# Penetration testing of devices

Z. Terneva, S. Dimitrova
Department of Communication Networks, Faculty of Telecommunications, Technical University of Sofia
8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria
Department of Industrial buildings, Faculty of ArchitectureUniversity of Architecture, Civil Engineering and Geodesy (UACEG)
1 Hristo Smirnenski Blvd., 1164 Sofia, Bulgaria
zterneva@tu-sofia.bg, sdimitrova_far@uacg.bg

*Abstract* – **This paper will examine the common problem of hacking smart devices, user's passwords and related methods to counter hackers. Security testing has become part of our daily lives, although the average user does not notice it. The report will discuss how useful ethical hacking is and why it is necessary to protect user data. The basic strategies for protection against cyber-attacks of black hat hackers will be presented and it will be shown why ethical hacking is important. The authors will point out the reasons why it is important that our devices do not remain unprotected. In the paper, the authors will show with an example how important password complexity is.**

*Keywords* – **cyberattacks, hackers, security, device, IoT (Internet of things), penetration testing**

## I. Introduction

Hacker attacks on smart devices are becoming an increasingly common problem. People need to be very careful with the information they have on their devices and how they store it. Ordinary users use different security options - applications that remember their passwords and keep them; antivirus 'firewalls', etc. But nowadays this is not enough to protect our personal information from an alleged attack.
Penetration testing is a type of attack simulation to verify the security of a system or environment that needs to be analyzed. This test can be performed through hardware attacks or through software attacks. The purpose of this test is to examine in extreme circumstances the behavior of systems, networks or personal devices. In this way, their weaknesses and vulnerabilities can be identified. [1] There is a variety of tools for this purpose. Some tools simply analyze and scan the software / system, while others attack the system and look for its vulnerabilities.

It is important to note that penetration testing is performed by security professionals. They are also called hackers with white hats or ethical hackers. They receive permission from the owner of the device or system to perform the necessary testing. These hackers or specialists are not intended to cause harm. They detect vulnerabilities in the system and devise strategies to address them so that malicious hackers do not exploit these vulnerabilities. Ethical hackers also use the same methods and tools as hackers in black or gray hats, but their actions are well-intentioned.

Technical University of Sofia
8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria
zterneva@tu-sofia.bg
University of Architecture, Civil Engineering and Geodesy
1 Hristo Smirnenski Blvd., 1164 Sofia, Bulgaria
sdimitrova_far@uacg.bg

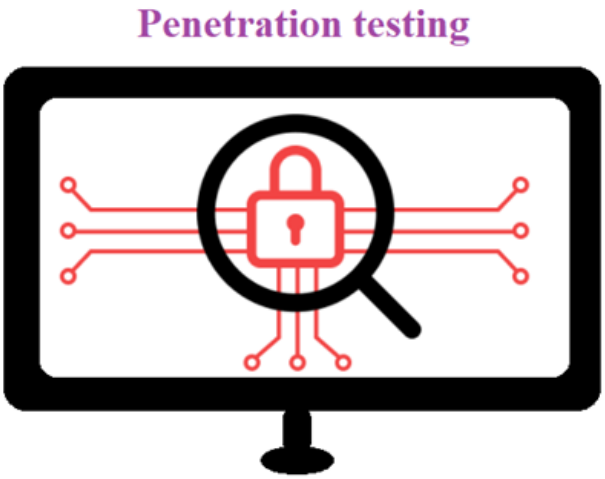


Figure 1: Penetration testing

Figure 1 shows that by using intrusion testing by ethical hackers, personal data is much better protected. Penetration testing can be automated with software applications or can be done manually. There are several stages of this type of testing, which are shown in Figure 2. The process involves gathering information about the system - scouting; identification of possible entry points, penetration attempt and reporting of the obtained results.

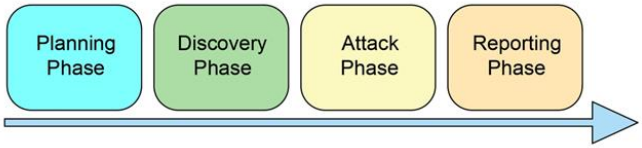


Figure 2: Penetration testing phases

## II. Smart home security problems

Security has a significant impact on the design and management of software systems. The last decade has witnessed the discovery and abuse of many vulnerabilities in software security [2]. This had led to catastrophic effects. Despite all efforts, the potential for undetected vulnerabilities in software is a grim reality [3].

Ethical hackers and malicious hackers are at the root of exploiting these vulnerabilities. But while hackers in white

hats do so with good intentions to strengthen the protection of the system, hackers in black hats use the information for selfish purposes and personal interests. It is essential that as few vulnerabilities as possible be detected by inappropriate hackers. It is not uncommon to resort to social engineering attacks, because man is the weakest link. Even if a system is very well secured, a person can slip in and allow malware to infiltrate this system.

As the years go by, more and more people use different types of smart devices - phones, computers, TVs, different types of sensors, etc. Detecting their vulnerabilities and loopholes is critical to storing sensitive information.

Another important point is that we must be extremely careful when using Wi-Fi, especially when it is public. There is no guarantee of network security, even if a password is required. There are Wi-Fi attacks that malicious hackers use to access the data of unsuspecting victims.

One of the biggest threats these days is that security is one of the biggest problems with IoT devices [9]. Each of the attacks is related to the weaknesses in the system discovered by the hackers. In IoT, hackers need a vulnerability to gain access to all available information. The reason is that all IoT devices are closely connected and this makes it easier for attackers.

The number of IoT and smart devices in in people's lives and in their homes is increasing in general. This leads to the need for an increasing understanding of the role of security and how important it is. Ensuring smart home security practices are very important to keep it safe, but first and foremost is using the right technology. In this regard, there are the main aspects that should be kept in mind when thinking about home security:

*Passwords*

Updating passwords increases the security of devices, but often the most important password that needs to be changed is the default password. Created by manufacturers and almost always the same for all manufactured devices, default passwords make devices more vulnerable to attacks. One commonly used way for botnets to "subordinate" devices is to look for passwords that are encrypted in the respective devices.

Despite the danger of default passwords, it is important to change and diversify passwords in general. It is recommended that they are more difficult to guess and are not words or phrases. Some of the hacker attacks are full of rich vocabulary and can easily find such a password.

*Wi-Fi access*

It's important to keep coming up with new and varied Wi-Fi passwords, and they need to be changed regularly. If a guest is given access, it is advisable to cancel it as soon as he leaves the network. This contributes to the network’s better governance.

For better protection, disconnecting devices that do not need to be connected at the moment is highly recommended. The ability to centrally control smart home devices and systems also allows connections to be controlled. If negligence is shown, malicious hackers can much more easily access the network and the sensitive information they want.

*Personal devices*

Before buying a new home appliance, you should consider and research this hardware or software in advance. It is important to understand what features are included in it. Devices in which quality and safety are set as the main characteristics are being selected. Those who look too good and safe are very likely to be dangerous. Finding out what devices everyone already has and how they could affect their smart home is also helpful. There are still many loopholes in the use of smart homes, and hackers are aware of this. They look for vulnerabilities not only in technology but also in consumer ignorance.

Despite the constant fight against cybercriminals, we often leave gaps and loopholes without us realizing it. It is also important to keep in mind what large and important part is occupied by various devices in our homes and pockets.

Wi-Fi is the lifeblood of a smart home, and routers are the gateways. They should not be ignored and should be protected, because hackers will immediately take advantage of the gaps. Secure routers with the ability to automatically monitor and reliably secure your home network are the future of smart home security. Some modern routers give parents extended control to ensure the safety of their children.

The convenience and benefits that intelligent systems can offer are unprecedented. But these devices can also be dangerous if not properly understood and managed. The security of the smart home must be taken as seriously as the physical security and surveillance of the home. But unlike the average thief, cybercriminals threaten to steal much more from the TV, for example, and all of this may go unnoticed until it's too late. Innovations such as smart locks aimed at ensuring a high level of security have in some cases proven to be easily susceptible to cyber breaches. As technology advances, consumers are increasingly using such products and services for convenience. But the more you increase the convenience without increasing security and privacy, the easier targets will ordinary users be for malicious hackers.

Wi-Fi assessment tools are available. There are operating systems that combine these tools [5]. The disadvantage is that the user must have in-depth knowledge to know how to use them and enter everything manually. Cisco [6] offers a combined training solution to develop security infrastructure, identify threats and vulnerabilities to networks, and mitigate security threats [7].

Laboratories designed to test the penetration of mobile devices carefully cover the top 10 mobile vulnerabilities of OWASP [11]. The reason is that many modern users are increasingly choosing mobile devices as their primary method of communicating with the network. With the help of smartphones, tablets and laptops can meet almost any need on the Internet. It is therefore not surprising that cybercriminals are targeting mobile platforms and the need to protect them is extremely important.

Example of testing mobile devices:

*Static analysis test process* [4]

For Android devices: Static analysis involves identifying insecure APIs or may include information flow through the program to determine potentially dangerous or weak handling of program inputs. Conducting static testing on a mobile device using various tools and services is shown in Figure 4. To perform static testing, you must first install the APK file on the mobile device through the Google Play Store.

For iOS devices: Initially, each tester or analyzer must set up a test environment to analyze mobile applications for iOS and jailbreak the device. Jailbreaking exploits the iOS vulnerability and gets root access to the device; it is necessary because as a tester or analyzer one must have root user rights to access all types of data, whether stored on an SD card or sent over the network. After the device is jailbroken, the Cydia icon appears on the iDevice. Then we perform a static analysis.

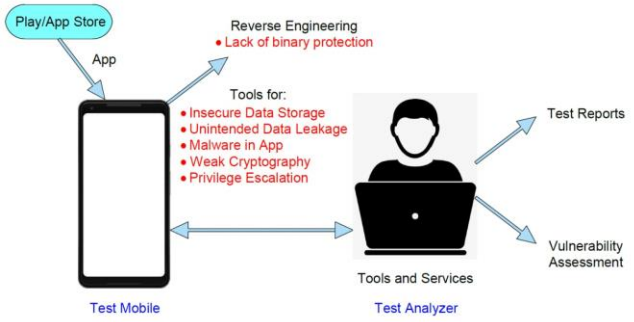


Figure 3: Conducting static testing on a mobile device [4]

*Test process in dynamic analysis* [4]

To perform a MitM simulation during dynamic analysis, four devices are required for the test. A laptop that will serve as a compromised access point. The CISCO router will be a wireless access point. One smartphone with minimum requirements - "dual-core 1.2 GHz, 1 GB RAM, with Android 4.1.2 (Jelly Bean)". Finally, a web server for implementing MitM. In this dynamic analysis, the tester simulates the real attacker and targets the victims and web servers. The test scenario is shown in Figure 5, which is the situation of a MitM attack using a Burp proxy. The attacker sets up a fake Wi-Fi access point by connecting a test mobile user (192.168.60.18) to the Internet through the access point. Therefore, any network communication that takes place between each participant and the respective server now passes through the Burp Proxy.

Wi-Fi penetration testing is a proactive and authorized attempt to assess the security of the IT infrastructure. It searches for vulnerabilities in the network, gaining network access and overflowing data.

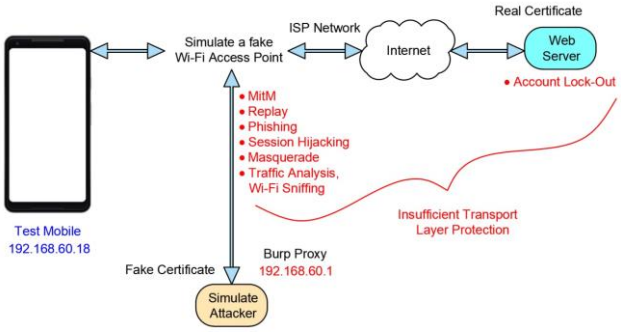


Figure 4: Conducting dynamic testing on a mobile device [4]

One of the main educational goals in higher education institutions [8] is to prepare students to achieve independent practical development and search for various solutions in the field of cyber security.

## III. Password Penetration Testing

Most IoT security research focuses on analyzing, defending, or attacking a specific device. There is still no approach to assessing the overall security of the IoT from an attacker's point of view [10]. Although penetration testing is the preferred method, the process requires significant financial costs and time. Automation can significantly improve the effectiveness of penetration testing.

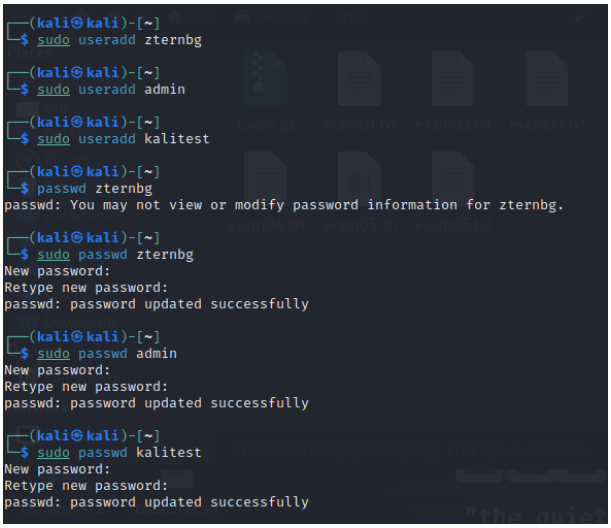


Figure 5: Three users are created

The next example will look at how resistant passwords are to hacker attacks. For this purpose, the John the Ripper tool was chosen. Three different users are created in Kali Linux. The first user's password is made up of letters only, the

second user's password is made up of numbers only, and the third user's password is a combination of letters and numbers. User passwords are stored in hashed form

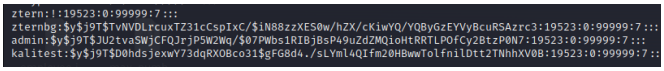


Figure 6: Hash form on passwords

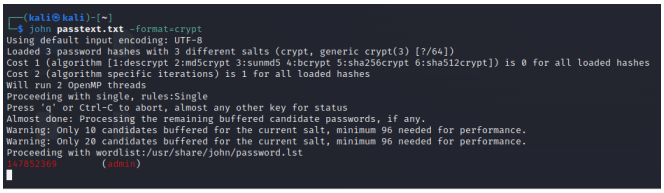


Figure 7: Hacking passwords with John the Ripper

In 12 hours, the tool John the Ripper was able to hack only the password with the numbers. The second password was not compromised. It consists of 9 letters and is a combination of two words. The third password was also not compromised. This test shows how important password length and complexity is. The penetration testing exercise conducted using John the Ripper on three different user passwords provided valuable insights into the importance of password complexity and length in resisting hacker attacks.

The John the Ripper tool used is a widely used open source software tool for cracking passwords. The program is primarily designed to test and improve password strength.

## IV. Conclusion

The paper has discussed the main issues with the security of smart devices. As technology advances, vulnerabilities in devices continue to grow. This allows attackers to use a variety of attacks to access sensitive information from their victims. Ethical hackers are also evolving and their services are gaining popularity among businesses and the general public. Their job is to test the software and look for vulnerabilities that could harm the alleged victims.

Mobile devices, which are part of the daily lives of ordinary users and devices using IoT, have the greatest risk to security. IoT is also gaining popularity among the population and threats to it are also growing. Ethical hackers are faced the difficult task of finding new methods and approaches to protect against malicious hacker attacks.

The results of this penetration testing task underscore the significance of strong, complex, and sufficiently long passwords in safeguarding against cyberattacks. Users and organizations must prioritize these factors to enhance their security posture and protect sensitive data from malicious actors. The John the Ripper tool is relatively simple and easy to use. It is designed to hack easier passwords. But there are much better tools that would crack passwords of user 2 and user 3.

## Acknowledgment

This research was funded from the Scientific and research sector of the Technical University of Sofia under contract 222ПД0018-07.

## References

[1] M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies,", IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016;

[2] N. Munaiah, A. Rahman, J. Pelletier, L. Williams and A. Meneely, "Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition,", ACM/IEEE International Symposium on Empirical Software Engineering and Measurement *(*ESEM*)*, 2019;

[3] J. D. Mireles, J. Cho, S. Xu, “Extracting Attack Narratives from Traffic Datasets,”, International Conference on Cyber Conflict (CyCon USA), October 2016;

[4] S. Bojjagani and V. N. Sastry, "VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps,", IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), 2017;

[5] S. P. Kadam, B. Mahajan, M. Patanwala, P. Sanas and S. Vidyarthi, "Automated Wi-Fi penetration testing,", International Conference on Electrical, Electronics, and Optimization Techniques *(*ICEEOT*)*, 2016;

[6] Cisco Certified Network Associate Security (CCNA Security) training;

https://www.cisco.com/c/en/us/training-events/trainingcertifications/certifications/associate/ccnasecurity.html

[7] A. Ilovan and B. Iancu, "Penetration Testing Solution for Wireless Networks using mobile devices,", 17th RoEduNet Conference: Networking in Education and Research *(*RoEduNet*)*, 2018;

[8] L. Peculea, A. Peculea, “A Correlative Study Learning at First Year Students Preparing to Become Teachers, International Conference Education and psychology challenges - teachers for the knowledge society”, Journal of Educational Sciences & Psychology, Vol. VII (LXIX) No. 1B/2017.Between Learning Strategies and Independent

[9] G. A. Abdalrahman and H. Varol, "Defending Against Cyber-Attacks on the Internet of Things,", 7th International Symposium on Digital Forensics and Security *(ISDFS)*, 2019;

[10] G. Chu and A. Lisitsa, "Penetration Testing for Internet of Things and Its Automation,", IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS*)*, 2018;

[11] S. Jadhav, T. Oh, Y. H. Kim and J. N. Kim, "Mobile device penetration testing framework and platform for the mobile device security course,", 17th International Conference on Advanced Communication Technology *(ICACT)*, 2015;