = -A, to enable OS and version detection, script scanning -T4 for traceroute

4. When searched up the version for both ftp and irc is backdoor command execution



5.

False positives: These are vulnerabilities that the scan has identified, but that do not actually exist on the system. They can be caused by a lack of accuracy in the scanning software or by the system's configuration.

False negatives: These are vulnerabilities that the scan has missed, but that do exist on the systemhis can be caused by a lack of coverage in the scanning software, or by the system's configuration or defenses which are blocking the scanner from identifying them.

Incorrect vulnerability information: This can include incorrect descriptions, incorrect severity ratings, or incorrect information about the affected systems or software.

Outdated vulnerability information: This can include vulnerabilities that have already been patched or mitigated, but are still listed in the report as outstanding.

Inaccurate asset information: This can include incorrect IP addresses, incorrect software versions, or incorrect system configurations.

6. Base vector is a string of characters that represents the various factors that contribute to the overall score of a vulnerability, including the severity of the vulnerability, the attack vector, and the complexity of the exploit. The base vector is used to calculate a vulnerability's CVSS score

7. The solution to fix this attack vector is to install the updated package and validate it by using the signature

8. When prioritizing vulnerabilities for remediation we need to think about 3 things they are:

1. System criticality

2. Information sensitivity

3. Vulnerability severity