hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.17, NO.06

BEST HACKING TUTORIALS IN 2022

Wi-Fi Hacking

OSINT Tools for Hackers

Hacking Smart Devices

Phishing Techniques

AND MORE...

Hakin9

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor

Marta Sienicka
sienicka.marta@hakin9.com

Editors:

Marta Strzelec
marta.strzelec@eforensicsmag.com

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

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.

Betatesters & Proofreaders

Lee McKenzie

Hammad Arshed

Avi Benchimol

Amit Chugh

Kevin Goosie

Craig Thornton

Paul Mellen

Daniel W. Dieterle

Alex Giles

Filipi Pires

Matthew Sabin

Jonathan Ringler

Gregory Chrysanthou

Alexandre D'Hondt

Steve Hodge

Shanika B

David Molik

Gilles Lami

Girshel Chokhonelidze

Dear readers,

We would like to present you with a special edition of Hakin9 - we gathered our best 20 hacking tutorials from last year in one place. The articles are focused on different topics such as Mobile hacking, attacking smart devices, phishing campaigns, Wi-Fi hacking, OSINT tools in practice and many more. Inside you will find more than 200 pages of “how-to” and “step-by-step” tutorials that will surely contribute to your development as a professional pentester or ethical hacker.

Stay safe and enjoy!

Magdalena Jarzębska and Hakin9 Editorial Team

Contents



Stealth Chained WiFi Attacks

by Roberto Camerinesi



How Social Networks Are Directly Connected With The Improper Application of Social Engineering

by Felipe Hifram



Lightning Fast Profile Lookups Using NExfil

by Lohitya Pushkar



Twitter OSINT Using Tinfoleak and Reverse Imaging

by Jeff Minakata

Contents



Hacking IoT with IoT

by Daniel W. Dieterle



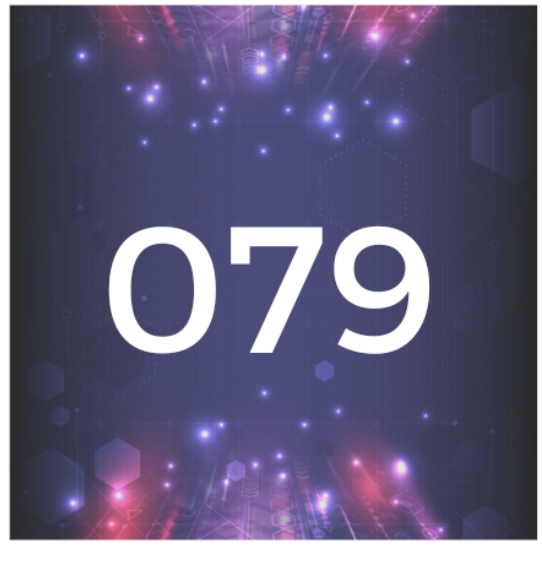
Red Teaming via ICS and SCADA Adversary Tactics

by Alexandros Pappas



Automating the Mitre Att&ck with Python

by Bruno Rodrigues



Manual Pentesting? Automate it with Metasploit Framework!

by Thomas Moosmüller

Contents



Build your own Brute Force Tool

by Daniel García Baameiro



Crawling Websites Using Burp Suite

by Mayukh Paul



Solving an Expert Lab from Web Security Academy

by Michael Sommer



Hacking Techniques for Beginners: How to get the Control of a System

by Verónica Berenguer Garrido

Contents



Nmap, The Perfect Tool

by Daniel García Baameiro



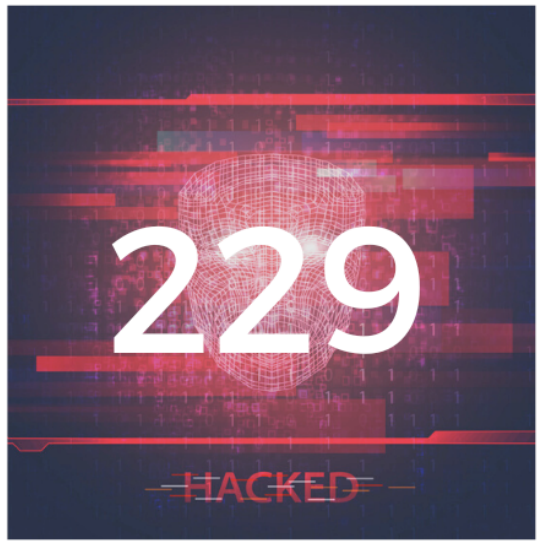
Kali NetHunter - For Those That Have a Fear of Commitment

by Atlas Stark



Intercepting Data via iPhone

by Jordan Bonagura



Phishing Using NexPhisher

by Mayukh Paul

Contents



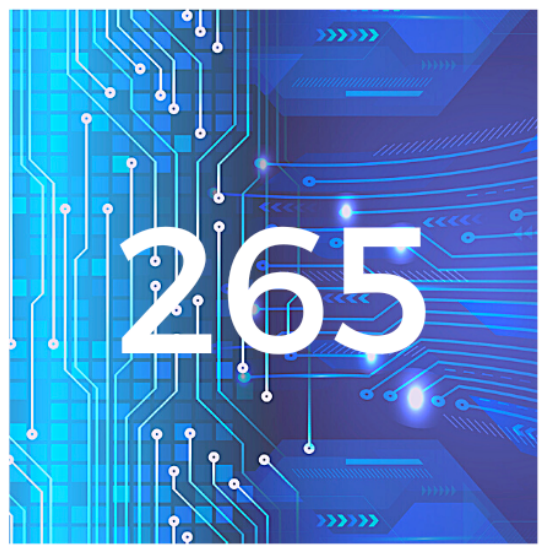
SMISHING - Phishing Attacks Through Messages

by Cleber Soares, Deivison Franco



Project Indigo Brick. New Pathways in Data Handling

by Atlas Stark



Rogue - Hackers, RAT and "Marketing" on the Dark Web

by Felipe Hifram



Securing The Supply Chain

by Syed Peer

STEALTH CHAINED WIFI ATTACKS





ROBERTO CAMERINESI

Roberto Camerinesi is a computer security researcher and developer.

Embracing the philosophies of ethical hacking since adolescence, he has been working for over 11 years in the ICT and security industry.Today he is CTO of Cyber Evolution, working specifically on cyber security in IoT and In- dustrial environment.

He believes that security should be a concept that accompanies digitization, so he spreads and studies systems to capillarize security, inventing and pat- enting air-gap defense systems.

"Obtain persistence without leaving traces."

Greetings readers,

Wireless has revolutionized the way we can be connected, opening the way to countless application fields.

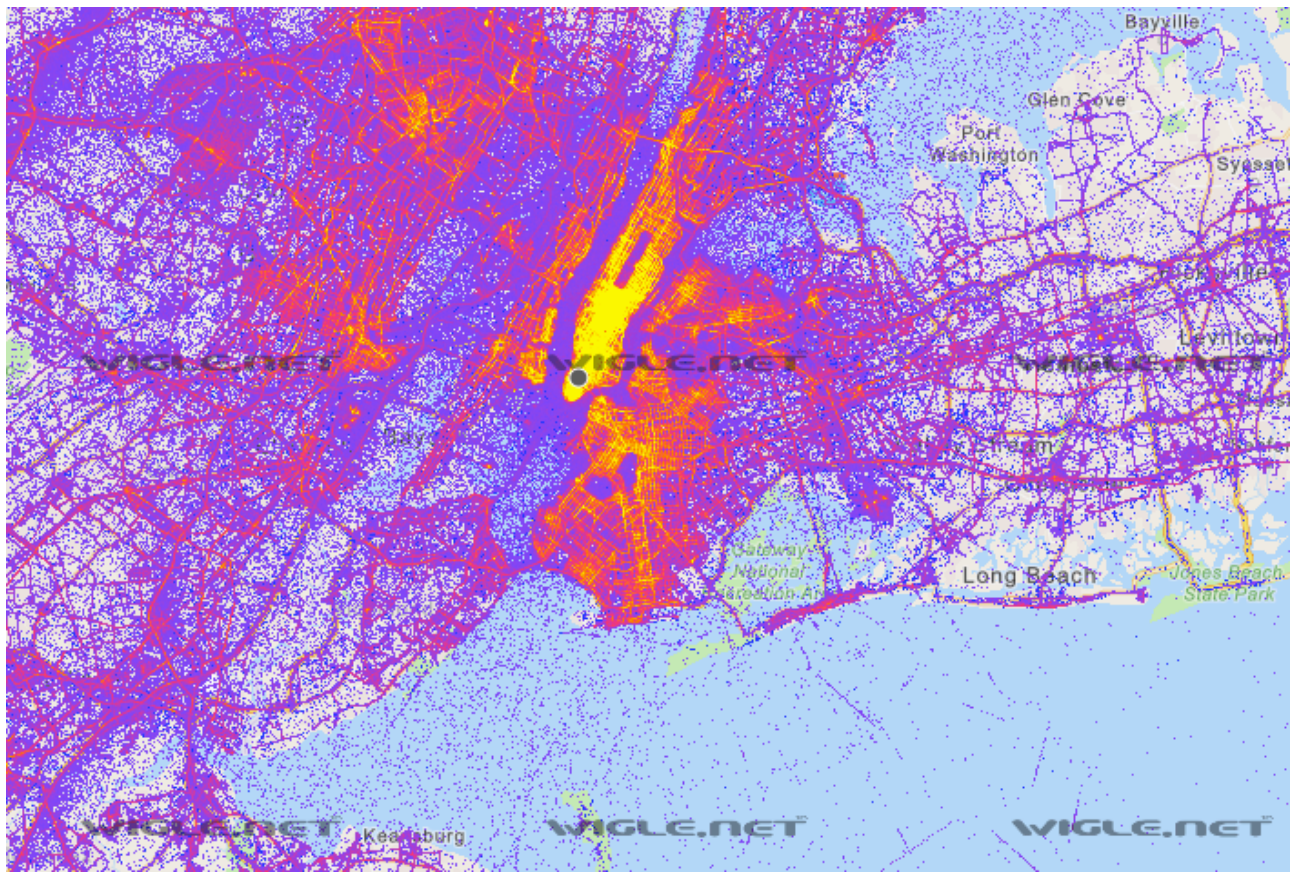
We find it, in fact, from home networks to public networks but not only; it is used in companies supporting the BYOD (Bring Your Own Device) model and working methods and today it is coming in Industry 4.0 and sensor networks.

An important note deserves to be mentioned, that of IoT and automotive. The exponential growth of these two sectors has given a boost to wireless networks, connecting all kinds of devices, from smart TVs to automatic opening garages.

Born in Hawaii in 1971 with the Alohanet project and then became an IEEE standard around 1997 with 802.11a. The wave frequency used for communication was initially equal to 2.4Ghz, well above 4G - today's cellular connections, for example, which work at about 2.6Mhz, but then, obviously over time, the standard 802.11 has evolved, with important breakthroughs such as the implantation of MIMO technology, which allows you to expand "physically" the band using multiple antennas and multiple receivers and the support of 5Ghz (as before it was reserved for some use and in some specific country).

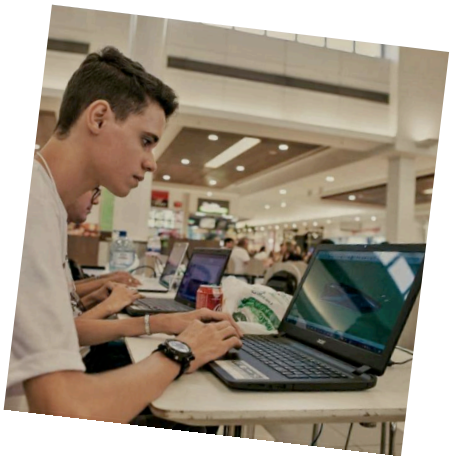
All the implementations and improvements that concern the transmission of wireless networks are collected in nomenclature instead of using IEEE acronyms. Today we are in fact in the Wi-Fi 6 standard and we are going towards Wi-Fi 7, always with more bandwidth, optimized consumption and performance in terms of latency and security.

In short, its use and continuous evolution does not stop, considering that today there are estimated to be over 500 million hotspots in the world. The capillarity is disarming as reported by WiGLE (https://wigle.net/) in the single portion of New York:



HOW SOCIAL NETWORKS ARE DIRECTLY CONNECTED WITH THE IMPROPER APPLICATION OF SOCIAL ENGINEERING





FELIPE HIFRAM

He is currently an information security professional focused on habits of good use and privacy on the Internet. He has done work for companies in Brazil, Ukraine, Oman and Bahrain, in addition to writing several other articles.

"Privacy for the weak, transparency for the powerful!"

(Julian Assange)

SOCIAL ENGINEERING, A BRIEF INTRODUCTION

At some point in your life, when checking your emails, you came across "your bank" asking you to reset your account password, or perhaps, some raffle result where you would have been the winner...

These and similar cases are already well known (although they still work), what really matters here is the root of this type of attack, the purpose of inducing people to provide data and information. An attack that affects ordinary people and even large corporations.

Social Engineering is defined by attacks that dispense with the use of technologies, focusing only on obtaining, through the lack of security policies of a company, valuable information, usually commercial.

SOCIAL NETWORKS, A DOOR TO SCAMS

Imagine yourself as a developer for a large technology company, you are currently working on a new project that promises to revolutionize your company's niche.

On a Friday, after work, you decide to go to a bar for a cold beer and rest from the busy week in your leisure time, until you are interrupted by someone who claims to have recognized you through Facebook or Instagram and who characterizes your job as “how incredible”. You automatically, like most people, find this interesting (after all, it's a compliment) and allow that person to come closer.

"Today with social networks, people tend to be more easily manipulated, through a common weakness, vanity."

Returning to your character... The person you know presents himself as a professional in his area, demonstrating in-depth knowledge in defense of what he says, and here you already established a bond by professional affinity. *"Usually, social engineers - very good at manipulation - can guide the conversation to get the information they are looking for, making it seem natural."*

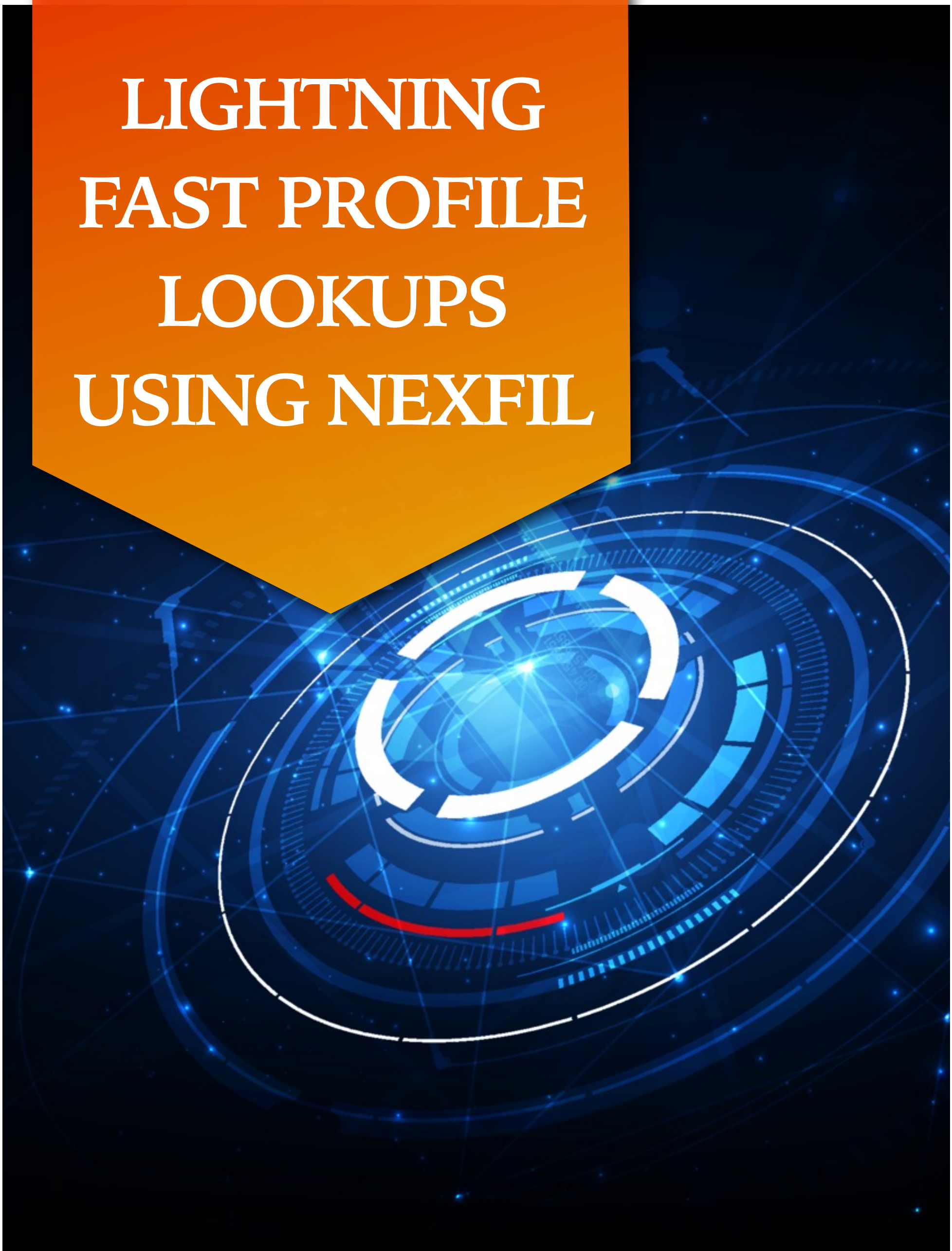
As a result of the ingenious gift of the manipulator, you want to impress him even more, and show him how amazing you and your work are. Then comes the moment when the attacker asks, in a harmless tone: *"But then, what are you working with at the moment?"*

At this point, by revealing details of the project you're working on, you put the company you work in at risk, revealing business information that can easily now be sold to competing companies, which could result in financial losses for yours.

To give an example of the consequences and facilitate understanding of the problem, I will create an assumption:

Today Apple has its Chip M1 [an entire system, in addition to just processing, is included in it], currently used in its MacBook; the launch of this technology revolutionized the market, making its products much more attractive.

LIGHTNING FAST PROFILE LOOKUPS USING NEXFIL





LOHITYA PUSHKAR (THEWHITEH4T)

Security Assessment Engineer and Community lead at The White Circle. I have created multiple open source tools for the infosec community. You can find my projects on GitHub. Please give them a star if you like my work. I am currently learning and practicing Red Teaming, Network Penetration Testing and OSINT.

Blog : https://thewhiteh4t.github.io

GitHub : https://github.com/thewhiteh4t

Twitter : https://twitter.com/thewhiteh4t

LinkedIn : https://www.linkedin.com/in/lohityapushkar

Discord : https://discord.gg/UM92zUn

In this day and age, the internet is widely populated with social media platforms. Some are well known and used by the majority of the people; meanwhile, some have lost interest of people as they move to newer platforms, and there are new platforms being launched every year. During OSINT investigations, usernames are like seeds from which new branches open up in an investigation and we can get loads of information. All these platforms help in their own way, each platform is capable of displaying something that might help an investigator. Some show joining dates while others can reveal birthdays. We can check five or ten websites manually but after a certain point it becomes repetitive and exhaustive. I believe that OSINT investigations are best done manually but I also believe that tools can give us an edge. Tools can automate the workflow and greatly reduce the time of certain tasks such as user profile lookups on a given username. If you have performed profile lookups before then I am sure you will be aware of some existing tools for the same. Some honorable mentions are instantusername.com and sherlock. Profile lookup tools are available on both websites as well as command line tools. I personally prefer and recommend command line tools due to the fact that they offer more control over the tool.

WHAT IS NEXFIL?

NExfil is a new free and open source profile lookup tool written in Python. The goal of NExfil is to fetch accurate results quickly, which means low amounts of false positives in a short amount of time. It comes loaded with over 350 social media platforms, which can be expanded. Most of the popular social media platforms have been added and tested for accurate results. The nature of the tool is modular so it is very simple to add new modules or new websites to the pool for going beyond the current count.

WHY I CREATED NEXFIL

I play a lot of capture the flag competitions to practice my cyber security skills and to gain more knowledge. Fortunately, new CTF competitions are acknowledging OSINT and have started including it as a category of its own. This is great because now we can practice our OSINT skills as well, and so far in each competition, I found myself using some sort of profile lookup tool, mostly the ones I mentioned before, i.e. instantusername.com and sherlock. If you have been using them then you know there are certain issues with both. Let's talk about instantusername first. It sticks to its name and it is very fast, which is great, but it has support for about 100 social media platforms, which is decent, but then comes the major issue of false positives. CTFs have a time limitation and the way the challenges are created, we end up finding a needle in a haystack. False positives really pull us back from reaching the goal because it increases the time and effort we put into checking the results. Eventually, I switched over to sherlock. One major benefit of command line tools is that the tools are immediately accessible, you don't need to open some GUI application or browse to some website, which is why I prefer most of my tools in command line mode instead of a graphical user interface. Sherlock is a very popular tool but it has its own set of issues. It is actually slow, which is again not what we want and it has the same major flaw like instantusername.com, it has lots of false positives and it does not depend on the username you input, you can input any random non existent username and it will show you results, which obviously do not exist.

```
twh ~
❯ time sherlock kjnwkqne314bh
[*] Checking username kjnwkqne314bh on:
[+] AllTrails: https://www.alltrails.com/members/kjnwkqne314bh
[+] Anobii: https://www.anobii.com/kjnwkqne314bh/profile
[+] Cent: https://beta.cent.co/@kjnwkqne314bh
[+] Chess: https://www.chess.com/member/kjnwkqne314bh
[+] NameMC (Minecraft.net skins): https://namemc.com/profile/kjnwkqne314bh
[+] ProductHunt: https://www.producthunt.com/@kjnwkqne314bh
[+] Steamid: https://steamid.uk/profile/kjnwkqne314bh
[+] Twitter: https://mobile.twitter.com/kjnwkqne314bh
Traceback (most recent call last):
  File "/usr/share/sherlock/sherlock/sherlock.py", line 675, in <module>
    main()
  File "/usr/share/sherlock/sherlock/sherlock.py", line 630, in main
    with open(result_file, "w", encoding="utf-8") as file:
PermissionError: [Errno 13] Permission denied: 'kjnwkqne314bh.txt'
sherlock kjnwkqne314bh  11.61s user 0.57s system 8% cpu 2:16.69 total
twh ~
❯
```

So it took about 2 minutes and 16 seconds to show 8 false positive results. The results are similar if I use a valid username.

```
❯ sudo time sherlock thewhiteh4t
[sudo] password for twh:
[*] Checking username thewhiteh4t on:
[+] AllTrails: https://www.alltrails.com/members/thewhiteh4t
[+] Anobii: https://www.anobii.com/thewhiteh4t/profile
[+] Asciinema: https://asciinema.org/~thewhiteh4t
[+] Cent: https://beta.cent.co/@thewhiteh4t
[+] Chess: https://www.chess.com/member/thewhiteh4t
[+] Disqus: https://disqus.com/thewhiteh4t
[+] Docker Hub: https://hub.docker.com/u/thewhiteh4t/
[+] Giphy: https://giphy.com/thewhiteh4t
[+] GitHub: https://www.github.com/thewhiteh4t
[+] Gravatar: http://en.gravatar.com/thewhiteh4t
[+] HackTheBox: https://forum.hackthebox.eu/profile/thewhiteh4t
[+] Imgur: https://imgur.com/user/thewhiteh4t
[+] NameMC (Minecraft.net skins): https://namemc.com/profile/thewhiteh4t
[+] Patreon: https://www.patreon.com/thewhiteh4t
[+] Periscope: https://www.periscope.tv/thewhiteh4t/
[+] ProductHunt: https://www.producthunt.com/@thewhiteh4t
[+] PyPi: https://pypi.org/user/thewhiteh4t
[+] Reddit: https://www.reddit.com/user/thewhiteh4t
[+] Slashdot: https://slashdot.org/~thewhiteh4t
[+] Steam: https://steamcommunity.com/id/thewhiteh4t
[+] Steamid: https://steamid.uk/profile/thewhiteh4t
[+] Telegram: https://t.me/thewhiteh4t
[+] TryHackMe: https://tryhackme.com/p/thewhiteh4t
[+] Twitch: https://www.twitch.tv/thewhiteh4t
[+] Twitter: https://mobile.twitter.com/thewhiteh4t
[+] VirusTotal: https://www.virustotal.com/ui/users/thewhiteh4t/trusted_users
[+] YouTube: https://www.youtube.com/thewhiteh4t

11.43user 0.63system 2:18.43elapsed 8%CPU (0avgtext+0avgdata 124824maxresident)k
3032inputs+48outputs (0major+30813minor)pagefaults 0swaps
twh ~
❯
```

So as you can see, some valid results along with false positives in 2 minutes 18 seconds.

TWITTER OSINT USING TINFOLEAK AND REVERSE IMAGING



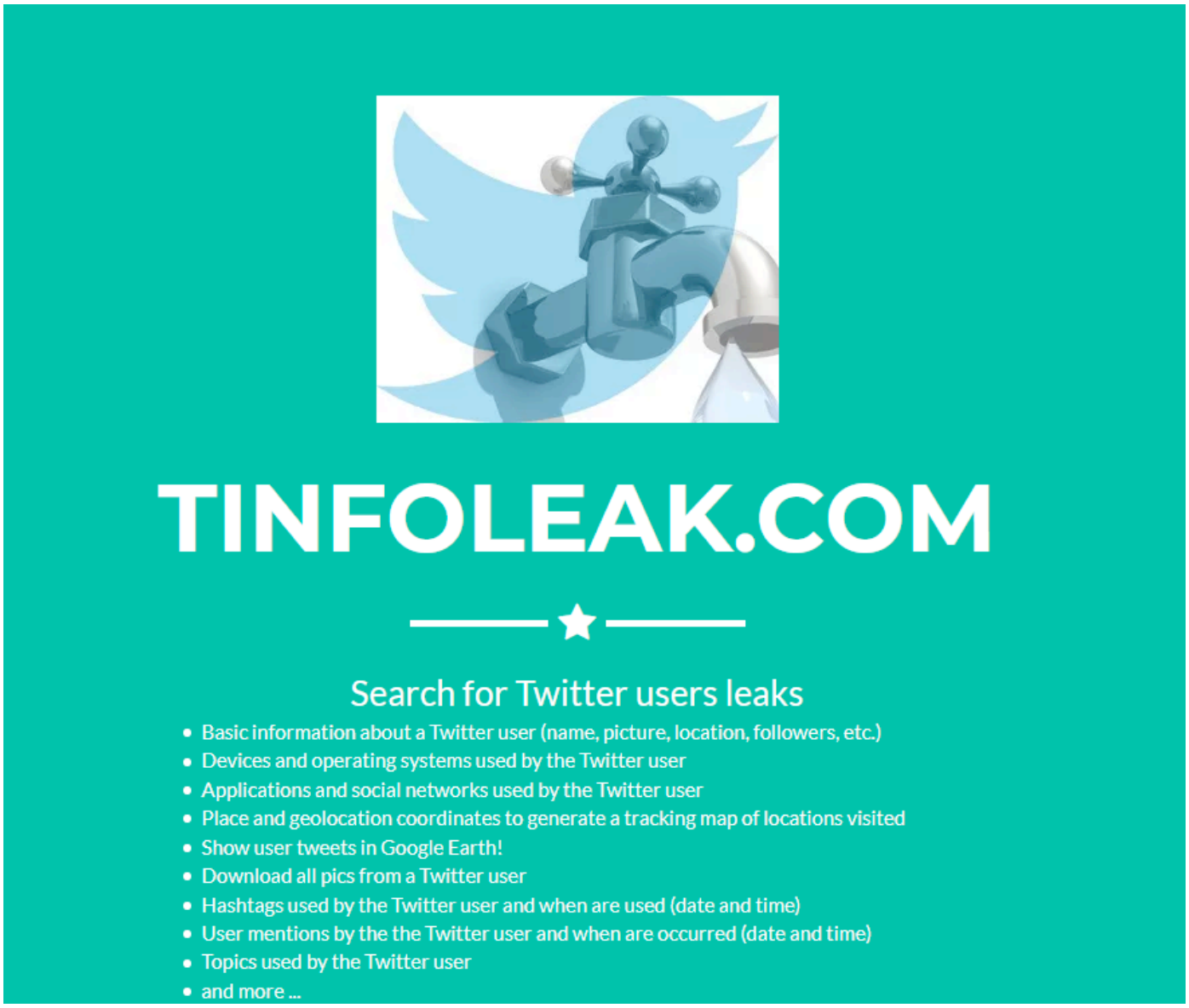
JEFF MINAKATA

Trained in CEH8 and CEH9, CISP, Metasploit certified, Accredited Certified Engineer (ACE), 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 Hackin9 and eForensics magazine. keyboardkomando@protonmail.com

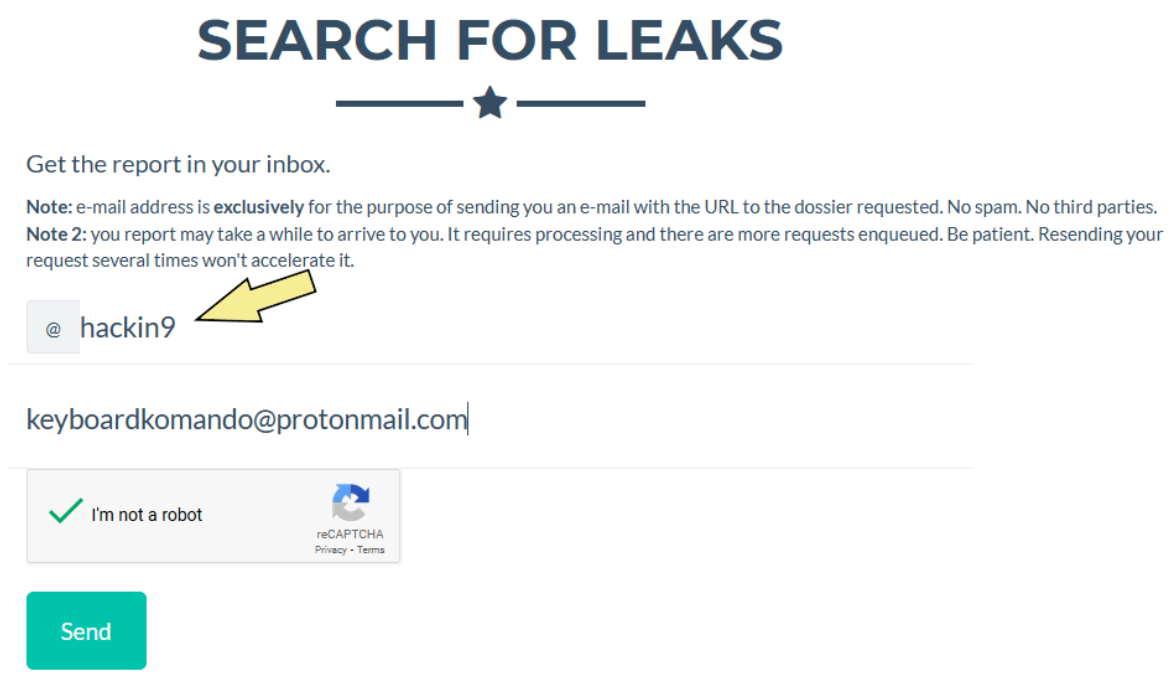
In this article, we will be talking about using OSINT for our Twitter investigations. We will be breaking this up into two sections, the first section is information collection on Twitter and the second part is verification of that information.

To follow along with this article, you will need a web browser and an internet connection. We will be using browser based tools for this tutorial.

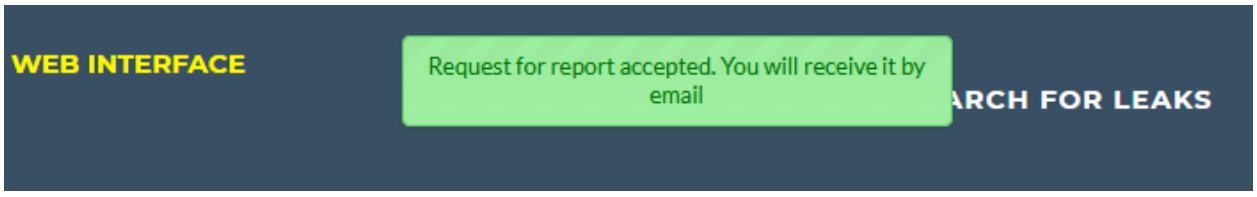
The goal of this article is to understand how we can leverage online tools to collect information on Twitter users and also some tips on analyzing a post that may be misleading.



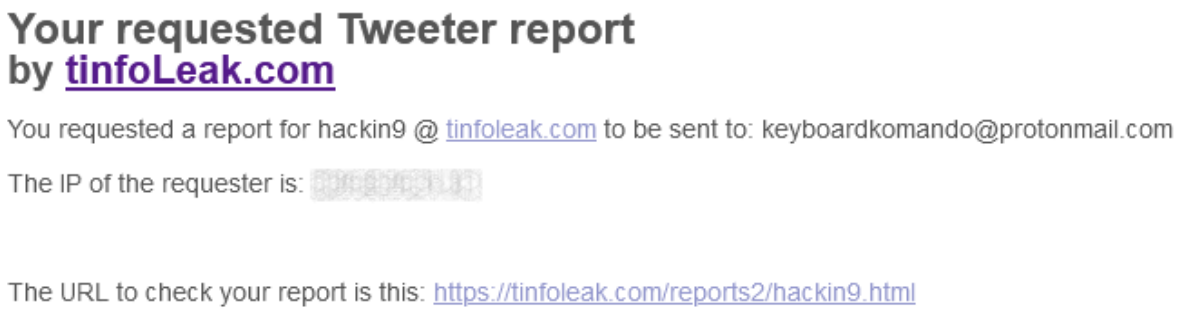
The website that we will be using is TINFOLEAK (see the **On the Web** section for the link). This site will help us collect a variety of information from our target's Twitter account all in one place.



The site's operation is pretty simple. If we scroll down to the bottom, we can enter the target's Twitter handle right after the @ in this example we are using Hacking9. Next we need to enter in an email address for the report to be sent to (the site claims that you will not be spammed or have third parties involved). Finally, we need to solve the CAPTCHA and click the **Send** button.



Once this is done you will see a verification at the top that you will receive your report by email. This can take several minutes to get. If you do not see an email after 15 minutes or so, check your spam folder.



In your email you will receive an email from the site along with the IP of the requester and the URL to check the results of the scan.

HACKING IOT WITH IOT





DANIEL W. DIETERLE

Daniel W. Dieterle, aka “CyberArms”, has been in the computer industry for over 20 years, and has worked as a security author, researcher & consultant. He has authored six books based on Kali Linux, and is currently working on his seventh, “Advanced Security Testing with Kali Linux”. Daniel also runs two tech blogs - cyberarms.wordpress.com & DanTheIOTMan.com

IoT (Internet of Things) vs IOT - reminiscent of the old Mad Magazine “Spy vs Spy” cartoon where there were two identical-looking cartoon spies of different colors that were always trying to kill each other. The rise of vulnerable deployed IoT devices and the offensive use of IoT devices is skyrocketing. In this article, we will cover attacking an IoT device, an office building security camera system, with another IoT device, a Raspberry Pi.



IOT DEVICES - WHAT ARE THEY?

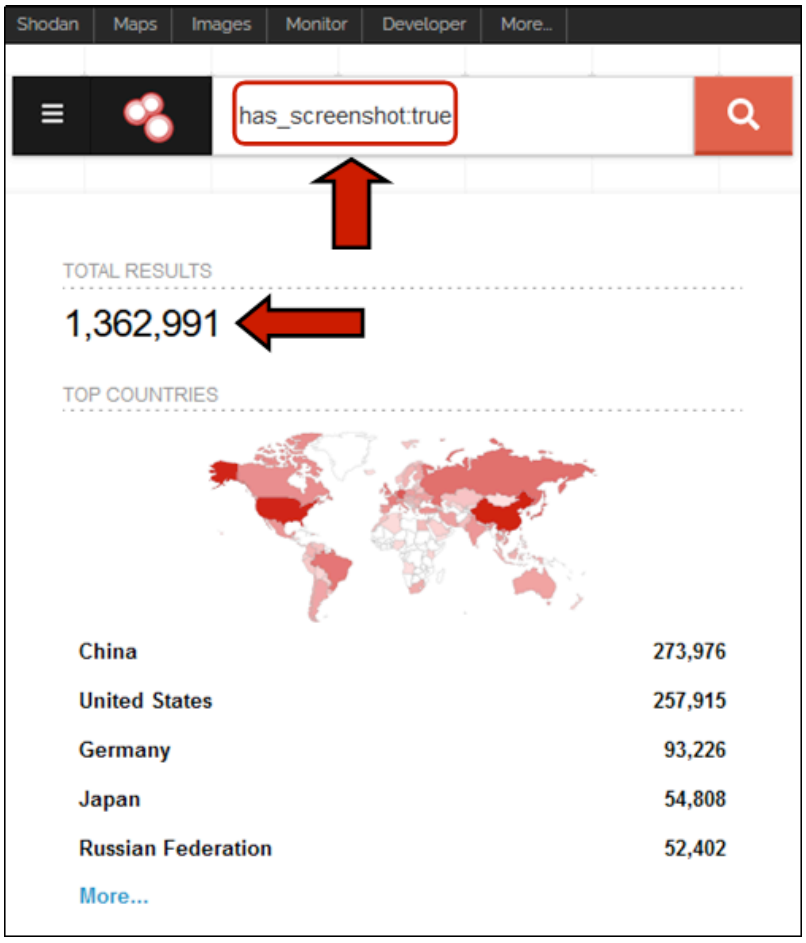
An IoT device is a physical device with intelligence (sensors, data collection, monitoring) that communicates with other devices over the network. IoT devices include security systems, smart appliances (online TVs, refrigerators, coffee makers, etc.), building and machine control, monitoring devices, scanners, and sensor arrays that are accessible over the Internet. Many “Maker” boards like the Raspberry Pi and Arduino are also used frequently in IoT applications. For this article, we will specifically focus on the Raspberry Pi and a Smart Camera security system.

VULNERABLE SYSTEMS - WHAT PEOPLE DON’T UNDERSTAND

IoT devices are so popular because they bring online connectivity and monitoring to almost every industry. The large problem, and what people don’t understand, is that there is a mini web server hiding inside them, and it is usually Linux based. Once an IoT device is deployed, many times it gets forgotten. It just sits on the wire, collecting or monitoring, and not usually getting updated. Security monitoring IoT devices are still fairly uncommon in the business world, and as we say jokingly in the Red Team world, “they don’t make anti-virus for refrigerators”. This makes them a prime target for unethical hackers.

FINDING IOT DEVICES IN MERE SECONDS

Shodan.io makes finding deployed IoT devices worldwide effortless. With just entering a few keywords, Shodan will return almost endless connected IoT devices, in seconds. Online security systems, video cameras, building control devices, and monitoring devices can be located almost instantly by entering the right search phrases. This is usually just the manufacturer's name or the server software that they are running. In most circumstances, you can see what software a target is running, what ports are open, and their geographical location. Shodan sometimes even lists CVEs for known vulnerabilities.



The free Shodan account is pretty limited. If you have a registered Shodan account (great membership sales usually around the major US holidays!) you can use the full set of search filters and can access a lot more returns. For example, using the search filter, "`has_screenshot:true`" returns almost a million and a half online devices of which Shodan was able to take a screenshot. This includes industrial, building, security, and monitoring devices. It also includes VNC and remote access sessions and lots of cameras!

Hackers use Shodan frequently, but security teams and companies also heavily use Shodan. For example, a company can quickly see what devices they have publicly exposed with a few filter-keyword searches. Shodan's professional monitoring services are also a huge asset for protecting companies.

HACKING WITH IOT

IoT devices aren't just targets; with the rise of powerful "Single Board Computers", they are increasingly being used as offensive security devices. The offensive security world is in love with them. To borrow a term from the military, we see IoT

RED TEAMING VIA ICS AND SCADA ADVERSARY TACTICS



ALEXANDROS PAPPAS

Alexandros Pappas BSc works as Security Incident Response at Epiq. Working for several big companies, he is responsible for conducting Tactical Threat Intelligence with integrated solutions, and Incident Response. At the same time, the author extends his knowledge in Purple Team Tactics, Penetration Testing and Red Teaming. Additionally he is Contributor for the GHDB with 300 dorks published. Highly motivated and passionate about security, he can be reached via an

email at pappasvar@gmail.com

INTRODUCTION

Industrial Control Systems (ICSs) are embedded cyber-devices that operate critical infrastructures (e.g., energy, transportation, water, oil, etc). ICS devices are lesser known and are typically unique to the Operational Technology (OT) framework of cyber, which differs from enterprise Information Technology (IT). Cyber-threats in ICSs manifest themselves in different ways. Cyber attacks on industrial control systems (ICSs) differ in impact based on a number of factors, including the adversary's intent, their sophistication and capabilities, and their familiarization with ICS and automated processes. Generally speaking, cyber attackers target these ICS environments via a campaign of attempts that allows access and provides enough information to invent an effect. However, the most important point when it comes to ICSs, is that the knowledge of the adversary's operations can help defenders appreciate the attacker's possible intent, level of sophistication, capabilities and familiarization with the ICS, which together work to unveil the potential impact of the attack on an organization.

DEFINITIONS AND TERMINOLOGY

PowerShell: is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language. Initially a Windows component only, known as Windows PowerShell, it was made open-source and cross-platform on 18 August 2016 with the introduction of PowerShell Core. The former is built on the .NET Framework, the latter on .NET Core.

ICS: In manufacturing, industrial control system (ICS) is a general term used to describe the integration of hardware and software with network connectivity in order to support critical infrastructure.

SCADA: Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management. The operator interfaces that enable monitoring and the issuing of process commands, such as controller setpoint changes, are handled through the SCADA supervisory computer system. However, the real-time control logic or controller calculations are performed by networked modules that connect to other peripheral devices, such as programmable logic controllers and discrete PID controllers, which interface to the process plant or machinery.

CYBER KILL CHAIN

The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs). Lockheed Martin derived the kill chain framework from a military model – originally established to identify, prepare to attack, engage, and destroy the target. Since its inception, the kill chain has evolved to better anticipate and recognize insider threats, social engineering, advanced ransomware and innovative attacks.

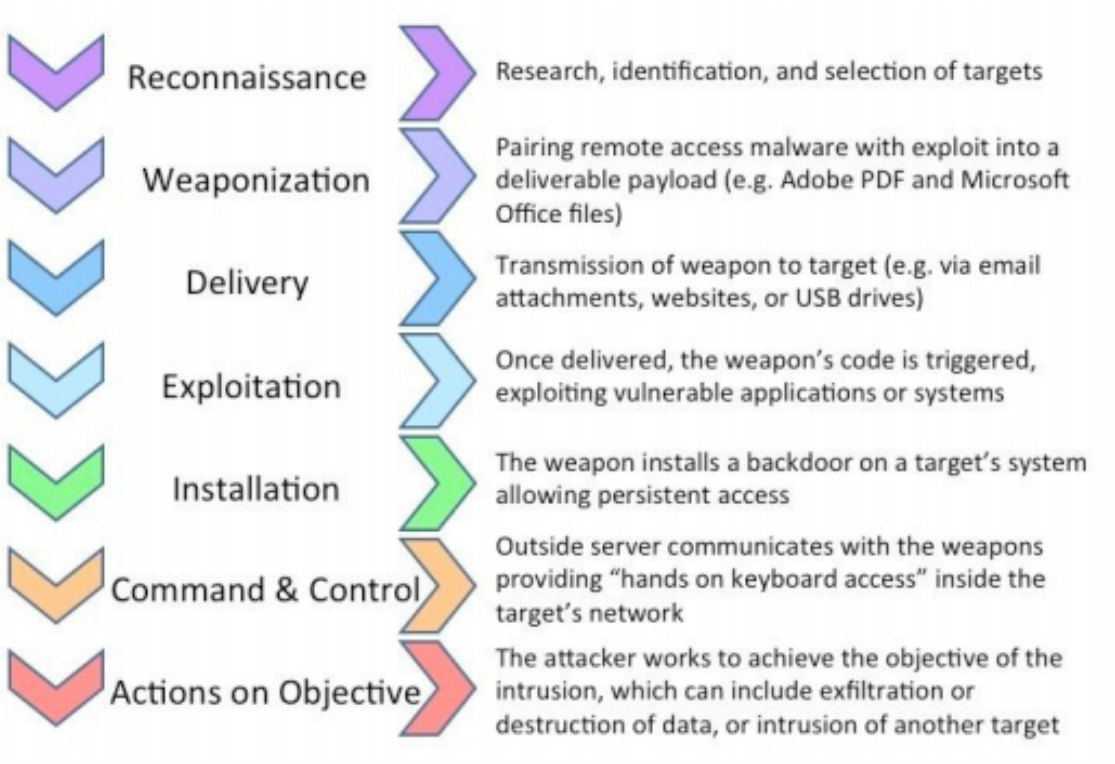


Figure 1. Cyber Kill Chain model by Lockheed Martin.

ICS CYBER KILL CHAIN

The idea of the ICS Cyber Kill Chain provides a structure and visibility in a high level of what is going on with regards to different attacks and how the good guys can defend against those with what kind of counter attacks in place. Due to the specific characteristics of features deployed on control systems and the exclusive configurations presented by them, carrying out a successful attack requires considerable knowledge.

ICS CYBER KILL CHAIN STAGE 1 BREAK DOWN

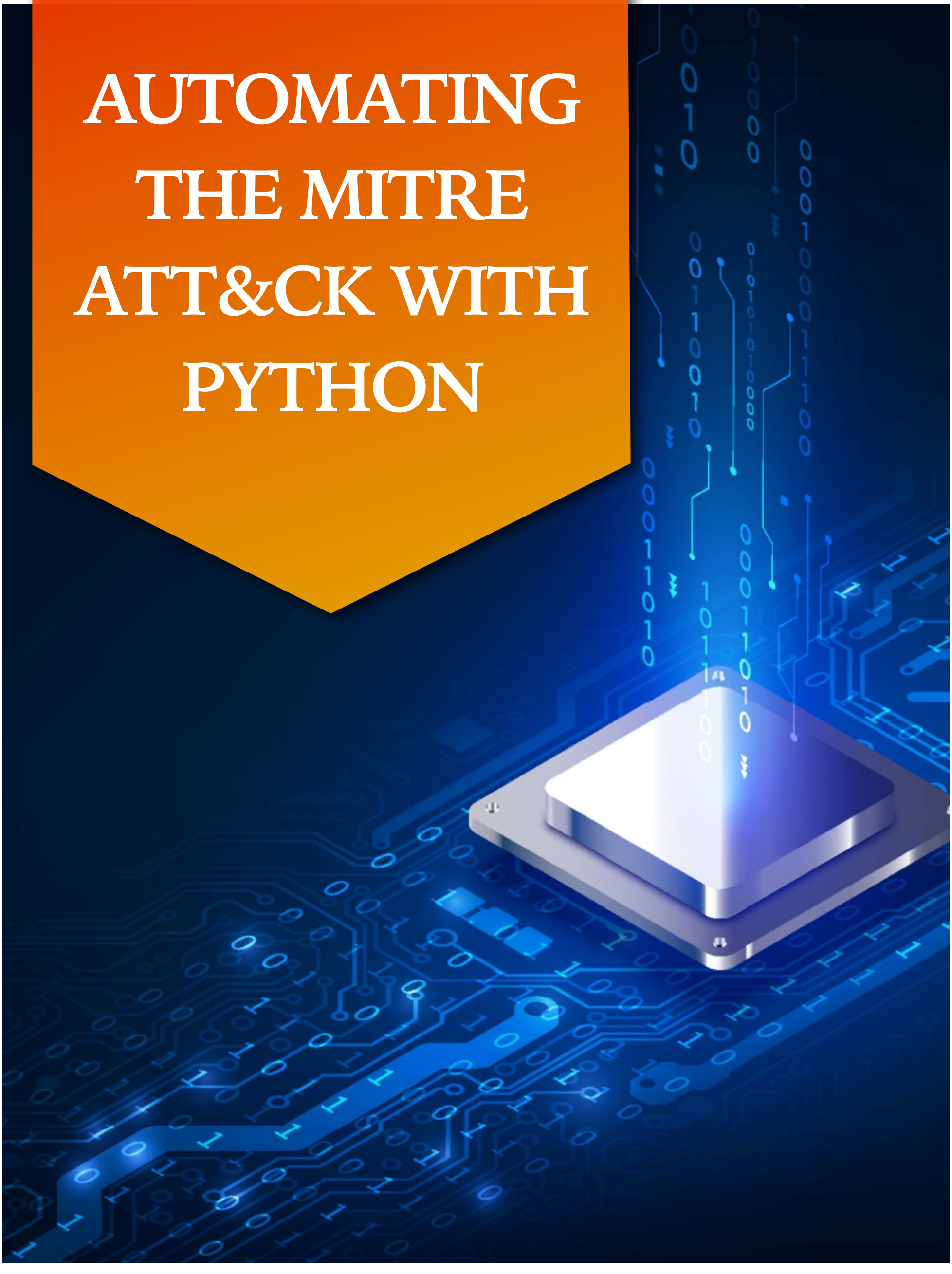
Planning Phase

The first step of Stage 1 is the planning phase where the objective is to reveal weaknesses and identify information that support attackers in their efforts to target, deliver and exploit elements of a system. This can be done via reconnaissance where attackers conduct research about the target using OSINT (Open-source intelligence) tools and searches of publicly available data. By doing this, they are able to map a target's publicly or privately accessible attack surfaces, patterning activity and determining versions of operating system software through routine queries.

Preparation Phase

The second phase of Stage 1 is the preparation that includes both weaponization or targeting. Weaponization and targeting can both take place, but both are not required. Weaponization includes modifying an otherwise harmless file, such as a document, for the purpose of enabling the adversary's next step. Targeting can also take place in the second phase and occurs when the adversary or its agent (such as a script or tool) identify potential victim(s) for exploitation. For example, if there is an authenticated VPN (Virtual Private Network) directly connected to a SCADA environment, which is using Windows 10 with PowerShell, then an attacker doesn't necessarily need to weaponize the VPN and install any malware to break in. Rather, just logging in and using the PowerShell environment or trying different modifications via the PowerShell

AUTOMATING THE MITRE ATT&CK WITH PYTHON





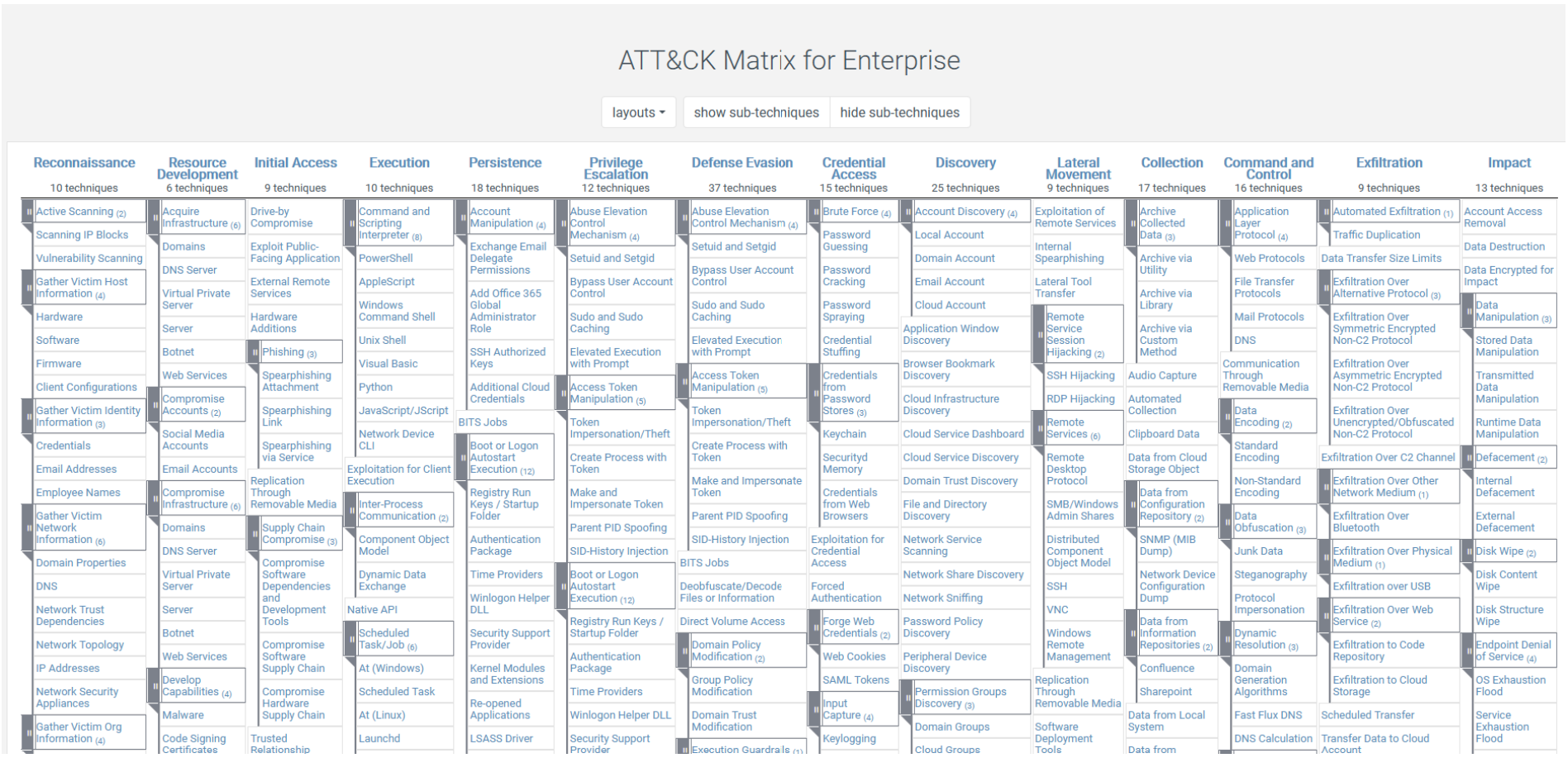
BRUNO RODRIGUES

Creating a better world through technology is now a life time mission of the author. He hopes you can join him in creating a safer e-one.

INTRODUCTION

I'm a firm believer that we cannot continue doing cyber security as we do it today - not enough time, not enough resources. It's a lost war. Attacks are getting more sophisticated, bad hackers are becoming more advanced, techniques more elaborate. Security or cyber security, if your concern is with the attacks, it will require a lot more automation than currently implemented.

In this article, I'll focus on the Mitre Att&ck. Why? Because it's a trend subject and because it's the perfect example of what I said. If you look at the picture below, you'll see that this framework allows to explore multiple threats, technologies, and attacks, making it a daunting task to keep organizations protected.



Our goal today is to get you, the reader, on the right track to automate the attack as a form of defense. Look at this simple scenario – you and your team oversee implementing security as a way to protect against the Mitre Att&ck framework. You start by deciding on which vendors to implement and there are a lot. This article will not focus on what you choose to protect yourself.

Nevertheless, during a PoC phase, or after you implement the chosen solutions, you decide to test its efficiency. You do it because you want to understand what weaknesses remain, because you have a red team or just because you're evaluating multiple solutions at once. Looking at the above picture, you quickly realize you are understaffed and do not have enough time to properly test.

The only option would be, in a certain way, to automate the multiple attacks that you need to constantly run against your perimeter. You probably know how fast and easy the perimeter changes, mutates, or becomes vulnerable. This is the journey path I'm taking you on, using our good friend Python and programming a couple of real attacks. This will be your

MANUAL PENTESTING? AUTOMATE IT WITH METASPLOIT





THOMAS MOOSMÜLLER

Thomas Moosmüller is the CEO of BreakinLabs and a specialist in penetration testing, vulnerability assessments, and social engineering. Thomas holds various certifications including CISSP, CIEH, OSCP, OSCE, and has a Master's degree in Informatics.

BreakinLabs is the creator of www.hackinlabs.com, a virtual environment that recreates a company with many vulnerabilities and various subnets. Every customer can practice the different exploit techniques on the different hosts with the help of our courseware and some hints, if required.

Visit us on www.breakinlabs.com for penetration testing, live hacking, and consulting or on www.hackinlabs.com to learn how hacking and penetration testing works for yourself!

HackinLabs

BreakinLabs

INTRODUCTION:

Metasploit is a heavyweight in the field of hacking and is an almost worry-free package. Metasploit's main focus is the exploit phase of hacking, but it also provides useful tools in information gathering and can centralize it in one place.

WHAT IS METASPLOIT?

Metasploit is an open-source project and is currently developed and published by Rapid7. There is a free version of the "Metasploit Framework" as a console tool and an additional paid version with some features such as a browser-based GUI and further automation. I believe the free version is suitable for everyone who wants to learn with Metasploit. This article refers exclusively to the free version of Metasploit.

It is a very comprehensive tool and includes the exploit framework as well as other tools for creating exploit code and payloads.

Metasploit is a very comprehensive tool and includes the exploit framework and several different modules that can also be used outside the actual Metasploit environment. This includes, in addition to the start of the Metasploit Console ("msfconsole"), the options of payload generation and encoding (msfvenom), the module especially for advanced Windows exploits (msfrop), and an advanced payload with an in-memory DDL injection called "meterpreter".

INSTALLATION:

Since Metasploit is a standard program in penetration testing, it is already included in a large number of distributions (Kali Linux, Parrot, etc.) and does not need to be installed separately. If this is not the case, there is a detailed manual on the Rapid7 Github repository:
https://github.com/rapid7/metasploit-framework/wiki/Setting-Up-a-Metasploit-Development-Environment

After installation, the Postgresql service must be enabled and started. The added database must also be initialized with the command "msfdb init".

LAUNCH METASPLOIT:

The Metasploit Console can be started with the command "`msfconsole`". The start screen looks like this:

```
root@kali  ~  msfconsole


 ------------------------------------------------------------------------------
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|                                                                              |
 ------------------------------------------------------------------------------
      \                                 /                      /
       \     .                         /                      /              x
        \                             /                      /
         \                           /          +           /
          \            +            /                      /
           *                       /                      /
                                  /          .           /
    X                            /                      /                X
                                /                    ###
                               /                    # % #
                              /                      ###
                             /
                .           /
     .                     /              .          *            .
                          /
                         *
                 +                             *

                                       ^
####        __     __     __          #######       __     __     __        ####
####      /    \ /    \ /    \      ###########   /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.0.33-dev                          ]
+ -- --=[ 2103 exploits - 1134 auxiliary - 357 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 >
```

In addition to the version, the scope of exploits and other scripts contained in the database are also displayed.

SHOW COMMAND:

The show command can be used to display all the available modules. These are:

- ☑ `auxiliary` (modules of the category scanner, sniffer, fuzzing, sniffing, etc.)
- ☑ `payloads` (exploit code for remote connections)
- ☑ `encoders` (mainly for AV-evasion of payloads by polymorphic encodings)

BUILD YOUR OWN BRUTE FORCE TOOL



DANIEL GARCÍA BAAMEIRO

Daniel García Baameiro is passionate about hacking. A computer engineer from the Complutense University, he holds a master's degree in cybersecurity from the Carlos III University and is certified by the OSCP. During his professional career, he has dedicated himself exclusively to the offensive side.

Currently, he teaches the subject "Offensive Security" at the International Graduate School and works as a Red Team for the company ISDEFE.

If you liked the article, don't hesitate to give him feedback! He will appreciate it very much: daniel@garciabaameiro.com

His website is the following: http://garciabaameiro.com

DEDICATION

I would like to dedicate this article to Pablo, my ex-boss and my friend. For those good times, for those laughs, and for the epic jobs we've done, those CTF afternoons are still pending!

INTRODUCTION

When performing a web audit, one of the first challenges you will face is access through a login portal. These portals have been implemented to protect the private part of a website from the public part. Usually, it is in

the private area where sensitive private information or even an administrator's own functionalities that allow the management and editing of the website can be found.

In order to try to gain access to the private part of a website, brute force attacks tend to be used. These attacks are carried out by using a dictionary of possible usernames and passwords of a website. If valid credentials are found, access has been gained.

This article aims to help users understand how web portals work so that they can then create their own tool in the programming language they feel most comfortable with.

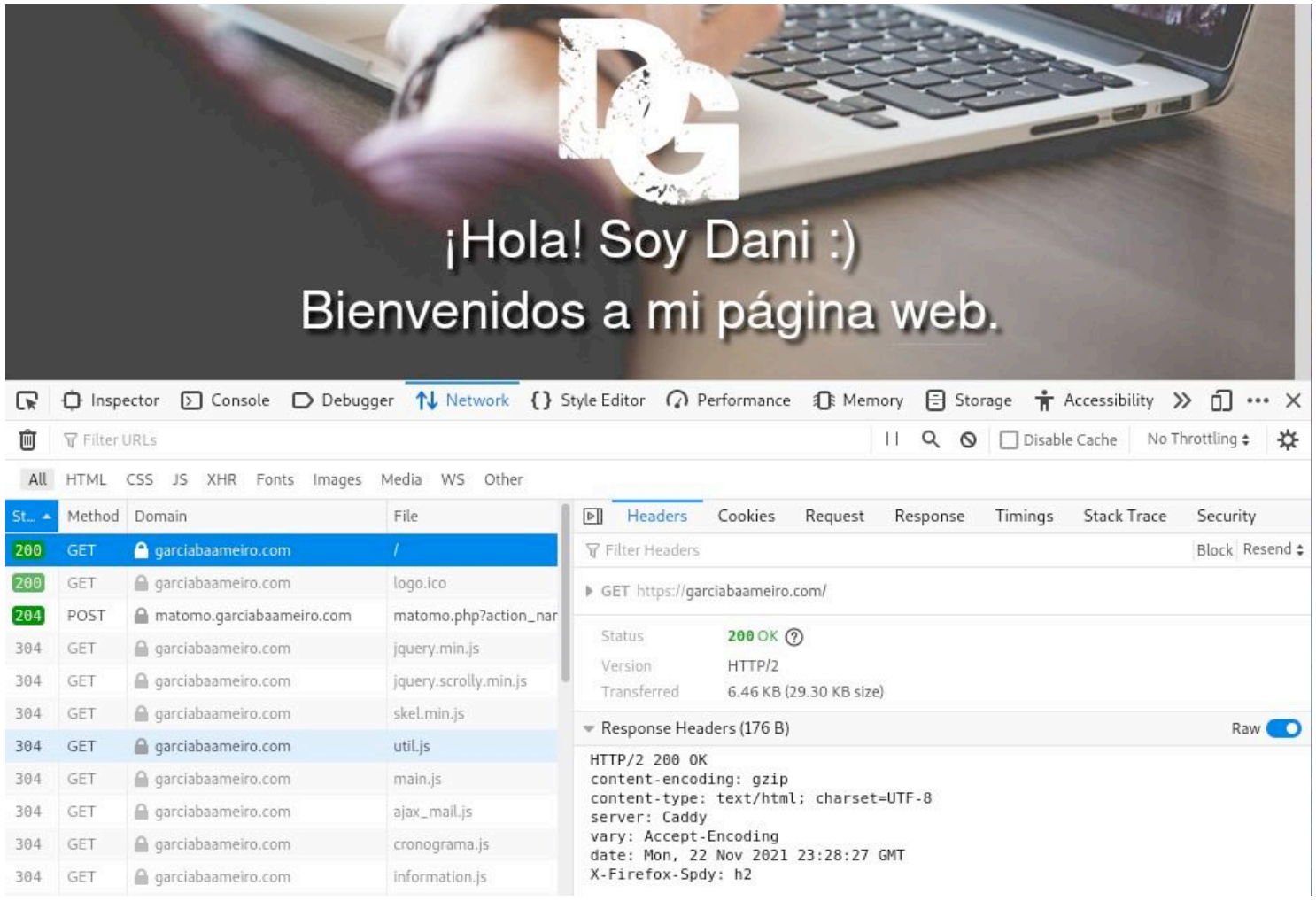
BASIC KNOWLEDGE

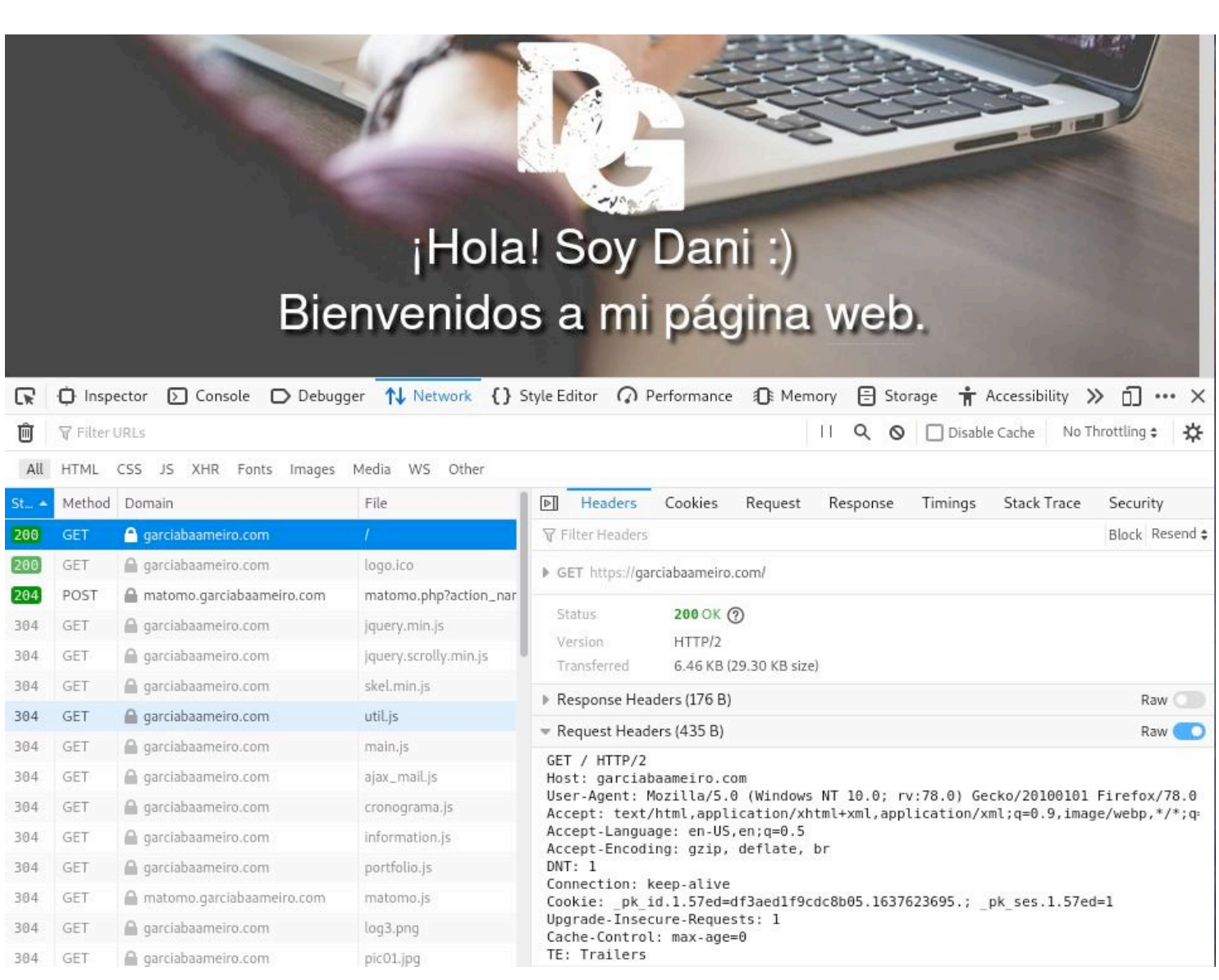
Before we get down to the practical part of this article, it is important for the reader to be aware of certain definitions.

HTTP protocol

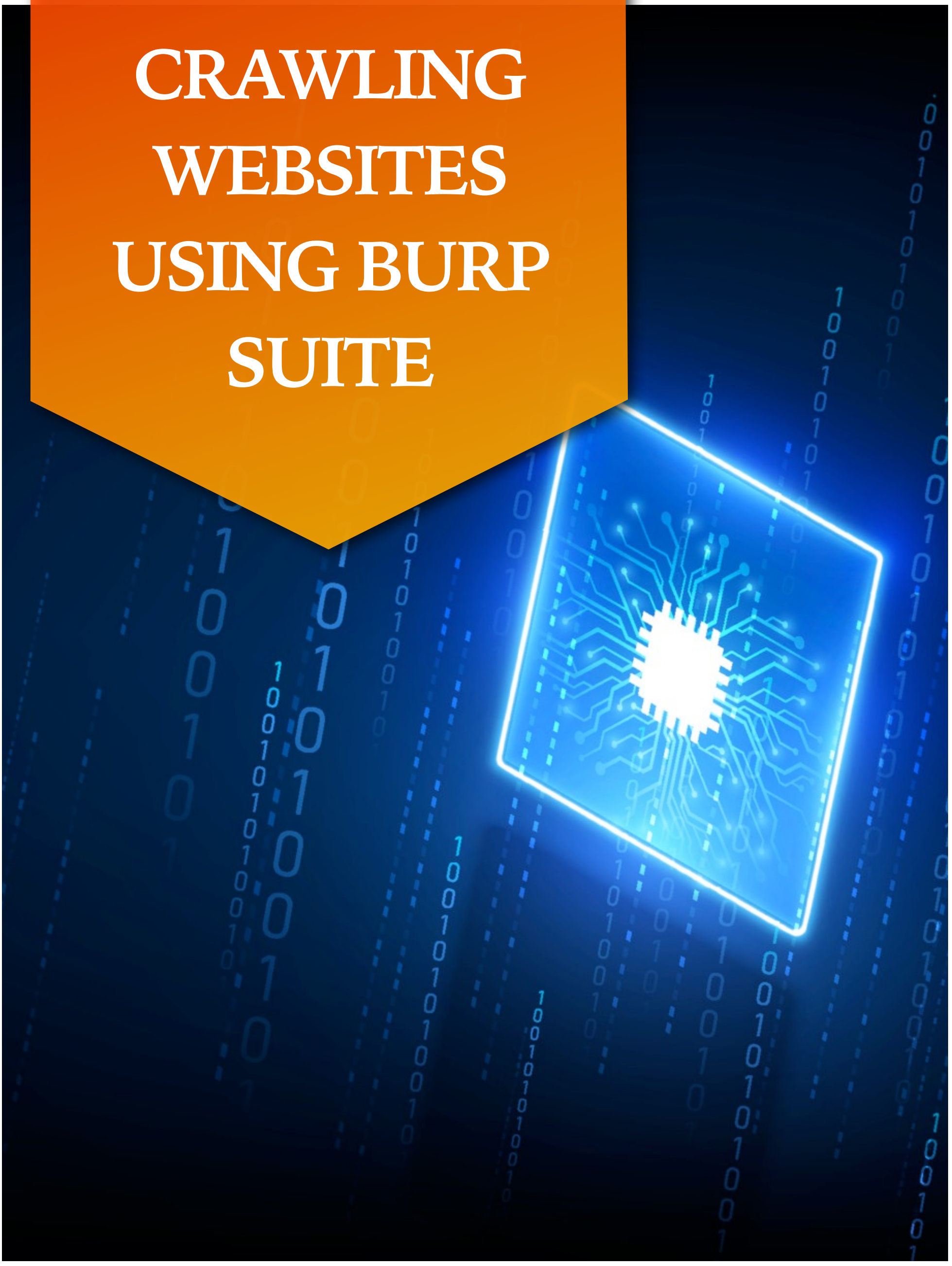
The HTTP protocol is a hypertext transfer protocol through which information can be transmitted. This protocol is mainly used for web browsing on the internet. When a user accesses a website such as

"https://garciabaameiro.com", several HTTP requests are generated, requesting content from the web server...


¡Hola! Soy Dani :)
Bienvenidos a mi página web.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
St... Method Domain File
200 GET garciabaameiro.com /
200 GET garciabaameiro.com logo.ico
204 POST matomo.garciabaameiro.com matomo.php?action_nar
304 GET garciabaameiro.com jquery.min.js
304 GET garciabaameiro.com jquery.scrolly.min.js
304 GET garciabaameiro.com skel.min.js
304 GET garciabaameiro.com util.js
304 GET garciabaameiro.com main.js
304 GET garciabaameiro.com ajax_mail.js
304 GET garciabaameiro.com cronograma.js
304 GET garciabaameiro.com information.js
Headers Cookies Request Response Timings Stack Trace Security
Filter Headers
Block Resend
GET https://garciabaameiro.com/
Status 200 OK
Version HTTP/2
Transferred 6.46 KB (29.30 KB size)
Response Headers (176 B) Raw
HTTP/2 200 OK
content-encoding: gzip
content-type: text/html; charset=UTF-8
server: Caddy
vary: Accept-Encoding
date: Mon, 22 Nov 2021 23:28:27 GMT
X-Firefox-Spdy: h2


¡Hola! Soy Dani :)
Bienvenidos a mi página web.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Filter URLs
Disable Cache
No Throttling
All HTML CSS JS XHR Fonts Images Media WS Other
St... Method Domain File
200 GET garciabaameiro.com /
200 GET garciabaameiro.com logo.ico
204 POST matomo.garciabaameiro.com matomo.php?action_nar
304 GET garciabaameiro.com jquery.min.js
304 GET garciabaameiro.com jquery.scrolly.min.js
304 GET garciabaameiro.com skel.min.js
304 GET garciabaameiro.com util.js
304 GET garciabaameiro.com main.js
304 GET garciabaameiro.com ajax_mail.js
304 GET garciabaameiro.com cronograma.js
304 GET garciabaameiro.com information.js
304 GET garciabaameiro.com portfolio.js
304 GET matomo.garciabaameiro.com matomo.js
304 GET garciabaameiro.com log3.png
304 GET garciabaameiro.com pic01.jpg
Headers Cookies Request Response Timings Stack Trace Security
Filter Headers
Block Resend
GET https://garciabaameiro.com/
Status 200 OK
Version HTTP/2
Transferred 6.46 KB (29.30 KB size)
Response Headers (176 B) Raw
Request Headers (435 B) Raw
GET / HTTP/2
Host: garciabaameiro.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Cookie: _pk_id.1.57ed=df3aed1f9cdc8b05.1637623695.; _pk_ses.1.57ed=1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
TE: Trailers

CRAWLING WEBSITES USING BURP SUITE





MAYUKH PAUL

I am a typical college student with a keen interest in the field of cybersecurity and social engineering. The art of psychologically manipulating people into performing actions or divulging confidential information intrigues me.

I enjoy trying out new tools and exploiting new vulnerabilities. The more vulnerabilities I exploit, my urge to learn increases.

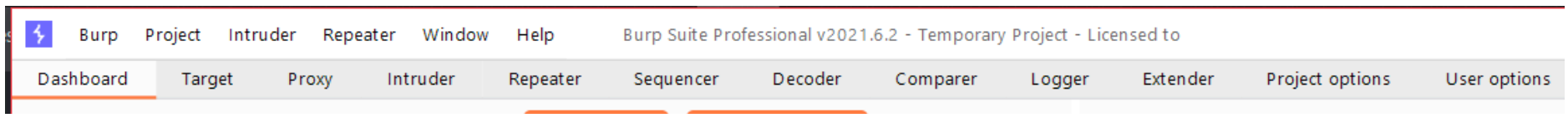
I aim to dive more into the field of cybersecurity research and protect company security against cyber threats.

Burp Suite is a platform created by PortSwigger consisting of various security tools used to perform web application penetration testing. These tools consistently work together to complete the testing process from analyzing surface attacks to finding and exploiting vulnerabilities.

Some of the security tools in Burp Suite are:

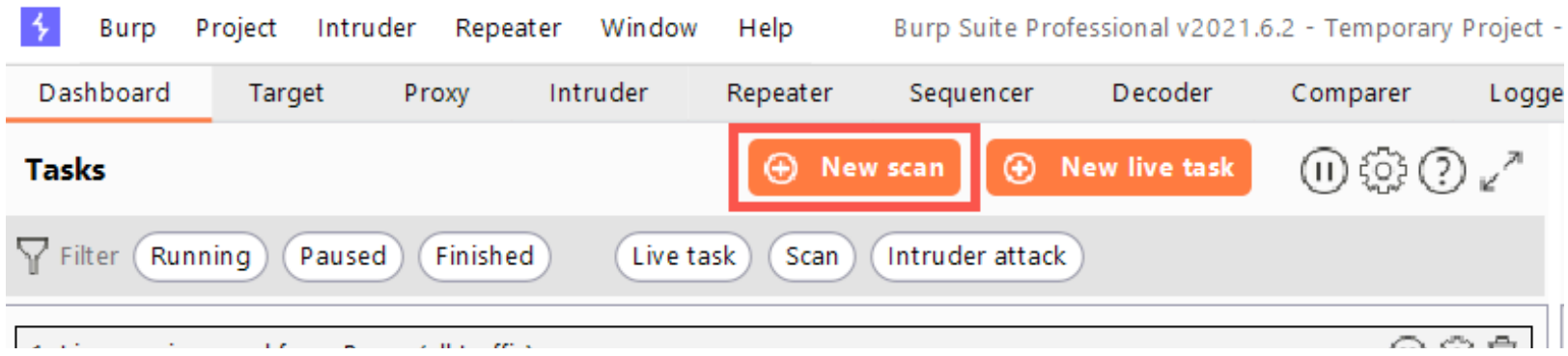
- ☑ **Target**: This tool contains detailed information about the target application.
- ☑ **Proxy**: This tool intercepts a web proxy that operates as a man-in-the-middle between the target web application and the end browser.
- ☑ **Intruder**: This is a customizable tool for carrying out attacks against web applications.
- ☑ **Repeater**: This tool manually manipulates and reissues HTTP requests, and analyzes the site's response.
- ☑ **Sequencer**: This tool can be used to analyze an application's session tokens that are intended to be random.
- ☑ **Decoder**: This tool is used to convert raw data into hashed and encoded forms.
- ☑ **Comparer**: This tool is used to compare two data items.

And many more.



In this article, I am going to use Burp Suite to crawl and audit a website..

1. Click on 'New scan' to open up the scan configuration window.



2. In the new scan window, we specify the target website. There are two scan types:
   - 2.2. Crawl
   - 2.3. Crawl and Audit

Here, I will demonstrate a default Crawl and Audit Scan and the website I used is 'http://testphp.vulnweb.com/'. This is a

SOLVING AN EXPERT LAB FROM WEB SECURITY ACADEMY

MICHAEL SOMMER

Michael Sommer is a security consultant and pentester at Consulectra Unternehmensberatung GmbH in Hamburg. He has been involved in IT security since 2006 and his focus is on web security, application security, cloud security and critical infrastructure security. Michael runs a YouTube channel where all the Web Security Academy labs are solved. Currently, there are more than 300 videos here. Some of them are still without audio commentaries, but these will be replaced gradually.

INTRODUCTION

This tutorial is a walkthrough to the lab “Stealing OAuth access tokens via a proxy page” from Web Security Academy by PortSwigger. The level of this lab is expert, and the reader should have a basic understanding of HTML and JavaScript. It is also recommended that the topic “OAuth 2.0 authentication vulnerabilities” has been worked through to this point. This lab can be solved with the community edition of Burp Suite, no professional version is needed. You should have configured your browser and Burp Suite so that you can intercept the traffic. In the reference section is a link where you can find information about browser configurations.

SOLVING THE LAB

Preparation

Before you can start solving the lab, you must create an account at the Web Security Academy. After successful creation, you can access the lab by clicking the button “Access the lab” at the bottom of the lab site.

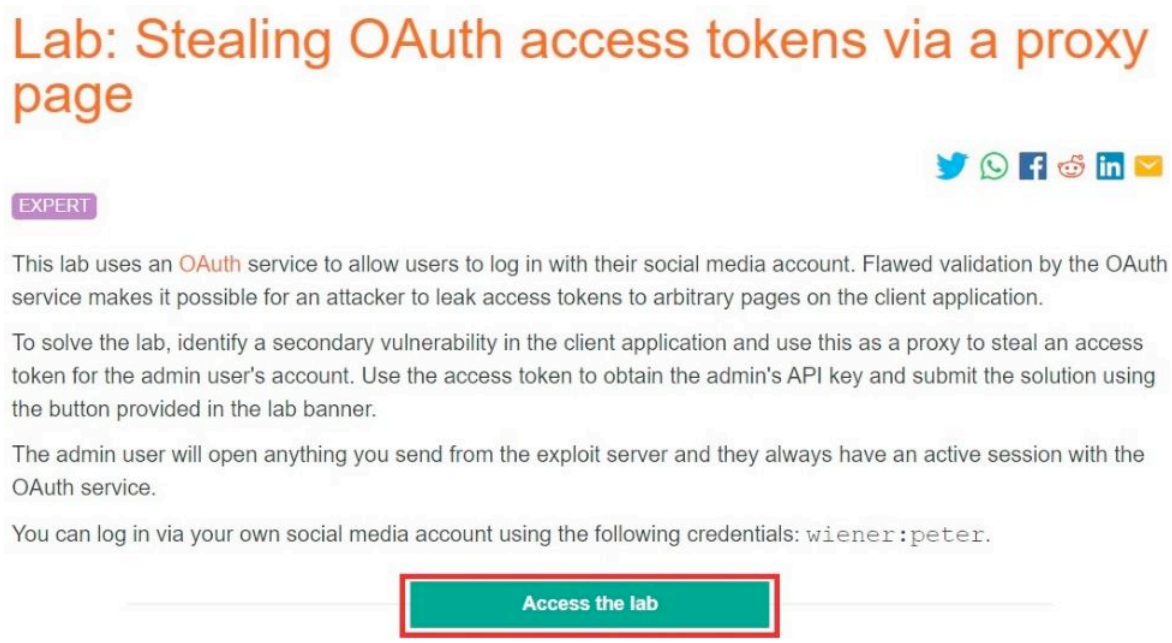
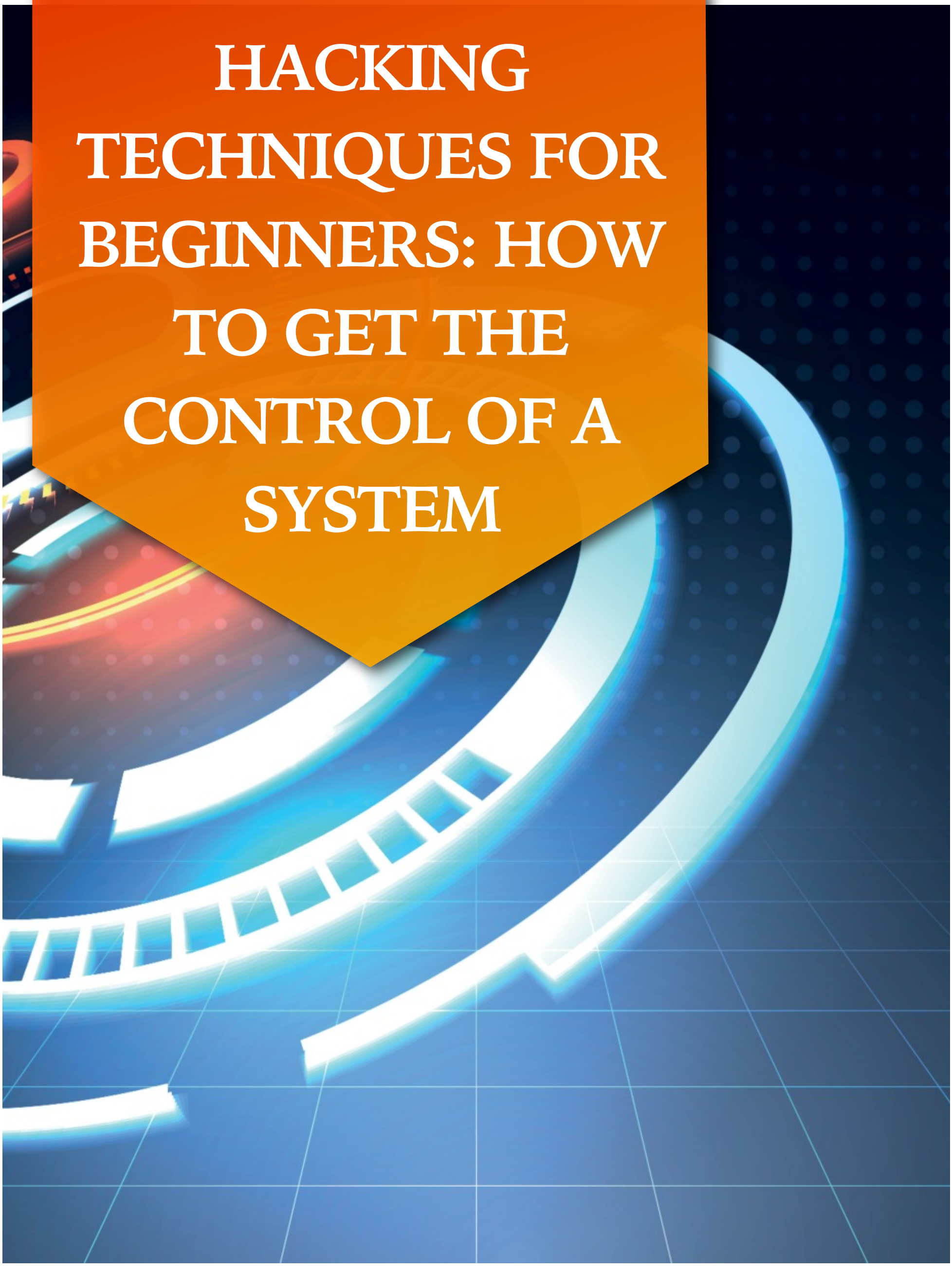


Figure 1: Access the lab

The blog should look like the following figure. Because the order of the blog posts varies, when you access the lab, it can happen that you see another blog post at the top. At the time of writing, the blog entries were always the same. If there are still other blog entries, this is not a problem, because the source code has not changed.

HACKING TECHNIQUES FOR BEGINNERS: HOW TO GET THE CONTROL OF A SYSTEM





VERÓNICA BERENGUER GARRIDO

I'm Verónica Berenguer Garrido, graduate in telecommunications engineering and specialized in the branch of cybersecurity by the University of Seville.

Nowadays, I work as an offensive security researcher in a Red Team, which allows me to analyze all kinds of vulnerabilities and exploit them. This helps me protect systems and networks from threats and malware.

My passion is to learn more every day and research new technologies that allow me to improve in my work.

In short, I love what I do.

When we hear the word “hacker” we usually imagine a person that wears a black hooded sweatshirt doing illegal activities in a sinister terminal. However, this is not always the case because there is a big difference between cybercriminal and hacker.

A hacker is a role that has knowledge of hacking techniques. Now, we can differentiate between ethical hackers and cybercriminals. Both have the same hacking knowledge, however, the first uses them to find vulnerabilities and report them to improve systems and applications, while the second pretends to obtain some benefit, such as economic compensation, extortion, etc.

In this article, we are going to learn basic hacking processes and techniques to be an ethical hacker, from port scanning to privilege escalation. Finally, we will see with a real example how we can hack a remote machine applying these techniques.

WHAT WILL YOU LEARN?

In this article, we will introduce the world of hacking, teaching all the steps to get control of a system.

The topics addressed are as follows:

- ☑ Port Scanning
- ☑ Vulnerability Scanning
- ☑ Exploitation Tasks
- ☑ Privilege Escalation

WHAT SHOULD YOU KNOW?

In this article, we will explain everything step by step, but the following prior knowledge will be necessary:

- ☑ Basic Scripting (Python, C, Bash, Perl, PHP, etc.)
- ☑ Basic Networking
- ☑ You just need to have fun reading, learning and researching.

INTRODUCTION

Nowadays, any person interested in cybersecurity is called a hacker, but really the value of a hacker isn’t just to launch automatic applications to find and exploit vulnerabilities. The real value of a hacker is the knowledge of techniques or basic tools or commands to research vulnerabilities and exploit them in systems and applications to improve them. The automatic tools can help or complement the investigation, but wisdom is the most precious treasure of an ethical hacker.

With this article, we hope to foment and teach beginners basic techniques to start in ethical hacking. We can see how, with a few commands, patience and calm, we can get a server in four phases, explained in the sections below. To apply this knowledge, we are going to hack a machine using a Kali Linux distribution.

Before starting, I would like to remind you that you must have the permission of an organization or entity to hack it. Normally, a company pays for pentesting their assets to patch the vulnerabilities before an authentic attacker hacks them. So, in this article, pretend you are a pentester and you have to perform a security test to an organization. Let's go there!

PORT SCANNING

The first step, called port scanning, is the process of checking for open TCP or UDP ports on a remote machine to find services, technologies and versions.

NMAP

One of the most popular and complete tools for port scanning is Nmap (Network Mapper). Nmap is an open source and free utility for security auditing and network discovery, which gets us a large amount of information about the computers, like open and filtered ports, which hosts are up in a network, traceroute, operating system, services and versions by banner grabbing and dozens of other characteristics. For the analysis, you can assign to Nmap a subnet, a single IP or a domain, such as we can see below.

Besides, Nmap allows us to write and execute scripts named as Nmap Scripting Engine (NSE) in order to detect or exploit vulnerabilities, enumeration tasks, backdoor detection, network discovery, etc.

Nmap has a very long list of options. Below, we are going to show the most efficient commands to obtain the necessary information for our pentesting:

- -v
    - This option shows the verbose of the application's execution (only if you want to see the scanning's advance).
- -A
    - This option, named "aggressive scan options", enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute).
- -p
    - This option is used to indicate the scanning ports. By default, Nmap scans the 1000 most popular ports on a given machine for UDP or TCP. There are three options:
        - If you want to scan all ports you can include the following option:

NMAP, THE PERFECT TOOL



DANIEL GARCÍA BAAMEIRO

Daniel García Baameiro is passionate about hacking. A computer engineer from the Complutense University, he holds a master's degree in cybersecurity from the Carlos III University and is certified by the OSCP. During his professional career, he has dedicated himself exclusively to the offensive side.

Currently, he teaches the subject "Offensive Security" at the International Graduate School and works as a Red Team for the company ISDEFE.

If you liked the article, don't hesitate to give him feedback! He will appreciate it very much: daniel@garciabaameiro.com

His website is the following: http://garciabaameiro.com

DEDICATION

I would like to dedicate this article to Erik, a great hacking and free culture enthusiast. In fact, it was thanks to him that I got to know Haking magazine. Never stop learning!

INTRODUCTION

When I decided to write this article under the theme proposed by the Haking team of "Best tools and techniques for hackers", my first thought was "nmap". This tool, key in a cybersecurity arsenal, allows information to be gathered about an asset. This information can be gathered by scanning ports, detecting the operating system or even obtaining information about the services present on a device.

This article is oriented both for those who have never performed a port scan before and for those who are performing an offensive security certification such as the well-known OSCP. After reading it, the reader will be able to understand what the tool does with each type of scan and how to adapt them accordingly.

PORT SCANNING

When we talk about ports in computing, also known as network ports or system ports, we are talking about a feature of operating systems to create connections between devices and exchange information over a network. These connections can be multiple and simultaneous, since after all the IP address of the device is the same but is addressed to different ports.

These ports are indicated through the network segments of the transport layer (following the OSI model), in which two data transmission protocols known as TCP and UDP can be found.

TCP scanning

TCP, known as Transmission Control Protocol, is a connection-oriented network protocol. Simply put, for every packet sent to a remote device, it is expected to receive another packet from the remote device indicating that it has received it. To understand the types of scans that are performed with the nmap tool on this protocol, it is important to understand and know its network segment.

TCP frame segment

A segment of a TCP/IP frame includes the application layer information together with a layer added by the transport protocol. This segment is located inside the IP protocol segment. Visually, it looks like this:

KALI NETHUNTER: FOR THOSE THAT HAVE A FEAR OF COMMITMENT





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 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.

INTRODUCTION:

Do you have a fear of commitment? Are you growing tired of the phrase “Got Root?” Are you driving yourself mad with all of the root your phone tutorials and bad apps? If you answered yes to any of these questions then this is the article for you. Whether you are new to penetration testing or a veteran in the biz, you will find some valuable knowledge in this article and perhaps a new weapon to add to your arsenal. After reading this article you will be able to pick up any stock device and get Kali NetHunter up and running.

Kali NetHunter is an extremely valuable tool and a game changer within the world of mobile penetration platforms. It is also more conveniently within reach than you might think. I have specifically chosen the rootless version of Kali NetHunter for this article because of how approachable it is; if you can utilize basic functionalities of a smartphone then you can implement this tool. The best part is that the only equipment items needed are a standard issue smartphone, charging cable, and a positive attitude.



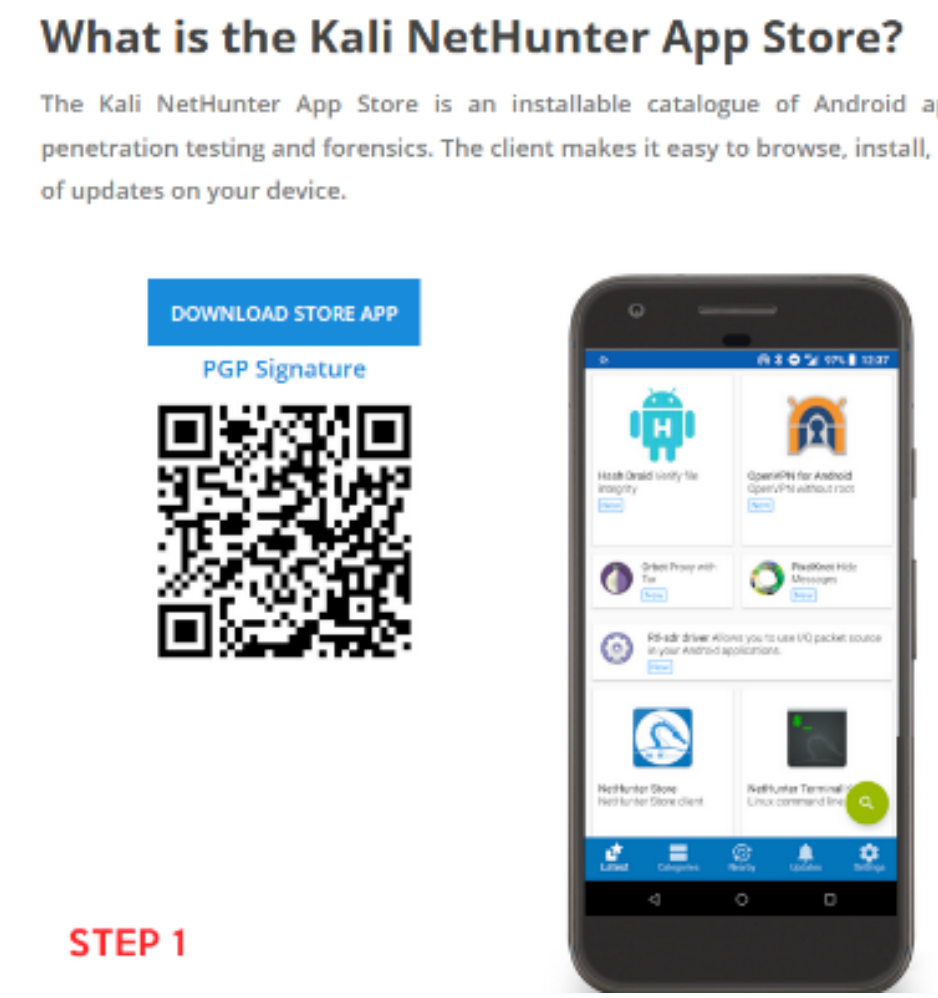
LANDSCAPE:

The current landscape of office environments, shared work-spaces and cafes today are bustling with traffic from a variety of devices including smartphones, watches, tablets, and more. Many of these devices are being utilized with little to no security measures in mind. Today, within organizations around the world, you will find a mixed bag of these items being utilized at a fast growing rate, from employees to the top level executives; the use of mobile machines is here to stay and we need a competent way to test these environments.

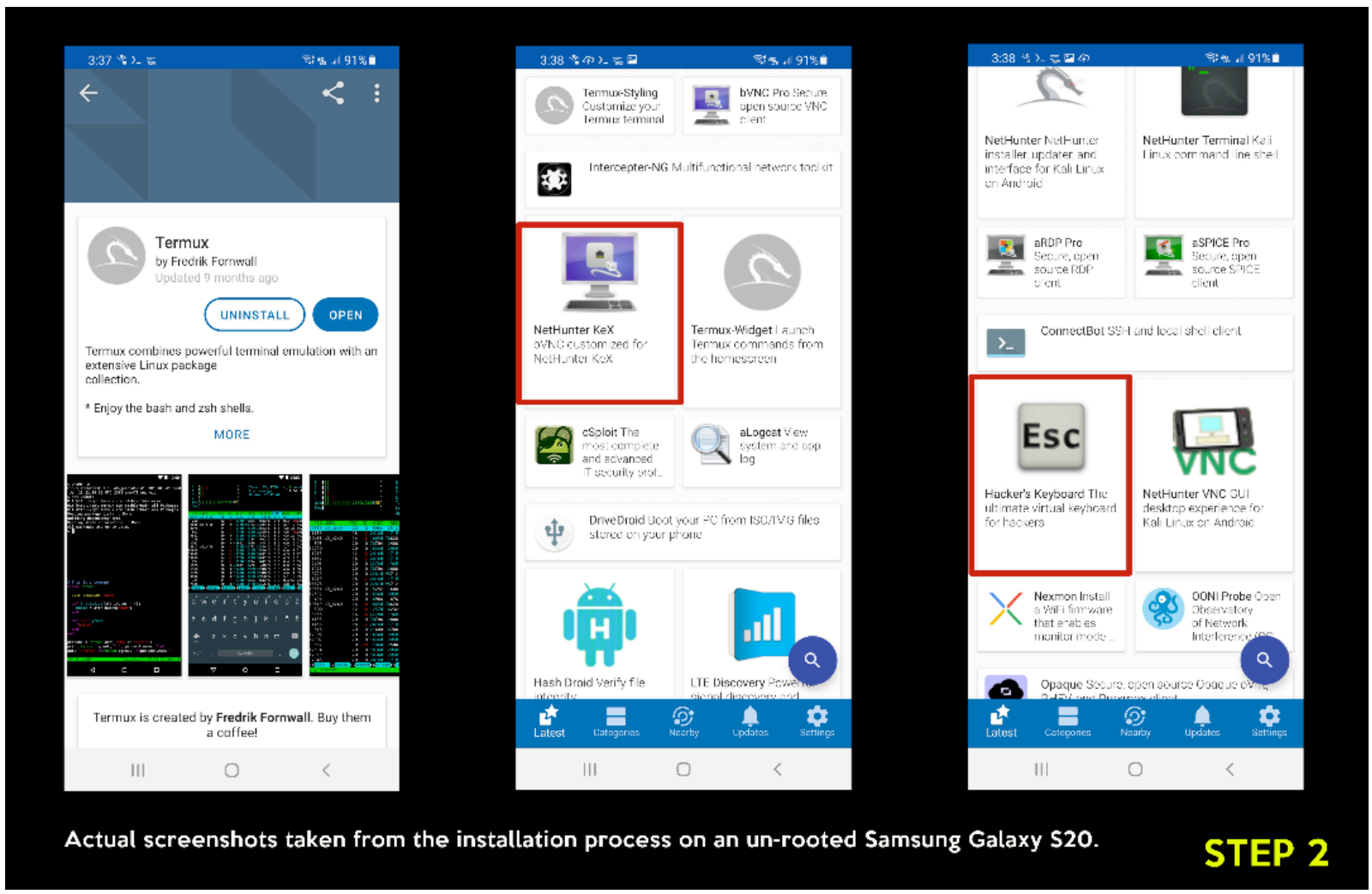
INSTALLATION

Installation of the rootless version of Kali NetHunter only takes a few moments. Just follow the steps below and, before you know it, you will be up and running with Kali NetHunter. *(I would suggest keeping the phone on the charger during setup.)*

1. Navigate to https://store.nethunter.com/en/ and install the NetHunter store app.
2. Once downloaded, install Termux, NetHunter-KeX Client, and Hacker’s Keyboard from the store interface. (The hacker’s keyboard is optional, however it does make typing from your device super simple.)
3. Open the Termux interface and enter the commands found in the Step 3 figure.



As you can see from the image in step one, you can scan the QR code or directly download the store app. Either way it works with the same result, ultimately the choice is yours.



INTERCEPTING DATA TRAFFIC VIA IPHONE





JORDAN BONAGURA

- CISO and Information Security Researcher - CEH
- Hacker is NOT a Crime Advocate
- Stay Safe (Magazine and Podcasts) Founder
- Computer Scientist
- Post Graduated - Strategic Business Management, Higher Education Methodology Innovation and Research Methodology
- Organizer of Vale Security Conference - Brazil
- Director Member of Cloud Security Alliance - Brazil
- Advisory Member of Digital Law and High-Tech Crimes OAB (Association of Brazilian Lawyers)
- IT Teacher and Course Coordinator
- SJC Hacker Space Founder
- Speaker (AppSec California, GrrCon, Angeles y Demonios, BSides Augusta, BSides SP, BalCConf2k14, H2HC, SegInfo, ITA, INPE, CNASI, RoadSec etc.)

INTRODUCTION

This article aims to demonstrate, in a simplified way, a different approach for capturing and intercepting network traffic data originating from an iPhone device.

Obviously, the iPhone is not the only device subject to these approaches, and the strategies presented here are not the only ones capable of performing such intercepts.

The simplest way to get this data is to use a proxy server. In the first part of this article, we will adopt BURP software to exemplify this operation. After collecting the data, we will analyze the packages of a given application and its connection to the WEB services.

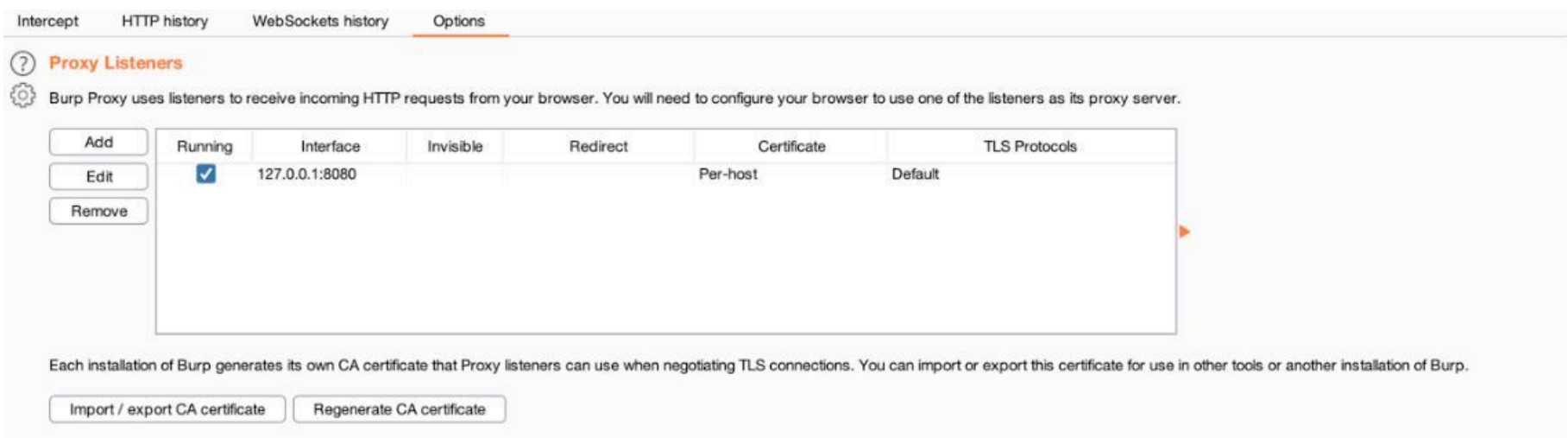
However, if the objective is a more detailed analysis of the traffic of an application that uses communication ports other than WEB requests, we can diversify the strategy and use a remote virtual interface (RVI), as we will demonstrate in the second part of this article.

PART 1 - USING A PROXY SERVER – BURP

When we mention the use of a proxy server, we are basically referring to intercepting and analyzing requests related to the HTTP (Hypertext Transfer Protocol), whether the one with the TLS (Transport Layer Security) security layer or not.

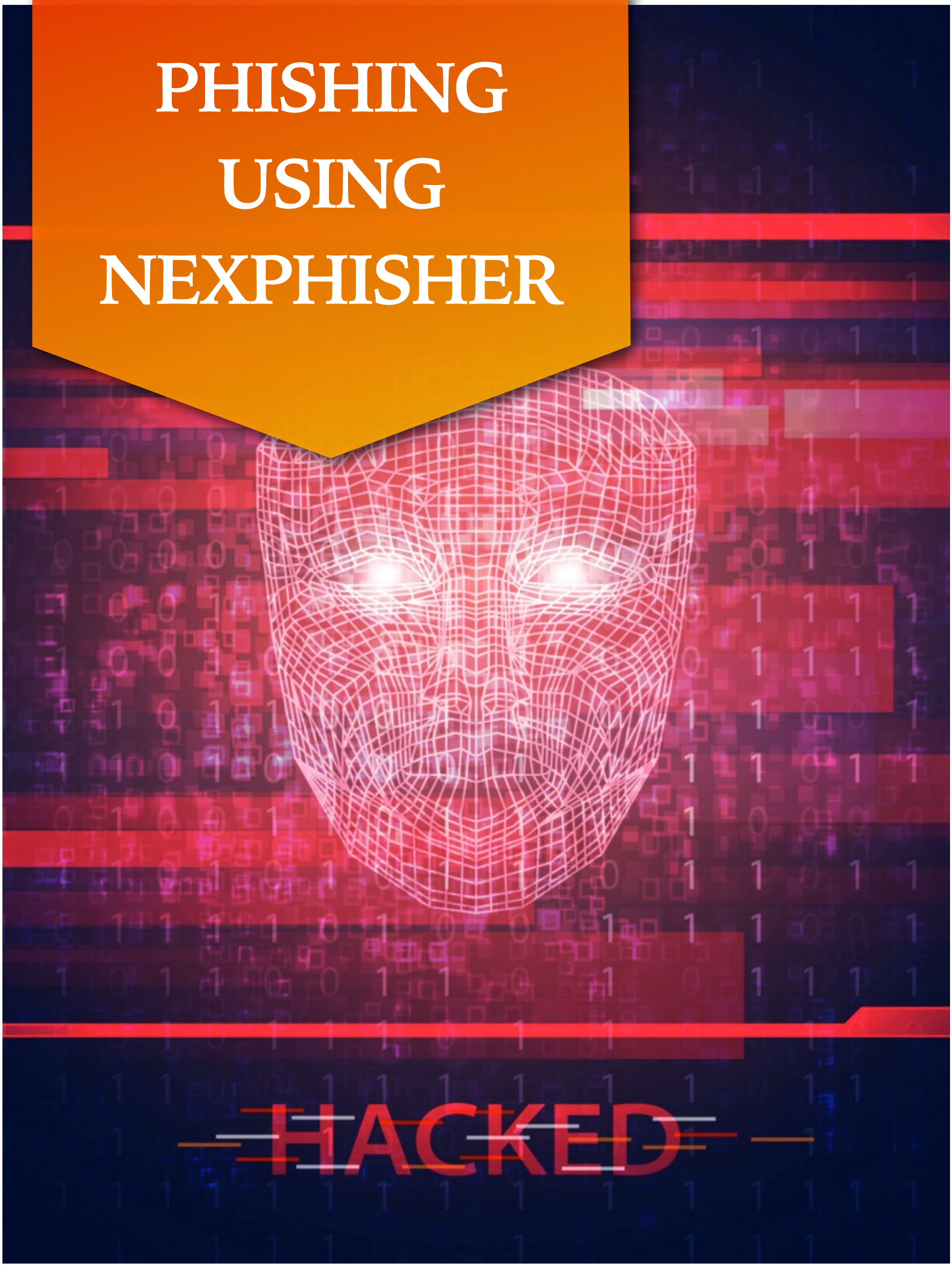
Some of the applications we have on our smartphones still only use the HTTP protocol, which means that data travels in plain text form, that is, without any encryption, making sensitive information fully exposed to any attacker who adopts techniques like man in the middle.

To configure our proxy, the first step is to open BURP software, by default the interface it will be listening to will be the equipment itself, that is, the IP address 127.0.0.1 and port 8080, as we can see in the image below:



In BURP, every capture is by default related to the local machine, but to execute our strategy of intercepting the data that

PHISHING USING NEXPHISHER





MAYUKH PAUL

I am a typical college student with a keen interest in the field of cybersecurity and social engineering. The art of psychologically manipulating people into performing actions or divulging confidential information intrigues me.

I enjoy trying out new tools and exploiting new vulnerabilities. The more vulnerabilities I exploit, my urge to learn increases.

I aim to dive more into the field of cybersecurity research and protect company security against cyber threats.

Phishing is a category of social engineering attack often used to trick a victim and steal their data, such as login credentials, credit card details, PIN, etc.

Phishing takes place when an attacker deceives a victim into opening a malicious link through email, messages, etc., which leads to a ransomware attack, installation of malware, and in most cases revealing sensitive information, which might lead to huge losses. Such an attack might be very devastating to the user as it might lead to identity theft, unauthorized purchases, or stealing of funds.

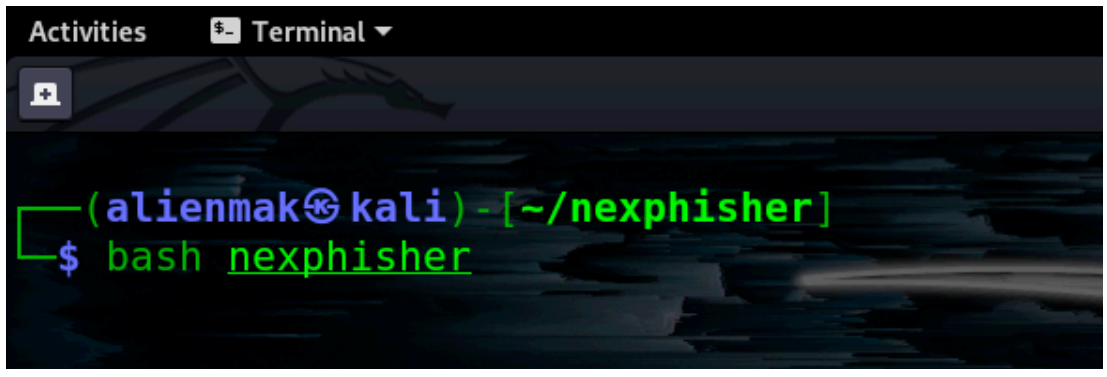
Some of the common types of phishing are:

- **Spear Phishing:** This type of phishing is mostly targeted to a specific group or individual.
- **Whaling:** This type of phishing attack is targeted to an employee in a high position, such as CEO, CTO, etc.
- **Smishing:** This attack is executed by using text messages or SMS.
- **Vishing:** This attack is executed over a voice call. Vishing is short for Voice Phishing.
- **Search Engine Phishing:** This type of phishing involves the attacker aiming to be the top search of a search engine to trick a mass amount of users. Clicking on the link, the users are tricked into visiting their malicious website.

Let me show you how easy it is to create a phishing page for various social media sites. Here I have NexPhisher, an automated Phishing tool having 37-page templates. It also has five port forwarding options.

You can clone NexPhisher from here: https://github.com/htr-tech/nexphisher

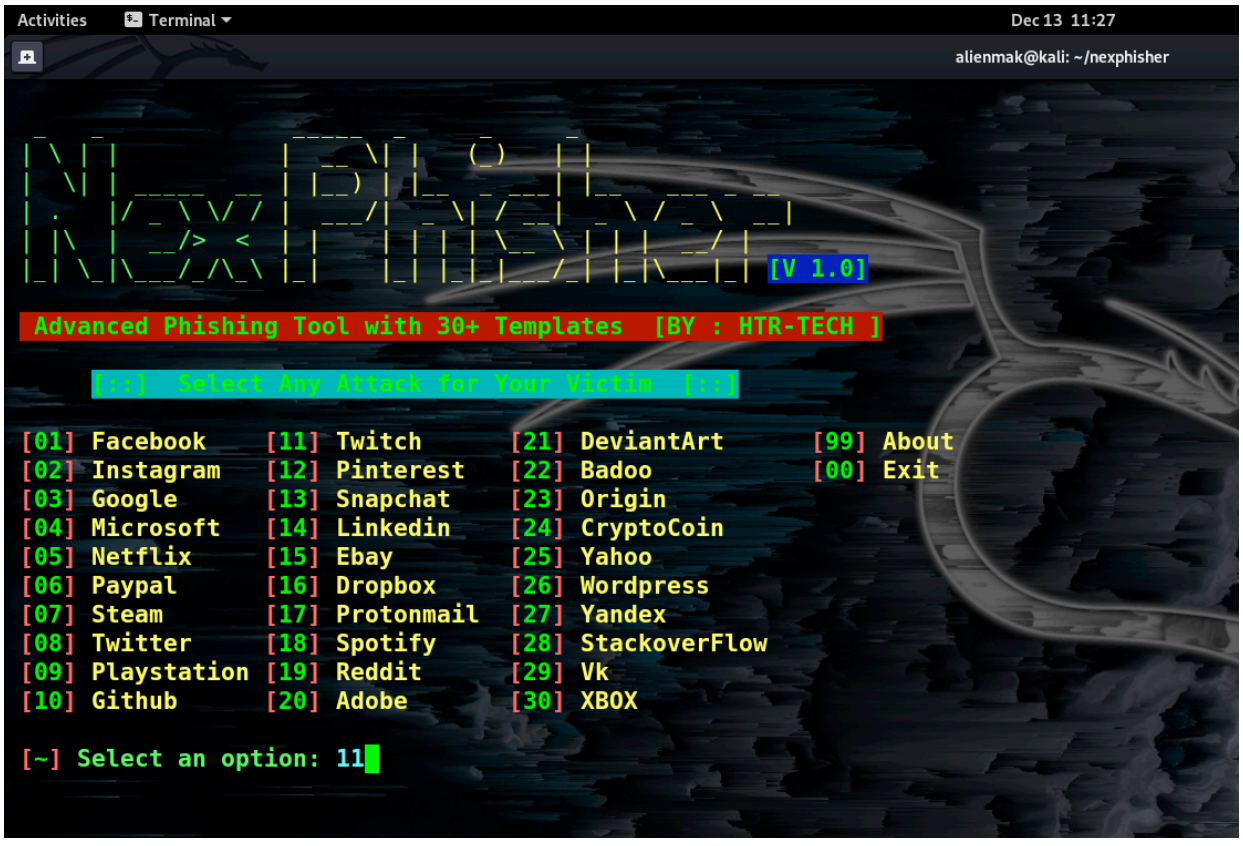
To start up NexPhisher once installed we use the command 'bash nexphisher' as NexPhisher is written in shell.



NexPhisher has initial 30 templates of different social media.



Let's try cloning a twitch page to phish for a twitch username and password.



Next, we get five port forwarding options:

- ☑ LocalHost
- ☑ Ngrok
- ☑ Serveo
- ☑ LocalXpose

SMISHING - PHISHING ATTACKS THROUGH TEXT MESSAGES



CLEBER SOARES

Enthusiast and researcher in Information Security adept at free software culture, he has worked in the technology area for more than 20 years, passing through national and multinational companies. Has technical courses in Data Processing, graduated in Computer Networks and some postgrad work in Ethical Hacking and Cyber Security. Acts as Information Security Analyst and Ad-hoc Forensic Computer Expert. Leader of the OWASP Belém Chapter at the OWASP Foundation and author at Hacker Culture.



DEIVISON FRANCO

CEO at aCCESS Security Lab. Master's degrees in Computer Science and in Business Administration. Specialist degrees in Forensic Science (Emphasis in Computer Forensics) and in Computer Networks Support. Degree in Data Processing. Researcher and Consultant in Computer Forensics and Information Security. Member of the IEEE Information Forensics and Security Technical Committee (IEEE IFS-TC) and of the Brazilian Society of Forensic Sciences (SBCF). CIEH, CIHFI, DSFE and ISO 27002 Senior Manager. Author and technical reviewer of the book "Treatise of Computer Forensics". Reviewer and editorial board member of the Brazilian Journal of Criminalistics and of the Digital Security Magazine.

The world is evolving so fast that it's hard to keep up with all the new technologies. Thus, crimes committed through technological devices are full of peculiarities that differ from conventional crimes. Phishing, for example, which is fraudulently obtaining electronic data over the internet, is generally typified as embezzlement or qualified theft, the consequences of which can open security breaches and cause damage to companies.

In this article, Smishing will be presented, a type of technological fraud, a variant of Phishing, as well as Spear Phishing, Vishing, Offline Phishing, Dumpster Diving, Typosquatting, QR Code phishing, Pharming and Link Shorteners. This article will clarify and help the target audience to know the possibilities of attacks it is exposed to and to position itself in front of them, as well as ways to prevent and avoid them in the corporate use environment, or in the personal use environment.

THE ORIGIN OF PHISHING

On January 28, 1996, the term phishing emerged from an attempt to obtain Internet access credentials from employees of the world's largest Internet provider, AOL-America Online, which distributed promotional floppy disks and CDs with some hours of free internet access, making it quite popular.

In a forum called "AOL for free?", user mk590 posted the following sentence:

"*What happens is that in the past, you could make a fake AOL account once you had a credit card generator. However, AOL was smart. Now, after entering the card details, a check is done with the respective bank. Does anyone else know any other way to acquire an account than through Phishing?*"

At that time, to connect the dial-up internet to the digital world from the AOL provider, users had to register using their credit card.

Cybercriminals starting to share a free distributed program called AOHell, having its first version released in 1994 by unknown authors who generated random credit card numbers to perform the registration to open accounts, because AOL did not carry out validation. As time went on, the company started to validate the numbers together with the credit card companies.

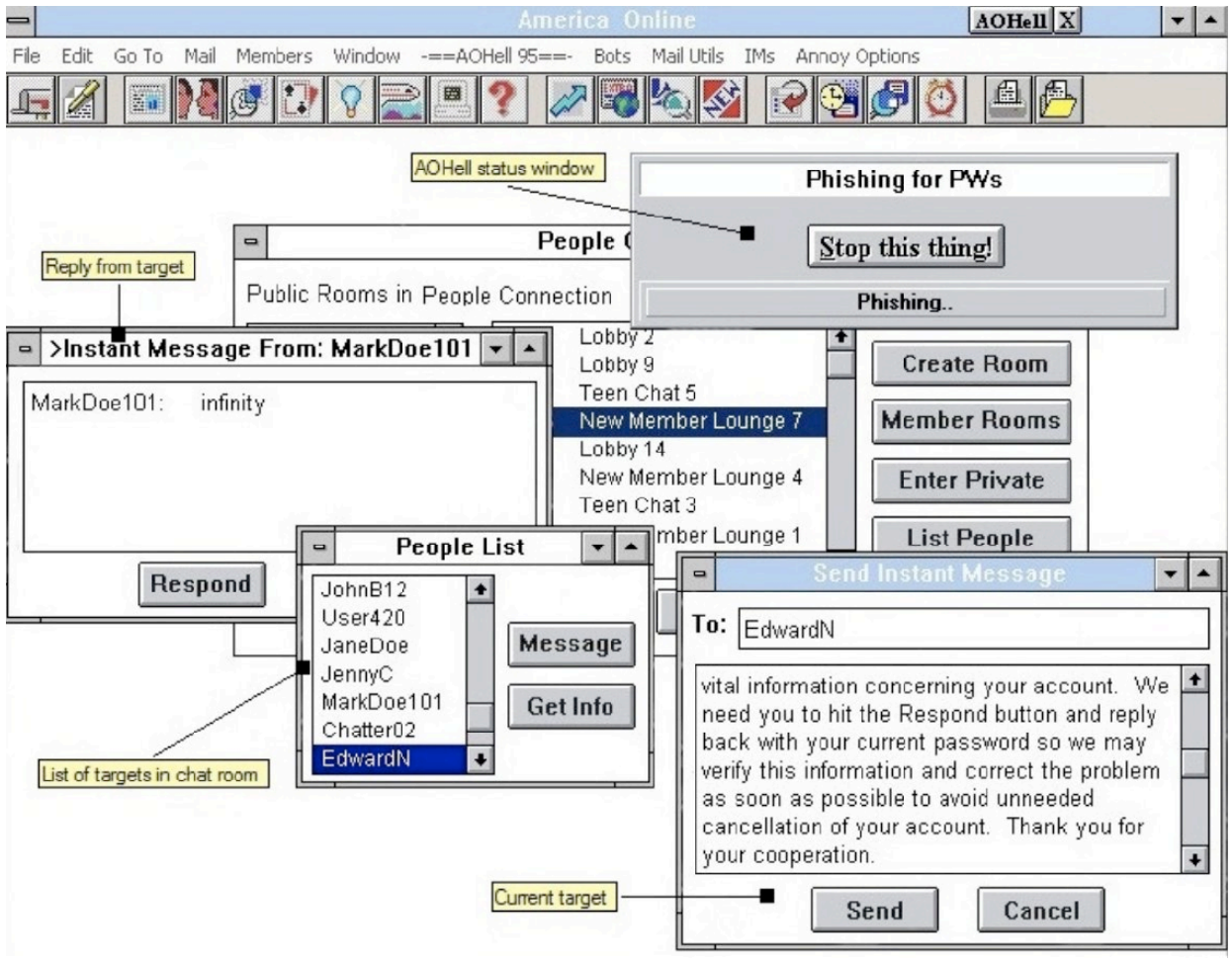


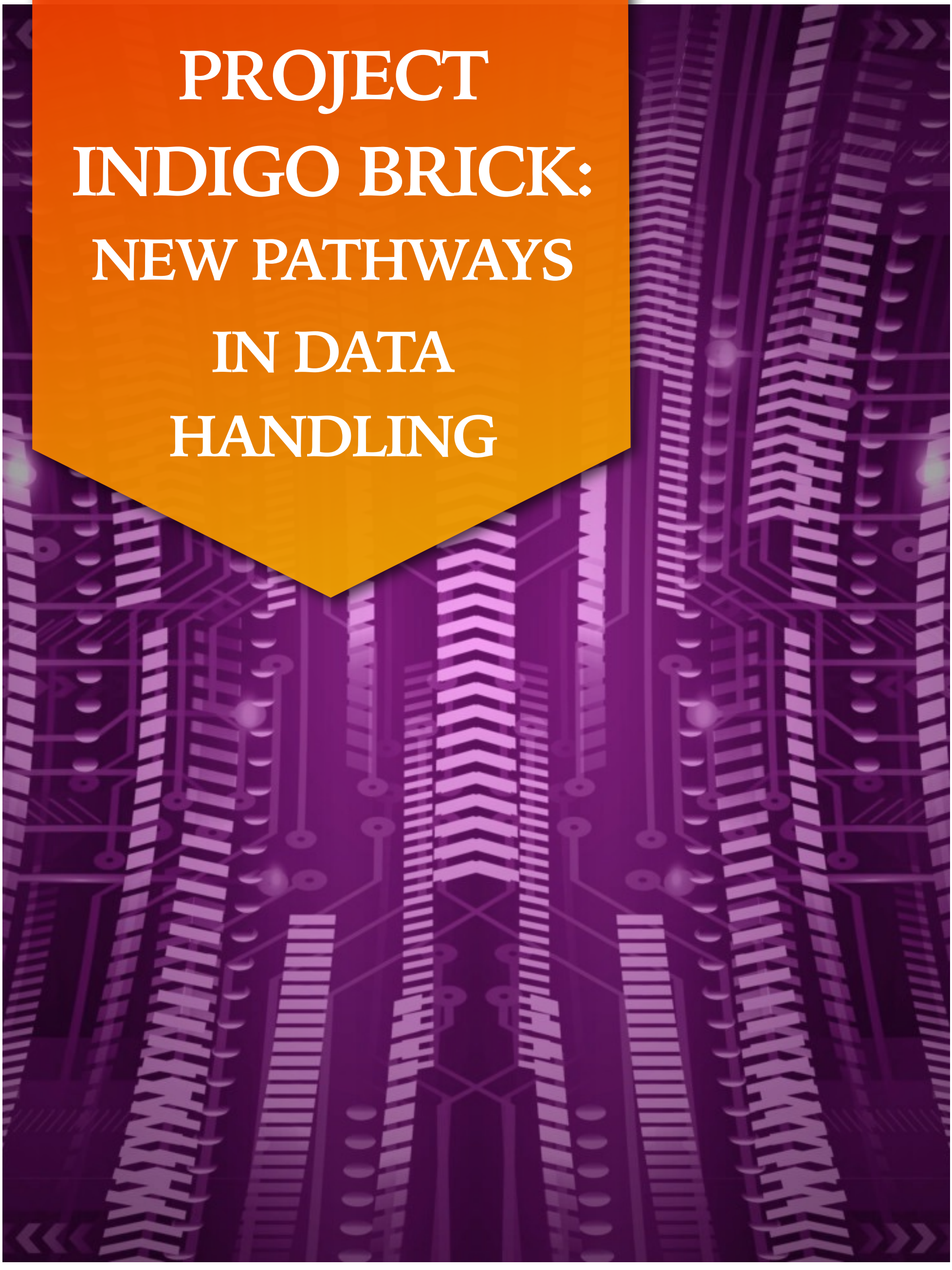
Figure 1. AOHell program, managed AOL credentials and credit cards.

SPAM AND PHISHING: WHAT DO THEY HAVE IN COMMON?

The acronym Spam corresponds to “Sending and Posting Advertisement in Mass”. Making an analogy, we can say that it would be those flyers, posters or a link offering some product. Spammers, as those in charge of this type of action are known, have their main objective to propagate the greatest possible number of inopportune emails to various users, which may be malicious or just sending advertisements for products and services, sometimes questionable, as having excessive advantages.

Many email services have protections and provide reporting tools. However, according to Cert.br, the group responsible for responding to and handling Internet Security Incidents in Brazil, maintained by NIC.br (Ponto BR Information and Coordination Center), in 2019, 867,920 unwanted emails were reported.

PROJECT INDIGO BRICK: NEW PATHWAYS IN DATA HANDLING





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 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.

Let's face it, you can't look at your phone, catch the local news or your favorite tech blog and not see or hear about a recent ransomware attack and each attack seems to be getting more sophisticated and severe with each occurrence. From Linux to Windows, and all the OS's in between, it seems there is a new security patch everyday to combat the growing ransomware problem. Vast resources from private and government entities have been allocated to fight this war. If it was a mere resource problem, we would be closer to a solution, given the major corporate players that are dumping millions into the coffers to solve the issue. However, this is a new quandary that needs a fresh fix.

In this article, we will not only explore the landscape of the problem that arises from ransomware attacks, but also some patent pending software we have created that we believe can make a global difference in this fight and secure our data with a new, dynamic solution. What is this solution, you ask? It's called Project Indigo Brick.

It can be utilized as middle-ware, virtualized or configured and installed at the bare metal layer of any data infrastructure.

Project Indigo Brick is the project's internal code name and was derived from one of my gamer profiles. We are still working on marketing for a new name for the technology.

WHAT IS RANSOMWARE?

Simply put, ransomware is a piece of malware that is employed to hold the victim's data hostage until a fee or "ransom" is paid to release the encryption key so the victim can unlock and access their data. Some of the first instances of ransomware, you may remember, utilized an "antivirus out of date" alert box that would pop up and once you interacted with the message, it would deploy the malware thus locking your system. Later on, the victim would receive a phone call or an email with a demand for payment to unlock the system and return control of the data back to the victim. This was the early days of ransomware and involved attacking individuals rather than today's attacks on large enterprises.

Today ransomware has graduated to a very sophisticated level of exploitation that has put our livelihoods at stake by attacking the very infrastructure in which our systems and processes deliver goods and services, thus providing convenience, health and safety to billions of people worldwide.

Ransomware has become an example of a "dark business model" being adopted by a variety of threat actors in many theaters, and cyber criminals from a variety of backgrounds are cashing in on the trend. Creation and resale of ransomware is also a huge business in which nefarious engineers can find a niche in this sector of this growing threat landscape. While the true cost of ransomware is hard to truly determine, the shock waves definitely ripple throughout our current infrastructure and usually ends in a chaotic spiral that impacts the bottom line of many industries.

IMPACT OF RANSOMWARE

Data worth trillions is at rest on servers all over the world. Data at rest on a server is a sitting duck, waiting to be stolen by highly intelligent, extremely skilled and strikingly malicious cyber criminals who can literally out-think and outmaneuver

current security infrastructure and professionals whose job it is to protect the data that their enterprises require to stay in business.

Cybercrime has become an acceptable loss that costs industries around the world billions every year. In fact, damage related to cybercrime is set to hit $6 trillion by the end of 2021, making investing in security spending a priority.

Our world requires a more effective and global defense against frontal attacks on the data foundation and infrastructure that, when compromised, can bring the downfall of the financial systems, the grid, healthcare, transportation, all branches of government, the military, every business, charities and schools. It all runs on data, and all of that data is at risk in the hands of hackers, both foreign and domestic, who have figured out how to penetrate some of the largest and most secure data stores on earth. Below are some, but definitely not all, of the statistics that display only a fraction of the impact of ransomware attacks.

- 90% of all financial institutions have experienced ransomware in the past year. (betanews.com)
- Atlanta – The ransomware demand was $51,000 (unpaid) while the recovery costs were estimated at $17 million.
- The NotPetya ransomware attack cost FedEx $300 million in Q1 2017. (Source: Reuters)
- A disabling virus spread to 10,000 machines in TSMC's most secure and advanced facilities.
- The fitness brand Under Armour breach affected 150 million users.

Financial Institutions – in 2019:

- More than 204,448 users experienced an attempt to hack their banking information
- More than 280,000,000 URLs were identified as malicious
- Cybersecurity statistics show attacks were launched from within more than 190 countries
- Attacks on individuals doubled in 2018
- Attacks on businesses increased to one every 40 seconds
- Colonial Pipeline in 2021

LASTING IMPACT:

Another aspect of a ransomware attack is the lasting impact it inflicts upon communities everywhere. Long after the ransom is paid, the company somewhat rebounds with stored backups and the attackers are apprehended, the effects of the incident can still be felt once the dust settles. Whether it is a temporary loss of a service, an increase in the cost of a utility or, in some cases, as in the case of several clinics around the world, it can be total financial ruin, thus cutting support from thousands of people who depend on those services to maintain their daily quality of life. It seems not even healthcare and

ROGUE - HACKERS, RAT AND "MARKETING" ON THE DARK WEB



FELIPE HIFRAM

He is currently an information security professional focused on social engineering, good usage habits and privacy on the internet. He has already done work in Brazil, Germany, Ukraine, Oman and Bahrain, in addition to writing several other articles.

1 PRINCIPLE OF EVERYTHING

It is a fact that nowadays many cyber criminals expose their achievements in forums via the dark web, but I swear to you that in my years of experience with cybersecurity, I have never seen marketing as strong as I am seeing with RAT Rogue. A few years ago, in 2017, a hacker nicknamed Triangulum appeared on some forums on the dark side of the internet, apparently in search of recognition. For a while he exposed his skills (which were not at all impressive) in the forum, then tried to sell one of his products, but did not have the fame I believe he was looking for.

Triangulum sought partnerships, as revealed by some reports of its activity in the forum, in 2017. And we believe that it was in this search that it obtained the support of HeXaGoN, another hacker, known for his high ability in the development of RAT Tools and other malware. Support was what was apparently missing, so for more than a year Triangulum disappeared from the network, returning in April 2019, already with a new product to sell, and in the middle of 2020 announced four different products on the network.

The partnership with HeXaGoN was perfect, since now we had real “Steve Jobs and Steve Wozniack” together, while one was developing new tools, another was engaged in marketing.

Marketing started to be treated with more importance by Triangulum, it was noticeable his commitment in creating attractive and well made images to advertise his “products”.

Some failures in negotiations with Russian forums have also been found.

2 ROGUE, THE CROWN JEWEL

After acquiring some experiences with marketing within the forum environments, the pair started to focus their efforts on the newest product, a powerful MRAT malware, capable of giving almost full access to any infected Android phone.

After an analysis, it was discovered that Rogue is actually a mixture of two known malware, DarkShades and Hawkshaw.

DarkShades was developed by HeXaGoN, which announced its sales in 2019, but three days later officially sold the malware to Triangulum. And Hawkshaw was malware whose source code leaked onto the network in 2017.

The joining of the families of these malware resulted in what we know today as Rogue.

2.1 A technical look

Rogue is a persistent malware; when it infects a device, it will soon ask for all the permissions it needs to start its activity, and it will continue to request all of them until the user surrenders and gives permission. After that, the malware will camouflage itself, hiding its own icon, in addition to registering as a device administrator.

And it doesn't stop there, if the user tries to remove Rogue from his administrator post, a message will be displayed “Are

SECURING THE SUPPLY CHAIN



SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering, and Cyber Security teams.

“Software is eating the world" – Marc Andressen

INTRODUCTION

At no time since the dawn of the Industrial Revolution have manufacturing businesses thrived on the diversification and choice of vendors, the globalization of suppliers and manpower services, and the accelerated growth of the customer base due to improved infrastructure, shipping routes, and the internet.

However, as software has brought immense accessibility and reach to billions of customers, it has also become an Achilles heel when used in concert with bad actors to disrupt, destroy and debilitate otherwise healthy and profitable organizations.

DEFINITION

As defined by Wikipedia *"A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. A supply chain attack can occur in any industry, from the financial sector, oil industry, to a government sector.”*. Although there are many ways to define and explain this term, the key takeaway from this definition is the “*less-secure*” element that is a constant in all forms of cyber security defense conversations.

BACKGROUND

The “*modus operandi*” of a supply chain attack centers around an individual or team of bad actors targeting an organization not directly (as that would be too obvious) but rather through an external trusted partner or supplier who may have some manner of access to the organization’s systems. This new route for hackers has grown within the last few years and has transformed the attack surfaces significantly from not just the target organization itself but now across all companies, suppliers, and service providers that have any manner of touchpoints within the organization.