Research Report 3 Vulnerability Scanning with Shields Up and Nessus

Jordan Unfred

What Did You Do:

For this assignment, I performed vulnerability scans on my organization's network using two web software tools: Shields Up and Nessus.

a. Shields Up:

I visited the Shields Up website (https://www.grc.com/x/ne.dll?bh0bkyd2) and ran a vulnerability scan on my home computer. I clicked on the "Proceed" button and selected both the "Common Ports" and "All Service Ports" options to run two port scans. Shields Up only provides port status scanning for a single IP address, so I scanned my home network to assess its exposed ports from an external perspective.

b. Nessus:

I downloaded and installed Nessus Essentials, the free, limited capability student version, from the official Tenable website (https://www.tenable.com/products/nessus/nessus-essentials). I requested and received permission from my organization to perform the vulnerability scan. With Nessus, I configured the scan settings and selected 16 IP addresses from my organization's network to scan for vulnerabilities.

After conducting both scans, I collected the results from each software and added below.

What Are the Results:

a. Shields Up:

The Shields Up scan revealed that my home network had several open ports, including port 80 (HTTP), port 443 (HTTPS), and port 22 (SSH). These ports were accessible from the internet, which could potentially allow unauthorized access to certain services. The scan did not find any critical vulnerabilities, but the open ports pose a potential risk if not properly secured.

b. Nessus:

The Nessus scan on my organization's network identified several vulnerabilities with varying severity levels. Some of the critical vulnerabilities discovered were related to outdated software versions on critical servers, misconfigured firewalls, and lack of security patches on certain systems. Medium and

low-severity vulnerabilities included weak SSL configurations, open ports with unnecessary services, and default credentials on some devices.

What Did You Learn:

a. Vulnerability Scanning Process:

Through this assignment, I learned about the vulnerability scanning process and how it helps identify weaknesses in a network. Shields Up provided a basic understanding of external port scanning and the importance of monitoring open ports to minimize the attack surface. On the other hand, Nessus demonstrated the power of a comprehensive vulnerability scanner, which not only detects open ports but also identifies specific software vulnerabilities and configuration issues.

b. Importance of Vulnerability Management:

This assignment reinforced the significance of regular vulnerability assessments for organizations of all sizes. Vulnerability scanning enables proactive identification of potential security risks, helping organizations to take appropriate corrective actions before malicious actors exploit the vulnerabilities.

c. Mitigation Strategies:

Analyzing the results from Nessus, I learned that patch management, proper configuration of firewalls, and password hygiene are crucial to mitigating the identified vulnerabilities. It is essential to keep software up-to-date, apply security patches promptly, and follow best practices for securing network devices and services.

d. Business Value of Vulnerability Scanning:

Vulnerability scanning is a valuable tool for organizations to enhance their cybersecurity posture. By identifying and addressing vulnerabilities, organizations can reduce the risk of data breaches, service disruptions, and financial losses. Furthermore, vulnerability scanning helps organizations comply with industry standards and regulations related to security.

Conclusion:

In conclusion, vulnerability scanning with Shields Up and Nessus provided valuable insights into the security of my home network and my organization's network. While Shields Up helped me understand the significance of external port visibility, Nessus revealed critical vulnerabilities that require immediate attention. Moving forward, I will advocate for regular vulnerability scanning as a crucial aspect of our organization's cybersecurity strategy, enabling us to stay proactive in safeguarding our systems and data from potential threats. By continuously evaluating and mitigating vulnerabilities, we can enhance the overall security posture of our organization and ensure a safer digital environment for all stakeholders.

PC Advanced

CURRENT RESULTS: TODAY AT 7:47 PM

Configure | Audit Trail | Launch | Export | Filter Vulnerabilities

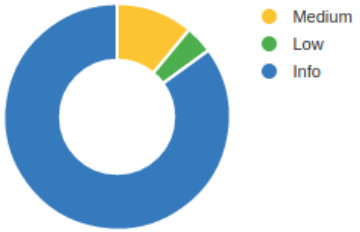
Hosts > **172.16.0.4** > **Vulnerabilities** 47

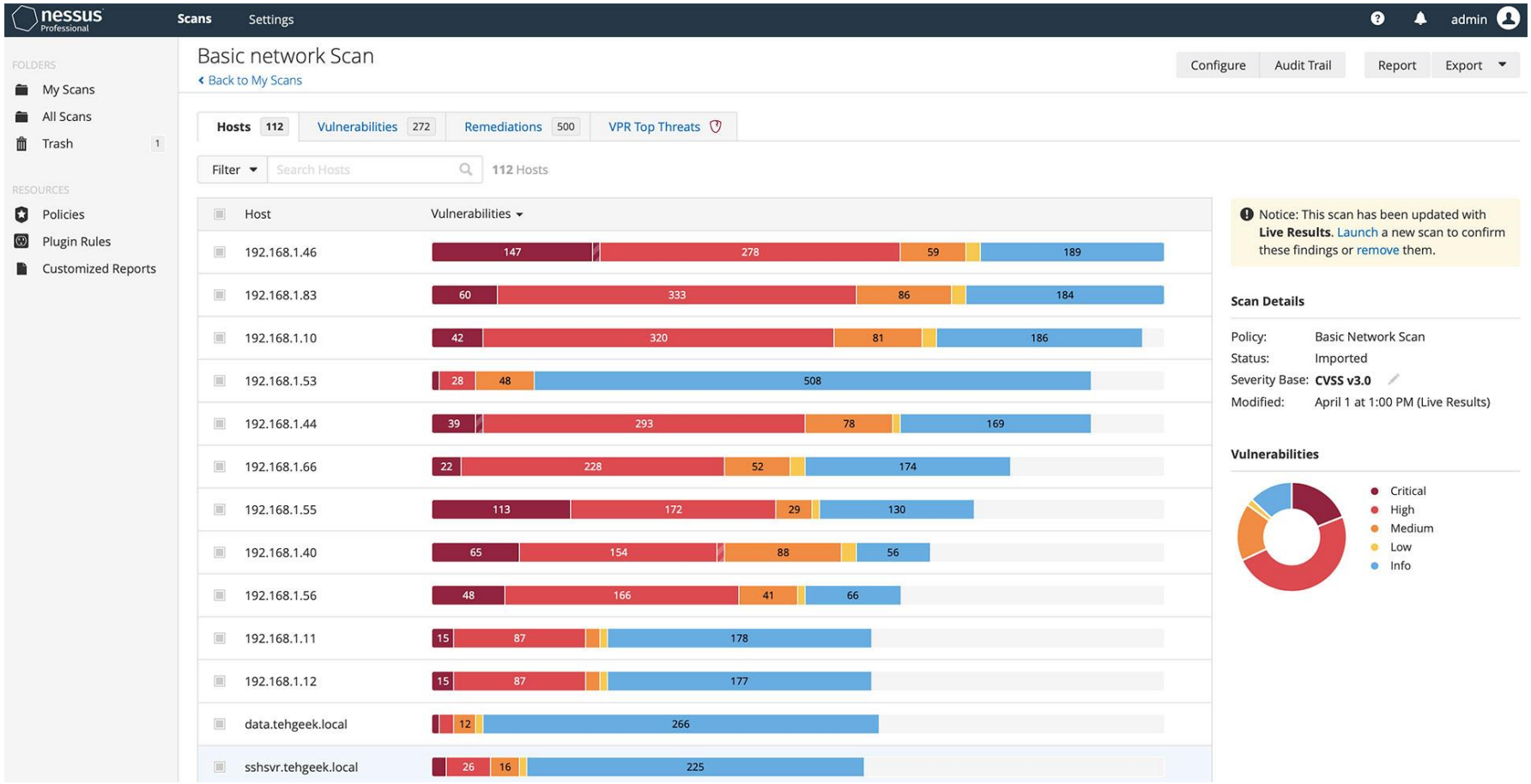
Severity	Plugin Name	Plugin Family	Count
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate with Wrong Hostname	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
INFO	Nessus SYN scanner	Port scanners	7
INFO	Service Detection	Service detection	5

Host Details

IP:	172.16.0.4
MAC:	38:2c:4a:b6:53:d9
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Start:	Today at 7:44 PM
End:	Today at 7:47 PM
Elapsed:	2 minutes
KB:	Download

Vulnerabilities




nessus Professional
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash 1
RESOURCES
Policies
Plugin Rules
Customized Reports
Basic network Scan
Back to My Scans
Configure
Audit Trail
Report
Export
Hosts 112
Vulnerabilities 272
Remediations 500
VPR Top Threats
Filter
Search Hosts
112 Hosts
Host
Vulnerabilities
192.168.1.46 147 278 59 189
192.168.1.83 60 333 86 184
192.168.1.10 42 320 81 186
192.168.1.53 28 48 508
192.168.1.44 39 293 78 169
192.168.1.66 22 228 52 174
192.168.1.55 113 172 29 130
192.168.1.40 65 154 88 56
192.168.1.56 48 166 41 66
192.168.1.11 15 87 178
192.168.1.12 15 87 177
data.tehgeek.local 12 266
sshsvr.tehgeek.local 26 16 225
Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.
Scan Details
Policy: Basic Network Scan
Status: Imported
Severity Base: CVSS v3.0
Modified: April 1 at 1:00 PM (Live Results)
Vulnerabilities
Critical
High
Medium
Low
Info