Phishing Simulation

Objective

Capture real user credentials through social engineering.

Tools

Gophish, Evilginx2

Evilginx2 Setup

sudo evilginx
phishlets enable google
phishlets hostname google login.<yourdomain>.com

Gophish Campaign

- Email template: “Password Expiration Notice”
- Target: Windows Test VM user
- Tracking enabled

Captured Log

Timestamp	Victim IP	Email	Username	Password	MFA token?	Notes
22:000x	192.168.84.138	test@local	testuser	pass123	Bypassed	Successful Stealth Borrow

Impact

✔ Phishing bypassed MFA token
✔ Attacker can log in as real user silently
✔ Live session hijacking possible

Summary

The phishing scenario proved how employees remain the weakest link in cybersecurity. The cloned login page looked identical to the real one, tricking the user into entering credentials. Evilginx2 captured session cookies allowing seamless access to the victim account. This demonstrates a critical need for improved email filtering and continuous phishing-awareness training among employees.

```
┌──(cybercheems㉿kali)-[~]
└─$ file gophish

gophish: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-
64.so.2, BuildID[sha1]=35cb0bc09b788298e8fa46e92548f71a252a347a, for GNU/Linux 3.2.0, not stripped

┌──(cybercheems㉿kali)-[~]
└─$ mkdir gophish_lab
mv gophish gophish_lab/
mv static gophish_lab/ 2>/dev/null
mv templates gophish_lab/ 2>/dev/null
mv config.json gophish_lab/ 2>/dev/null


┌──(cybercheems㉿kali)-[~]
└─$ cd gophish_lab
ls

config.json  gophish  static  templates

┌──(cybercheems㉿kali)-[~/gophish_lab]
└─$
```