Penetration Test Report

Genexis Pure E600

Hristo Kolev, Joep Vinken, Lyubomir Georgiev, Yoan-Asen Popov

Table of Contents

[Research Question 2](#_Toc135125925)

[Executive Summary 2](#_Toc135125926)

[Attack Narrative 2](#_Toc135125927)

[Vulnerability scan 2](#_Toc135125928)

[System Discovery 2](#_Toc135125929)

[DDOS 4](#_Toc135125930)

[WIFI cracking 4](#_Toc135125931)

[DOT Framework 4](#_Toc135125932)

[Conclusion 5](#_Toc135125933)

[Recommendation 5](#_Toc135125934)

[Risk Rating 6](#_Toc135125935)

[Risk Rating Scale 6](#_Toc135125936)

[Privilege Escalation through Weak Credentials 6](#_Toc135125937)

# Research Question

What are the potential vulnerabilities in the Genexis Pure E600, router, and how to exploit them?

# Executive Summary

Hristo, Joep, Lyubo and Yoan were contracted by Genexis to conduct a penetration test on Genexis Pure E600 in order to determine its exposure to targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the aforemetioned product with the goals of:

* Identifying if a remote attacker could penetrate Genecis Pure E600’s defenses
* Determinng the impact of a security breach on the available confidentiality

Throughout the tests were conducted with the same level of access as a general user of the system. All activities were performed under controlled conditions.

# Attack Narrative

## Vulnerability scan

The attack was made with the help of automation scripts, called RouterSploit. This tool has a number of exploits for different router models and they have the ability to check whether the remote target is vulnerable before sending off an exploit.

Our test was successful in that we were able to obtain access to the router by exploiting a vulnerability in the system. We discovered that one of the user's credentials was weak, with the username "operator" and password "operator" (see figure 1). We were able to log into the system using SSH from the LAN side, and found that the "operator" user had root acess to the system. This gave us the opportunity to change ant file on the system. With full access, we were able to access sensitive data stored within the router's system, which could have led to serious data breaches if exploited by malicious actors.

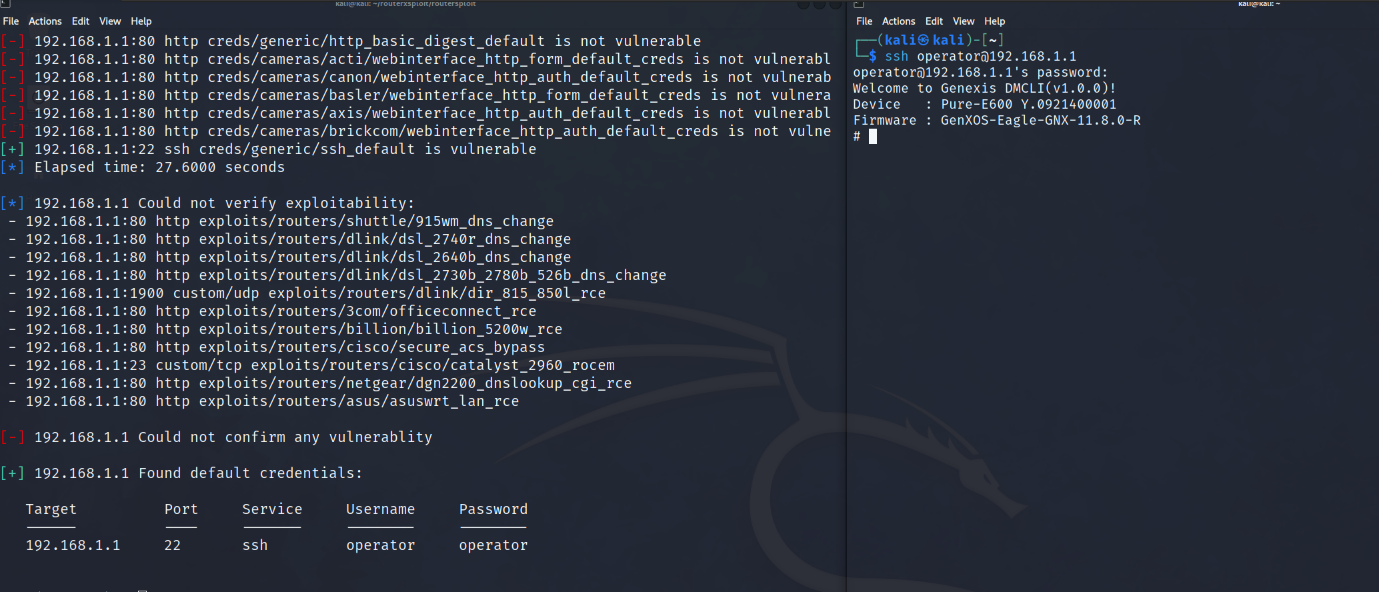
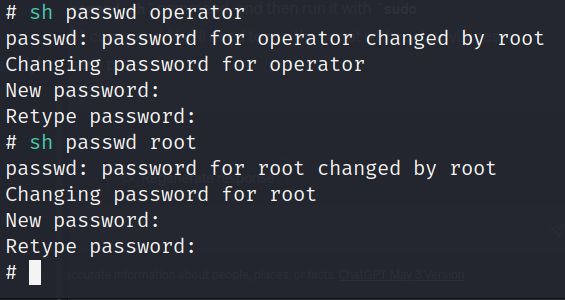
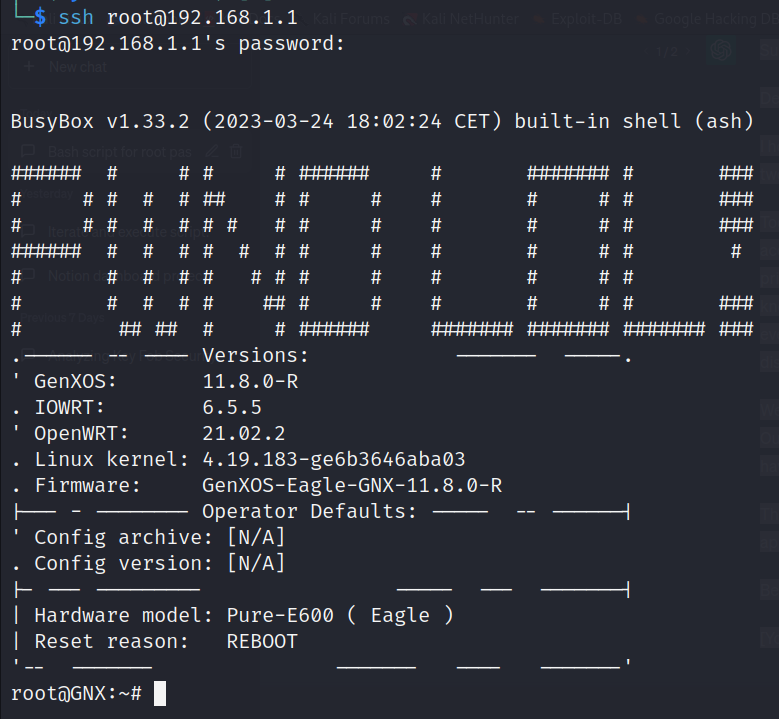
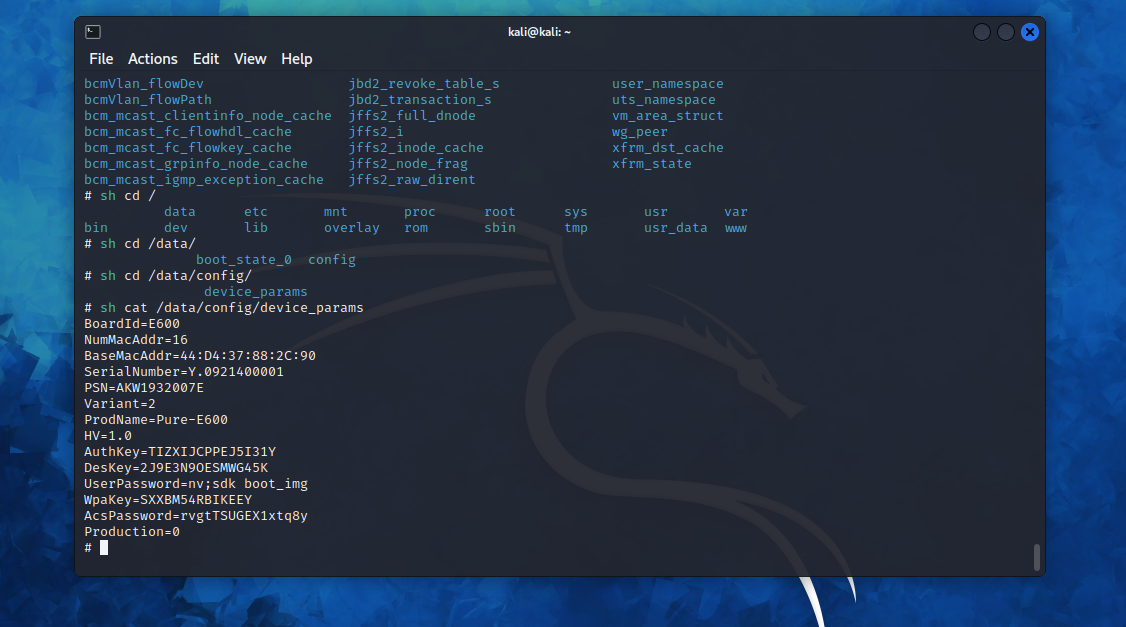


Figure 1 The Operator username and password found (red box)

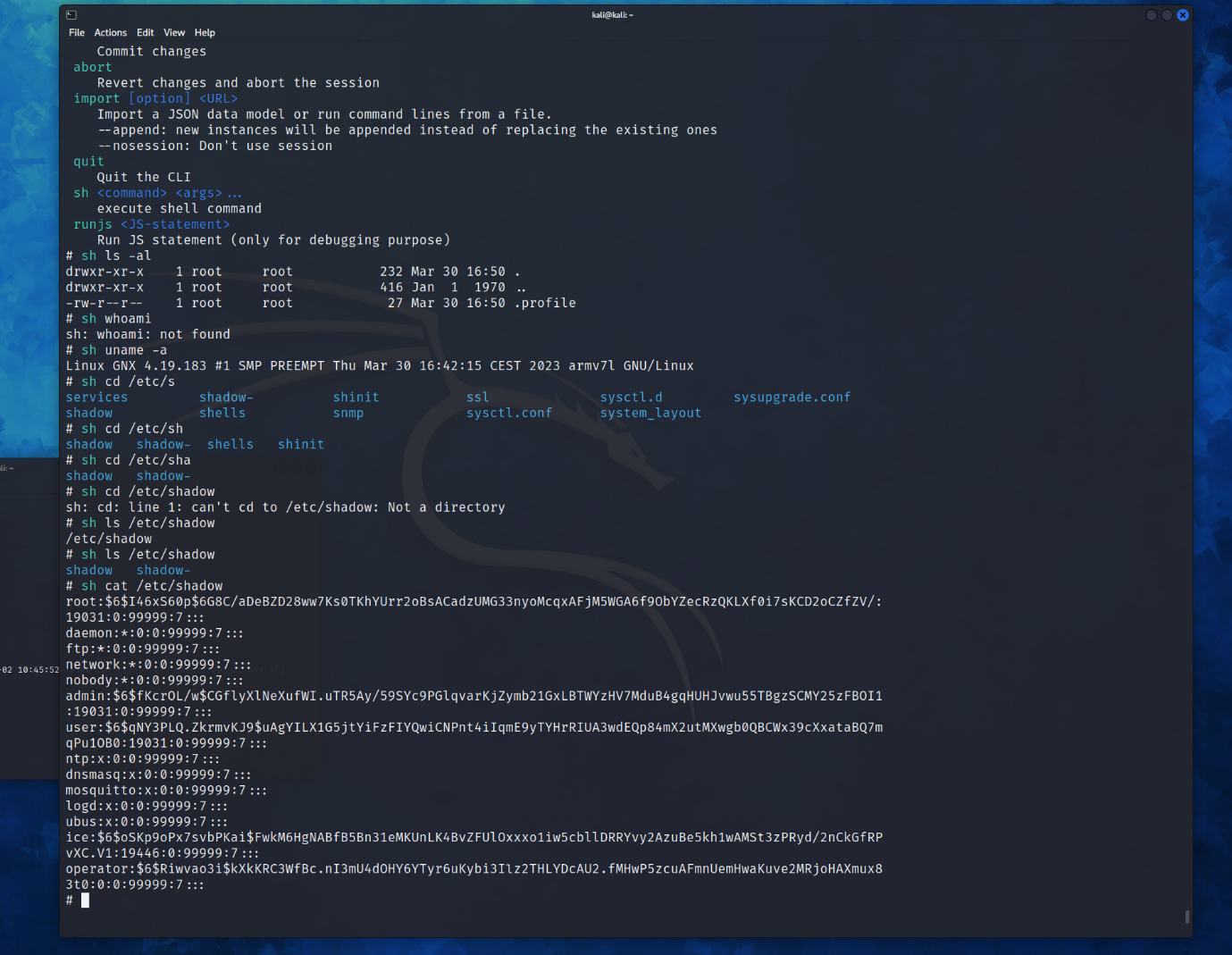


Change Admin password thru the operator account



Passwords and keys we found without having to decrypt

Changed banner thru operator account



The found hashes which are really hard to unhash

## System Discovery

In addition to the SSH login, we also conducted a Nmap scan on the WAN side (figure 2) and the LAN side (figure 3) to identify any potential open ports that could allow an external attacker to gain unauthorized access to the router's system. However, the scan revealed that there were no open ports, which is a positive indication that the router's firewall was configured correctly.



Figure 3 Nmap scan from the WAN (IP == 192.168.68.106)

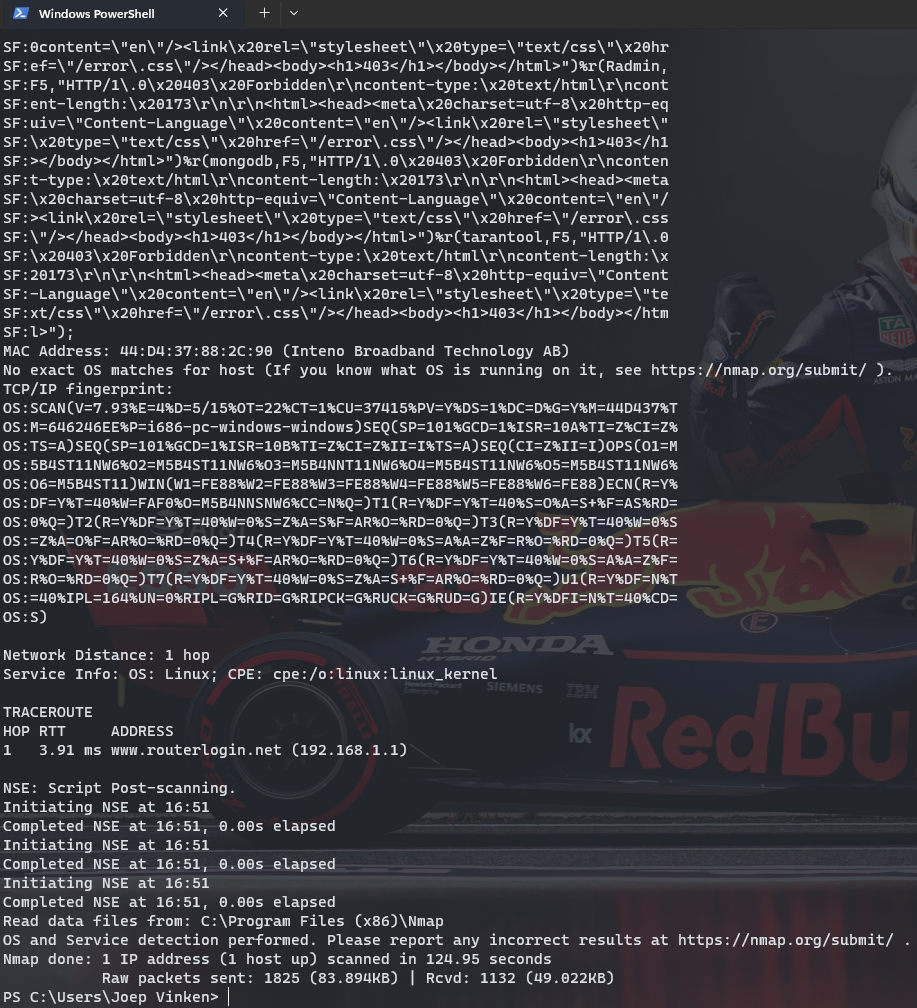


Figure 4 Nmap scan from the LAN (IP == 192.168.1.1)

Nonetheless, this does not guarantee that the router is completely secure as the vulnerabilities that we discovered on the LAN side can still be exploited by attackers within the network. It is therefore important for the router's manufacturer to address these vulnerabilities and ensure that the router's overall security posture is improved.

## DDOS

To conduct this test, we connected to the router's Wi-Fi network using a laptop running the LOIC (Low Orbit Ion Cannon) tool. We then launched a targeted Distributed Denial of Service (DDoS) attack on the router by flooding it with a large number of requests. This attack was designed to overwhelm the router's capacity to process incoming requests and disrupt its normal operation.

During the test, we observed that the router was able to withstand the DDoS attack generated by LOIC. The router remained operational throughout the test, and we did not notice any significant impact on its performance.

## DOT Framework

|  |  |  |  |
| --- | --- | --- | --- |
| Questons | Activity | Strategies | Methods |
| Are there any defaut credentials on Genexis Pure E600? | With the help of an device scanning tool, we scan the router for any possible vulnerabilities | Library, Field, Lab | Literature study, Document analysis, Security Test |
| Are there any vulnerable ports that are open? | We used the Nmap tool for scanning for open ports that can be exploited. | Library, Lab | Literature study, Security Test |
| Is Genexis Pure E600 susceptible to Ddos attacks? | Conducting availability analysis | Library, Lab | Literature study, Security Test |
| Is previladge escalation possible? | We managed to analized the local users on the router. | Library, Lab, Workshop | Literature study, Document analysis, Security Test, Component Test |
| Is it possible to brute force the router's login credentials? | We tried to test the strenght of the login credentials | Library, Lab | Literature study, Security Test |
| Are there any vulnerabilities that can be exploited on the GUI? | We test the GUI with several techniques for data breach | Library, Field | Best,good and bad practices, Literature Study |

# Conclusion

The penetration testing exercise successfully identified critical vulnerabilities within the router's security infrastructure. By exploiting the weak credentials of the "operator" user, we were able to escalate privileges and gain full control over the system. These findings underscore the significance of maintaining strong passwords, promptly patching vulnerabilities, and adhering to security best practices.

It is essential for the router's manufacturer to address the identified vulnerabilities promptly, enhance security measures, and regularly assess the system's security posture through comprehensive penetration testing. By adopting these measures, the router's resilience against potential attacks can be significantly improved, ensuring the protection of sensitive data and network integrity.

# Recommendation

Based on our findings, we strongly recommend the following actions to enhance the security of the router:

1. Vulnerability Patching: The router's manufacturer should promptly address the identified vulnerability to prevent further exploitation. Regular updates and patches should be implemented to mitigate potential risks and enhance overall security.
2. Password Security: All user accounts, especially privileged ones such as "operator" and root, should enforce strong password policies. Users should be encouraged to select complex and unique passwords to mitigate the risk of brute-force attacks.
3. Principle of Least Privilege: Implement a user access control mechanism that strictly adheres to the principle of least privilege. Limiting user privileges to only what is necessary for their designated roles helps reduce the potential impact of compromised accounts.
4. Conduct regular vulnerability assessments. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome.

# Risk Rating

The overall risk identified in the penetration test of the Genexis Pure E600 router is assessed as High. The test revealed a direct pathway from an internal attacker to a full system compromise. It is highly likely that a malicious entity could successfully execute a targeted attack against the Genexis Pure E600 router, posing a significant risk to its security.

## Risk Rating Scale

In accordance with NIST SP 800-30, exploited vulnerabilities are ranked based upon likelihood and impact to determine overall risk.

## Privilege Escalation through Weak Credentials

**Rating:** High

**Description:** An administrative interface is only protected with a weak password.

**Impact:** The impact of a successful Privilege Escalation through Weak Credentials attack can be severe. The attacker gains full administrative control over the router's system, allowing them to manipulate critical configurations, intercept network traffic, and potentially compromise connected devices. With elevated privileges, the attacker can access and exfiltrate sensitive data stored within the router, compromising the confidentiality and integrity of the network. The attacker may disrupt network services, causing downtime and hindering the normal operation of the router and connected devices. Once in control of the router, the attacker can use it as a launching point to perform further attacks on the internal network, compromising additional systems and escalating the overall impact.

**Remediation:** Ensure that all administrative interfaces are protected with complex passwords or passphrases. Avoid use of common or business-related words, which could be found or easily constructed with the help of a dictionary.