CyberForge
ACADEMY

Metasploit - 101

What, Why & How

$ whoami

- Software Engineer and Researcher at CyberForge Academy
- Research, Creating course content/setups, developing SaaS software and open source tools
- For past 6 months, interned with Singapore based Web3 education startup
- Final year, B. Tech. CSE @ LPU Jalandhar
- Interests:
  - Tech 👨‍💻
  - Cricket 🏏
  - Food 🍕

CyberForge
ACADEMY

Table of contents

01
What is Pentesting

02
vsftpd vulnerability

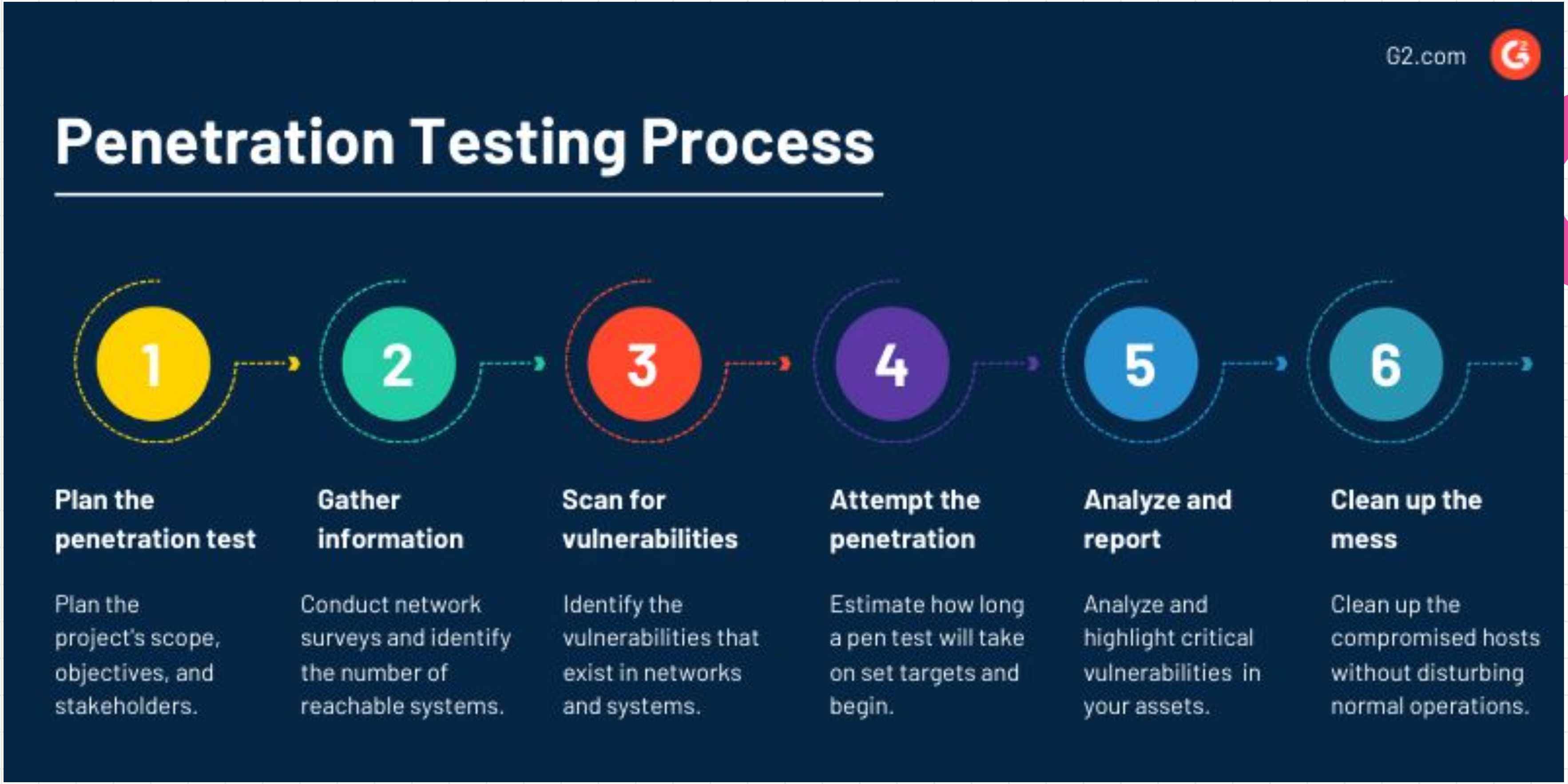
03
Exploit vsftpd manually

04
Introduction to Metasploit

05
Exploit with Metasploit

06
Post Exploit Modules

CyberForge
ACADEMY



G2.com

Penetration Testing Process

1. **Plan the penetration test**

   Plan the project's scope, objectives, and stakeholders.

2. **Gather information**

   Conduct network surveys and identify the number of reachable systems.

3. **Scan for vulnerabilities**

   Identify the vulnerabilities that exist in networks and systems.

4. **Attempt the penetration**

   Estimate how long a pen test will take on set targets and begin.

5. **Analyze and report**

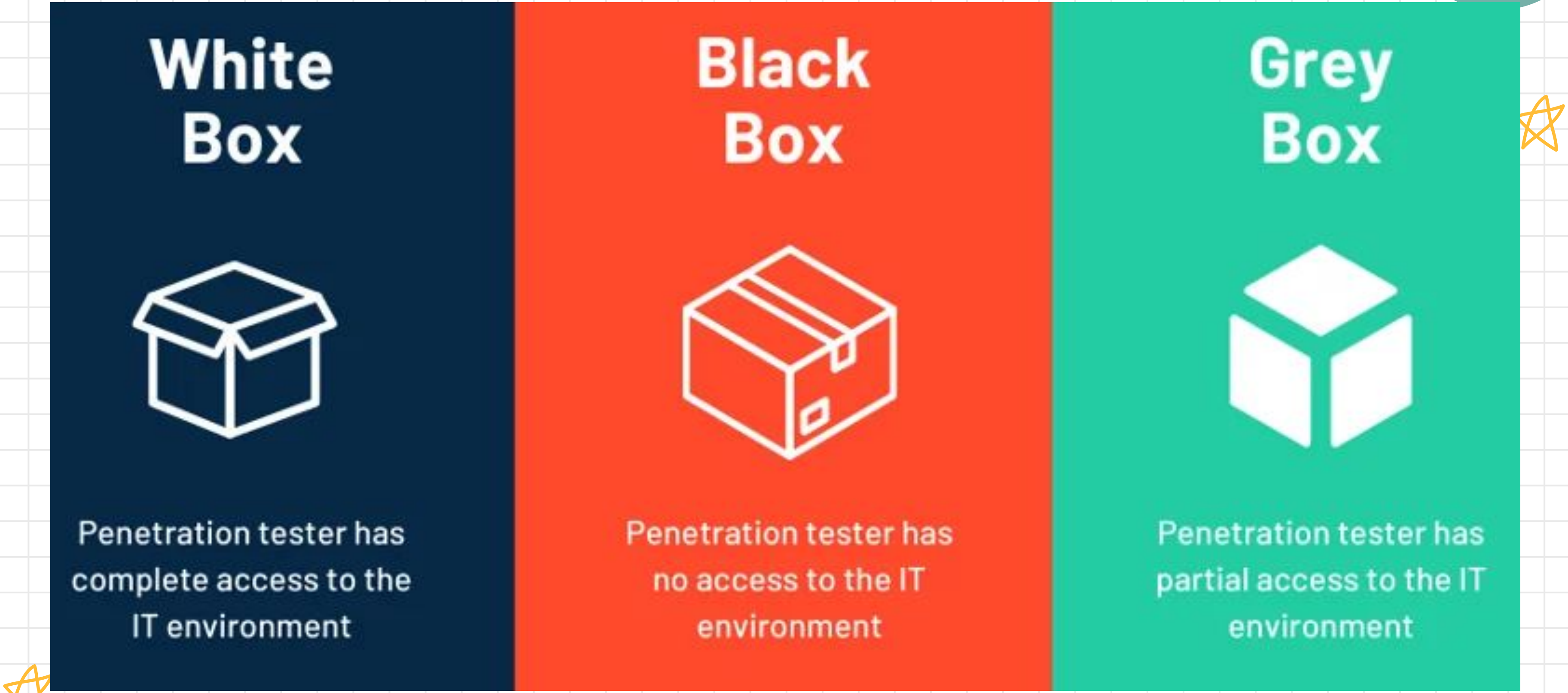
   Analyze and highlight critical vulnerabilities in your assets.

6. **Clean up the mess**

   Clean up the compromised hosts without disturbing normal operations.

Source: https://www.g2.com/articles/penetration-testing

CyberForge
ACADEMY



White Box

Penetration tester has complete access to the IT environment

Black Box

Penetration tester has no access to the IT environment

Grey Box

Penetration tester has partial access to the IT environment

Source: https://www.g2.com/articles/penetration-testing

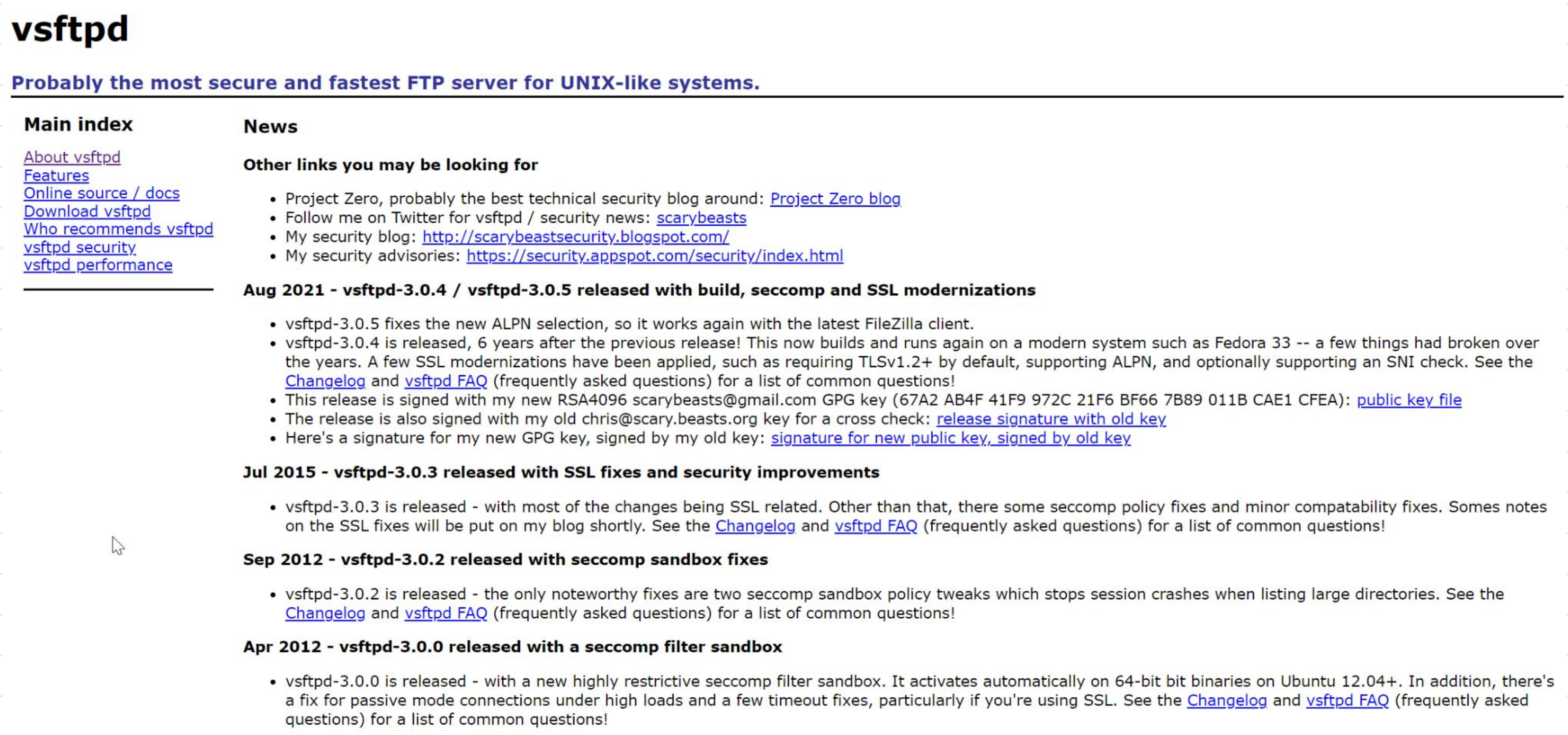
What is Vulnerability

- Weakness or flaw in a system
- Exploited by attackers to compromise its security.
- Forms:
  - Vulnerable System
  - Infected File
  - Backdoors
  - Spear Phishing
  - SQL Injection

vsftpd

- Very secure ftp daemon
- Lightweight, secure and stable
- Key Features:
  - Secure
  - Efficient
  - Configurable
  - User Management

CyberForge ACADEMY



vsftpd

Probably the most secure and fastest FTP server for UNIX-like systems.

Main index

- About vsftpd
- Features
- Online source / docs
- Download vsftpd
- Who recommends vsftpd
- vsftpd security
- vsftpd performance

News

Other links you may be looking for

- Project Zero, probably the best technical security blog around: Project Zero blog
- Follow me on Twitter for vsftpd / security news: scarybeasts
- My security blog: http://scarybeastsecurity.blogspot.com/
- My security advisories: https://security.appspot.com/security/index.html

Aug 2021 - vsftpd-3.0.4 / vsftpd-3.0.5 released with build, seccomp and SSL modernizations

- vsftpd-3.0.5 fixes the new ALPN selection, so it works again with the latest FileZilla client.
- vsftpd-3.0.4 is released, 6 years after the previous release! This now builds and runs again on a modern system such as Fedora 33 -- a few things had broken over the years. A few SSL modernizations have been applied, such as requiring TLSv1.2+ by default, supporting ALPN, and optionally supporting an SNI check. See the Changelog and vsftpd FAQ (frequently asked questions) for a list of common questions!
- This release is signed with my new RSA4096 scarybeasts@gmail.com GPG key (67A2 AB4F 41F9 972C 21F6 BF66 7B89 011B CAE1 CFEA): public key file
- The release is also signed with my old chris@scary.beasts.org key for a cross check: release signature with old key
- Here's a signature for my new GPG key, signed by my old key: signature for new public key, signed by old key

Jul 2015 - vsftpd-3.0.3 released with SSL fixes and security improvements

- vsftpd-3.0.3 is released - with most of the changes being SSL related. Other than that, there some seccomp policy fixes and minor compatability fixes. Somes notes on the SSL fixes will be put on my blog shortly. See the Changelog and vsftpd FAQ (frequently asked questions) for a list of common questions!

Sep 2012 - vsftpd-3.0.2 released with seccomp sandbox fixes

- vsftpd-3.0.2 is released - the only noteworthy fixes are two seccomp sandbox policy tweaks which stops session crashes when listing large directories. See the Changelog and vsftpd FAQ (frequently asked questions) for a list of common questions!

Apr 2012 - vsftpd-3.0.0 released with a seccomp filter sandbox

- vsftpd-3.0.0 is released - with a new highly restrictive seccomp filter sandbox. It activates automatically on 64-bit bit binaries on Ubuntu 12.04+. In addition, there's a fix for passive mode connections under high loads and a few timeout fixes, particularly if you're using SSL. See the Changelog and vsftpd FAQ (frequently asked questions) for a list of common questions!

vsftpd - Secure, fast FTP server for UNIX-like systems (security.appspot.com)

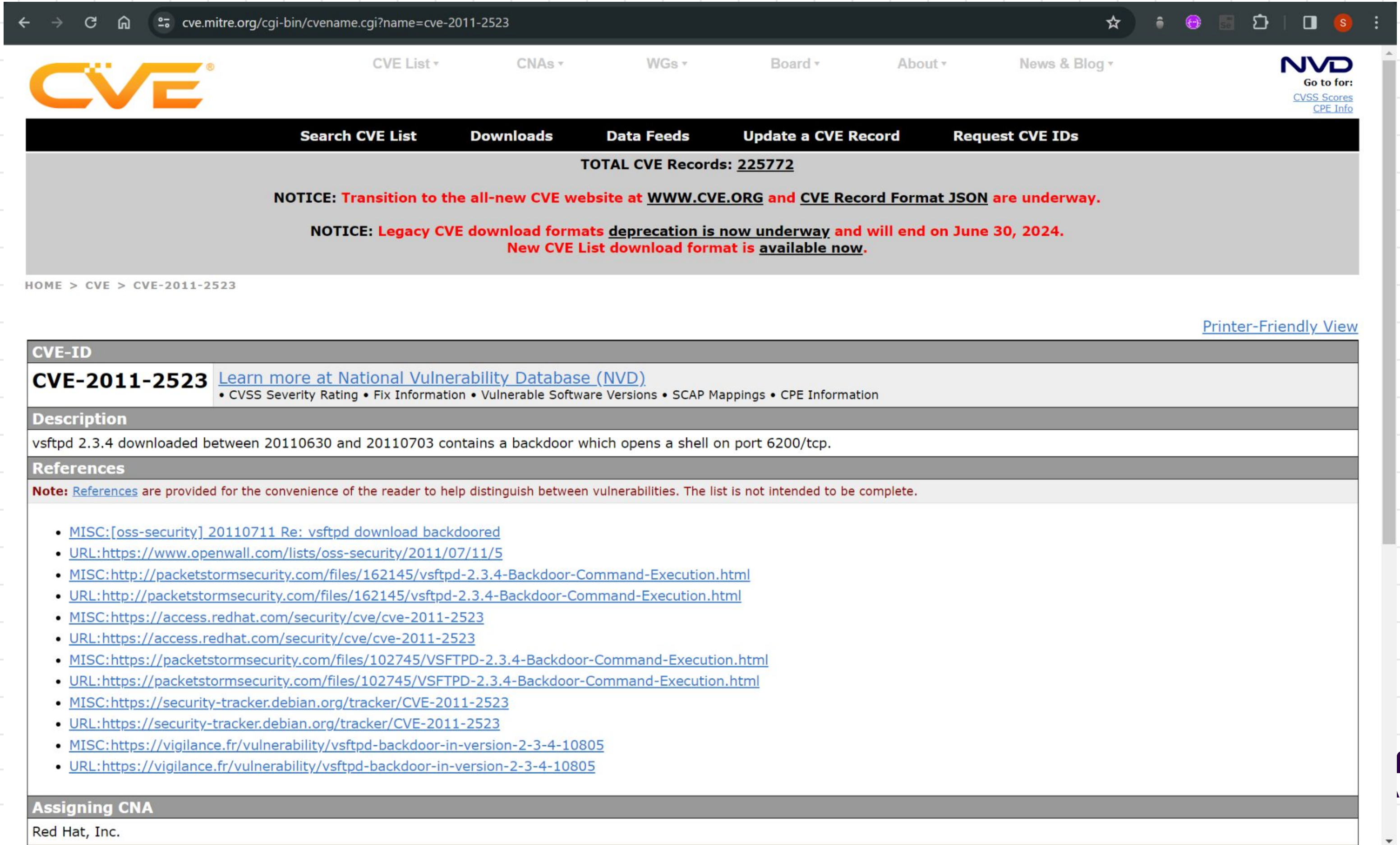
vsftpd backdoor vulnerability

In July 2011, it was discovered that vsftpd version 2.3.4 downloadable from the master site had been compromised. Users logging into a compromised vsftpd-2.3.4 server may issue a ":) " smileyface as the username and gain a command shell on port 6200.
This was not an issue of a security hole in vsftpd, instead, someone had uploaded a different version of vsftpd which contained a backdoor. Since then, the site was moved to Google App Engine.

Read more at: **CVE - CVE-2011-2523 (mitre.org)**

CyberForge ACADEMY

vsftpd backdoor vulnerability



TOTAL CVE Records: 225772

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2011-2523

Printer-Friendly View

CVE-ID	
CVE-2011-2523	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

References

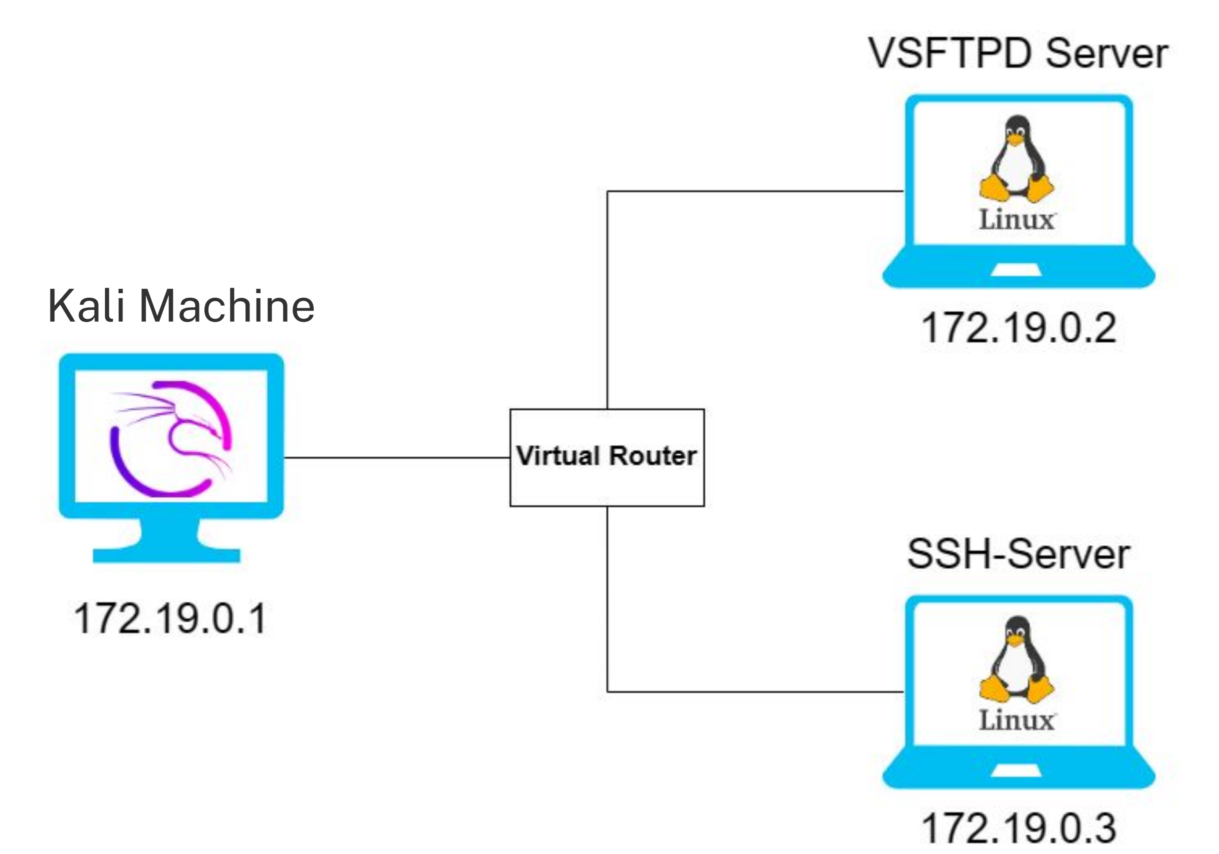
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:[oss-security] 20110711 Re: vsftpd download backdoored
- URL:https://www.openwall.com/lists/oss-security/2011/07/11/5
- MISC:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html
- URL:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html
- MISC:https://access.redhat.com/security/cve/cve-2011-2523
- URL:https://access.redhat.com/security/cve/cve-2011-2523
- MISC:https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html
- URL:https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html
- MISC:https://security-tracker.debian.org/tracker/CVE-2011-2523
- URL:https://security-tracker.debian.org/tracker/CVE-2011-2523
- MISC:https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805
- URL:https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805

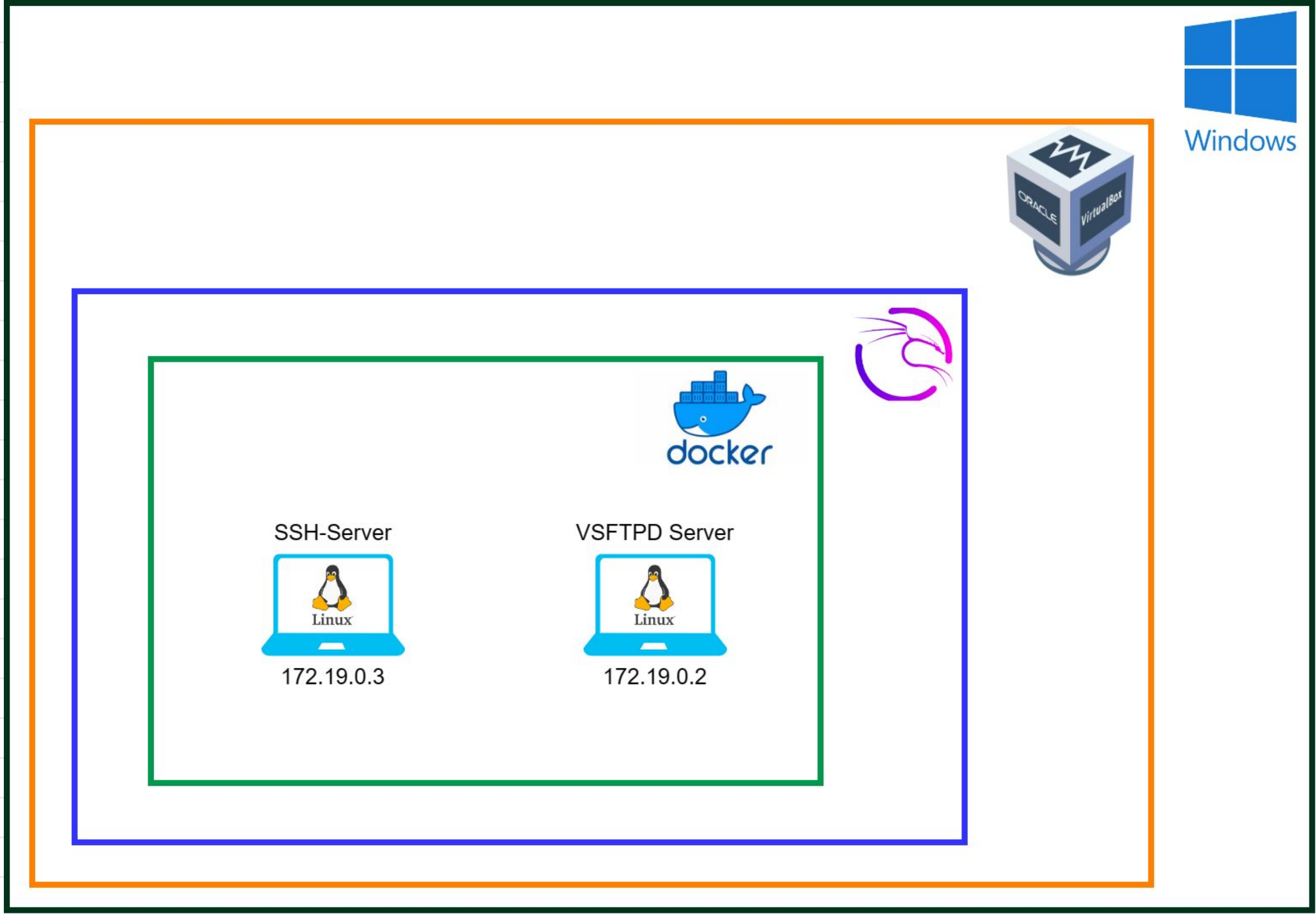
Assigning CNA

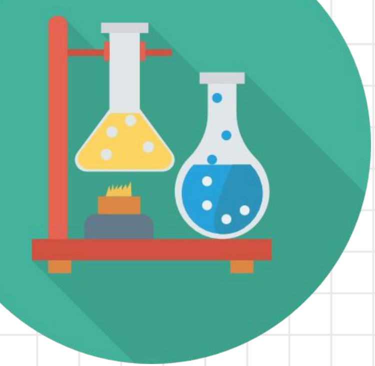
Red Hat, Inc.

Setup


VSFTPD Server
Linux
172.19.0.2
Kali Machine
172.19.0.1
Virtual Router
SSH-Server
Linux
172.19.0.3

Setup


Windows
ORACLE
VirtualBox
docker
SSH-Server
Linux
172.19.0.3
VSFTPD Server
Linux
172.19.0.2



Exploit vsftpd backdoor vulnerability manually

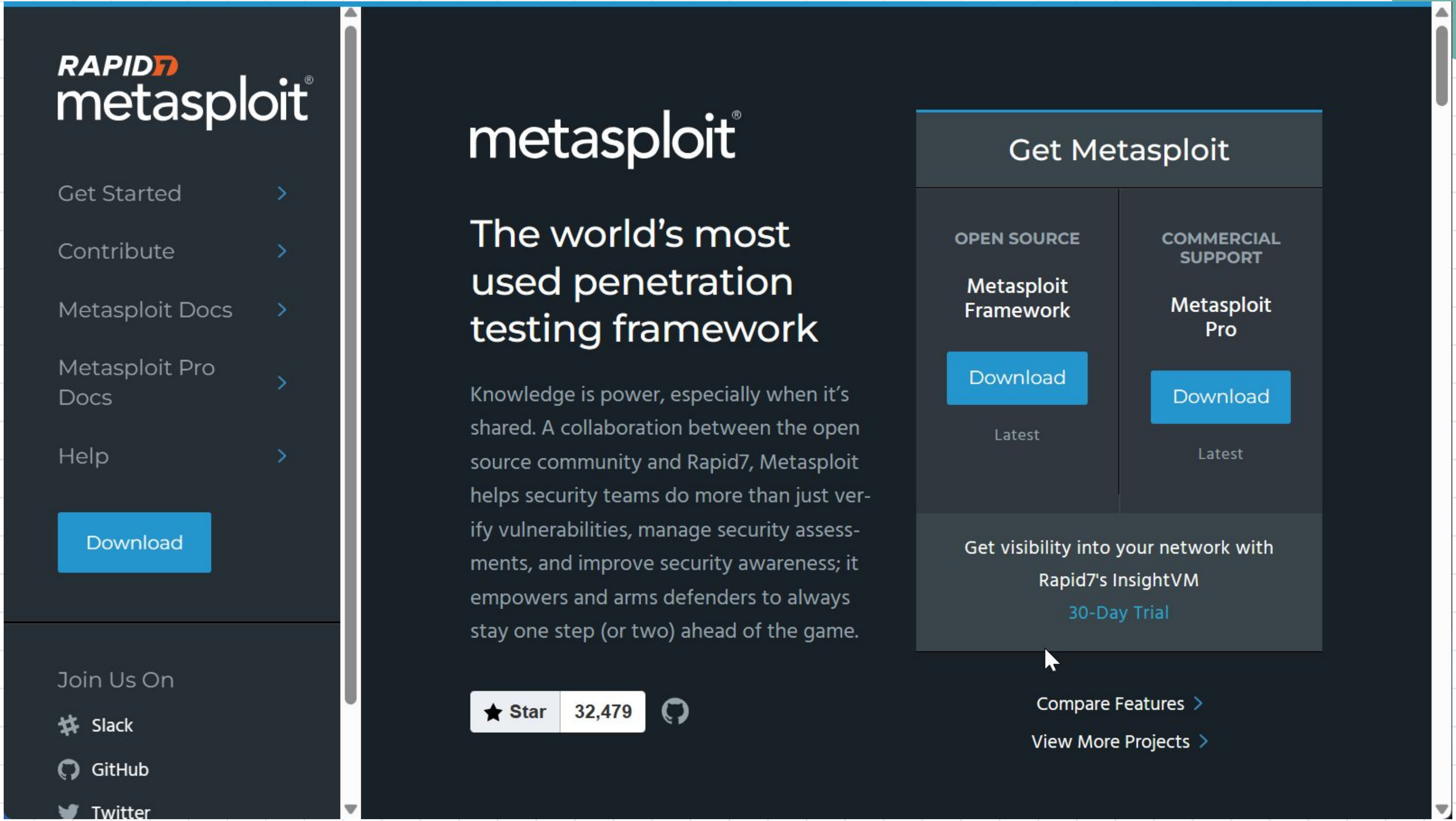
CyberForge
ACADEMY

What is Metasploit?

- Allows to write, test and execute exploit code.
- Most popular penetration testing framework.
- Written in Ruby
- Created by **HD Moore** in **2003**.
- Acquired by **Rapid7** in **October 2009**.
- Cross-platform (Windows/Linux/MacOS)

https://www.metasploit.com/

CyberForge ACADEMY

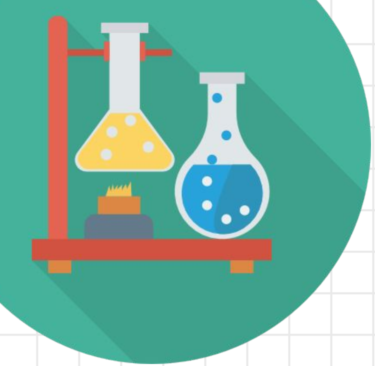


The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

Get visibility into your network with Rapid7's InsightVM 30-Day Trial

Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit



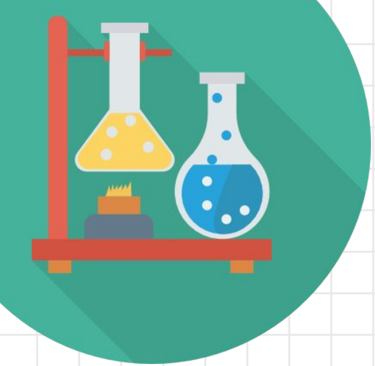
Exploit vsftpd backdoor vulnerability with metasploit

CyberForge ACADEMY

Meterpreter

- Advanced, dynamic payload in the Metasploit Framework.
- Powerful platform for various post-exploitation tasks
- Key Capabilities:
  - Shell Access
  - File system operations
  - Privilege Escalation
  - System Info Gathering

CyberForge ACADEMY



Assignment

Gain unauthorized access to the second machine depicted in the setup, which is currently hosting an SSH service, utilizing a brute-force technique facilitated through Metasploit.

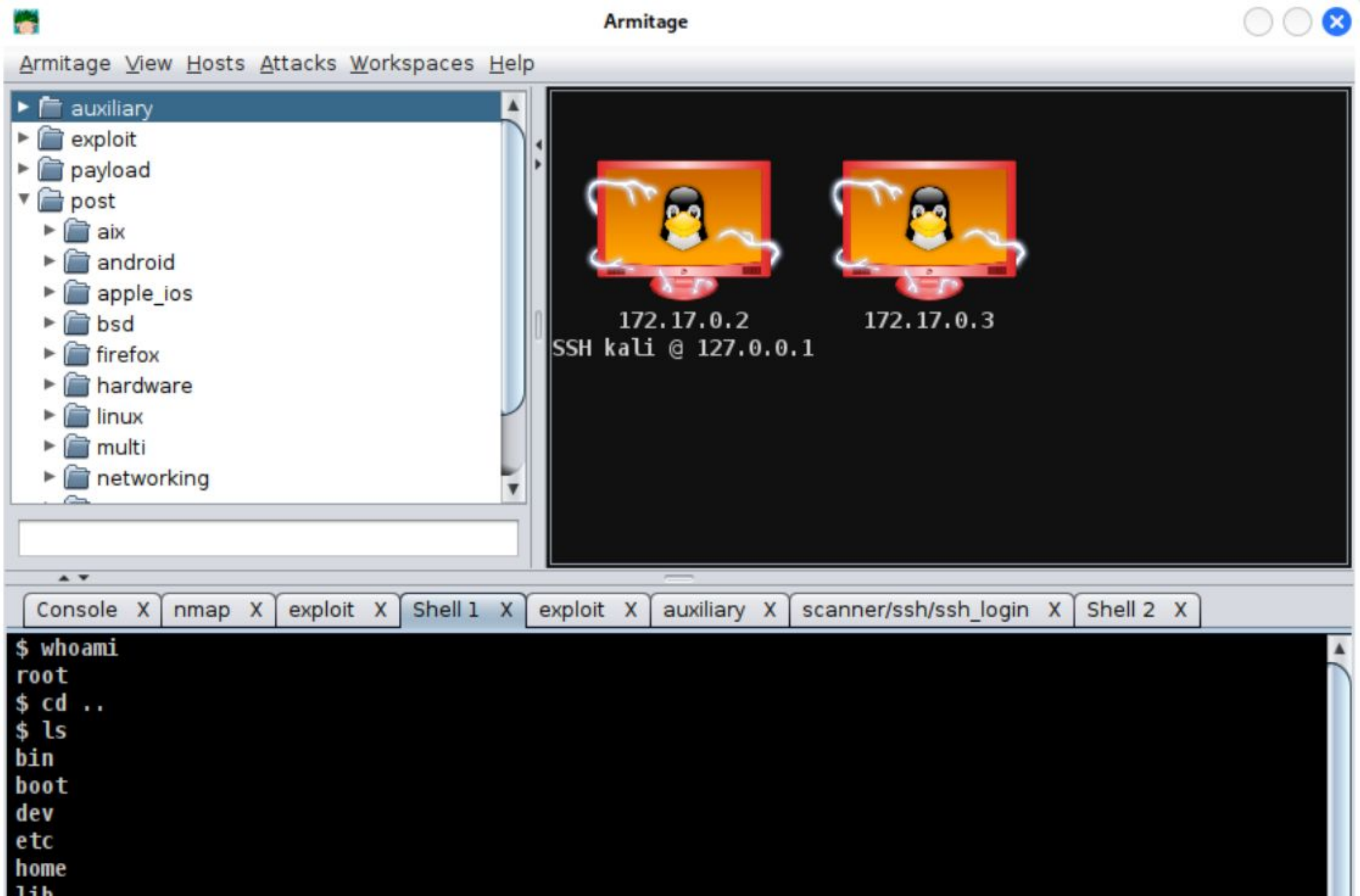
Click here for the github repository with:

- Docker-compose file for setup
- List of usernames
- List of password.

CyberForge
ACADEMY

Armitage

rsmudge/armitage: Automatically exported from code.google.com/p/armitage (github.com)



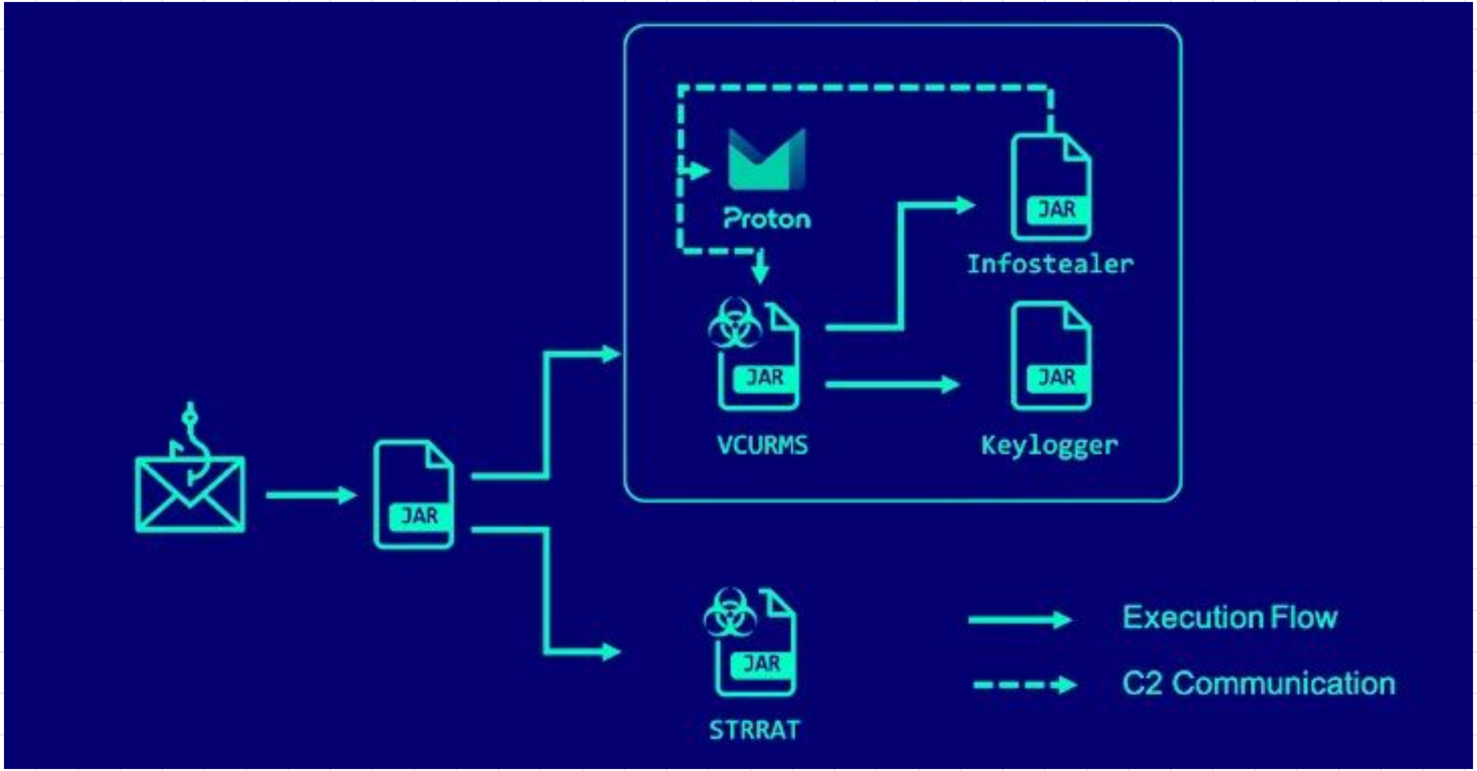
```
$ whoami
root
$ cd ..
$ ls
bin
boot
dev
etc
home
lib
```

CyberForge
ACADEMY

Weekly Cyber Security News

By

Apurva Sharma



Alert: Cybercriminals Deploying VCURMS and STRRAT Trojans via AWS and GitHub

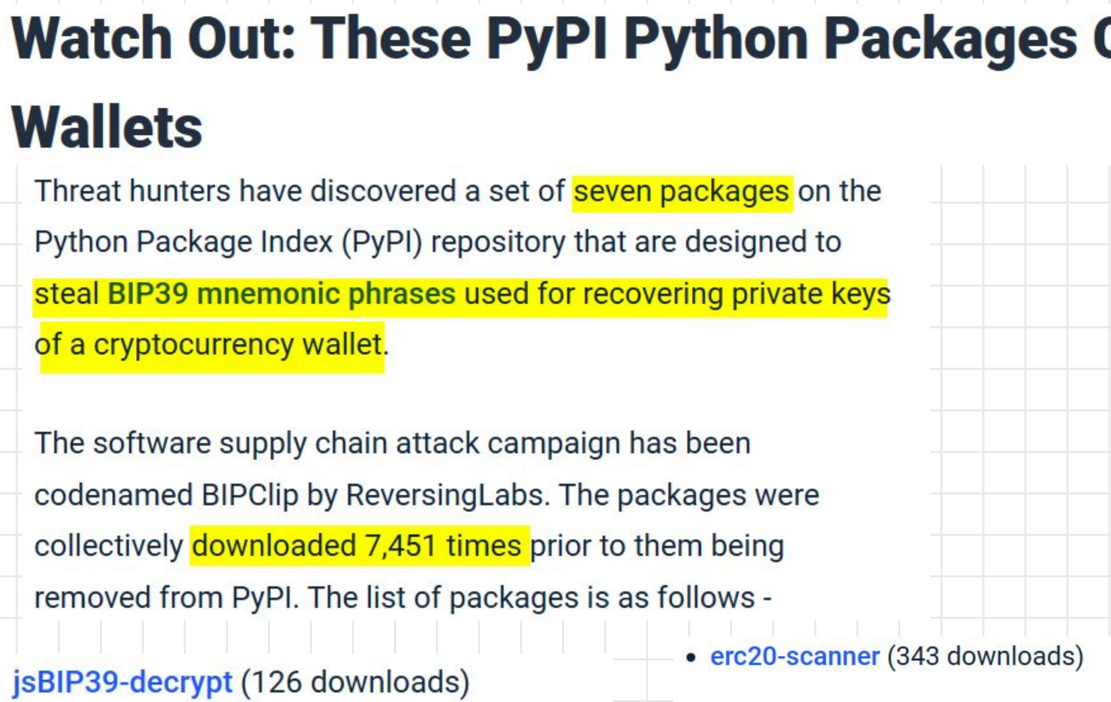
Source: Alert: Cybercriminals Deploying VCURMS and STRRAT Trojans via AWS and GitHub (thehackernews.com)

Researchers Highlight Google's Gemini AI Susceptibility to LLM Threats

Gemini
5G
9:30
Good morning
Find videos of how to quickly get grape juice out of a wool rug
How long will it take to walk from Times Square to Central Park?

Google's Gemini large language model (LLM) is susceptible to security threats that could cause it to divulge system prompts, generate harmful content, and carry out indirect injection attacks.

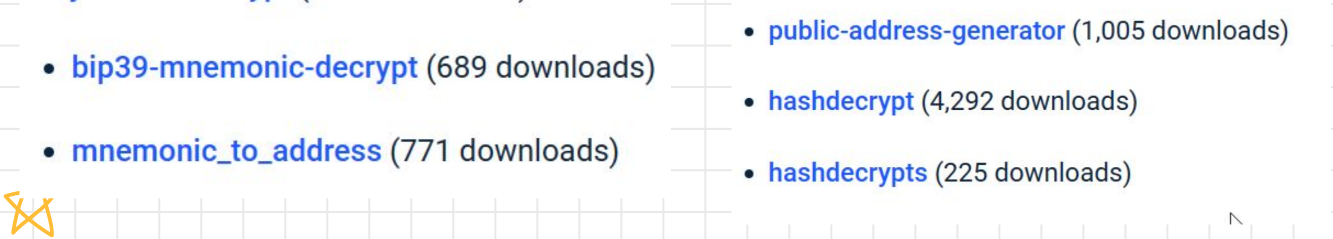
Source: Researchers Highlight Google's Gemini AI Susceptibility to LLM Threats (thehackernews.com)



Watch Out: These PyPI Python Packages Can Drain Your Crypto Wallets

Threat hunters have discovered a set of seven packages on the Python Package Index (PyPI) repository that are designed to steal BIP39 mnemonic phrases used for recovering private keys of a cryptocurrency wallet.

The software supply chain attack campaign has been codenamed BIPClip by ReversingLabs. The packages were collectively downloaded 7,451 times prior to them being removed from PyPI. The list of packages is as follows -



- erc20-scanner (343 downloads)
- jsBIP39-decrypt (126 downloads)
- public-address-generator (1,005 downloads)
- bip39-mnemonic-decrypt (689 downloads)
- hashdecrypt (4,292 downloads)
- mnemonic_to_address (771 downloads)
- hashdecrypts (225 downloads)

Source: Watch Out: These PyPI Python Packages Can Drain Your Crypto Wallets (thehackernews.com)

Thanks!

Do you have any questions?

contact@cyberforge.academy
+91 8837537763
https://cyberforge.academy
https://github.com/CyberForgeAcademy/Workshops

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**