

**LAN Turtle**

Technical Report

Abstract

The technical report explains the literature review of the Hak5 LAN Turtle’s open source modules and its functionalities. The LAN Turtle is an USB Ethernet adapter configured through Turtle Shell, acts as discrete remote access and penetration testing tool with covert backdoors. It is also used to gather network information and aids for Man-in-the-Middle surveillance for system administrators and pentesters. In this report, the abilities of the modules available in the LAN Turtle to scan the network for target devices to perform Man-in-the-middle attack, unlock Windows devices by stealing the user credentials, DNS Spoofing, URL Snarfing are explained in detail. The LAN Turtle is an affordable device which can be used by penetration testers to perform various attacks and discover security flaws in any given network.

Introduction

The usage of network technologies evolve at an exponential rate and so does its vulnerabilities. Network penetration testing is an authorised method used to assess the IT security infrastructure by performing vulnerability tests and unsafe user end behaviours. It helps to identify loopholes in the network which can be exploited by hackers and prevent the network from being compromised. Penetration testers provide effective guidance to improve the network security and remediate any issues.

With the help of penetration testing tools, system security can be tested regularly and security features can be updated to prevent illegal hacking and negative effect of system downtime. LAN Turtle is one such penetration testing device developed by Hak5. It provides stealth remote access, gather network intelligence and it appears to be housed within generic USB Ethernet adapter case.

The report explains literature revview of various modules available on the LAN Turtle and its mode of operations. By analysing every modules of LAN Turtle, we will be able to perform various attacks and discover security flaws in any given network. LAN Turtle is mainly used for attacks like stealing user credentials in hashed formats, target network scanning, Man-in-the-middle attacks, and establish a remote connection to use the device from any remote location over the internet.

This report will further discuss about the open source modules which are developed for LAN Turtle and its exclusive usages in hacking the network/devices which are connected to it. The information gathered are from Hak5 website and Swinburne Library journals as there is no advanced research performed specifically on this device.

Technical Review

The major features and modules of LAN Turtle are discussed in this technical report. A literature review is conducted to explain the methodologies of LAN Turtle modules and its functionalities. Below are the following attacks are performed by the pentesters with the help of LAN Turtle modules.

MAN IN THE MIDDLE ATTACK (MITM)

As the technologies evolve, the number of end devices increases, which consequently increases the amount of data transmitted over internet. It is predicted that by 2020, internet will carry over 35 trillion gigabytes of data. Analysing all the data through a dedicated device is time cost and resource consuming process. To overcome this issue, light weight edge device computing was introduced where, end devices resources are used to analyse, detect and secure the data. This reduces the latency of data transmission.

One drawback of this method is, it is easy to perform Man in the Middle (MITM) attack on end devices which has limited computation power and security. MITM can be implemented in two ways: Eavesdropping (monitoring the traffic passing through the network) and Manipulation (altering the data before it reaches the destination). Figure 1 shows how an attacker access the data between end devices. Most important point that needs to be understood from the below figure is, the end devices will be unaware of the attacker in between them.

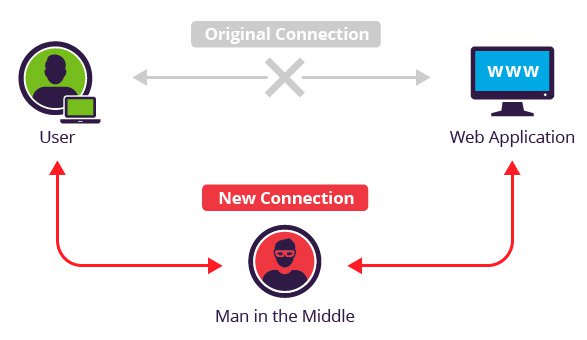


Figure 1: Man in the Middle between end devices.

Applying a security policy by implementing a centralised system can solve this issue and prevent this attack at great extent. The disadvantage of this method is that, it will not be energy efficient and cost-effective solution. To overcome this issue, [1] proposed a way to secure data against MITM. In this method, an intrusion is detected by periodic inquiring nearby neighbour devices and to prevent intrusion, the data is encrypted.

To test the level of security, penetration test is conducted in the network. LAN turtle is one of the penetration testing tools that can identify vulnerabilities and attack/defend the network. LAN turtle has modules like *Urlsnarf* and *dnsmasq*-*spoof* that can be used to implement MITM attack in the network. This is a good way of analysing the network vulnerability.

SNAGGING CREDENTIALS / ***quickcreds*** module

Due to advancement in the area of internet of things, securing a computer has become a significant aspect as any vulnerability can destroy an individual or an organization. One of such attacks is stealing password from computers as password secures critical information. Most of the times, computer users use the same password to login to most of the applications as it is difficult to remember all the passwords. So, the attackers using attacking methods like shoulder surfing attack, phishing attack and rogue devices such as USB flash drives to crack passwords and get access to personal information [2].

According to [2], a USB interface can be potential threat due to its ability of being used as a stealth attacking tool. These USB drives are registered as keyboard or mouse when they are inserted into a computer. So, the attacking tool goes undetected and can be used by the attacker to snag user credentials and also perform other network attacks. [2] Uses Rubber Ducky, a penetration testing tool to steal Wi-Fi password. Also, [3] suggest that stealing passwords can also be performed using USB Armory and LAN Turtle module designed by HAK5.

According to [3], the rogue devices should disguise as USB-to-Ethernet Local Area Network to get configured as a primary network for the targeted host. Most of the computers even though they are locked install the plug and play USB devices automatically [3] as these rogue devices disguise the hardware ID of keyboard or mouse according to [4]. The author of article [3] suggests a module Responder which can make the plugged USB device act as DNS server and gateway. Also, [3] provides a proof that this rogue device can steal hashed credentials from Windows 10 Operating System (OS) as well. So, it is not safe anymore to just lock the computer and leave it unattended.

URL SNARFING / ***urlsnarf*** module

The module ***urlsnarf*** in LAN Turtle is used to capture all the HTTP requests made by the user in Common Log Format. For effective URL Snarfing, the HTTP traffic is captured using MITM attack. In order to execute MITM attack, LAN Turtle must be physically connected to target computer. To power this device, USB side of LAN turtle should be connected to USB port on host computer. Ethernet cable should be connected to its other end for internet access. Urlsnarf module monitors web (only HTTP) activity from victim computer. Every HTTP request from victim computer passing through LAN Turtle gets logged on *urlsnarf.log* file.

Logs can be saved in two ways. One by saving log on tmp folder on LAN Turtle or on remote file system with help of other module SSHFS. Default configuration of this module monitors TCP ports 80, 8080 and 3128 (squid) with IP hostname disabled. It logs all requested URLs from sniffed HTTP traffic in CLF format used by most web servers for further offline post-analysis with other tools such as analog or wwwstat [5]. Log files are accurately stamped with dates and time which can be recorded and used for further investigation.

The syntax for this module is,

***urlsnarf –n –i –p***

where, **–n** denotes not to resolve IP to hostnames, **-i** denotes interface, **-p** denotes to process PCAP capture

DNS SPOOFING / ***dns-spoof***, ***dnsmasq-spoof*** modules

With the rise in internet application usage, data is encrypted through Secure Shell (SSL) for transmission between end users and web server. SSL protocol is widely used in exchange of electronic data, web page user accounts etc. The importance of SSL certification validation of web browsers is considered with rise in network security problems such as ARP Spoofing and DNS Spoofing [8].

In a typical DNS query, the DNS protocol matches the request or response packet with its packet ID. The client requests the DNS server for domain name resolution by sending query packet with a randomly generated ID. The DNS server sends the response to the same packet ID. The packet is accepted if both the request and response IDs are matched, else the packets are dropped. There are two main types of DNS attack which are, planted agent attack and sequence number attack.

A picture containing text

Description automatically generated

Figure 2 DNS Spoofing – Planted agent attack

In planted agent attack, the DNS database is manipulated directly by the hacker by modifying the IP address mapped to a specified domain name to the spoofed domain which looks the same as the original one. When the user requests for DNS query, the user will be redirected to the spoofed one which is a lookalike of the original webpage as shown in Figure 2.

DNS spoofing using sequence number is called as Sequence number attack. In this attack, when the clients sends a request query to the DNS server, the hacker forges the response ID and sends it to the client before the DNS server sends it. Hence, resulting in client using the spoofed website designed by the attacker rather than the original website. The LAN Turtle contains DNS Spoofing modules namely ***dns-spoof*** and ***dnsmasq-spoof***.

As an alternative to *dns-spoof*, *dnsmasq-spoof* can be used to forge replies to arbitrary DNS addresses / pointer queries on the LAN. This is useful in bypassing hostname-based access controls, or in implementing a variety of man-in-the-middle attacks. In some circumstances, *dnsmasq* may perform better than *dns-spoof*. The only configuration difference is the syntax of the hosts file. The computer connected to the Internet through the LAN Turtle attempting to browse to this domain may be redirected to the spoofed IP.

*dnsmasq* is lightweight DNS forwarder and acts as DHCP server to small network. The DHCP server provides address to each host machines connected to the LAN Turtle. When the victim computer searches for domain name, *dnsmasq* module serves as a DNS server and resolves the domain name to IP address configured in hosts file [6]. The LAN Turtle stores the host file in editable format to store the domain name and their spoofed IP address. For example, when the victim computer searches for domain “lanturtle.com”, the victim will be redirected to IP of LAN turtle i.e.172.16.84.1 or any desired IP address of web server. Each line on hosts file has IP address and one or more domain name separated by tab or space. For example,

172.16.84.1 Lanturtle.com [www.lanturtle.com](http://www.lanturtle.com) mail.lanturtle.com

This example configuration of host file directs victim to web server of 172.16.84.1 instead of real address of lanturtle.com.

NMAP

Nmap is a port scanning tool. Port scanning is a part of penetration testing where without the information of username, password and other typical methods accessing the assets of a host machine. Nmap is very useful to discover the IP address of any operating system. It helps us to find the available services and ports on a network. Nmap functionality includes not only just port scanning but also Operating System detection, Service discovery and Security auditing. Nmap can be installed on all kinds of operating system thus, making it platform friendly. For this project, nmap tool is installed on a [Linux](https://liveswinburneeduau-my.sharepoint.com/personal/101805688_student_swin_edu_au/Documents/Desktop/COS80013%20Lab%208%20week%208.doc?web=1) based operating system.

Nmap can also provide further more information on target system, device type , MAC address etc.[7] Nmap is widely used for penetration testers for finding out the vulnerabilities in their network but it can be also used as a exploit tool by the attacker to scan any network can finding out the open port in any target network. All the result captured by the nmap can be saved into a text file which helps the tester to generate a report. In our LAN Turtle device, nmap is one of the modules which can be enabled for scanning ports and mapping the LAN network as shown in Figure 3.

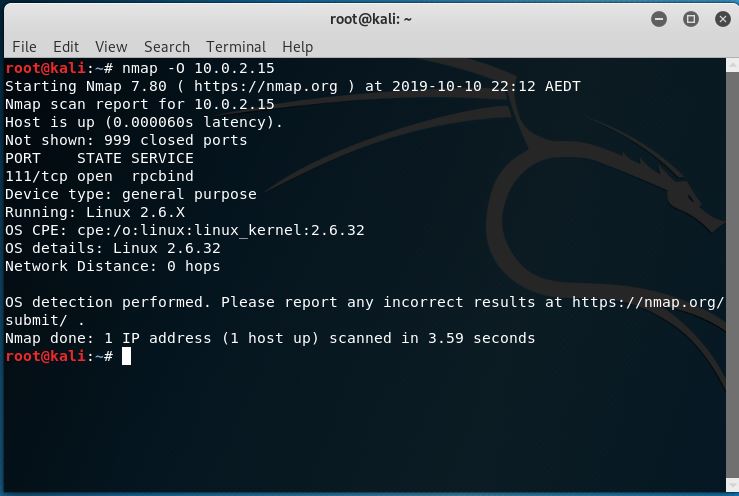


Figure 3: Nmap command -O displays the OS version of the target system.

Conclusion

The LAN Turtle has several exclusive modules which are used to perform network penetration testing. Modules such as *urlsnarf* and *dnsmasq*-*spoof* can be used to implement MITM attack in the network and helps in analysing the network vulnerability. With the help of *quickcreds* module, the LAN Turtle can steal hashed credentials from Windows 10 Operating System when the device is locked by the user. Nmap is used to discover the IP address of any operating system and find the available services and ports on a network. In future, this device can be further enhanced with addition of wireless technologies such as Wi-Fi and Bluetooth connections. The cost of the LAN Turtle is affordable and offers wide range of network testing application modules to test the network security of any IT infrastructure. With further development of open source modules, this device is highly recommended for network penetration testing purpose in enterprise environment.

References

1. Mitm F. Aliyu, T. Sheltami, Shakshuki and M. Elhadi, “A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing,” *Procedia Computer Scicence*, Article vol.141, pp. 24-31, 2018
2. Hansen Edrick Harianto, Dennis Gunawan, “Wi-Fi password stealing program using USB rubber ducky”, TELKOMNIKA, Vol.17, No.2, pp.754-752, 2019.
3. Smith, “’Stupid simple’ attack can steal credentials from locked Windows and Mac computers”, Ms. Network World (Online), 2016.
4. Tim IJntema, Christian Walet, Koen Smit, Dave van der Velde, “Analysing the Rogue Device Phenomena: An explorative View on Threats and Potential Solutions”, ECMLG 2018 14th European Conference on Management, Leadership, and Governance, pp. 98-104, 2018.
5. Linux.die.net. (2019). urlsnarf(8) - Linux man page. [online] Available at: https://linux.die.net/man/8/urlsnarf [Accessed 10 Oct. 2019].
6. Wiki.debian.org. (2019). dnsmasq - Debian Wiki. [online] Available at: https://wiki.debian.org/dnsmasq [Accessed 10 Oct. 2019].
7. [Penetration Testing - Reconnaissance with NMAP Tool](https://librarysearch.swinburne.edu.au/primo-explore/fulldisplay?docid=TN_proquest1901458135&context=PC&vid=SWIN2&lang=en_US&search_scope=Blended&adaptor=primo_central_multiple_fe&tab=combined&query=any,contains,nmap%20tool&offset=0) , Kaur, Gurline ; Kaur, Navjot, International Journal of Advanced Research in Computer Science, Mar 2017, Vol.8(3)
8. Zhang, Y. L., & Xia, G. S. (2013). The SSL MIMT attack with DNS spoofing. Applied Mechanics and Materials, 385-386, 1647.