Cat Scan Vulnerabilities

By Derek Mayen

Executive Summary

In this document, we will go over the findings of the network scan and the vulnerabilities that have been discovered on the network. Using the greenbone application to run a network wide scan. We will be looking into 3 different types of vulnerabilities to the network, ranging from high priority to low priority, to fully understand the steps that need to be taken to secure the network further.

Scan Results

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
172.16.14.50			1	0			Mon, Sep 25, 2023 10:11 PM UTC	Mon, Sep 25, 2023 10:44 PM UTC	1	1	2	0	0	4	10.0 (High)
172.16.14.52			3	3			Mon, Sep 25, 2023 10:11 PM UTC	Mon, Sep 25, 2023 10:45 PM UTC	3	3	2	0	0	8	10.0 (High)
172.16.14.53			2	1			Mon, Sep 25, 2023 10:11 PM UTC	Mon, Sep 25, 2023 10:49 PM UTC	1	3	2	0	0	6	10.0 (High)

Methodology

1. The command we will run is “sudo gmv-start”
2. set up a new scan with the target being the network “172.16.14.0/24”
3. Categorize and assess vulnerability based on CVE number
4. Common Vulnerability Scoring System (CVSS) calculator for custom results

Findings

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508	HTTP Brute Force Logins With Default Credentials Reporting	1	1	7.5 (High)
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1	5.0 (Medium)
CVE-2011-1473 CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	1	1	5.0 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2	2	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	7	7	2.1 (Low)

pplied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

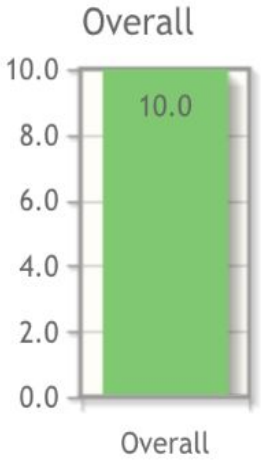
Example vulnerabilities that will be used:

HTTP Brute Force Logins with Default Credentials reporting

DoS (Denial of Service) Vulnerability

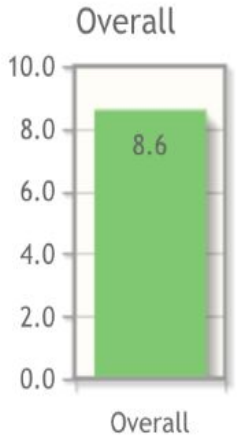
Internet Control Message Protocol (ICMP) Vulnerability

Risk Assessment (Brute Force)



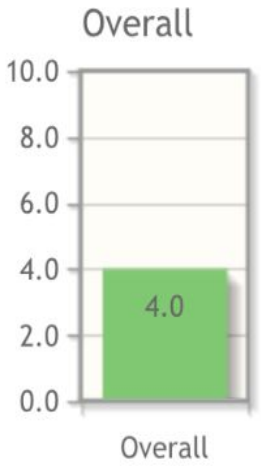
CVSS Base Score: 10.0
Impact Subscore: 6.0
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 10.0

Risk Assessment (DoS Attack)



CVSS Base Score: 8.6
Impact Subscore: 4.7
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.6

Risk Assessment (ICMP Recon Attack)



CVSS Base Score: 4.0
Impact Subscore: 1.4
Exploitability Subscore: 2.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 4.0

Mitigations

Brute Force Vulnerability:

- Set up password protection with MFA or 2FA

DoS Vulnerability:

- Set up Sensors to monitor network traffic with thresholds and warnings

ICMP Vulnerability:

- Set up Firewall to deny ICMP timestamp requests

Works Cited

NVD CVSS. **NVD. (n.d.). https://nvd.nist.gov/vuln/search**

CVE security vulnerability database. security vulnerabilities, exploits, references and more. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. (n.d.). https://www.cvedetails.com/

ICMP timestamp response and request vulnerability fix: Beyond security. **Vulnerability Security Testing & DAST | Beyond Security. (2023, February 6). https://www.beyondsecurity.com/resources/vulnerabilities/icmp-timestamp-request**

You are viewing this page in an unauthorized frame window. **NVD. (n.d.). https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator**