Design of Integrated Exploitation Console using Hak5

M. Jeevanantham, C. Thamarai Kani, N. Visweswaran, P. Deepalakshmi

Abstract -Hacking is hard for a beginner tech enthusiast to learn hacking or exploit vulnerabilities in real time network or organization. This proposal aims to provide the detailed information of the framework specifically created for HAK5 tools including rubber ducky, a keystroke injection tool looks like a generic flash drive. Computers recognize the rubber ducky as a regular keyboard and automatically accept its pre-programmed keystroke payloads at over 1000 words per minute. LAN turtle is an USB Ethernet adapter with set of backdoors which can be configured by the attacker. These USB Ethernet adapters can be used to remote access computers and create man-in-the-middle attack for testers and network administrators, bash bunny tricks computers into stealing data, documents and install backdoors and other exploits. Wi-Fi pineapple lets attackers to perform man-in-the-middle attacks, advanced reconnaissance, credential harvesting, open source intelligence gathering and more, all from a web based console. This helps the beginner to attack the victim's computer by helping to create payloads to steal data from victim computer or to create malware and inject them into the victim computer. In this project, we use our integrated console to configure the HAK5 tools to attack or pentest the network in an organization.

Keywords- HAK5, Rubber Ducky, Hacking, Security, LAN Turtle, WIFI PINEAPPLE, Pen Testing, Vulnerability Management

I. INTRODUCTION

Computer enthusiasts always wish to hack a computer or a network but they do not know how to do with advanced tool like HAK5gears. It takes lot of knowledge and time to learn the working of these tools. HAK5 devices can be used to inject payloads to the computer or steal information, access files from remote computer or destroy a computer by injecting viruses into the system. Also devices like rubber ducky can be used to inject payloads to mobile phones and access them through persistent shell or inject RAT (Remote Administrator Tools) and access valuable information. Payloads can be either downloaded from the internet or it can be programmed by the hacker as he/she wants the device to behave. Rubber ducky uses ducky script language for the it'sworking and these scripts must be encoded by the ducky encoder available on the internet. A payload for bash bunny isas simple as it is just a normal text file with basic commands.

Revised Manuscript Received on December 16, 2019.

***** Correspondence Author

M.Jeevanantham*, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: jeevandham70@gmail.com

C.Thamarai kani, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: thamaraikani69@gmail.com

N.Visweswaran, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: visweswaran.nagasivam98@gmail.com

P.Deepalakshmi, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India. Email: deepa.kumar@klu.ac.in

HAK5 WI-FI-PINEAPPLE is a rogue access point and Wi-Fi pentest toolkit and it is used for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices in the network.

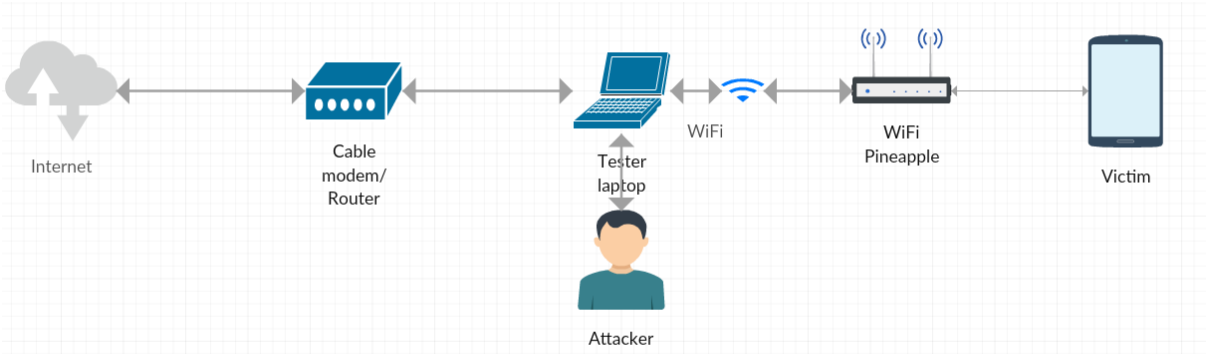
HAK5 USB Rubber Ducky as shown in Fig.1 has been a favorite tool among hackers, pen-testers and IT professionals. With its debut, keystroke injection attacks were discovered and it could attack the device with its simple scripting language, simple hardware design. HAK5 Bash Bunny is a simple and powerful multi-functional USB attack tool and automated platform for penetration testers and network administrators. HAK5 LAN Turtle is a system administration and penetration-testing tool providing stealth remote access, network intelligence gathering and man-in-the-middle attacks capabilities through a simple graphic shell. Hidden inside a generic USB Ethernet Adapter case, the LAN Turtle's appearance allows it to blend into many IT environments.

a) Fig.1Detailed picture of Rubber Ducky

(Source:https://shop.hak5.org/products/usb-rubber-ducky-deluxe)

WIFI PINEAPPLE [11] can be used as a rogue access point to monitor all the packets coming in and out the network as shown in Fig.2. It tricks the user to connect to the Wi-Fi of its own. There are modules available predefined which can be used to perform SSL Striping which means the http transactions or converted into simple text. Hence, all the username and passwords entered in the network are visible as clear text.

LAN Turtle payload are as powerful as they can grab a password from a locked computer running windows OS. The LAN Turtle device is connected to the computer in between the Ethernet and the USB port as shown in Fig.3. Therefore, it allows sniffing packets remotely through the persistent shell at other end. MITM (Man in the Middle) attacks are so easy to perform using a LAN Turtle stick. These can be controlled using a SSH shell either using putty on windows or SSH in Linux.



b) *Fig.2 Working of Wi-Fi PINEAPPLE*

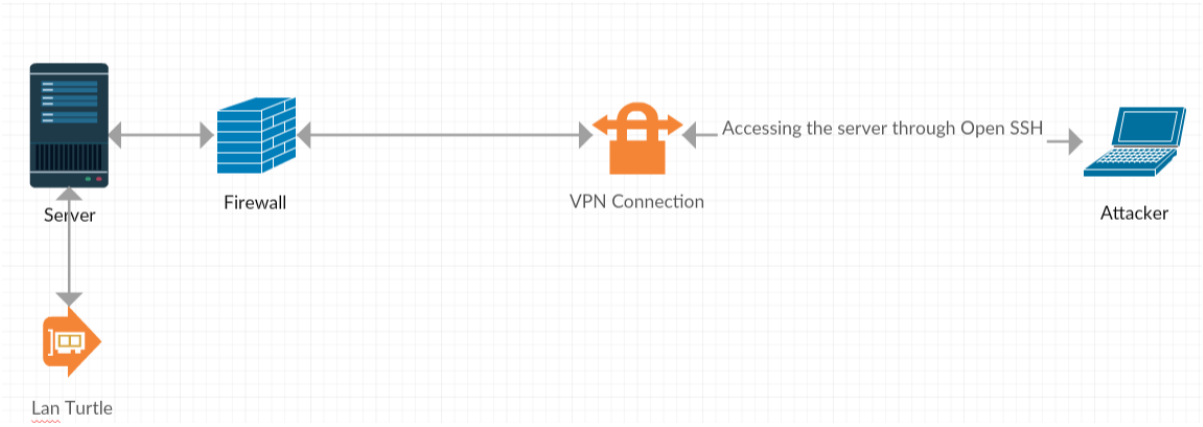


Fig.3 Working of LAN Turtle

II. RELATED WORKS

Dung V. Pham et al [1] investigated into hack tools on U3 platform and USB platform free portable hack tools, their working mechanism, and the compilation techniques. They also described about most dangerous hack tools with their payloads which can be compiled into portable format. They offered concise solutions for enterprise administrators to secure their systems from portable hack tools. One such solution, commercial malware can detect Hak Tools but not in all cases. The only deep-seated solution for such portable tools is software restriction policies with the enforcement of software policies or AppLocker with trusted executable files bundled with valid digital signature from trusted publishers.

Benjamin Cannoles [2] of university of North Georgia designed a payload for USB rubber ducky script to obtain the clear text logon of windows username and password in mere seconds. He laid out discussing the vulnerability, Details of attack on windows 7 operating system and higher. He used the convention method to create the payload using notepad and encoding it with the ducky encoder script available online.

Witemyre et al [3] exploited rogue access point using a Wi-Fi Pineapple in conventional browser method used to steal username and passwords of http login on website. Also they send deauth packets to the client to remove the client from the SSID. This tricks the client to connect the user into the Rogue access point created by the Wi-Fi pineapple

From literature review, we guessed that in case of all these conventional methods, The user must go through lot of learning process. He/she needs to encode all the payloads using different algorithms, which is a tedious process. Further, it takes lot of time to learn basics, learning different scripting languages is not possible, all altogether leading to time wastage in reconnaissance.

This paper aims to provide information about the framework created using python, which helps the beginner or techie to create or generate a payload and handle the device with ease. This framework is an integrated console where all devices are listed and each tabs in the console can be used to control different devices. Also it has preloaded with existing payload which can be also modified by the hacker according to the victim's machine. It means the attacker can configure or create his own payload to attack the victim's machine.

III. PROPOSED SYSTEM

This paper aims to provide information about the framework created using python, which helps the beginner or techie to create or generate a payload and handle the device with ease. The conventional method takes longer time and it is harder to learn about the device one by one. This framework is an integrated console where all devices are listed and each tabs in the console can be used to control different devices. In addition as shown in Fig.4, it has preloaded with existing payload which can also be modified by the hacker according to the victim's machine means defining the guest operating system such as windows, Linux or Mac.

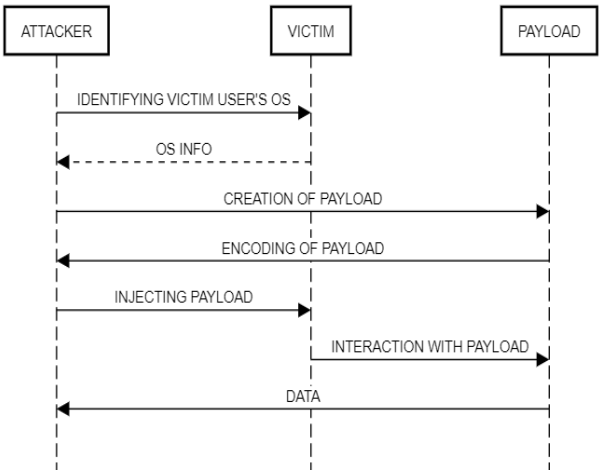


Fig.4 Sequence Diagram for interaction between attacker and payload

IV. ENVIRONMENTAL SETUP

B. *A. Performing Attack using Rubber Ducky:*

It's not needed for one to be a programmer to code on a rubber ducky. The rubber ducky has its own syntax, which is simple to understand and learn, it uses its own syntax. The syntax is given below.

- REM it is similar to comments used in C and C++, which is used to give a information and not executed by the compiler.
- STRING will type the line exactly into the target computer
- ENTER/SPACE will trigger the “enter” or “space” key.
- DELAY instructs the program to wait a specified number of milliseconds.
- GUI is used for pressing Windows Key on a PC. You will commonly see GUI SPACE, or GUI r to open the “Run” dialogue box on payloads meant for Windows systems

To create your own first Ducky Script, open the HAK5 integrated Consoleand switch to rubber ducky panel and begin entering your commands. You can save this file as a regular, text file anywhere on your computer. Fig.5 is a sample payload we came up with for delivery on a windows device.REM Leave a little reminder to lock your PC (just delete or comment this out if you don't want that).

```
GUI r
DELAY 400
STRING notepad
DELAY 400
ENTER
DELAY 400
STRING don’t forget to lock your pc
DELAY 3000
GUI l
```

Fig.5 Sample payload

Reading through above program, we can notice that line start with commands, and then have one or more characters followed by Reading the program, it is seen that this script starts up the “terminal” on the system so we get access to the command line of the system. Then the rubber ducky runs an ftp server and login using the username and the password given. Finally, it waits according to the DELAY seconds and executes the commands.

Algorithm 1 : For rubber ducky

```
#Loading the payload:

def load_payload(self):
    file_location =
QFileDialog.getOpenFileName(self, ".", "Select your
payload")
    if file_location is None:
        QMessageBox.information(self,
"RubberDucky", "Payload has not been loaded")
        return None
    file_location = file_location[0]
    with open(file_location, "r") as payload_reader:

self.payload_editor.setText(payload_reader.read())

# payload is selected by the user from the
directory.

Encryption as inject.bin
  def save_payload(self):
    directory =
QFileDialog.getExistingDirectory(self, "Select your
directory")
    payload =  self.payload_editor.toPlainText()
    if len(payload) == 0:
        QMessageBox.information(self, "Empty",
"Payload is empty")
        return None
    out_file = directory + "/inject.bin"
    duck_text = payload
    language = 'gb'
    encoder_response =
encoder.encode_script(duck_text.encode("utf-8"),
language)

#print("1", encoder_response)
    encoded_file
="".join(encoder_response['encoded_file'])
    duck_blob = io.BytesIO()
    write_bytes = encoded_file.encode()
    duck_blob.write(write_bytes)
    duck_bin = duck_blob.getvalue()
    duck_blob.close()
```

a) *Once we download the modules, we are able to see many options and if there are missingdependencies then the turtle can auto download them. The modulesshould then show up on your module list with a X next to it representing that it's ready to rock.*

C. *B. Performing attack using Bash Bunny*

1) ***Switch Positions:****In Switch Position 3 of Fig.6, the Bash Bunny [9] will boot the* arming mode, *which enables both Serial storage and Mass Storage. From the arming mode the payloads may be managed through the Mass Storage.*

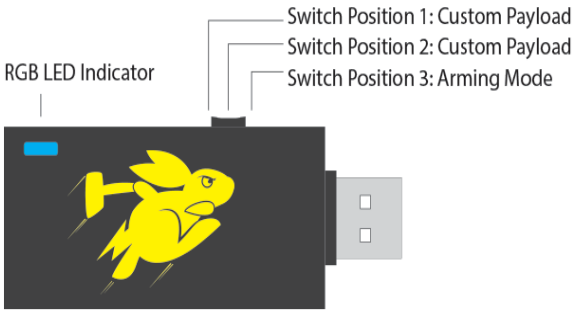


Fig. 6 Switch positions of Bash Bunny
(Src: https://wiki.bashbunny.com/#!index.md)

2) Mass Storage Directory Structure:*The default directory structure Bash bunny is given in Fig.7 and same is explained below.*

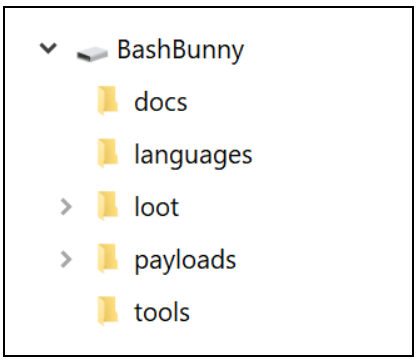


Fig.7 Default directory structure of the Bash Bunny

- "/docs" - home of the documentation.
- "/languages "- it has the Keyboard layouts/languages that can be used.
- "/loot" - used by payloads created by the user to store logs or the other data on attack.
- "/tools" – it is used to install additional deb packages.
- "/payloads" - home to active payloads, library and extensions.
- "/payloads/switch1 and /payloads/switch2" – stores thepayload.txt and a file which will be executed on boot when the bash bunny switch is in the payload mode.
- "/payloads/library "- home to the payloads library which can be downloaded from the Bash Bunny Payload git repository or online.
- "/payloads/library/extensions" - home to Bunny Script extensions

Type the payload in the console and save it in the payload/switch1 or switch 2. Then put the bash bunny in arming mode and inject into the victim's PC.

3) ***LED Status:****The color codes for identifying the status of bash bunny is given below.*

LED	Status
Green	Booting Up the device
Blue	Enabling Arming Mode
Red	Recovery Mode or Firmware Flashing mode

D. *C. Performing attack using Wi-Fi Pineapple*

SSLstrip works by monitoring the HTTP traffic as shown in Fig.8 and itwaits for links or redirects that using HTTPS. Once it is redirected using HTTPS, it will be transparently re-write it to the HTTP and pass it to the victim. In the example above of navigating to http://twitter.com, the Twitter server will respond with a redirect to https://twitter.com that SSLstrip then replaces. Once SSLstrip [7.3] has replaced, then it stores a map of all the replacements it has made. So, it can continue to interchange traffic between the HTTPS connection to Twitter and the HTTP connection to the victim.

To get Wi-Fi Pineapple ready for the attack, we need to download and install SSLstrip module from the Pineapple Bar, From the module bar, in the Wi-Fi pineapple modules tab and then in console press start process tab, we can get all clear texts passwords.

Algorithm2: For bash bunny

```
def switch_one_clicked(self):
    directory =
QFileDialog.getExistingDirectory(self, "Select your
directory")
    payload = self.payload_editor.toPlainText()
    if len(payload) == 0:
        QMessageBox.information(self, "Empty",
"Payload is empty")
    return None

    out_file = directory + "/payload.txt"
    with open(out_file, 'w') as out:
        out.write(payload)
    QMessageBox.information(self, "bash bunny",
"Payload has been created")

def switch_two_clicked(self):
    directory =
QFileDialog.getExistingDirectory(self, "Select your
directory")
    payload = self.payload_editor.toPlainText()
    if len(payload) ==
0:

QMessageBox.informat
```

```
ion(self, "Empty", "Payload is empty")
        return None

    out_file = directory + "/payload.txt"
    with open(out_file, 'w') as out:
        out.write(payload)
```

```
QMessageBox.information(self, "bash bunny", "Payload has been created")
```

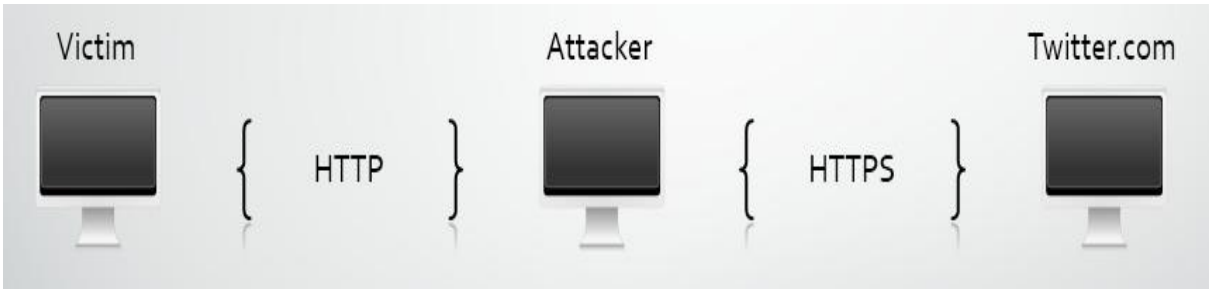


Fig.8 Working of SSLstrip

V. CONCLUSION

Integrated Console using HAK5 which is developed by us helps beginner hackers to learn and pentest a network. This is used to find all the possible way to hack a network or a user computer in an organization to defend its applications, networks, users and endpoints from internal and external attempts to dodge its security controls to achieve privileged or unapproved access to protected assets. Pen test results confirm the threat posed by particular security vulnerabilities or faulty processes, allowing IT management and security experts to arrange remediation efforts. Organizations can more efficiently anticipate emergent security threats and avoid unauthorized access to crucial information and critical systems through executing regular and complete penetration testing.

REFERENCES

[1]. Dung V. Pham, Ali Syed, Azeem Mohammad, Malka N. Halgamuge, "Threat Analysis of Portable Hack Tools from USB Storage Devices and Protection Solutions", IEEE International Conference on Information and Emerging Technologies, Karachi, Pakisthan, 2010

[2]. Benjamin Cannoles , Ahmad Ghafarian, "Hacking Experiment Using USB Rubber Ducky Scripting" Systemics, Cybernetics And Informatics, Vol.15, No.2, 2017.

[3]. https://www.youtube.com/watch?v=dE_xoj7HrIc

[4]. https://www.youtube.com/watch?v=AVqh5mcFcFU&t=907s

[5]. https://www.youtube.com/watch?v=myRgxB91cNI

[6]. https://github.com/kevthehermit/DuckToolkit

[7]. https://scotthelme.co.uk/wifi-pineapple-karma-sslstrip/

[8]. https://wiki.bashbunny.com/#!./index.md%23Languages

[9]. https://shop.hak5.org/products/lan-turtle

[10]. https://www.ssh.com/ssh/

[11]. https://www.seleniumhq.org/

[12]. https://pdfs.semanticscholar.org/55d9/e13a58d88797c03f4a43bf309e69f8eecc62.pdf

AUTHORS PROFILE

Mr. M. Jeevantham is a student graduated form Kalasalingam Academy of Research and Education (KARE), Virudhunagar, Tamilnadu, India and his area of interests is developing software and websites. Contact him @ jeevanantham70@gmail.com.

Mr. C.Thamarai kani is a student graduated from Kalasalingam Academy of Research and Education (KARE), Virudhunagar, Tamilnadu, India and his area of interest is to write code for web scraping and software using python flask.

Mr. N.Visweswaran is a professional programmer studying in Kalasalingam Academy of Research and Education (KARE), Virudhunagar, Tamilnadu, India. His area of interest is developing open source projects in machine learning and CNN. Contact him at visweswaran.nagasivam98@gmail.com

Dr.P.Deepalakshmi is currently working as a Professor in Department of Computer Science and Engineering at Kalasalingam Academy of Research and Education. She is also serving as Dean, School of Computing. Her research interest includes Optimization Techniques, Network Routing, Distributed Computing and Network Security. She has published her research in many journals and conferences and also recognized as an eminent speaker in the field of Computer Science in the nearly region. She also takes care of KARE ACM student chapter as faculty mentor. Contact her at deepa.kumar@klu.ac.in