



Knight Foundation School of Computing and Information Sciences

Knight Foundation
School of Computing
and Information Sciences

Fall 2023 Senior Design Project

Community-Powered Vulnerability Management

Students: Daniel Granados

Mentor: Masoud Sadjadi

Instructor/Faculty: Masoud Sadjadi, Florida International University

PROBLEM

The project addresses the cybersecurity challenge for smaller companies by integrating Greenbone Vulnerability Management (GVM) and custom NASL scripts, providing a cost-effective solution. GVM's open-source approach delivers enterprise-level vulnerability management at a fraction of the cost, while custom NASL scripts enable precise security adjustments. With a focus on scalability, GVM's flexibility ensures seamless adaptation to evolving security needs, offering a future-proof investment for resource-conscious organizations.

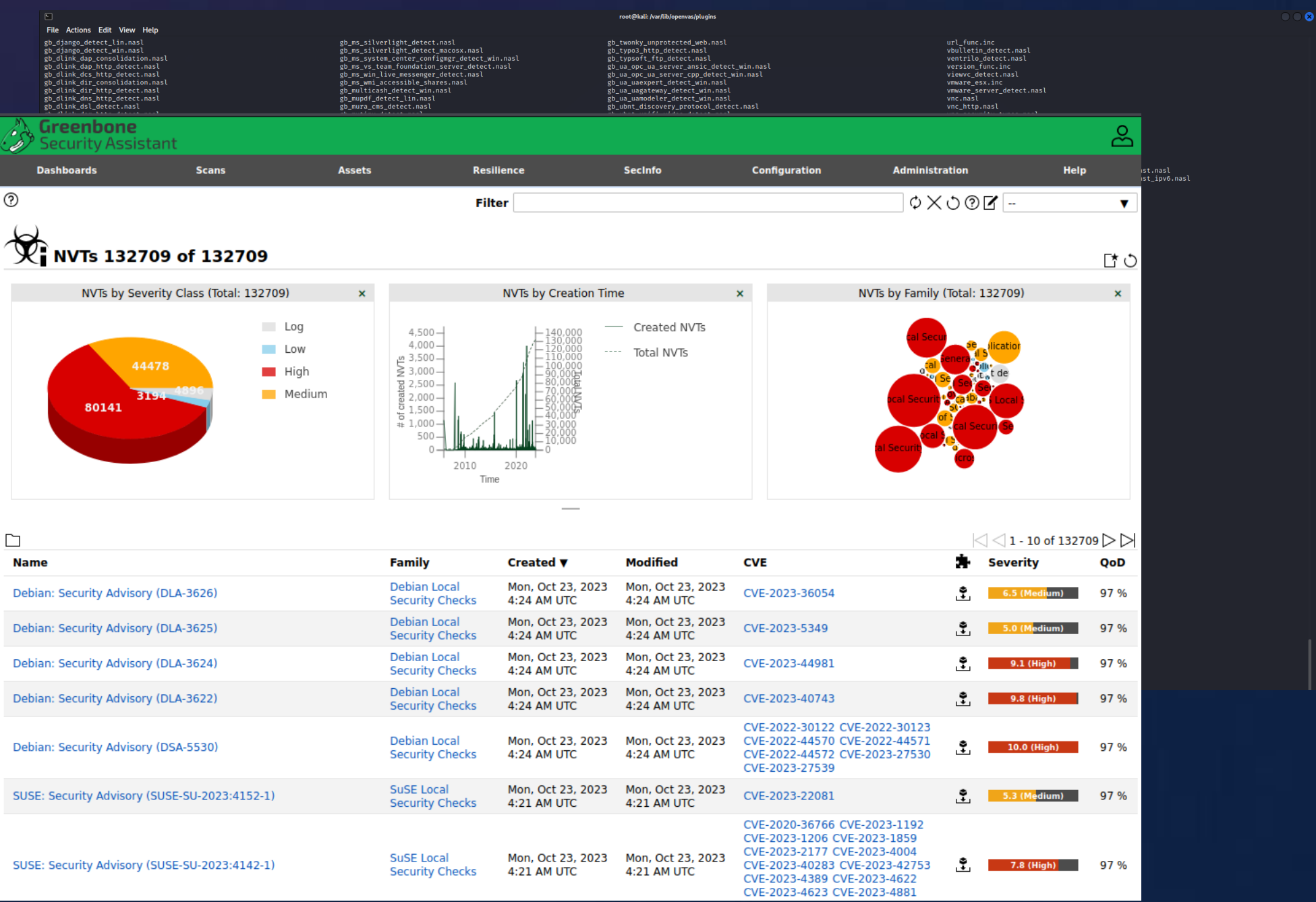
CURRENT SYSTEM

Greenbone Vulnerability Management (GVM) uses Network Vulnerability Tests (NVTs) to actively scan and identify vulnerabilities by cross-referencing data from National Vulnerability Databases (NVDs). It employs Common Platform Enumeration (CPEs) to uniquely identify software, connecting it to Common Vulnerabilities and Exposures (CVEs). This integrated approach enables GVM to conduct efficient vulnerability scans, categorize issues, and prioritize remediation based on CVE severity.

SYSTEM DESIGN

Our system design involves integrating custom Network Vulnerability Tests (NVTs) into Greenbone Vulnerability Management (GVM), addressing specific security challenges within organizations. Through meticulous analysis and development, these NVTs enhance GVM's capabilities by providing targeted assessments for vulnerabilities unique to each organization's infrastructure. The seamless addition of these custom NVTs to the GVM library ensures a continual and tailored approach to comprehensive vulnerability management.

TESTING



Lacking NASL script assistance, we opted for reverse engineering of the GVM NVT library. This not only fulfilled immediate vulnerability testing needs but highlighted the imperative to invest in custom NVT development, especially in the absence of a robust NASL script community

RESULTS

```
1 # Description: Check if Cisco device supports IPv6
2
3 # Initialize plugin
4 if(description)
5 {
6   script_oid("1.1.6.1.4.1.11111111.11111111"); # Replace XXXXXX with the organization's OID
7   script_version("1.0");
8   script_name("Cisco IPv6 Capability Check");
9   script_copyright("Copyright (c) XXXXXX Organization");
10  script_category("ACT_GATHER_INFO");
11  script_family("Cisco"); # Adjust the family to match your target devices
12  script_require_ports("tcp", 22);
13
14  # Description of the plugin
15  script_description("Checks if the Cisco device supports IPv6.");
16  exit(0);
17 }
18
19 # Connect to the target over SSH
20 port = get_port_number(default: 22);
21 if (!get_port_state(port)) exit(0);
22
23 soc = open_ssh_connection();
24 if (!soc) exit(0);
25
26 # Execute a command to check for IPv6 support (adjust the command as needed)
27 cmd = "show ipv6 interface brief";
28 response = ssh_cmd(cmd, soc, soc);
29
30 # Check if the response contains information about IPv6 interfaces
31 if (stristr(response, "IPv6 Address")) {
32   security_message(port: port, data: "The Cisco device supports IPv6.");
33 } else {
34   security_message(port: port, data: "The Cisco device does not appear to support IPv6.");
35 }
36
37 # Close the SSH connection
38 close(soc);
39
```

While successful in scripting a couple NVTs, the integration into the NVT library posed challenges, primarily due to their unique OID and other contributing factors. This obstacle underscores the need for a streamlined process for incorporating custom NVTs into the broader GVM framework.

DEFENSE/SOLUTION

Implementing custom NVTs within the open-source Greenbone Vulnerability Management (GVM) framework provides a cost-effective solution for companies with budget constraints. While requiring a certain level of expertise and experience with NASL scripts, which currently lacks a large development community, this approach enables organizations to avoid the expenses associated with more complex vulnerability scanners. Currently custom NVT development is akin to early programming in the late 20th century, may seem less practical now but holds the promise of long-term benefits for tailored and resource-efficient vulnerability management.

RISK ASSESSMENT

The existing challenge of integrating custom NVTs into the GVM library, owing to unique OIDs and other factors, presents a moderate risk. However, with additional time and investment, these hurdles can be systematically addressed. This ongoing commitment to refinement and enhancement positions the initiative to not only fulfill immediate testing needs but also to potentially become a cornerstone in the broader vulnerability testing community.

SUMMARY

With successfully scripted custom Network Vulnerability Tests (NVTs) within the Greenbone Vulnerability Management (GVM) framework, it enhanced tailored vulnerability assessments. Challenges in integrating these NVTs into the library pose a moderate risk, prompting consideration of alternative open-source software solutions that may offer a simpler integration process. This avenue will be explored further in the ongoing investigation by the project team.

REFERENCES

- Greenbone VT development: <https://forum.greenbone.net/t/vt-development/226/1>
- Registering custom VT: <https://forum.greenbone.net/t/how-do-i-register-my-custom-vt/8864>
- NASL scripting assistance: <http://www.vijaymukhi.com/seccourse/nasl.htm>



Engineering
& Computing

The material presented in this poster is based upon the work supported by Masoud Sadjadi. I thank Masoud Sadjadi for his assistance and mentorship that I received throughout the senior design project.

FLORIDA INTERNATIONAL UNIVERSITY