CVE - 2020 - 5902

De Silva K.R.K.D

2023/11/04

INTRODUCTION

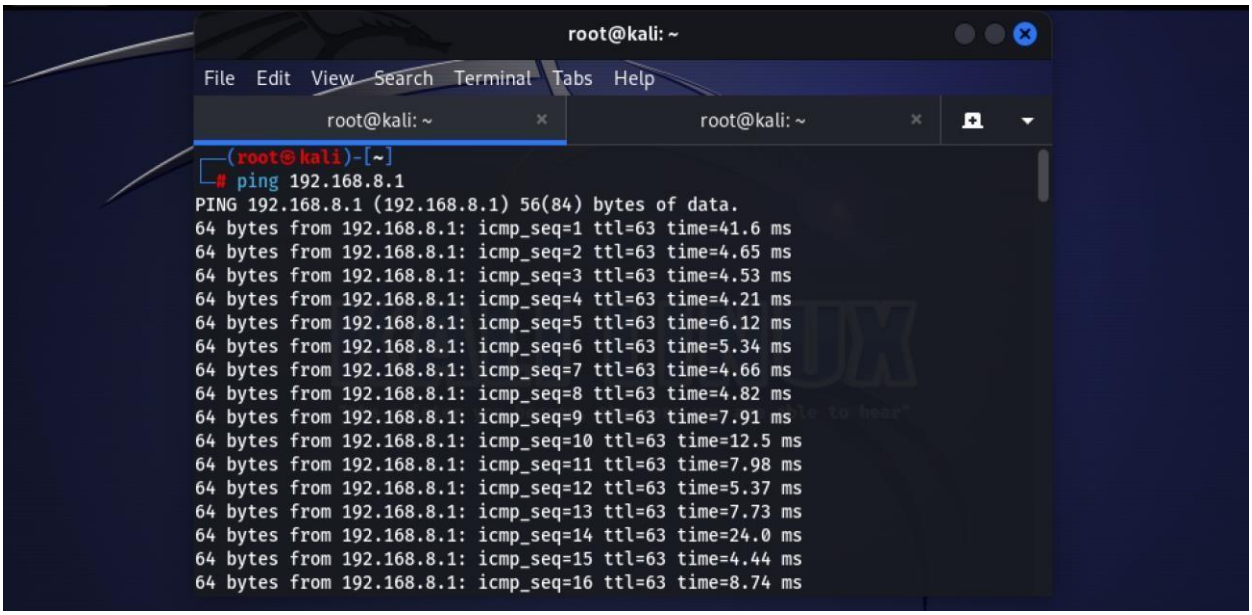
A critical security flaw called CVE-2020-5902 was found in the F5 Network BIG-IP advanced firewall manager(AFM) and BIG-IP application delivery controller(ADC) products. This flaw gives unauthorized users access to the system and the ability for unauthenticated attackers to run arbitrary code on susceptible systems, possibly remotely executing code. This vulnerability, which falls under the category of remote code execution, is caused by an issue with the configuration of the Traffic Management User Interface(TMUI) of the impacted products. A weakness in its implementation could be used by hostile actors to take control of the BIG-IP system, which is managed and configured through this interface.

Because of its critical impact and potential for exploitation, CVE-2020-5902 has drawn a lot of attention from the cybersecurity community. Organizations utilizing the impacted products were advised to install the patches as soon as possible to reduce risk and safeguard their systems. F5 Networks released updates to address this vulnerability.

Table Of Content

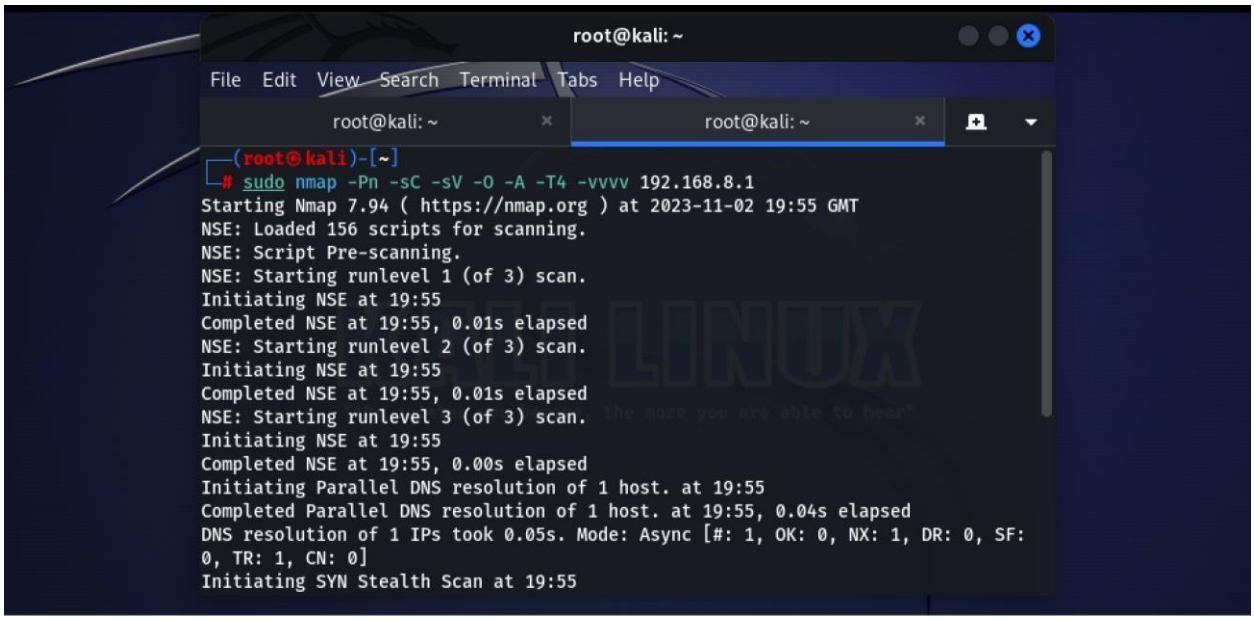
Exploitation Steps

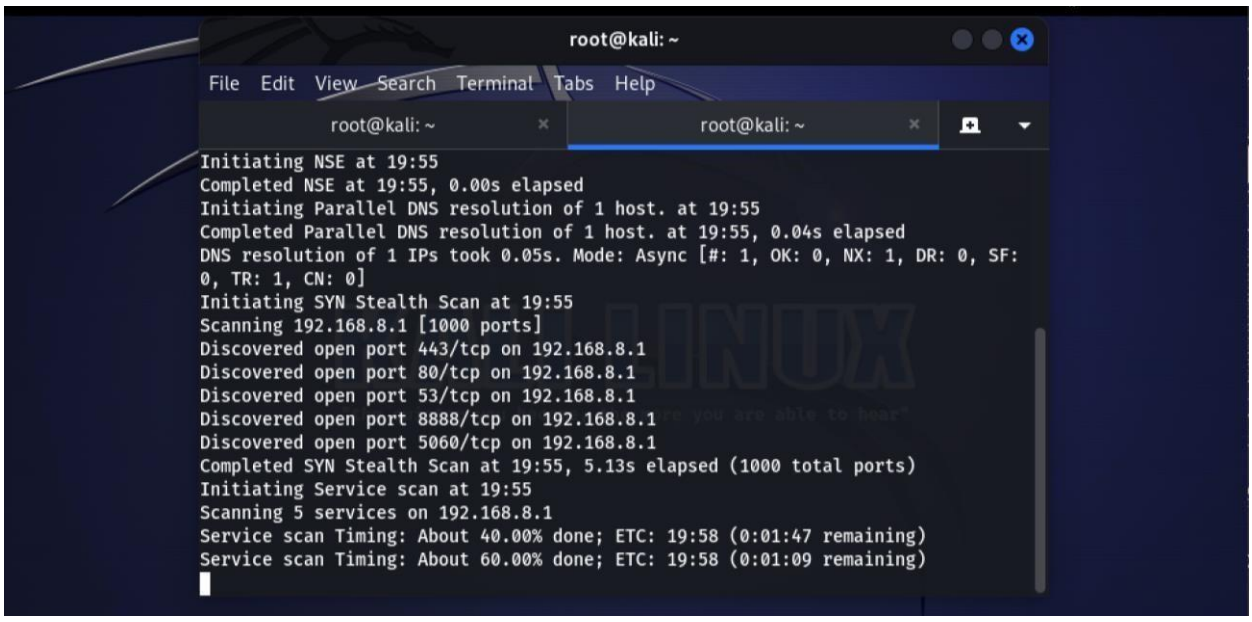
I used an IP address to exploit this vulnerability. First, I used “ping” command. This command is a useful network tool that determines how reachable a host or network device is over an IP network and how long it takes for data packets to travel back and forth from their source. Numerous operating systems, including Linux, Windows, and others, are compatible with it. This tool is commonly used for network diagnostics. It helps to confirm host responsiveness and assess network performance by measuring data packet round-trip times. It functions as a vital tool for network monitoring and troubleshooting.

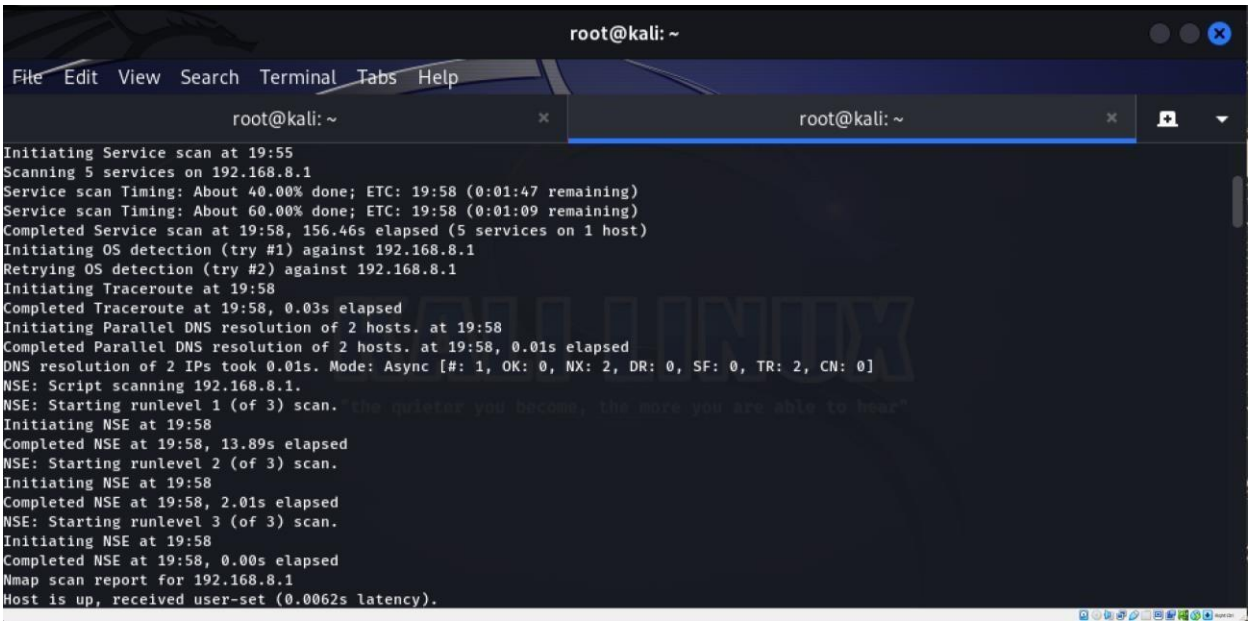


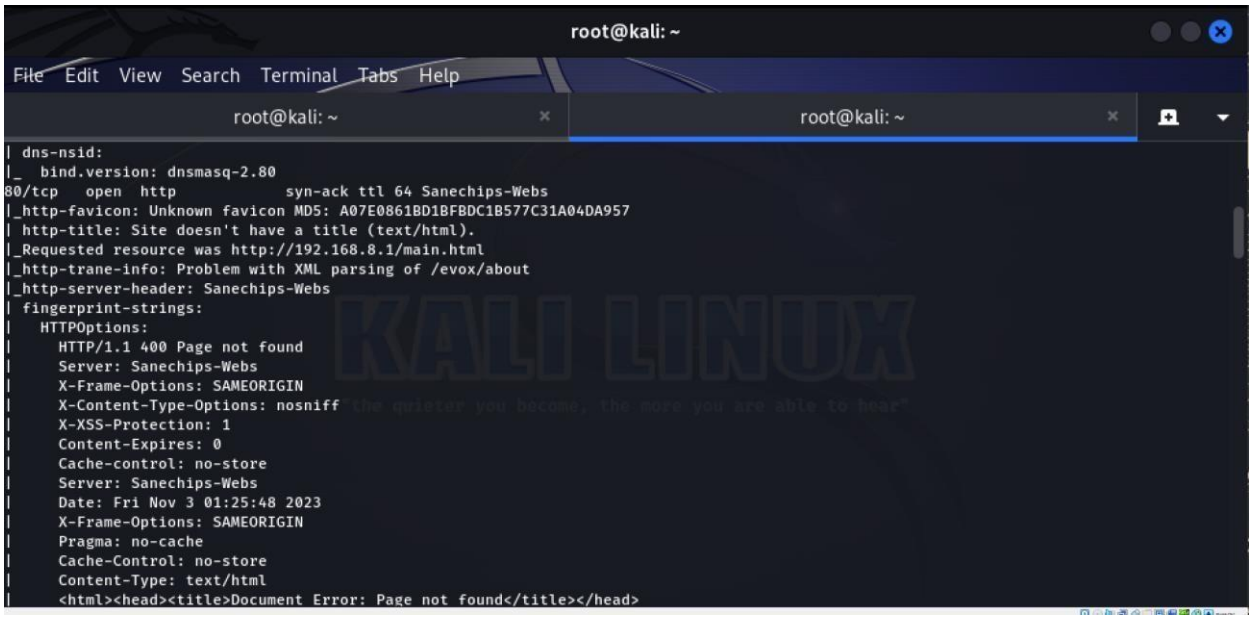
Then, I scanned that IP address using “sudo nmap -Pn -sC -sV -O -A -T4 -vvvv <ip>”. This command executes a comprehensive and aggressive scan of the target host without first confirming the host’s reachability. It wants to determine the operating system, find open ports and services, and run different NSE scripts for more data gathering and vulnerability analysis. Using such aggressive scans

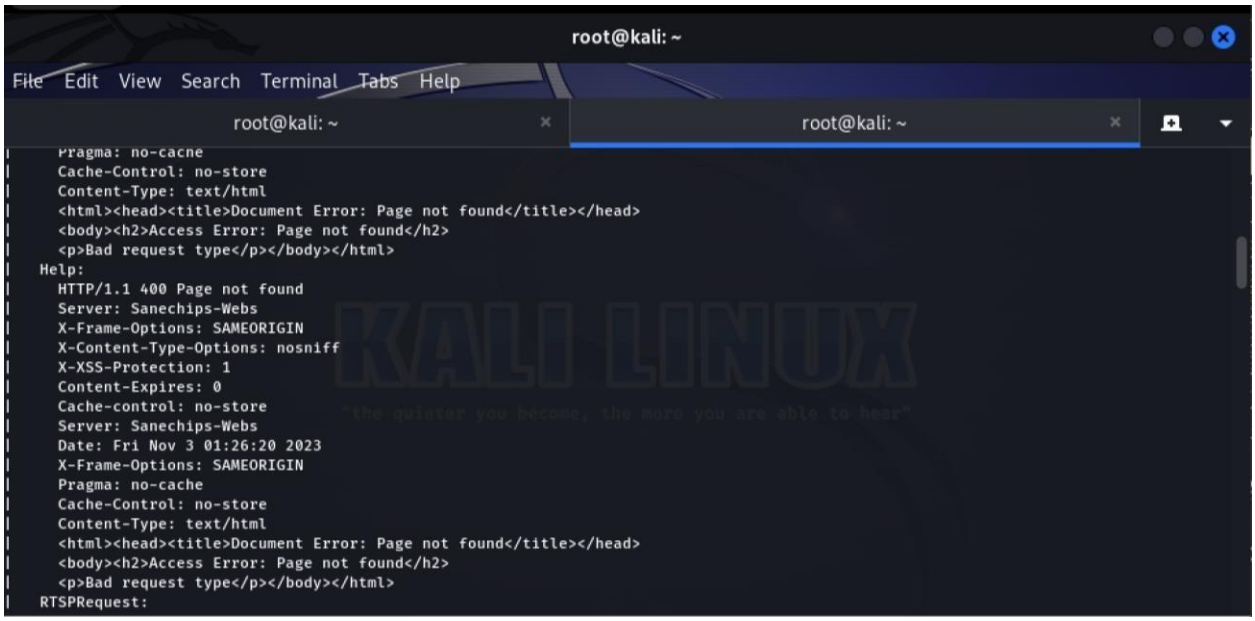
responsibly is essential because they can be more noticeable and generate a significant amount of network traffic. When performing network scans.

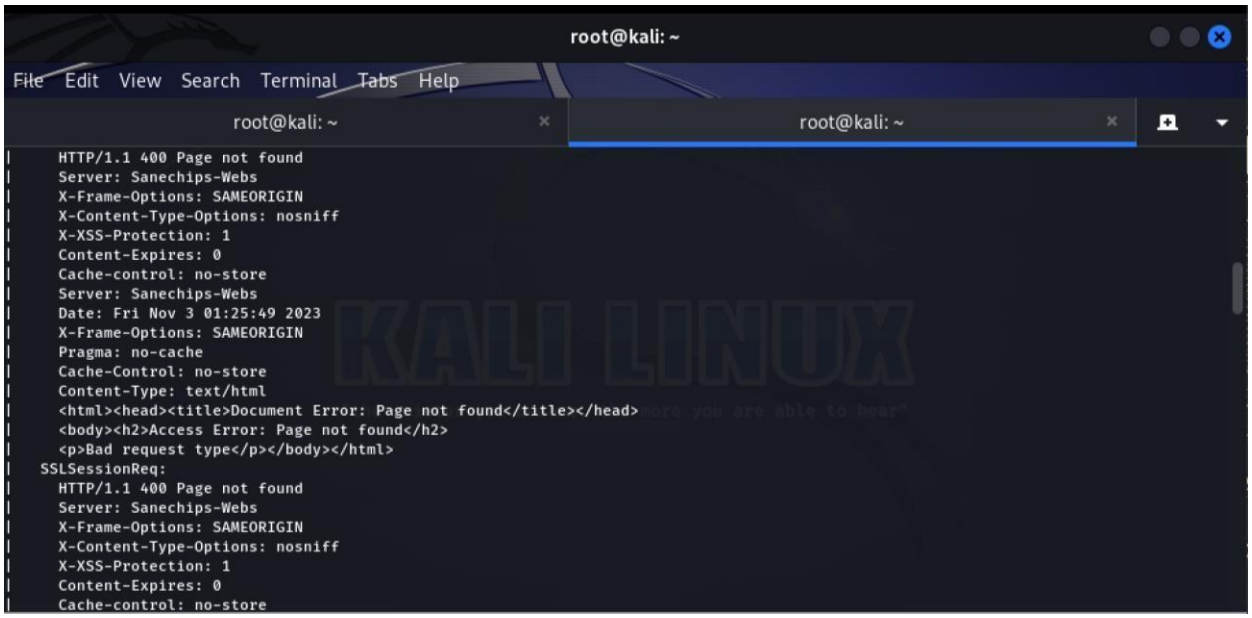


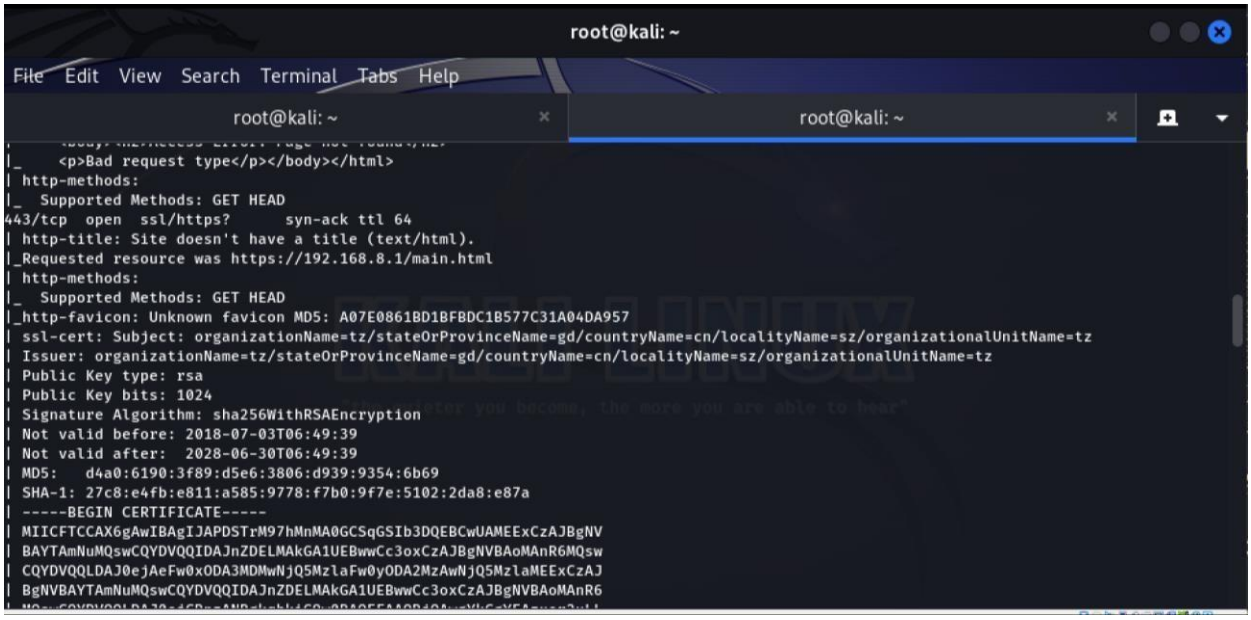


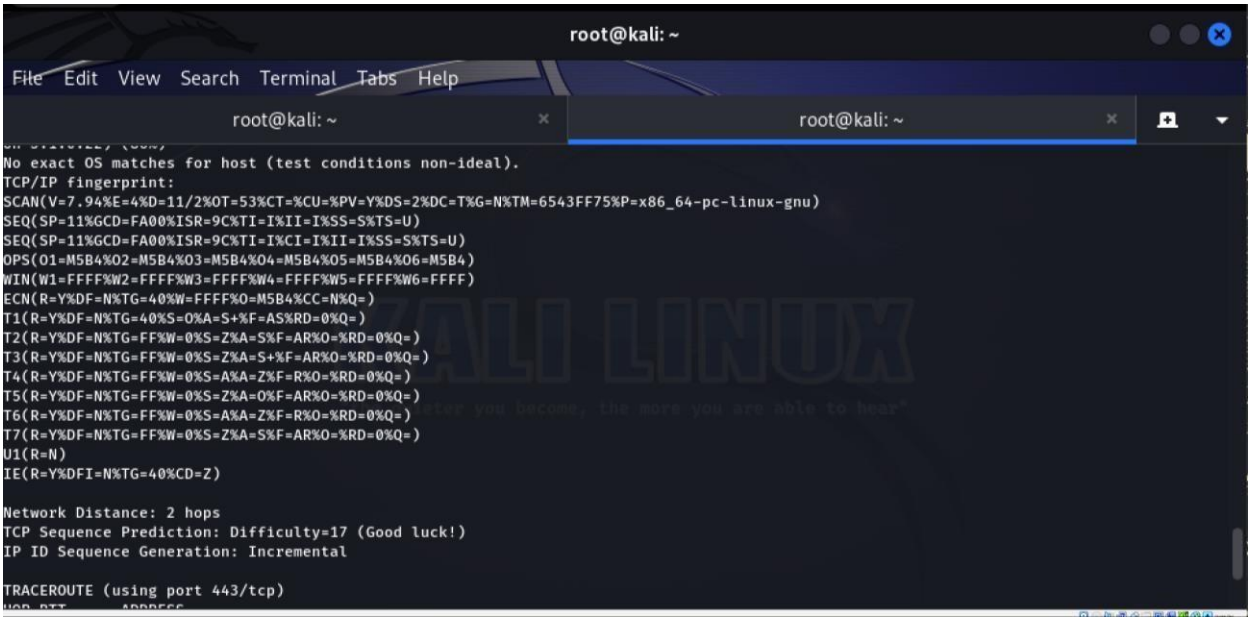

root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
Initiating Service scan at 19:55
Scanning 5 services on 192.168.8.1
Service scan Timing: About 40.00% done; ETC: 19:58 (0:01:47 remaining)
Service scan Timing: About 60.00% done; ETC: 19:58 (0:01:09 remaining)
Completed Service scan at 19:58, 156.46s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 192.168.8.1
Retrying OS detection (try #2) against 192.168.8.1
Initiating Traceroute at 19:58
Completed Traceroute at 19:58, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 19:58
Completed Parallel DNS resolution of 2 hosts. at 19:58, 0.01s elapsed
DNS resolution of 2 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]
NSE: Script scanning 192.168.8.1.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:58
Completed NSE at 19:58, 13.89s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:58
Completed NSE at 19:58, 2.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:58
Completed NSE at 19:58, 0.00s elapsed
Nmap scan report for 192.168.8.1
Host is up, received user-set (0.0062s latency).


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
| dns-nsid:
|_ bind.version: dnsmasq-2.80
80/tcp open http syn-ack ttl 64 Sanechips-Webs
|_http-favicon: Unknown favicon MD5: A07E0861BD1BFBDC1B577C31A04DA957
| http-title: Site doesn't have a title (text/html).
|_Requested resource was http://192.168.8.1/main.html
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: Sanechips-Webs
| fingerprint-strings:
| HTTPOptions:
| HTTP/1.1 400 Page not found
| Server: Sanechips-Webs
| X-Frame-Options: SAMEORIGIN
| X-Content-Type-Options: nosniff
| X-XSS-Protection: 1
| Content-Expires: 0
| Cache-control: no-store
| Server: Sanechips-Webs
| Date: Fri Nov 3 01:25:48 2023
| X-Frame-Options: SAMEORIGIN
| Pragma: no-cache
| Cache-Control: no-store
| Content-Type: text/html
| <html><head><title>Document Error: Page not found</title></head>


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
Pragma: no-cache
Cache-Control: no-store
Content-Type: text/html
<html><head><title>Document Error: Page not found</title></head>
<body><h2>Access Error: Page not found</h2>
Bad request type </body></html>
Help:
HTTP/1.1 400 Page not found
Server: Sanechips-Webs
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Expires: 0
Cache-control: no-store
Server: Sanechips-Webs
Date: Fri Nov 3 01:26:20 2023
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Content-Type: text/html
<html><head><title>Document Error: Page not found</title></head>
<body><h2>Access Error: Page not found</h2>
Bad request type </body></html>
RTSPRequest:


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
HTTP/1.1 400 Page not found
Server: Sanechips-Webs
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Expires: 0
Cache-control: no-store
Server: Sanechips-Webs
Date: Fri Nov 3 01:25:49 2023
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
Cache-Control: no-store
Content-Type: text/html
<html><head><title>Document Error: Page not found</title></head>
<body><h2>Access Error: Page not found</h2>
Bad request type </body></html>
SSLSessionReq:
HTTP/1.1 400 Page not found
Server: Sanechips-Webs
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Content-Expires: 0
Cache-control: no-store





As a result, I got this IP's ports and attempted to detect the OS and run various NSE scripts.

How to mitigate

- Install a fixed software version.
- By limiting access to all TMUI interfaces and utilizing the mitigation procedures listed below for self Ips and the management interface, the risk can be reduced. [1]

CONCLUSION

In conclusion, F5 Networks' BIG-IP and advanced firewall manager products are susceptible to a critical vulnerability known as CVE-2020-5902. Network security is seriously threatened by this vulnerability, which could enable unauthorized attackers to run arbitrary code on impacted systems. The vulnerability can allow malevolent actors to access susceptible systems and insert malicious code, even when MFA is enabled. Even though more recent FortiGate versions may reject some requests, the potential consequences of this vulnerability make it a serious worry. Patching and mitigating this security risk immediately is essential to securing vulnerable systems.

References

[1] "MyF5 (TMUI RCE vulnerability CVE-2020-5902)," 1 July 2020. [Online]. Available: https://my.f5.com/manage/s/article/K52145254.