

HACKING

PREVIEW
PERIPHERAL PROTECTION

IT SECURITY MAGAZINE

VOL.17, NO.07

ETHICAL HACKING TOOLS

AUTOReCON:

YOUR NETWORK RECONNAISSANCE GATHERING AUTOMATION TOOL

HOLEHE

EFFICIENTLY FINDING REGISTERED ACCOUNTS FROM EMAILS

INTRODUCTION TO RECON-NG

GOBUSTER - BRUTE FORCE TOOL FOR HACKERS

AND MORE...

HAKIN9

TEAM

Editor-in-Chief

Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Managing Editor

Marta Sienicka

sienicka.marta@hakin9.com

Editors:

Marta Sienicka

sienicka.marta@hakin9.com

Agata Staszelis

agata.staszelis@software.com.pl

Bartek Adach

bartek.adach@pentestmag.com

Michalina Szpyrka

michalina.szpyrka@eforensicsmag.com

Proofreader:

Lee McKenzie

Senior Consultant/Publisher:

Paweł Marciniak

CEO:

Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

Marketing Director:

Joanna Kretowicz

joanna.kretowicz@eforensicsmag.com

DTP

Marta Sienicka

sienicka.marta@hakin9.com

Cover Design

Hiep Nguyen Duc

Joanna Kretowicz

Publisher

Hakin9 Media Sp. z o.o.

02-676 Warszawa

ul. Bielawska 6/19

Phone: 1 917 338 3631

www.hakin9.org

BETATESTERS &

PROOFREADERS

Lee McKenzie

Hammad Arshed

Avi Benchimol

Amit Chugh

Kevin Goosie

Craig Thornton

Paul Mellen

Jaimandeep Singh

Jordan M. Bonagura

Paul Mellen

Danish Zia

Girshel C

Humberto A. Sanchez II

Daniel D. Dieterle

Gabriel Carvalhaes

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

DEAR READERS,

When performing penetration testing or hacking, we may need to automate our operations because there may be hundreds of conditions and payloads to test, and testing them manually can be time-consuming. In this edition, we decided to focus on the most popular and effective tools available in the Kali Linux system.

We start with an amazing article *Running Kali Linux on an M1 Mac*. There are several options to run Kali Linux on an M1 Mac OS device and in this tutorial the author focused on an open-source application called UTM. Once we set up our lab we can start using our tools!

We have two tutorials about two information-gathering tools: *Recon-Ng* and *Autorecon*. If the reconnaissance phase is what you are looking for, those two articles are perfect for you!

If you prefer something with an offensive approach, you must read the tutorial about *GoBuster*. This tool is used to brute-force URIs (directories and files) in websites, DNS subdomains (with wildcard support), Virtual Host names on target web servers, and Open Amazon S3 buckets. Sounds great right?

For OSINT fans we have an introductory article about *Holehe*. This tool allows you to check if the mail is used on different sites like Twitter, Instagram and will retrieve information on sites with the forgotten password function.

Introduction to SQLMap tool will show you how to automate the process of detecting and exploiting SQL injection flaws and taking over database servers.

We have two articles about *Metasploit*. The first one is focused on general information and its usage. In the second one, you will learn how to perform the SYN flood attack with Metasploit.

But that's not all! We have an article about *Breach and Attack Simulator* and *Understanding Internet of Things Malware*.

As you can see, this month's issue is full of tutorials that will help you up your hacking skills! We hope you'll find something that suits your needs best! We would also like to send gratitude to our contributors, reviewers, and proofreaders, who helped us create this issue!

Stay safe and enjoy!

Hakin9 Editorial Team

Contents



Running Kali Linux on an M1 Mac

by Erik Santana



GoBuster - Brute Force Tool For Hackers

by Michael Sommer
Thorn Deil



Introduction to Recon-Ng Tool

by Atlas Stark



AutoRecon: Your Network Reconnaissance Gathering Automation Tool

by Greg Thomas

Contents



071

Holehe - Efficiently finding registered accounts from emails

by Jeff Minakata



076

An Introduction to SQLMap

by Jomon Thomas Lobo



083

All you need to know about Breach and Attack Simulator

by Jesus Garcia



094

SYN Flood Attack Launched Through Metasploit

by Vinesha Selvarajah

Contents



Penetration Testing using Metasploit Framework

by Dr Saju Mohanan



Understanding Internet of Things Malware

by Hisham Alasmay

RUNNING KALI LINUX ON AN M1 MAC





ERIK SANTANA

Erik Santana is a husband and father to the most wonderful wife and son in the world. Network Security Analyst, Security Software Developer, Pentester, Android/iOS Developer with 8+ years in cybersecurity. CISSP and eCPPT with degrees in Computer Science and Biology. Born and raised in Puerto Rico, he now works from North Carolina as a web application pentester, security consultant, and a student of Kyokushin Karate.

Mac OS has been my operating system of choice for many years. It is my favorite way of running a virtualized instance of Kali Linux when performing pentesting work. Previously, with Intel Macs, virtualizing X86_64 operating systems was a very easy task. You could run most X86_64 versions of Windows and Linux as a virtual machine (VM) or inside a separate partition. Now, with Apple's latest change in CPU architecture (Apple Silicon), only ARM (Advanced RISC Machines) based operating systems can be virtualized in Mac OS. This limits the way we can run Kali Linux on the new M1 Macs.

There are several options to run Kali Linux on an M1 Mac OS device. I will be focusing on an open-source application called **UTM**. This is a step-by-step guide on how to run Kali Linux on an M1 Mac using UTM.

DOWNLOAD THE KALI LINUX (ARM64) IMAGE FILE

Our first step is to download the Kali Linux ARM64 image from the kali.org website. We will use this image in UTM to create the Kali virtual machine.

1. Go to <https://www.kali.org/get-kali/>
2. Select the “Bare Metal” option.

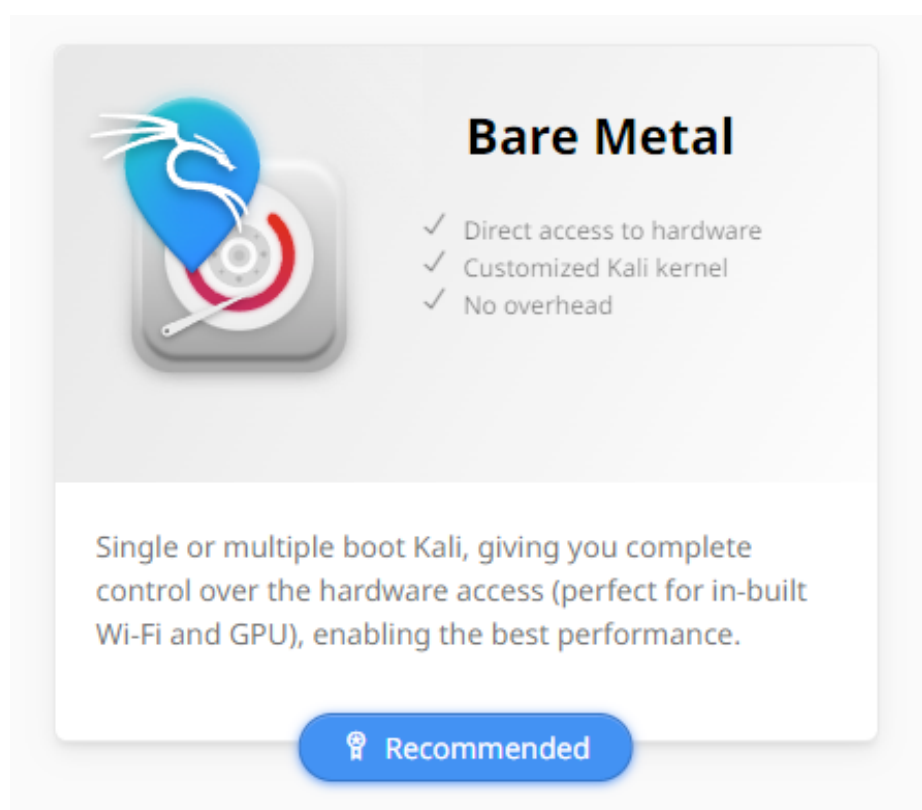


Figure 1 - Kali Linux Bare Metal Option

3. A bit further down the webpage, choose the Apple M1 tab and download the “Installer” image file using direct download or a torrent file. You should end up with a file called **kali-linux-2022.2-installer-arm64.iso** or a later version, depending on when you read this. This is the image file we will be using to install Kali Linux.

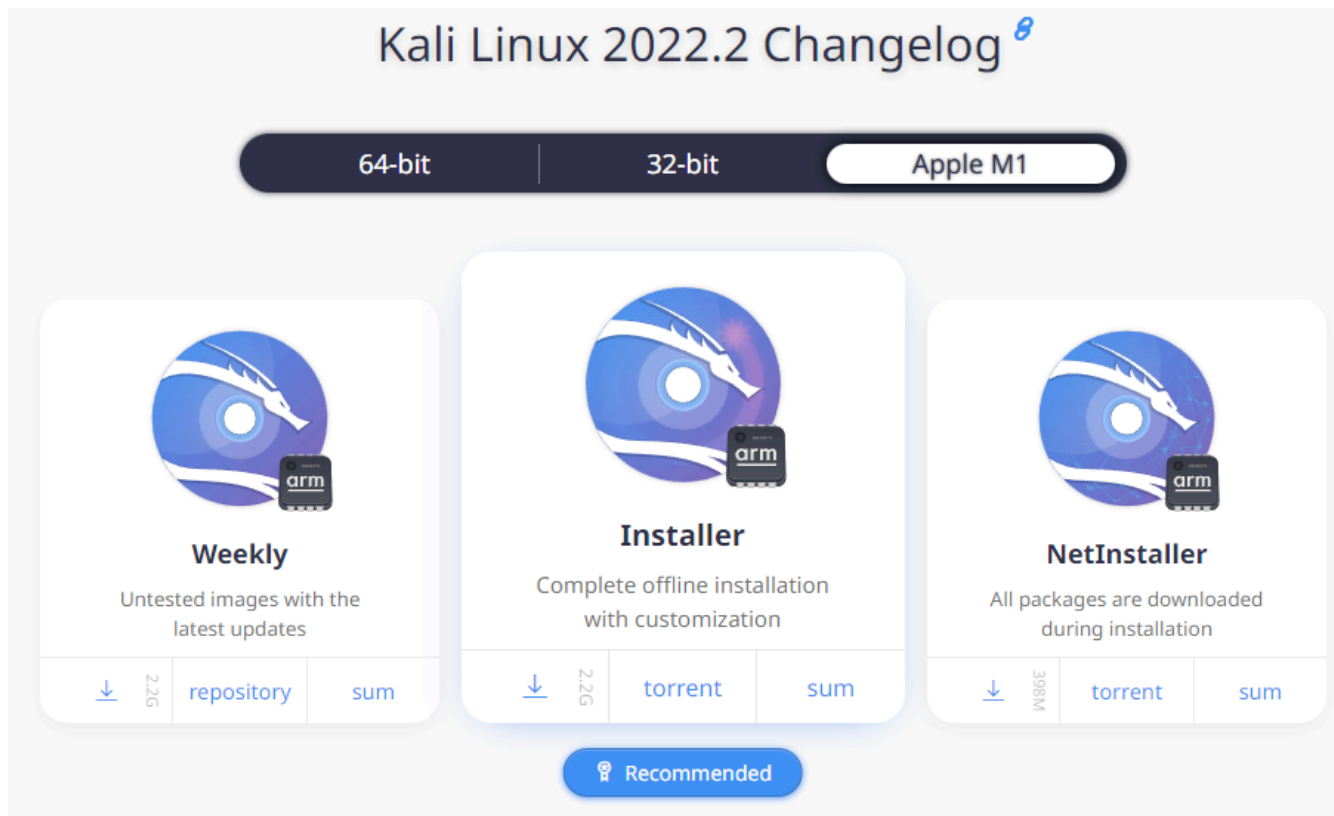


Figure 2 - Kali Linux Apple M1 Installer Download

UTM

UTM is an open-source virtualization framework that utilizes the Apple Hypervisor to run ARM64 images.

1. Visit the site <https://mac.getutm.app/> and click the “Download” button. Note that this application is free and open-source, but if you want to help with the project, you can also download the app from the Mac App Store for \$9.99.

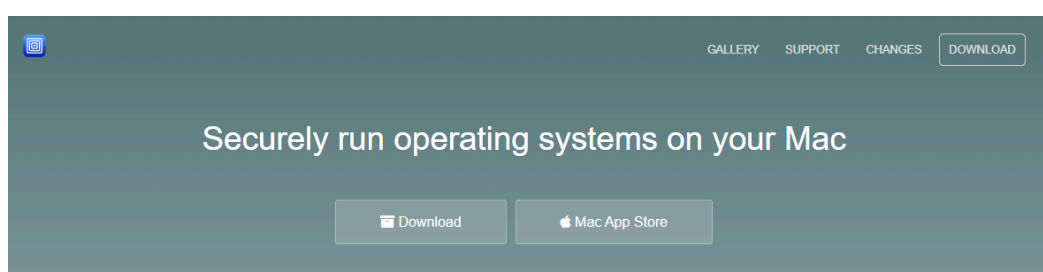


Figure 3 - UTM Download Page

2. You should end up with a file called UTM.dmg. Open the .DMG file.
3. Drag and drop the app into the applications folder.

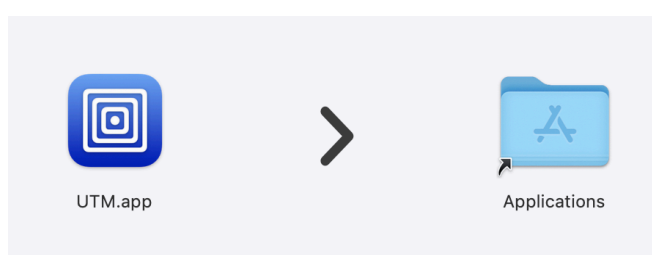


Figure 4 - UTM Install to Applications Folder

GOBUSTER - BRUTE FORCE TOOL FOR HACKERS





MICHAEL SOMMER

Michael Sommer is a Senior Information Security Consultant and CISO at CONSULECTRA GmbH in Hamburg. He started in security in 2006. His focus is on penetration testing, critical infrastructure, live hacking, cloud security, ISMS consulting and more. He runs a YouTube channel for solution videos of web security labs.



THORN DEIL

Thorn Deil is a Junior Security Consultant and Pentester at CONSULECTRA GmbH since 2022. He completed an apprenticeship as an IT systems electronics technician at the Wilhelmshaven Naval Arsenal in 2018 and graduated with a bachelor's degree in applied computer science with a focus on IT security from University of Applied Sciences Mittweida in 2021.

WHAT IS GOBUSTER?

Gobuster is a brute force tool that can be used for different use cases within pentests or bug bounty programs. One of Gobuster's strengths is brute-forcing directories and files on web servers. Another use case is the brute-forcing of subdomains. There is also the possibility to identify s3 buckets and VHOSTs. In the current version of Gobuster, at the time of writing this article, it was version 3.1, the fuzzing mode has been added. In this article, all modes of Gobuster are presented and explained with practical examples. Gobuster is developed in the Go programming language by OJ Reeves and Christian Mehlmauer. The project has about 6200 stars on GitHub and quite a few supporters.

Brute-Forcing

To use Gobuster effectively, it is necessary to have an understanding of brute forcing. If brute forcing is known, then this section can be skipped.

A brute force attack is an attempt to crack a password or username, or to find a hidden web page or the key used to encrypt a message. It involves a trial-and-error approach, hoping to eventually guess the desired information. This attack method is old, but it is still effective and popular among hackers. The duration of such an attack can last from a few seconds to many years. When searching for a password, the complexity of the password determines how long it takes.

Fuzzing

In this section fuzzing is described. If fuzzing is known, then this section can be skipped.

Fuzzing is an automated technique for software testing in which random data is repeatedly sent to the program under test at one or more input interfaces. The goal of this test is to induce unpredictable reactions of the program (e.g. program crashes) and thus to be able to identify vulnerabilities. Fuzzing was developed at the University of Wisconsin-Madison in 1989 by Barton Miller and his students.

HOW TO INSTALL GOBUSTER

There are three easy ways to install the latest Gobuster version 3.1.0, which are described in the following section. The following instructions have been tested on a Linux Kali 2022.2 system.

Advanced Packaging Tool (apt)

1. Install Gobuster via apt: `sudo apt install gobuster`
2. Check Gobuster version: `gobuster version`

INTRODUCTION TO RECON-NG TOOL

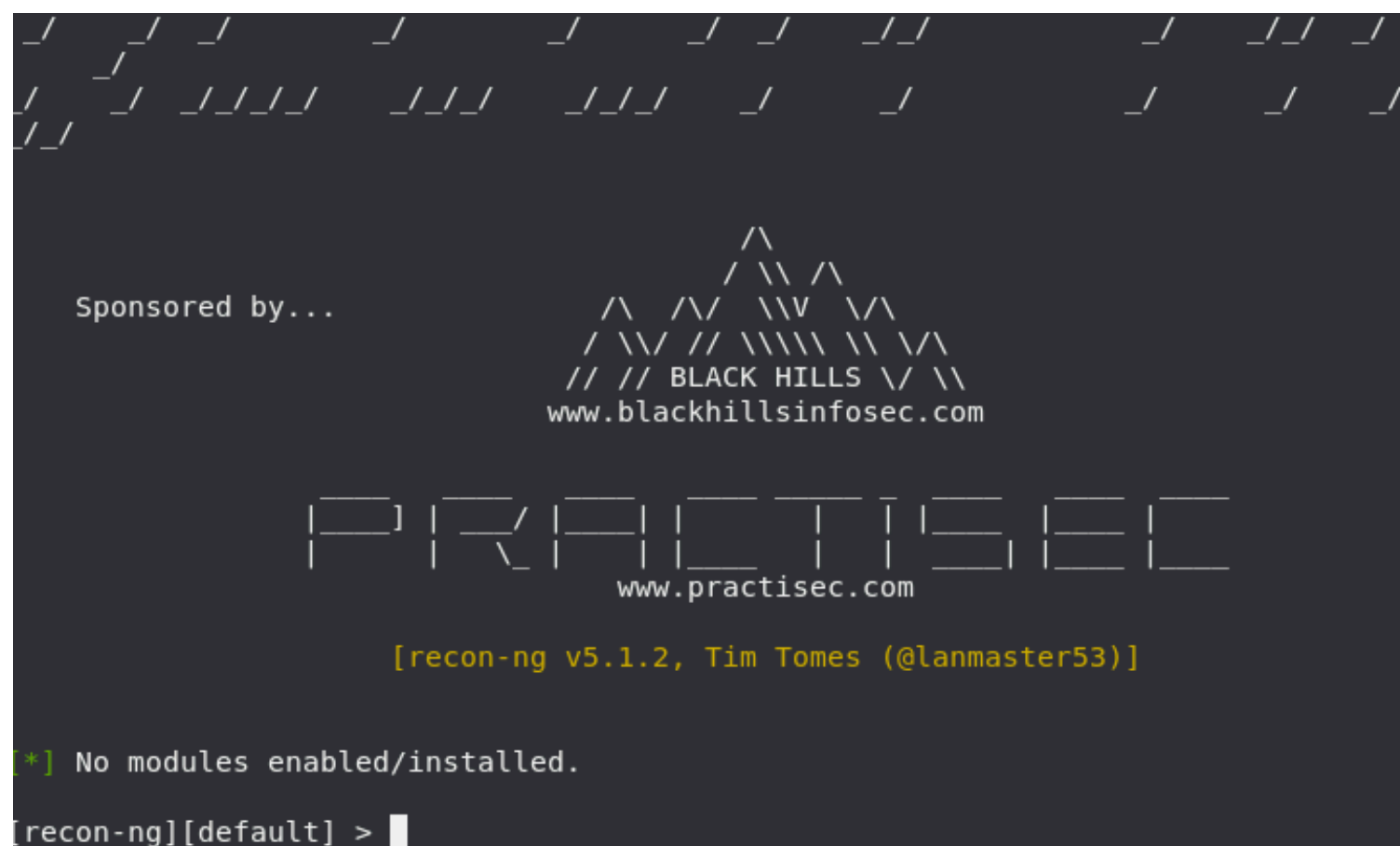


ATLAS STARK

Atlas Stark is a security researcher at Stark Industries Inc. with 16+ years in the technology industry. Currently providing cyber security solutions and OSINT services to anti-human trafficking non-profits that aid in the investigation and victim recovery. He also consults with state-level law enforcement agencies concerning hacking-related incidents. He splits his time between California and Tennessee.

Please email stark@starkinternational.se with any questions or concerns.

There are tools we use in the industry that are extremely effective and wildly popular, however, there are some tools that seem to only be popular among security professionals. I feel that one of those tools is recon-ng from Black Hills Information Security. Recon-ng is a tool I use with my students quite a bit because it has a Metasploit type feel to it and is extremely useful when teaching newcomers how to navigate within a framework, which can be a bit overwhelming in the beginning. I say hats off to the team at BHIS for producing a quality and approachable product. I am sure that by the end of this article you will have discovered a new tool to add to your arsenal of useful tools.



```

      /\
     /\ \
    /\  \
   /\   \
  /\     \
 /\       \
//  // BLACK HILLS \
//  // www.blackhillinfosec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

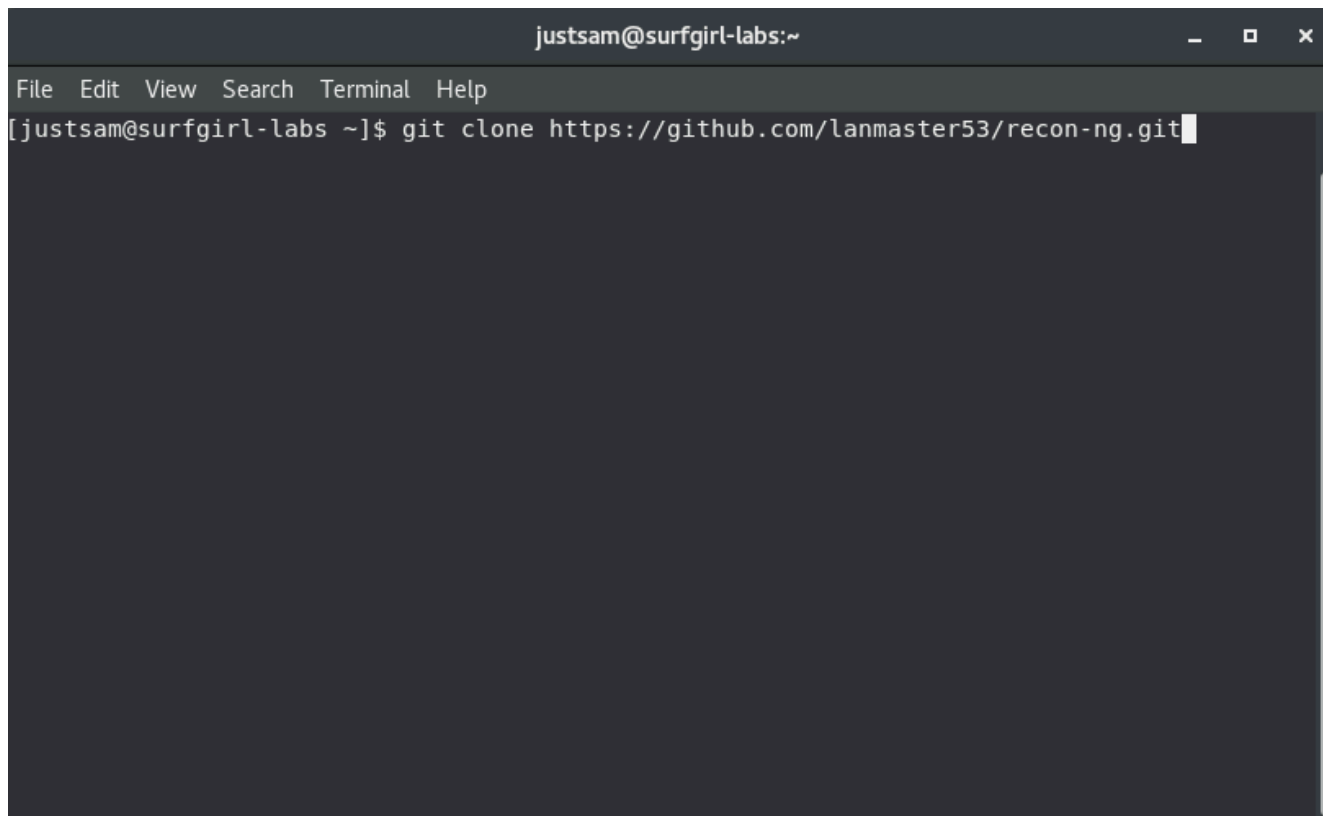
[recon-ng][default] >
```

Since the company's founding in 2008, the team at Black Hills Information Security, which is located in beautiful South Dakota, offers a variety of information security-related services such as penetration testing and Active SOC. Please visit their site for more information regarding their services; I have included their website in the links and resources. Aside from creating top-notch tools for the information security industry, Black Hills is also able to offer a variety of educational resources, services, and cool games to engage you regarding Cybersecurity related content. We could spend an entire article discussing the breadth and depth of the company's website. We may do that at some point, however, in this article, we are going to dive into recon-ng, which is only one of the many useful tools that are widely available. Let's get started.

According to the project page, recon-ng is a reconnaissance framework geared toward web-based targets and how you configure the framework will impact the results it produces during an audit. Recon-ng comes pre-installed within Kali Linux, but on the off chance it is not, I will include an installation walk-through for your reference in the upcoming section.

INSTALLATION

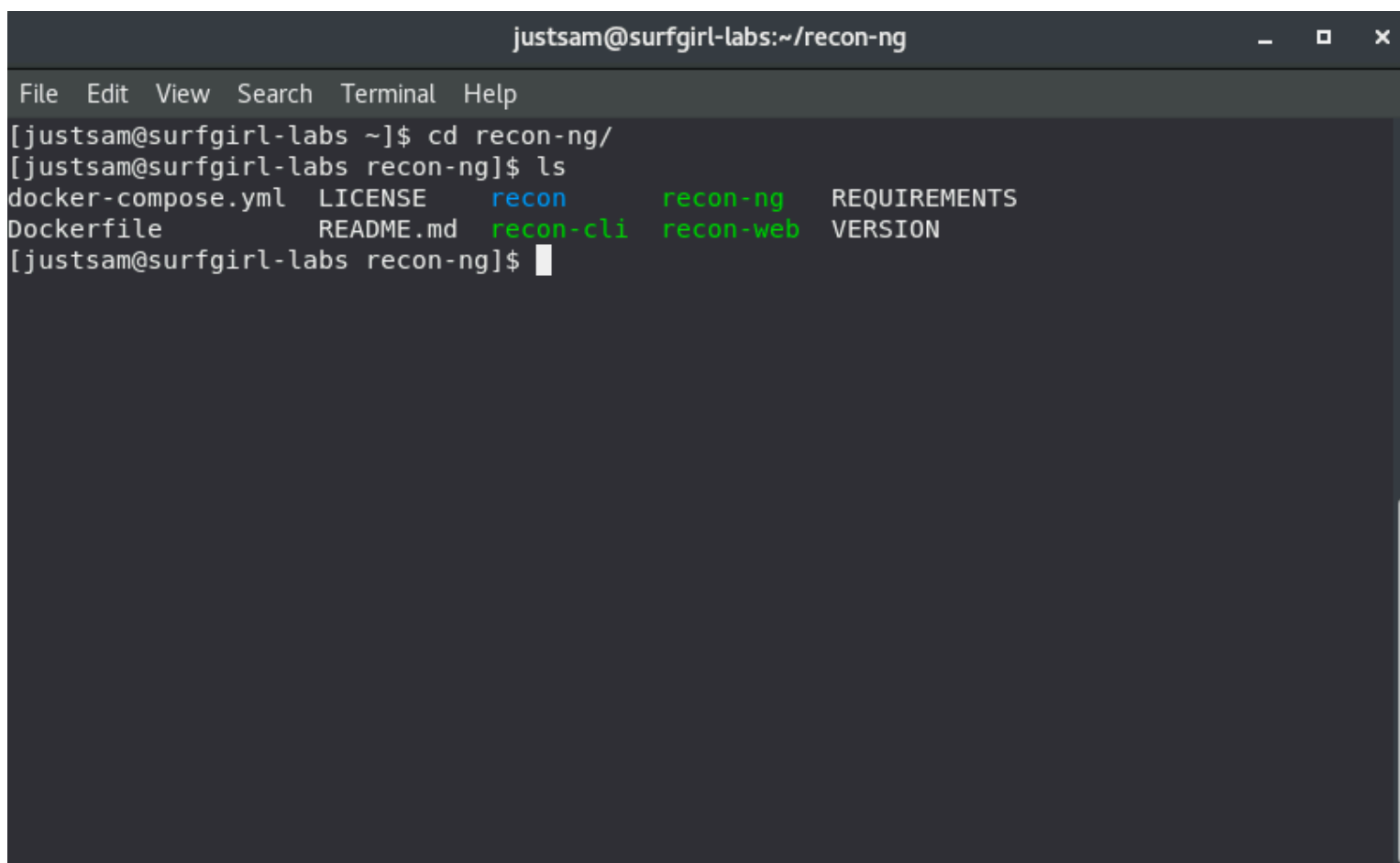
For this walkthrough, I will be using Alma Linux, because recon-ng is not installed by default. I will put a resource to Alma Linux in the link section just in case you want to check out Alma Linux for yourself.



```
justsam@surfgirl-labs:~  
File Edit View Search Terminal Help  
[justsam@surfgirl-labs ~]$ git clone https://github.com/lanmaster53/recon-ng.git
```

We use the following command to obtain the framework from the project site:

`"git clone https://github.com/lanmaster53/recon-ng.git"`.



```
justsam@surfgirl-labs:~/recon-ng  
File Edit View Search Terminal Help  
[justsam@surfgirl-labs ~]$ cd recon-ng/  
[justsam@surfgirl-labs recon-ng]$ ls  
docker-compose.yml  LICENSE      recon      recon-ng  REQUIREMENTS  
Dockerfile          README.md   recon-cli  recon-web  VERSION  
[justsam@surfgirl-labs recon-ng]$
```

Next we “cd” into the directory to continue.

Then we execute the following command to start the framework “./recon-ng”. When we do this, we are greeted with a successful start screen. You will notice that there are currently no modules installed by default. We will cover that in the next step.

AUTORECON: YOUR NETWORK RECONNAISSANCE GATHERING AUTOMATION TOOL





GREG THOMAS

Product Security Expert
Intel Corporation

Greg Thomas is a security researcher for Intel Corporation. Greg joined Intel in 2004 as a Software Validation Engineer, to validate cryptographic accelerators. In 2011, he started to work on security validation and lead teams through the Security Development Lifecycle (SDL). Greg introduced methods of threat modelling and fuzzing to project teams by establishing a training program to help spread knowledge across the organisation. In 2018 Greg moved to his current role and provides guidance to project teams on SDL. In 2021 Greg successfully obtained OSCP certification, and earlier this year he established a process for red teaming to perform security assessments across a range of different projects in the organisation.

INTRODUCTION

With the ever-increasing spread of networked devices in our society, the ability to automate reconnaissance gathering helps make efficient use of a penetration tester's time. Proper target enumeration is the key to a successful penetration test. This article introduces a very useful tool called AutoRecon that does a lot of that work for you.

AutoRecon as the name implies, is an automated network service enumeration tool based on Python that, at its heart, automates the process of running Nmap and then takes this one step further by running specific tools against specific services. AutoRecon is open source and free to use. The results are all gathered under a folder on your attack machine. From here you can find all the commands used for each tool, the results, and screenshots, which can be used in reports or to re-run specific commands if needed.

This article is a beginner's guide on getting started with AutoRecon; there are many options available that won't be discussed and are left to the reader to try out in their own time

INSTALLING

AutoRecon can be found here:

<https://github.com/Tib3rius/AutoRecon>

The instructions in this document were tested on Kali 2021-4a released Dec 2021.

If you are behind a proxy you will need to set the apt proxy. Create the file:

```
/etc/apt/apt.conf.d/proxy.conf
```

and add the lines as shown in Figure1, replacing {host} and {port} with your own settings:

```
Acquire::http::Proxy " http://{host}:{port}";  
  
Acquire::https::Proxy " http://{host}:{port}";
```

Figure 1. Kali Linux apt proxy settings

Then you can install Python 3.7+ and pip as shown in Figure2:

**HOLEHE -
EFFICIENTLY
FINDING
REGISTERED
ACCOUNTS
FROM EMAILS**





JEFF MINAKATA

Trained in CEH8 and CEH9, CISP, Metasploit certified, Accredited Configuration Engineer (ACE), MCSI OSINT Practitioner, and CWA certified. Over 20 years' experience in the IT industry. Online instructor for OSINT, ethical hacking, and network security. Has contracted courses for EC-Council and has written articles for Hakin9 and eForensics magazines. keyboardkomando@tutanota.com

In this article, we will be taking a look at the program HOLEHE and installing it on our Kali Linux computer. HOLEHE is an easy-to-use Python3 program that will take an email address and allow us to quickly and easily check if that email was



used on over 120 different sites. HOLEHE does this by retrieving the information from the forgotten password function. Fortunately, the program does not alert the user. This makes it an incredibly useful tool when it comes to reconnaissance and OSINT. As a penetration tester, or an OSINT investigator, having this information allows us to pivot from those accounts (collect information from those

particular accounts, look for data leaks for those particular accounts, etc.). Let's take a look at how to install the program and run it.

With PyPI

```
pip3 install holehe
```

With Github

```
git clone https://github.com/megadose/holehe.git
cd holehe/
python3 setup.py install
```

For the installation, you can install it with PyPI (if installed) or through the git clone command (which we will be using for this tutorial).

```
(kali@kali)-[~]
$ git clone https://github.com/megadose/holehe.git
```

To install HOLEHE, open your terminal and type the following:

```
git clone https://github.com/megadose/holehe.git.
```

With this command, the program will be downloaded to the root of your Kali Linux.

```
(kali@kali)-[~]
$ cd holehe
```

It should take less than a minute to download the program (depending on your internet connection). Next, we will want to

AN INTRODUCTION TO SQLMAP





JOMON THOMAS LOBO

Jomon Thomas Lobo is a web developer with more than 6+ years of experience from India. He is a cyber security enthusiast and who has reported vulnerabilities in various web applications.

JOMON THOMAS LOBO

me@jomonlobo.online

This tutorial is intended for cyber security beginners with basic knowledge of SQL and Web Application working. This tutorial intends to give a basic understanding of how to perform an SQL Injection attack using SQLMap. As an example, I will provide the step by step process of SQL Injection using a query string.

SQL INJECTION

SQL Injection is a web application vulnerability that occurs when a user inputs an SQL string instead of the intended value and that is executed in the database. In other words, SQL Injection is an attack that occurs when a malicious user injects a SQL Query with a destructive intention.

SQLMAP

SQLMap is an open source SQL Injection and database take over tool written in Python. SQLMap works by injecting a malicious SQL script to a Query String, API Endpoint or form data.

SQLMap getting started

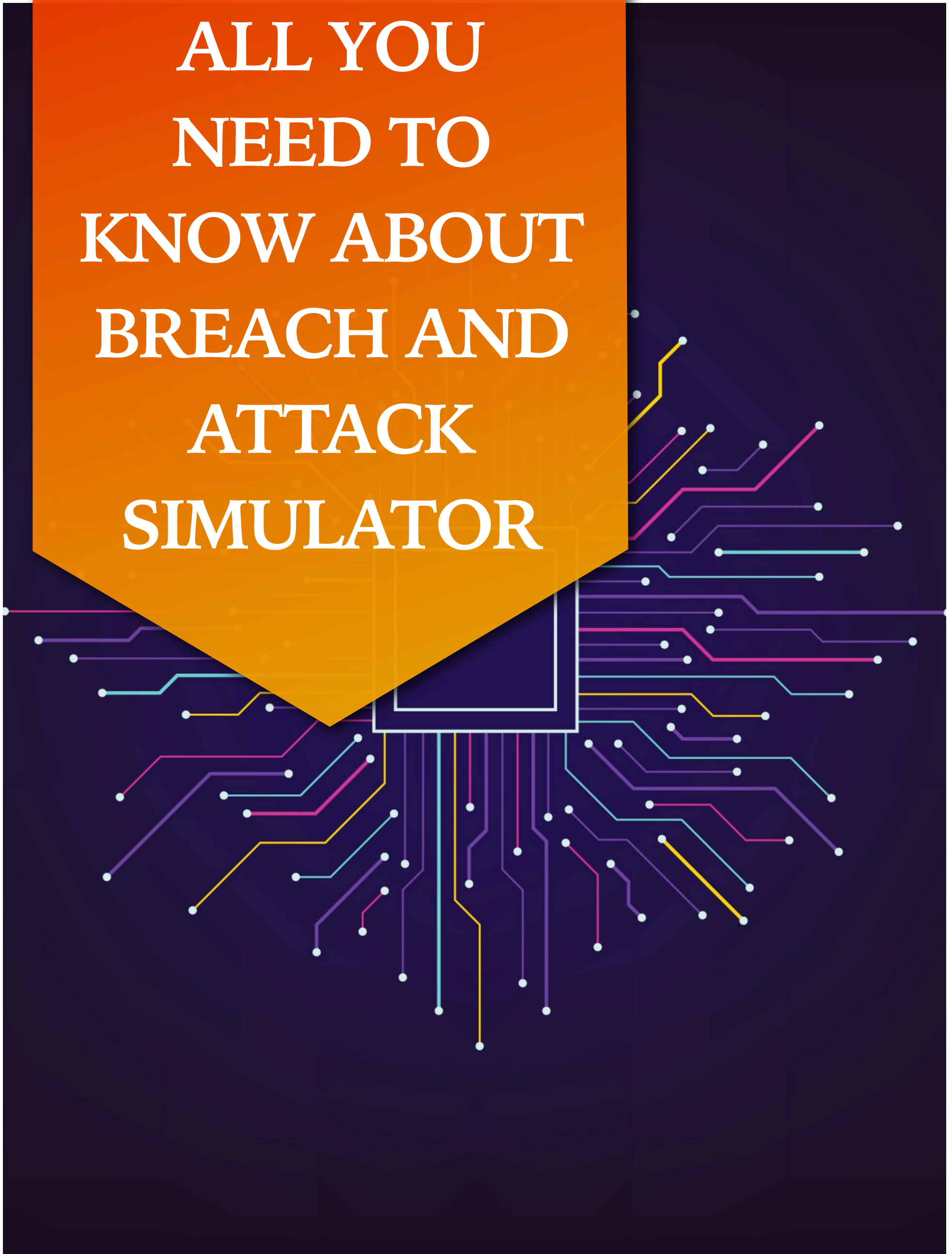
SQLMap is available by default in operating systems especially built for pen testing. For example, in *Kali*, you just need to type *sqlmap* but if you have cloned from the **GitHub** repository, you need to install **Python** in the machine and prefix *python sqlmap.py* to execute the SQLMap.

For cloning the SQLMap repository from the GitHub repository, run the following command *git clone <https://github.com/sqlmapproject/sqlmap.git>*

SQLMap Common Options

Important options in the SQLMap application are listed below:

ALL YOU NEED TO KNOW ABOUT BREACH AND ATTACK SIMULATOR





JESUS GARCIA

CTO and rThreat Creator

Offensive security speaker, validation malware writer, currently responsible for rThreat's technology roadmap and creator of new features for this platform.

INTRODUCTION

Following the development of the "Zero Trust" security model in recent years, methods for validating the success of cybersecurity processes have grown. Naturally, this has led to more discussion of what differing validation approaches truly show, resulting in comparisons of the automation of validation processes versus human actions, controlled simulation versus a real attack, and the proliferation of continuous validation solutions versus point-in-time validation testing.

The purpose of this article is to explore some aspects of Breach & Attack Simulation (BAS) solutions that are overlooked, or perhaps underexplained, by many of their vendors. To make an accurate decision when purchasing this type of security solution, it is important to know these aspects to ensure that you are getting the most value and security from your validation processes.

Let's begin by defining what BAS is - BAS systems can continuously simulate or emulate, validate, and, in some cases, even remedy cyber-attack paths, at any time of day, any day of the week. Many BAS solutions in the market today also claim to have precise information on the behavior of advanced persistent threats (APT) used by today's threat actors, as well as the tactics, techniques, and procedures (TTPs) that characterize them. If we consider this to be true, that BAS manufacturers actually have this information, either from their own research groups or from third parties (such as a cyber threat intelligence subscription), then these BAS platforms would appear to be quite the impressive solutions. They purport to simulate an advanced attack, using the exact TTPs, and the appropriate malware is implemented across the most important attack vectors: network, endpoint, and email.

Already, some initial questions will naturally arise. If it is a simulation, how do they simulate a complex and orchestrated attack through all of its phases? How can they certify that the attacks reflect current TTPs, and are still worth testing? If an attack methodology is placed in the BAS for validation use, how can you know if it reflects those found in use in the wild? These can be very uncomfortable questions for manufacturers of this type of technology.

Next, we'll classify the four types of BAS according to their design and describe their basic outcomes:

Agent-Based

These BAS solutions utilize software agents that are deployed within an organization's LAN across multiple machines (PCs, VMs and physical servers), typically on different VLANs to test different postures across the organization. Using a database of known vulnerabilities and common malware, they scan the different endpoints, performing a simple vulnerability analysis on the current defense. At the end of the test, exposed machines are then mapped, including a potential attack path between them that could be exploited by a threat agent.

Traffic-Based

Traffic-based BAS solutions target the network security solutions of an organization. This is achieved by generating malicious traffic within the internal network and configuring virtual machines provided by the BAS manufacturer to serve

SYN FLOOD ATTACK LAUNCHED THROUGH METASPLOIT

```
File file = new File("C:\\temp\\file.txt");  
//check first if supplied file name is a folder  
if(file.isDirectory())  
    Get listFile = new ArrayList<>();  
listFile = Arrays.asList(file.listFiles(new FileFilter() {  
    @Override
```

VINESHA SELVARAJAH

Vinesha Selvarajah completed her PhD in 2020 at Monash University, Malaysia. She is also a Rochester Certified Trainer as of 2019 with both RCCE 1 and RCCE 2 certified cyber security engineer. In 2014, she received funding from the Japanese Government to pursue her Master's Research in Informatics (Information Security) at Kyushu University, Japan under the supervision of Professor Dr. Kouichi Sakurai. She was also appointed as a Special Research Assistant at the Institute of Systems, Technologies, and Nanotechnologies (ISIT), Japan during her candidature in Kyushu University. The same year before leaving Japan, she received her BSc (First class Honors) in Information Technology with specialism in Forensic Computing under the supervision of Dr. Mueen Uddin at Asia Pacific University of Innovation and Technology (APIIT), Malaysia.

There are many different types of Denial of Service attacks like Ping flood attack and ICMP flood attack, but this case study is about Denial of Service SYN flood attack that floods the victim machine with SYN packets and causes the victim machine's performance to become slower. In this case study, the Kali Linux machine is used as a virtual machine and acts as an attacker that attacks the victim machine, and the victim machine is using Windows 2008. Kali Linux is a well-known operating system used by unethical and ethical hackers out there performing their hacks to the victim or performing pen-testing. And there is a tool that used in Kali Linux to perform the SYN flood attack; the tool is Metasploit framework, which is also a well-known penetration testing framework that is currently used by all professional ethical hackers and also the unethical hackers because it is easier to use and it is a command-line interface, which is more professional compared to the tools that have a graphical user interface. Hackers can easily launch the SYN flood attack if the hackers know the IP address of the victim machine and send all the SYN packets to the victim machine to jam the victim machine.

1. INTRODUCTION

In this case study, the attack is a Denial-of-Service attack from Kali Linux, which is also a virtual machine, to make the target machine, which is a Windows 2008 virtual machine, become slow and lag by sending a lot of SYN packets to flood the target machine. This is also known as SYN flood. What is a SYN flood? It is a type of Denial-of-Service (DoS) attack that can slow a machine or a server, by non-stop sending SYN packets. By doing so, the attacker that launches this attack can overwhelm all the ports that are available on the target server machine [8-13].

There are a few types of Denial of Service (DoS) attacks and SYN flood Denial of Service (DoS) is just one of them. Other than SYN flood attacks, ICMP flood, also known as Ping flood, is also one of the common Denial of Service (DoS) attacks. ICMP flood attack is usually used by the cybercriminals or hackers to overwhelm the victim's machine by sending lots of ICMP echo requests, and this is the purpose of ICMP flood attack, it floods the victim's network with tons of request packets because the network will only able to respond to a certain number of reply packets, but it will overwhelm the system when there are tons of request packets suddenly coming in. Other than that, there are a few ways of launching ICMP flood attack by using the code or some tools which are hping and scapy. Hping is a TCP and IP packet assembler and analyzer using command line orientation [2]. Other than sending ICMP echo requests, hping can also be used to test firewalls, it performs very well in port scanning too, and it is a very good and useful tool for the students who are learning TCP/IP and many more [2]. Hping can support more than two operating systems, including Linux, Windows, Solaris, FreeBSD, NetBSD, MacOS X and OpenBSD [2]. Other than hping, Scapy is also a good tool, Scapy is a very strong interactive packet manipulation program [7]. It can do scanning, probing, tracerouting, attacking and many more. It can do many actions that others can't do, such as sending frames that are not available, injecting our own 802.11 frames and many more [7].

Other than that, Ping of Death, also known as (POD), is also one of the Denial of Service (DoS) attacks. How does Ping of Death (POD) work? The purpose of Ping of Death (POD) is to crash or even freeze the victim's machine or server by way of sending overcapacity or abnormal packets just by typing a ping command [6]. Ping of Death (POD) is an older version of the ping flood attack. In the old days when computers were not as advanced as today, the old version of computers couldn't handle large packets, and when one of the computers received one of the big-sized packets, the computer would crash. Besides, sending a ping packet is already larger than 65,535 bytes; it is already against the Internet Protocol. Because of this

PENETRATION TESTING USING METASPLOIT FRAMEWORK



SAJU MOHANAN

A highly professional academician and full stack web developer with an ability to work independently and as part of a team in a dynamic multitasking environment. Having a strong career vision, delivery focus and active commitment to continuous improvement and quality standards. Passionate in developing interactive web applications using client and server side technologies. Capable of training and coordinating a professional group, a self-learner and always up-to-date with latest technologies. Fourteen years of work experience in universities and higher educational institutions.

The need to ensure confidentiality has expanded exponentially with the increase of recent Internet usage. For users and enterprises, the reliability and accessibility of their networks have become critical, and the development of secure infrastructure to protect user identity and privacy information is crucial. Internet development and popularity have generated many issues such as cyber theft, hacking, phishing, spamming and many more. Individuals and companies have migrated their data to a cloud architecture that poses new data protection issues and threats. According to the Cybersecurity Ventures survey, cybercrime exposure could cost 6 trillion dollars a year worldwide by the end of 2021. Ethical Hacking enables consumers and companies to investigate the vulnerability in their infrastructure and of their network to take appropriate steps to secure their networks and systems from illegal and malicious attacks. It further protects networks and processes by recognizing common vulnerabilities and enabling them to take appropriate safeguards. In the research paper, we have discussed the Ethical Hacking and Penetration Testing process and practical experiments to brief fresh researchers and students on the deployment and use of the Metasploit framework as a student-centred learning approach. We have performed both server-side and client-side exploitations to understand the process. We have used the Kali Linux Operating System (OS) tool to complete these ethical hacking and penetration testing. In the end, we have proposed mitigation measures and security enhancement to resist hacking attacks.

INTRODUCTION

Cybercrimes on the Internet are increasing exponentially. The recent attacks using network flaws and vulnerability loopholes exploitation have become serious issues for the end-users and businesses. Data privacy and network safety of Internet users have become critical fields of distress. Network security scientists and engineers focus on developing robust architectures and solutions to secure networks, platforms, and software from illegitimate hacking, although in this developed era, current security infrastructure offers some degree of protection. Therefore, the fundamental safety directives must be understood by businesses and individuals to resist these assaults.

The Internet has been a requirement in every field of life due to its usability. As an Internet user carries out an operation, it increases the chance of criminals using personal data in identity fraud. The company and the client should ensure that these events do not arise often and that their networks are secure. The websites and systems contain sensitive information such as financial records, users' details, and other confidential information protected with suitable policies. When designing a secure network infrastructure, three criteria must be considered: confidentiality, integrity, and availability [1].

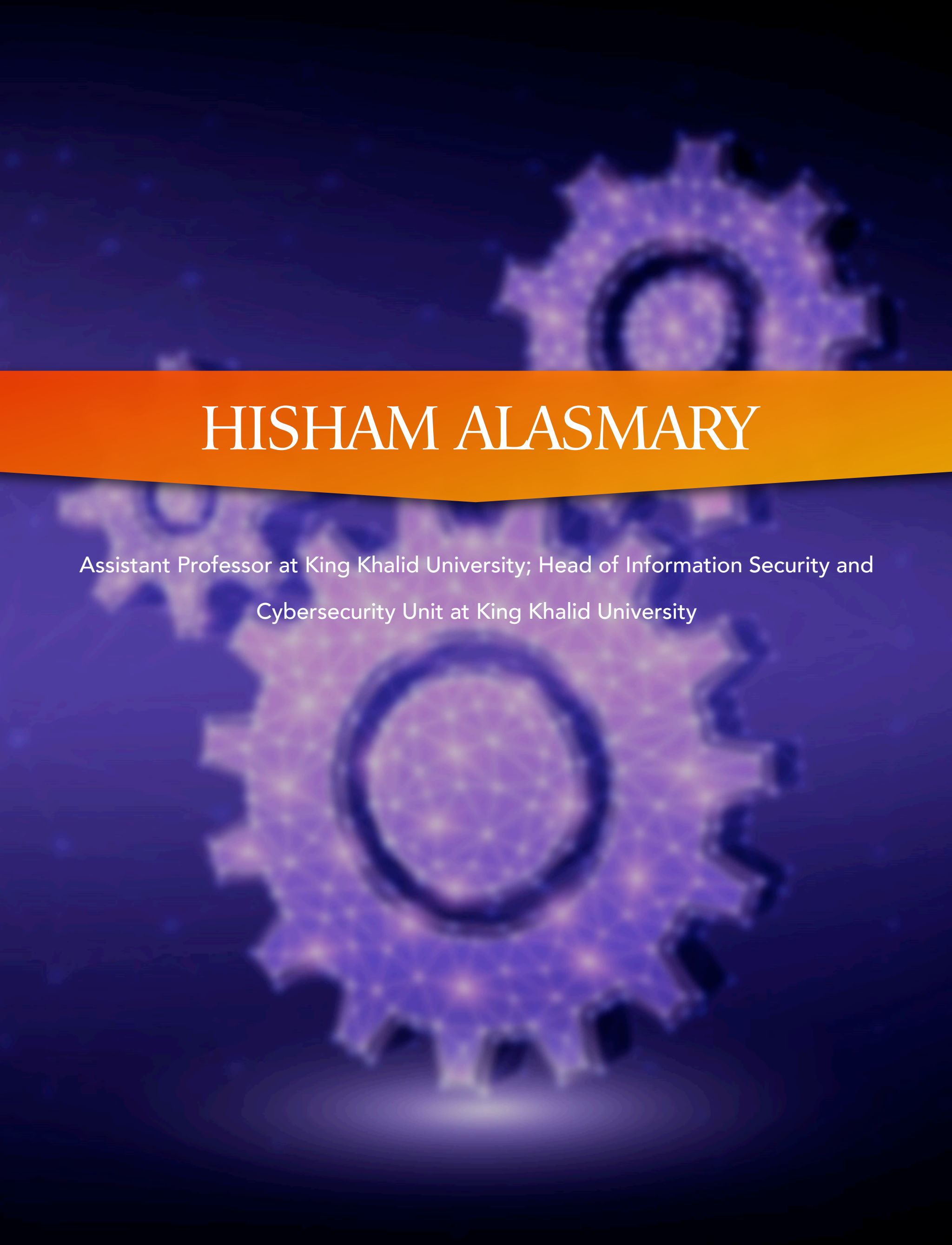
Attackers have several ways to exploit any network and obtain private information. By hacking a web portal or device, they may destroy the network and interrupt the application services. The appropriate network firewall, protection protocols and equipment must also be enforced and tracked carefully.

Many firms, such as Google, Banking and Microsoft, are encouraging Ethical Hacking to address their network flaws and offer the ethics hacker big prize money. In addition, many network consultants are available to analyze the network flaws of organizations and provide them with best practices and recommendations for improved network and asset protection.

Kali Linux is a reliable tool that can be used to examine networks, systems, and application vulnerabilities [2]. This paper has used Kali to perform Metasploit-related experiments on a preconfigured network and procedures as part of Ethical

UNDERSTANDING INTERNET OF THINGS MALWARE





HISHAM ALASMARY

Assistant Professor at King Khalid University; Head of Information Security and
Cybersecurity Unit at King Khalid University

The lack of security measures among the Internet of Things (IoT) devices and their persistent online connection gives adversaries a prime opportunity to target them or even abuse them as intermediary targets in larger attacks, such as distributed denial-of-service (DDoS) campaigns. In this paper, we analyze IoT malware and focus on the endpoints reachable on the public Internet that play an essential part in the IoT malware ecosystem. Namely, we analyze endpoints acting as dropzones and their targets to gain insights into the underlying dynamics in this ecosystem, such as the affinity between the dropzones and their target IP addresses, and the different patterns among endpoints. Towards this goal, we reverse-engineer 2,423 IoT malware samples and extract strings from them to obtain IP addresses. We further gather information about these endpoints from public Internet-wide scanners, such as Shodan and Censys. For the masked IP addresses, we examine the Classless Inter-Domain Routing (CIDR) networks accumulating to more than 100 million ($\approx 78.2\%$ of total active public IPv4 addresses) endpoints. Our investigation from four different perspectives provides profound insights into the role of endpoints in IoT malware attacks, which deepens our understanding of IoT malware ecosystems and can assist future defenses.

1. INTRODUCTION

The Internet of Things (IoT) has reshaped the way in which people, businesses, and even cities interact with their environment through Internet-connected devices. There is no doubt that IoT devices have benefited the global economy and made our lives more efficient. With the number of IoT devices soaring into the tens of billions [30], the potential adversaries have set their sights on these devices knowing that they are always connected. To this end, malicious code that targets IoT devices is on the rise that infects the device itself and receives code updates from dropzones around the world. Acting as intermediate nodes, these infected devices have the potential to launch attacks on other targets to form a massive distributed denial-of-service (DDoS) attack [38, 41, 46, 48]. Moreover, the majority of these IoT devices are at a high risk to the new threats due to the lack of security awareness among consumers and the lack of consensus on security standards among the IoT industry [49, 58].

Bastys et al. [24] demonstrate that popular IoT app platforms are susceptible to attacks by malicious applet makers. With less than half of consumers changing default passwords on their IoT devices [33], it is no surprise that malware like Mirai has been able to amass a large botnet to launch massive DDoS attacks by simply using a dictionary of common IoT login credentials [22]. Compared to traditional hardware with operating systems with automated updates, IoT devices tend to have slower patch times and insecure communication [26]. It makes them “ideal targets” for additional attacks like the Key Reinstallation Attack (KRACK) exploit [50]. It abuses design flaws in cryptographic Wi-Fi handshakes to reinstall existing keys, which allows attackers to eavesdrop on network traffic or even inject malicious content [67].

Alrawi et al. [19, 20] revisited the literature and evaluated security of IoT devices and software, unveiling various outstanding issues in the existing ecosystem that could be resolved with existing solutions. With the proliferation of IoT devices in today’s world, we even see decades-old attacks resurface to take advantage of vulnerable IoT devices [20]. For example, the SSHoWDoWN Proxy attack discovered by Akamai [32] utilizes a 12-year old vulnerability in OpenSSH to effectively take over the device to remotely generate attack traffic.