

## APPROACH ON INCREASING USER SECURITY AWARENESS

Romana OANCEA, Ghiță BÂRSAN, Luminița GIURGIU

\*“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania

oancea.romana@gmail.com, ghbarsan@gmail.com, luminita.giurgiu.a@gmail.com

**Abstract:** *Currently, social engineering attacks are increasingly sophisticated and the main factor that can influence the success of these techniques is the employee. Awareness of these types of attacks through permanent information sessions can be a good practice for any organization. In this work, besides the approach to the development of eLearning content accessible to employees, there are presented some methods and tools that can be used to avoid the theft of sensitive information or the infection of hosts on the network.*

**Keywords:** social engineering, weaponization, email phishing, attached files

### 1. Introduction

Currently, the main threats to data security are social engineering and implicitly uninitiated employees and/or users. In addition, opportunities to connect to the organization's network with various mobile devices or PCs can introduce security breaches. The most vulnerable link in the technology-human-data chain is man. Most cyber-attacks exploit the vulnerability of users and only some of them exploit the technical flaw. In many situations, systems are compromised only by users [1]. The development of a human firewall is difficult. On the one hand, social engineering techniques and attack methods are more ingenious, and on the other hand awareness sessions for employees may not be sufficient and always appropriate. Most users think they are protected and their negligence cannot break into the network. Controlling a device can lead to activity monitoring, by default to credentials theft or to new security threats.

Using the same credentials for multiple accounts, connecting to the internal network of different types of devices using either wired or wireless connection, using outdated software, or disabling firewalls and antivirus applications - especially on personal devices -, involuntary disclosure of sensitive information to unauthorized people are just a few common practices at the employee level. They are fully exploited by hackers. Speculating user weaknesses can gain access to sensitive, credential data or malware downloads. A device infected with a malware and then connected to the network can lead to infection of other hosts without human intervention.

Awareness-raising, to be effective both for the employer and the employee, is often conducted in the on-line environment by developing content and structuring them appropriately in a content management system. There are many approaches in literature to develop content that meets the needs of learners, regardless of their previous level of knowledge.

Building an adaptive path that fits the

background of each individual is challenging in both e-learning and m-learning or microlearning [2]. Many MOOC platforms have developed courses for end user awareness [3-5], but in general employees think they are cautious enough, the data and information they hold is not sensitive, or even more, that they cannot be the target of any attack.

## 2. Methods and tools

### 2.1. The methodology used

For users to be constantly informed about new approaches to phishing attacks, eLearning content has been developed. On the eLearning platform of the academy were created content objects describing the following: social engineering attacks, examples of actual attacks, the ways of preventing, analysing the damage and analysing the measures that should be taken to avoid phishing, pretexting, baiting or any type of attack involving the human factor (fig. 1). Vulnerability exploitation methods used by hackers that all employees need to be aware of have been structured in short bit-size pieces with a length of between 3 and 15 minutes. Microlearning modules or bit-sized pieces increase attention and retention for learners [6]. After each section, the learner goes through a series of quizzes to fix knowledge, but also to test attention and the level of retention [7]. However, the major concern is that after a certain period of time employees relax and can again neglect security issues. In this sense, it was intended that, in addition to classical content and quizzes, various types of social engineering attacks should be “simulated”, attacks that can be done through infected links and attachments sent via emails. These attacks will be tested at certain time intervals on a random number of users to track whether security policies are complied with, and devices with which users connect to the local network comply with the necessary protection requirements.

## 2.2 Instruments and approaches. Simulation of attacks

Lately, software for the exploitation of computer or network security has increased in popularity and many people, for inadequate reasons, can use Kali Linux and Metasploitable to exploit different software vulnerabilities [8].

Due to the low interest in the content projected over a period of time, a similar approach to a hacker was simulated, so that in order to infect a target with the purpose of a possible benefit, the following steps are followed: information gathering, intrusion, lateral movement, privilege escalation, move laterally, collect and exploit, affect and report [9], [10]. The article will only track the steps of collecting information and how to mount attacks through email attachments, so that impact analysis and victim awareness will be monitored over a longer period of time in order to be eloquent.



Figure 1. eLearning objects Information gathering

At the information gathering stage, it was attempted to identify email addresses for university users, students who need to go online. Although on the platform the login is based on an account and password, and for each user an email address is known, this information has been disregarded and a simulation of a hacker behaviour has been attempted. Emails were identified by analysing the information displayed on the site and using dedicated Kali Linux or Web search tools, and the collected information was saved in a file; later on, all emails were

sent from a fake email address without using the Kali Linux SET-social-Engineering Toolkit and Metasploit tools specifically designed for attacks against the human.

Initially, to identify email addresses other than those found on the site, *the harvester* Kali Linux's tool was used, a passive recognition tool (fig.2) [11].

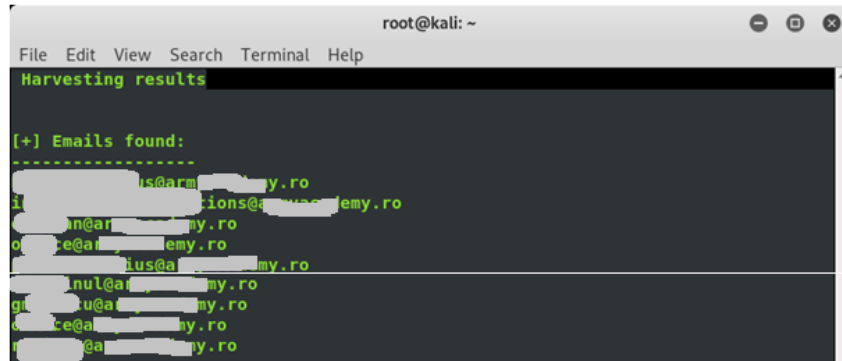


Figure 2. Sample of some detected emails using the harvester Kali Linux's tools

In order to have a consistent database containing employees' email addresses, the information on the institution's site was analysed and various search engines [12] or social sites were used to identify themselves and other emails. The database is used to send emails randomly with infected attachments or links to determine user alertness, vulnerabilities, and potential security risks.

#### Weaponization

During the information gathering phase, users' concerns have also been identified, which will be used to build emails as credible and of interest to most users.

Metasploit from Kali Linux allows you to inject various payloads into Ms Word, .pdf files, and more, files that can later be attached to emails. Spear-phishing or spam campaigns use, as the main ingredient, weaponized documents, in order to trick victims into open attached files and, after that, to steal the credential that can be used later for backdoor or new vulnerability.

Starting from the interest of employees for scientific research, a .pdf template (fig.3) was used to which malicious code was injected using the Kali Linux Metasploit (fig.4). The generated file can only affect the host if it can be opened on a computer.

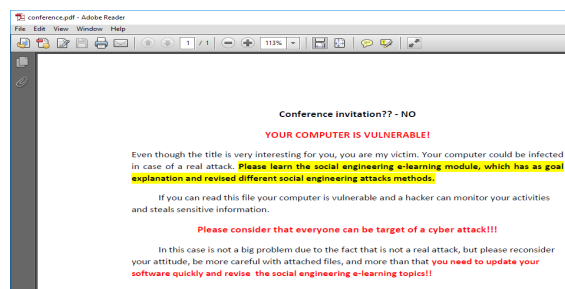
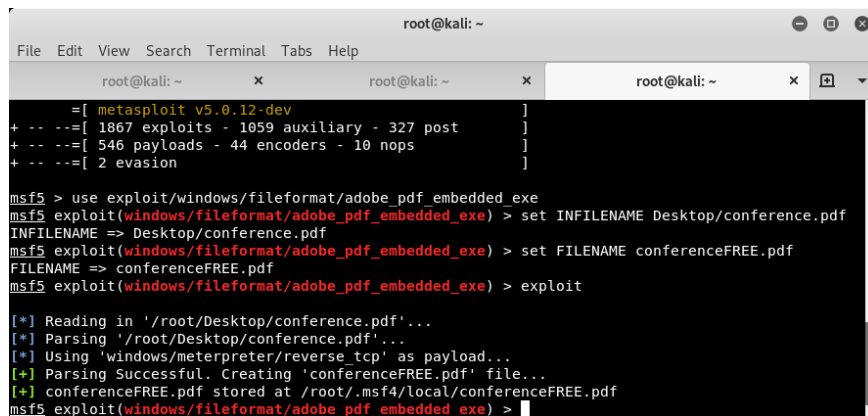


Figure 3. Template used by the payload



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x  
=[ metasploit v5.0.12-dev ]  
+ -- --=[ 1867 exploits - 1059 auxiliary - 327 post ]  
+ -- --=[ 546 payloads - 44 encoders - 10 nops ]  
+ -- --=[ 2 evasion ]  
msf5 > use exploit/windows/fileformat/adobe_pdf_embedded_exe  
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME Desktop/conference.pdf  
INFILENAME => Desktop/conference.pdf  
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME conferenceFREE.pdf  
FILENAME => conferenceFREE.pdf  
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit  
[*] Reading in '/root/Desktop/conference.pdf'...  
[*] Parsing '/root/Desktop/conference.pdf'...  
[*] Using 'windows/meterpreter/reverse_tcp' as payload...  
[+] Parsing Successful. Creating 'conferenceFREE.pdf' file...  
[+] conferenceFREE.pdf stored at /root/.msf4/local/conferenceFREE.pdf  
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Figure 4. Exploit - embedded Adobe pdf file

Vulnerability of pdf files is not necessarily recent, but there are several types of files that can be armed and attached to emails - word files, excel or so on, or even files containing images. Opening files on a host device can cause tangible and intangible damage.

#### Exploitation

In the exploitation phase, emails will be sent at certain time intervals, which will have as attachments generated files. Emails will be sent to users randomly, in order to keep employees vigilant.

Even if these types of exploitation are not very new, they are still very useful in security awareness and there are still used in different purposes.

#### 2.3. Discussions

Kali Linux tools have allowed malicious code attachment for different file types, files that are attached to an email. The user's opening can introduce new vulnerabilities that allow later exploitation of independent devices connected to the network or even the network. Following the simulations made it is possible to highlight and discuss the following issues. First - sending emails to different target addresses can be done using the Kali Linux tool. Although emails have been sent to a small number of users, an email vulnerability has been determined, a vulnerability that can be addressed by implementing additional filters. Instead, for some email addresses hosted on public servers, emails that had infected attachments were not received.

Second - an attached pdf file cannot be opened if the Acrobat Reader version is updated and the user is also alerted about a possible infected file. However, if the version of Acrobat Reader is not updated and the user has not installed the packs to fix the vulnerability, the file can be read without any problems, but the host will be infected when it is opened.

#### 3. Conclusions

In most situations, classical employee awareness sessions on cyber security are not enough, because social engineering attacks are growing in popularity. In order to minimize security risks at the organization level and starting from the idea of e-learning by doing or leaning by experience, emails that contain links or malicious code will be generated periodically to be sent to the addresses in the created database.

Even if for some vulnerabilities of operating systems or applications proper packs have already been developed, it is known that many users do not update their software, especially for their own devices. Additionally, it is common practice for local firewall and antivirus to be blocked if users connected to the network have more rights than needed or want to install certain applications in a shorter time. Moreover, the use of unlicensed software or for which packs are no longer developed is still a much-accepted practice.

It is very important that email links that claim to be very urgent are never accessed and that not any http link should be opened. Because the employee awareness process needs to be a permanent one, further

development will evaluate their behaviour and vigilance by sending emails with attachments or “dubious” links at various time intervals.

### References

- [1] Ian Mann, *Hacking the Human. Social Engineering techniques and Security Countermeasures*, Gower, 2018, ISBN 978-0-566-08773-8.
- [2] Samir E. Hamada, Khaled Elleithy, Ioana Badara, Saeid Moslehpour, *Automated Adaptive Mobile Learning System using Shortest Path Algorithm and Learning Style*, in International Journal : Interactive Mobile Technologie, iJIM – Vol. 12, No. 5, 2018, pp. 4-27, ISSN: 1865-7923.
- [3] <https://www.cybrary.it/course/end-user-security-awareness-1-hour/>
- [4] <https://www.eset.com/us/cybertraining/>
- [5] <https://training.advisera.com/awareness-session/security-awareness-training/>
- [6] David Winograd, *Ways Microlearning increases attention and retention*, eLearning Industry, <https://elearningindustry.com/microlearning-increases-attention-retention-ways>, accessed on march 2019.
- [7] Debadrita Sengupta, *5 Ways you can use microlearning in corporate training*, eLearning Industry, <http://cblpro.com/blog/2019/02/25/5-ways-you-can-use-micro-learning-in-corporate-training/>, accessed on 15 February 2019.
- [8] Duffany J.L., *Computer Security*, in Computer and Network Security Essentials, Springer, 2017, ISBN 978-3-319-58423-2, pp. 3- 20.
- [9] Raphaël Hertzog, Jim O’Gorman, and Mati Aharoni, *Kali Linux Revealed. Mastering the Penetration Testing Distribution*, Offsec Press, 2017, ISBN 978-0-9976156-0-9.
- [10] Department of Defence, *Cybersecurity Test and Evaluation Guidebook*, Version 2, April 2018.
- [11] Beggs, Robert W. *Mastering Kali Linux for advanced penetration testing*, Packt Publishing Ltd, 2014, ISBN 978-1782163121.
- [12] Oriyano Sean-Philip, Solomon Michael G., *Hacker Techniques, Tools, and incident Handling*, 3rd Edition, Information Systems Security and Assurance Series (ISSA), Jones & Bartlett Learning, 2018, ISBN 978-1284147803.