Phishing cybersecurity students

Authors: Martin Řepa, Lukáš Forst

Phishing has been recently the most efficient attack. It exploits human naivity and none vigilance - attack vector which is actually very hard to defend. In the following text, we describe how we managed to phish passwords of cyber-security students.

Introduction

During practices within subject Introduction to Computer Security we were split into two-man teams to play the Capture The Flag challenge and practise techniques we learnt. Each team owned one virtual machine in a virtual network. Everything was allowed - except the (D)DOS attacks.

First hack (change subttitle)

Our first task was to use nmap to discover secret services on secret machines within our virtual network and lastly find the token. Many jokes and baits were setup to confuse our search. One service for example offered following link https://bit.ly/take-your-token.

After we found our token, we got an idea to make our own service to confuse our school mates. Firstly, we launched simple python http server, which was just replying following text:

```
> The ip 192.168.1.150 might be useful :P
```

Of course this ip was not useful at all. Yeah, now to me it seems unnecessarily mean as well. Nonetheless, we thought we could do much more.

1st version

We created simple TCP service asking for passwords. By asking for passwords we mean asking for passwords - nothing sophisticated. See figure below.

// TODO add below figure of our first service

To be honest, we did not expect stealing any password. It was just for fun, however, in about an hour we saw first attemps in our logs.

2nd version

Describe 2nd version

3rd version

Describe 3rd version

Summary

Second hack (change subttitle)

Intro

What, where, technology, why

Result

how it actually went

Conclusion

Sum this up. What we learnt and gained, what we shall memorize

Appendix

links to github etc.