Using Ethical Hacking to Analyze BYOD Safety in Corporations

Roman Jašek, Jakub Nožička
Faculty of Applied Informatics
Tomas Bata University in Zlín
Zlín, Czech Republic
e-mail: {jasek, nozicka}@fai.utb.cz

***Abstract*—Tablets and smart phones using the Android platform are still more popular for the general population than devices using operating system Microsoft Windows or iOS. This fact is useful for hackers. For hackers, it is important to always carry with them tools to scan the network traffic in a manner that is not obvious to others. It may be difficult, and sometimes impossible, to connect to a network that the hacker wants to attach using metallic cable. Hackers are less striking in scanning network traffic on the wireless network and even less striking in scanning when using tablets. For this purpose, is perfect to use tablet with Kali Linux (Android platform). Such a tablet can be modified to be used for attacks on corporate wireless network and potential hacker becomes even less striking. Kali Linux distribution does not have high hardware department, therefore can be used at tablets with basic hardware equipment.**

Keywords- hacking; tablet; android; Kali Linux; wireless network.

I. INTRODUCTION

The aim of the work was to demonstrate that BYOD (Bring Your Own Device), which is becoming still more popular in organizations and can provide security weakness in organization. Percentage of organizations that use BYOD is unstoppably growing every year. Potential hacker, who wants attacking on wireless networks in organization that using BYOD tablets will be conspicuous with using of notebook. This problem can be solved with using of tablet for this purpose. Also was proved that tablet is a universal tool, which can be used for penetration testing of wireless networks, and also that this solution is low cost while maintaining all its functions, compared with a laptop.

Some technical papers were published with this aim. Security of Tablets in BYOD Programs are published, for instance in [4] and [5]. These papers are describing present security of tablets, and forecasting how many tablets will be using in next years. Aim of this paper were verify, than tablet can be suitable tool for hacking of wireless networks in corporations. Some technical papers were published with this aim. Security of Tablets in BYOD Programs are published, for instance in [4] and [5]. These papers are describing present security of tablets, and forecasting how many tablets will be using in next years. In [7] and [8] the authors are describing just possibilities of sending secure data from BYOD devices to public cloud or to private server.

Firstly, basic information about hardware which was used for this research. In next section software which was used for hacking are described. In section IV and are presented how to install Kali Linux in to tablet and how can be executed attack to wireless network via tablet. There were created two testing tablets, which can be using for penetration of wireless network in corporations.

II. HARDWARE DESCRIPTION

A partial goal of research was to prove that the tablet is a suitable and low cost solution for penetration testing of wireless networks. For verification of the solution, Kali Linux was installed on 2 tablets. As a representative of tablets with the lowest price, was used tablet Prestigio multipad 7.0 ultra duo. And as a tablet, which have better HW (hardware) equipment was chosen Lenovo Yoga 2.

A. Tablet Prestigio multipad 7.0 ultra duo

As already mentioned above, the tablet Prestigio multipad 7.0 ultra duo was chosen as a representative of tablets with the lowest price. The goal was to verify that the hacking can be done on this type of device. The device has a processor DualCore ARM A9 (RK3066) with 1.6GHz, 1GB RAM (Random-access memory) memory and 8 gigabytes of storage. This configuration is the minimum required to ensure all functions of Kali Linux.

B. Tablet Lenovo Yoga 2

Tablet Lenovo Yoga 2 was chosen as the representative of popular tablets. Compared with the tablet Prestigio multipad 7.0 ultra duo, it has better technical parameters and is therefore more suitable for hacking. The device has a processor Intel Atom Z3745, 4 x 1.86 GHz, 2GB of RAM and 32 GB storage. This HW configuration gives Kali Linux better support and faster response of system.

C. Antenna

For better reaction radius of hacking of wireless networks is needed to enhance the reach of the antenna. This can be ensured by using the external antenna. Android does not support all standard architectures chipsets used in antennas. Android supports just antennas with architecture realtek, as an example can be used popular antenna Alfa AWUS036H.

III. SOFTWARE DESCRIPTION

Kali Linux is a Linux distribution derived from Debian. Kali Linux is designed for digital forensics and penetration

 ISBN: 978-1-61208-493-0

testing. Before Kali Linux was widely used Linux distribution BackTrack. However, that did not fully support tablets architecture, despite modifications to the tablet were not fully stable. Kali Linux can be installed on a computer hard drive or it can run without installation from Live CD (Compact Disc). Kali Linux is distributed in 32 and 64 bit version. Kali Linux is even available for ARM processors used in Raspberry Pi computers. Kali Linux is available in versions for i386 and amd64 architectures, where is minimal configuration needed: 1GHz CPU (Central processing unit), 8GB HDD (hard disk drive), 300 MB of RAM.

Kali Linux contains a lot of selected applications designed for penetration testing. An attacker would likely begin at application EvilAP. EvilAP is application for creating a false Wi-Fi hotspot, which is ready for eavesdropping. EvilAP can know how to redirect all requests from the surroundings at the same time; because of that hotspot with the client (another phone, tablet, and laptop) can connect without their owner knowing. Once that happens, all communications can be monitored. If this attacker fails to create a fake hotspot, Aircrack-ng remains the most important application for network injection which is used to crack passwords of secured wireless networks using WEP (Wired Equivalent Privacy) or WPA-PSK (Wi-Fi Protected Access). This application requires Wi-Fi card or Wi-Fi adapter, which can be switched into monitoring mode, connecting the wireless adapter is possible on tablet. Application Wireshark (formerly Ethereal) is a protocol analyzer and packet sniffer. Among the most common applications is included analysis and debugging problems in wireless networks, software development, development of communication protocols and scanning network communication. Another useful tool for hackers is Wireshark application that allows setting the network interfaces to various modes, allowing seeing all the traffic on these interfaces, including broadcast and multicast. Wireshark has collected a lot of raw data and hackers then use many filters and select just data which are important. Default version of Kali Linux is provided with more than 300 security tools for hacking and penetration testing. If it still misses some application, user can instantly install it from the repositories of Linux. Kali Linux contains every tool, which hacker needs and expects from Linux distributions.

As it is written below Kali Linux is a Linux distribution, which is free and easy to HW, also there exists images for small computers ranging from the popular Raspberry Pi and ending by some Chromebooks, this fact makes Kali Linux even more useful for low costs projects.

A phenomenon known as BYOD, is increasing worldwide. Solution where employees use their private device is used in foreign countries and in the Czech Republic by more and more companies. BYOD solution has many advantages and disadvantages. The primary advantage for the company is economic saving, saving of the acquisition of working devices and software, employee together do not have to carry more equipment and working with it, to which they are accustomed. On the other side, this solution has many disadvantages, main disadvantage is security.

BYOD in organizations is increasingly common, at present 38 percent of organizations does not provide employees with working IT (Information technology) equipment. According to a global survey by Gartner CIO (Chief information officer) is expected that by the end of the year will exceed the number of steps minded companies 40 percent. The main reason why more and more organizations are thinking this way, is economic fact. But apart from the costs which organizations save on IT devices and the renewal of IT devices, employees are also more satisfied if they can work on their devices. BYOD also supports organization's innovation by increasing the number of users of mobile applications in the organization's environment. When BYOD is most prevalent in medium and large organizations, it is suitable for smaller business that can help development of organizations without large investments. BYOD is widespread throughout the world; however, the organizations in the United States use BYOD more than organizations in Europe. Not surprisingly, the highest safety arouses interest in using the technology BYOD. Risk of data lost on mobile platforms is particularly urgent. Some security policy organizations using BYOD are designed to share data taking place only in the cloud, which generally reduces the risk of safety.

Since 2012, tablets have become a phenomenon in organizations, the organization overwhelmingly reaching for tablets running Android and iOS, tablets with Windows OS (operating systems) and other, occupy at market a negligible 2% popularity. BYOD tablets were at the beginning of 2012, the domain of iOS, which occupied a market of over 60%, but by 2013 this number is reduced when Android gets to the forefront. According to analysts, this is due to one thing and that is the economy, the cheapest devices which use iOS participate at the market price of 250 USD (United States dollar), while the price of useful Android devices start at US (United States) $ 100. Currently, the difference is clearly noticeable, tablets running Android, with nearly 70% share of installations in organizations; clearly defeats tablet devices running iOS.

This fact is playing right into potential hackers hands for attacking wireless networks using tablets running Android. Hacker who uses attack tablets must use the Android system, as shown by surveys, most organizations use precisely the Android device and the attacker becomes less conspicuous for the neighborhood [1]-[6].

IV. KALI LINUX INSTALLATION FOR ANDROID

For Kali Linux developers, it was firstly important to make their products work seamlessly even on devices that are using Android. Currently, Kali Linux distribution can be installed on devices with Android 4.4 and above. Installation requires at least 5 GB of free memory in the internal memory or external storage and a fast Internet connection [3].

A. Configuring Kali Linux for Android

To install Kali Linux user must do a few basic things. The user can select their architecture to verify that the downloaded distribution Kali Linux is genuine; set the type

and location of the installation on the device. In Figure 1 are all necessary settings for the installation of Kali Linux [3].

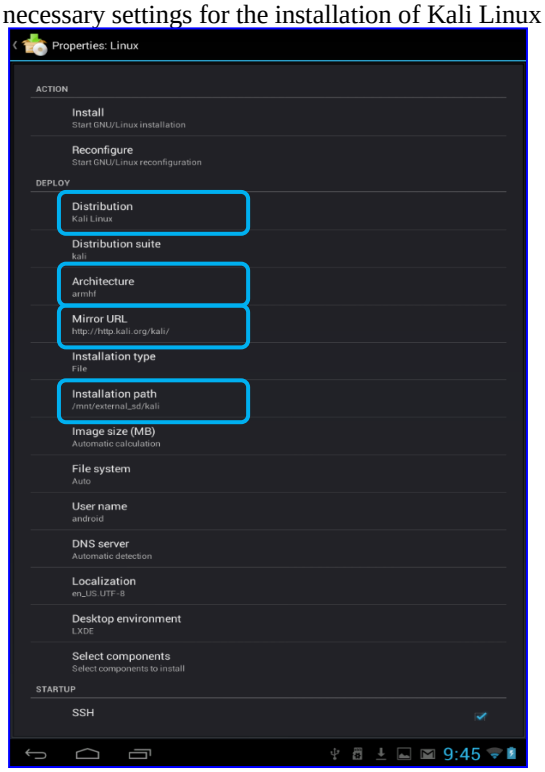

Figure 1. Linux Deploy properties.

B. *Downloading Kali Linux image*

Once the user makes all settings as you can see in Figure 2, Kali Linux begins to download image from Linux servers. This process is directly dependent on the speed of your Internet connection.

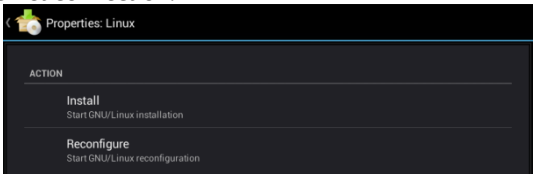

Figure 2. Linux Deploy properties.

C. *Starting chroot Kali Linux*

Once the user makes all settings, as you can see in Figure 3, Kali Linux begins to download image from Linux servers. This process is directly dependent on the speed of your Internet connection.

Figure 3. Starting Linux Deploy properties.

D. *Login to chroot Kali Linux*

After installing and starting Linux Kali user must login into the GUI (Graphical User Interface), to begin working in Kali Linux. For this purpose were used androidvnc. Android browser VNC (Virtual Network Computing) needs to set just a few trinkets, first he selects the new connection type, enters a nickname, enters a password changeme, and 5900 as a port. After this is all filled in, just click a button to connect, as you can see in Figure 4. [3].

Figure 4. Android VNC properties.

 ISBN: 978-1-61208-493-0

After logging in to the tablet version of Kali Linux users will work with the same graphical interface as in classical version of the desktop Kali Linux.

V. KALI LINUX ENVIRONMENT

After successful installation of Kali Linux, users will see graphic environment of Kali Linux. As seen in Figure 5, Kali Linux distribution has the same graphical environment both on a tablet and a laptop; moreover tablet version of Kali Linux offers the same features as the live version that runs on a laptop.

Figure 5. Linux Deploy environment.

For hacker is most important to connect to the organization's wireless network. Depending on the used device, networks can be scanned by device's internal antenna, or by external antenna connected to the tablet as seen in Figure 6.

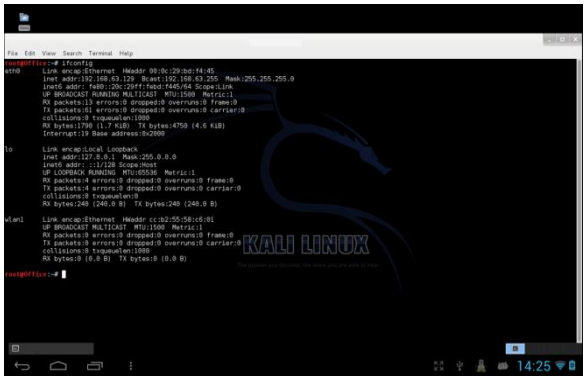

Figure 6. Kali Linux ethernet settings.

In case it is possible to scan wireless network, so for sniffing passwords is ideal tools Aircrack-ng, as shows Figure 7.

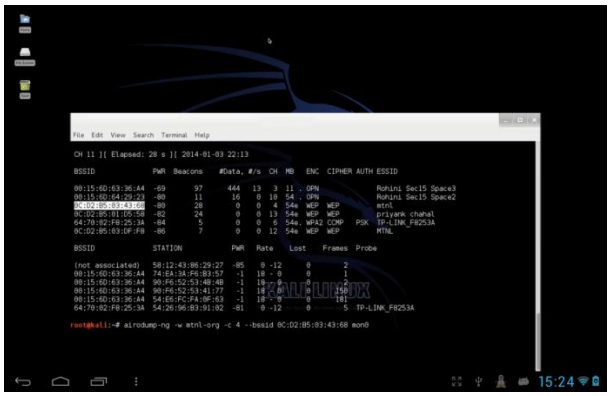

Figure 7. Kali Linux Aircrack-ng.

After connecting to wireless network hacker is already able to do all sorts of network security tests or security attacks. It is important to hacker to monitor network traffic, for this purpose it is suitable Wireshark, Dsniff, TShark, through which hacker can capture passwords, for example passwords from POP3 (Post Office Protocol) email accounts. Furthermore hacker can use Nmap tool, which enables it to obtain information about the computers on the network, what services are available in the network, what types of network firewalls and uses and much more. Hacker can also forge AP (access point) in an organizationn and can use the tablet as a fake AP, on which the other users can connect. Except of attacks on organizations network, attacks can be realized via tablet bluetooth attacks on mobile phones in the organization.

VI. CONCLUSION

In this work, we described security risks of BYOD solution when using a tablet. The main advantage of this BYOD solution is another chance for security attack by an organization, which organizations often ignore. Tablet as a penetration tool provides same value as a notebook, but with less cost and far less conspicuous for the surroundings. It was closely examined that the tablets with the installation of Kali Linux provide the same attacks as a full-fledged notebook. The motivation for the approach that was outlined in work is absolutely inconspicuousness of attacker in an organization which uses BYOD for their employees. Popularity of BYOD is still growing, organizations says, that primary advantage is economic savings compared to buying your own equipment. Organizations are aware of security risks of BYOD and primary separate corporate and user's private data. If an employee uses a BYOD tablet in organization, so in most cases employee works with corporate data in the cloud, on remote desktop, which is connected to the tablet. Proposed solution provides hacker more anonymity, because attacker with the tablet in an organization which uses BYOD tablets becomes even more unobtrusive than attacker who uses a laptop.

ACKNOWLEDGMENT

This work was supported by Internal Grant Agency of

Tomas Bata University under the project No. IGA/FAI/2016/026.

REFERENCES

[1] B. Hayes and K. Kotwica, "Bring Your Own Device to Work: Trend Report," Oxford: Newnes, 2013.

[2] D. Assing S. Calé, "Mobile Access Safety: Beyond BYOD, " London: John Wiley & Sons, 2013.

[3] M. Alamanni, "Kali Linux Wireless Penetration Testing Essentials, " Birningham: Packt Publishing Ltd, 2013.

[4] M. Karch, "Android for Work: Productivity for Professionals," New York: Apress, 2010.

[5] Gartner, "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. " [Online]. Available from: http://www.gartner.com/newsroom/id/2466615

[6] Gartner. Gartner Says Tablets Are the Sweet Spot of BYOD Programs. " [Online]. Available from: http://www.gartner.com/newsroom/id/2909217.

Article in a journal:

[7] U. Vignesh and S. Asha, "Modifying Security Policies Towards BYOD" Procedia Computer Science, vol. 50, May 2015, pp. 511 – 516, doi:10.1016/j.procs.2015.04.023

[8] M. Olalere, M. Abdullah, R. Mahmod and A. Abdullah, "A Review of Bring Your Own Device on Security Issues" Volume 4, No. 4, April 2015, pp. 62-73, doi: 10.1177/2158244015580372

 ISBN: 978-1-61208-493-0