EchidnaTermApp Penetration Test Assist & Learning Tool

Terada Yu

2024

CODE BLUE

BECAUSE SECURITY MATTERS

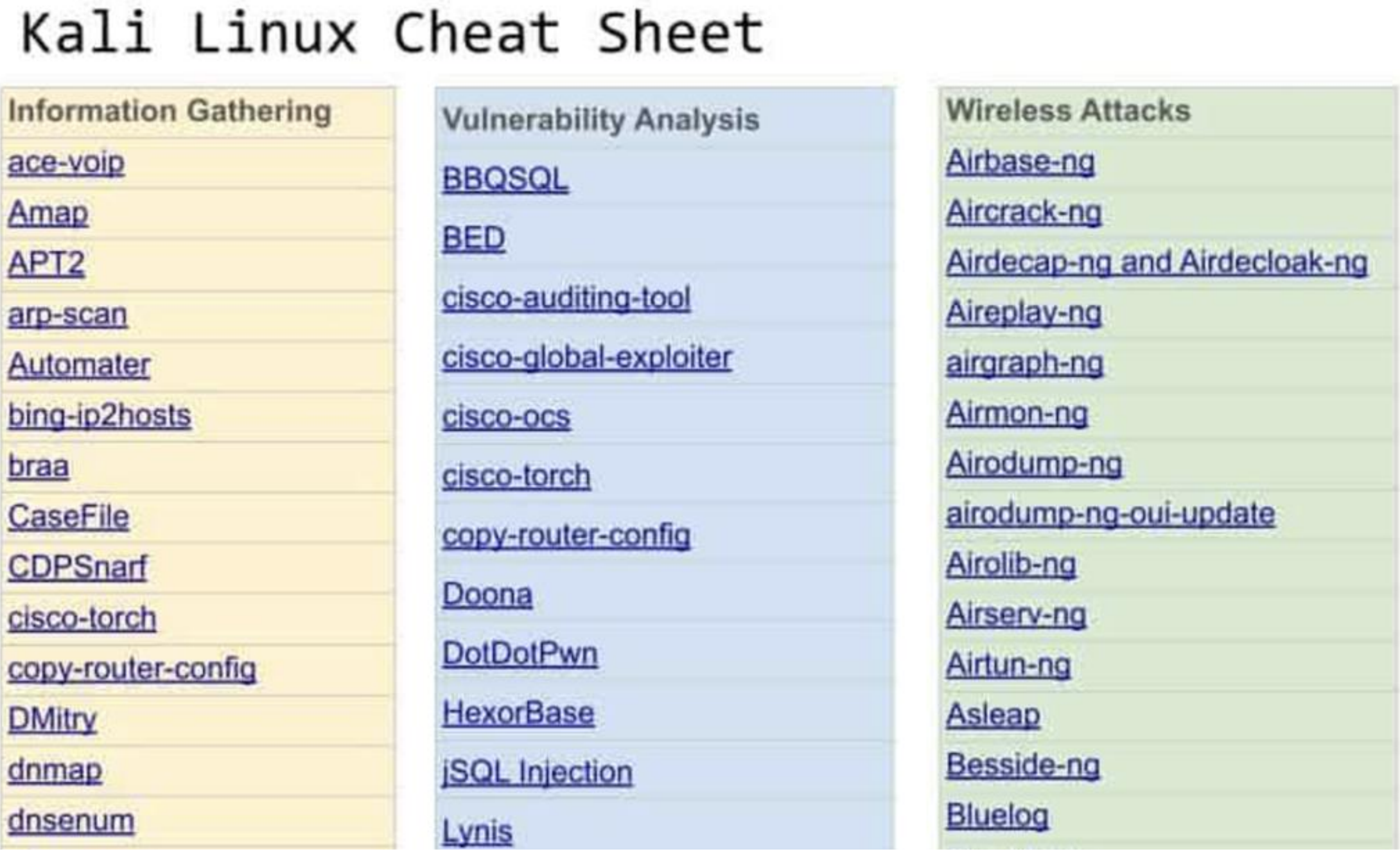
About US

Yu Terada

- Security Researcher for FUJITSU DEFENSE & NATIONAL SECURITY LIMITED
- Developer for EchidnaTermApp and Echidna
- Speaker for Black Hat USA/Europe (Arsenal), AVTokyo, OWASP
- 5 years as a SOC Analyst
- Master in CS, OSEP, OSCP, CRTL, CRTO, CISSP, CKS, GIAC (GMON)

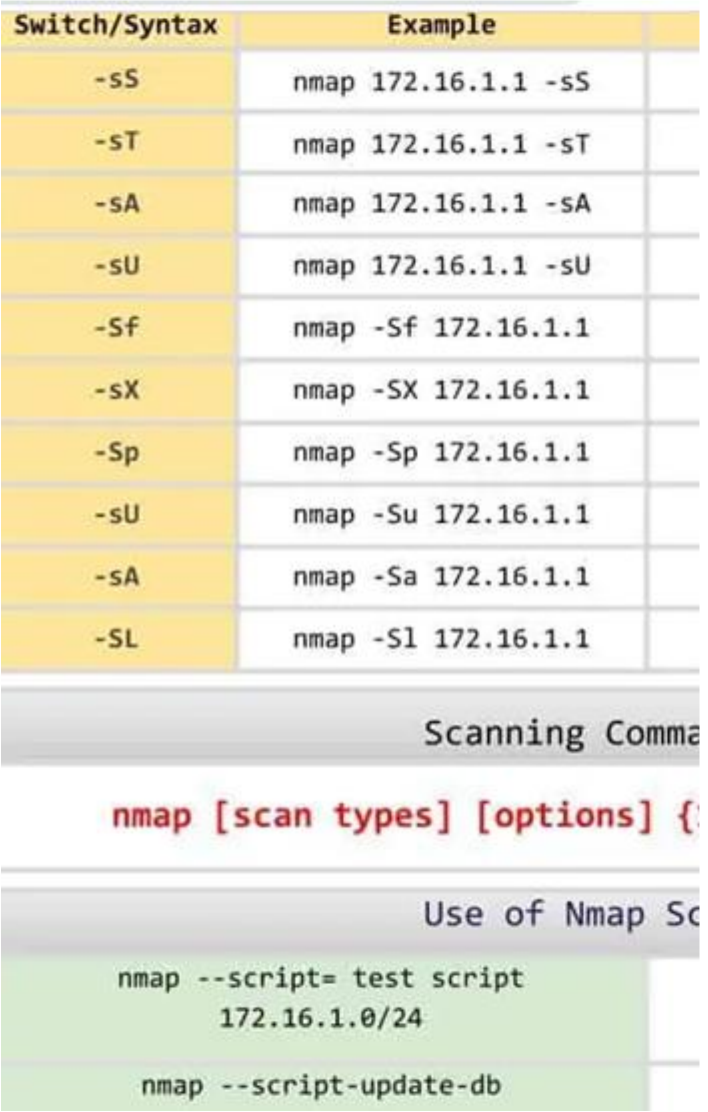
Primary Reason for Develop EchidnaTermApp

- Learning attacking techniques is important for everyone to enhance our Cybersecurity.
- However, so many attack techniques can be overwhelming for beginners and students.



Kali Linux Cheat Sheet

Information Gathering	Vulnerability Analysis	Wireless Attacks
ace-voip	BBQSQL	Airbase-ng
Amap	BED	Aircrack-ng
APT2	cisco-auditing-tool	Airdecap-ng and Airdecloak-ng
arp-scan	cisco-global-exploiter	Aireplay-ng
Automater	cisco-ocs	airgraph-ng
bing-ip2hosts	cisco-torch	Airmon-ng
braa	copy-router-config	Airodump-ng
CaseFile	Doona	airodump-ng-oui-update
CDPSnarf	DotDotPwn	Airolib-ng
cisco-torch	HexorBase	Airserv-ng
copy-router-config	jSQL Injection	Airtun-ng
DMitry	Lynis	Asleap
dnmap		Besside-ng
dnsenum		Bluelog



Switch/Syntax	Example
-sS	nmap 172.16.1.1 -sS
-sT	nmap 172.16.1.1 -sT
-sA	nmap 172.16.1.1 -sA
-sU	nmap 172.16.1.1 -sU
-Sf	nmap -Sf 172.16.1.1
-sX	nmap -SX 172.16.1.1
-Sp	nmap -Sp 172.16.1.1
-sU	nmap -Su 172.16.1.1
-sA	nmap -Sa 172.16.1.1
-SL	nmap -Sl 172.16.1.1

Scanning Comma

```
nmap [scan types] [options] {
```

Use of Nmap Sc

```
nmap --script= test script
172.16.1.0/24
```

```
nmap --script-update-db
```

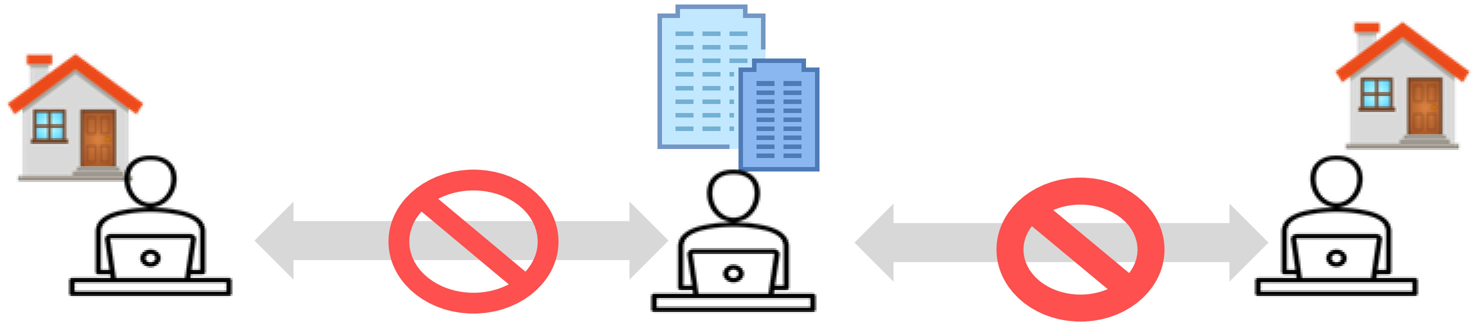
Additional Reasons for Developing Echidna

Each security member works independently, resulting in duplication of effort.

- Scan the same host and port. Exploit the same vulnerability.

It is difficult for managers and new members to understand the operations and progress of other members.

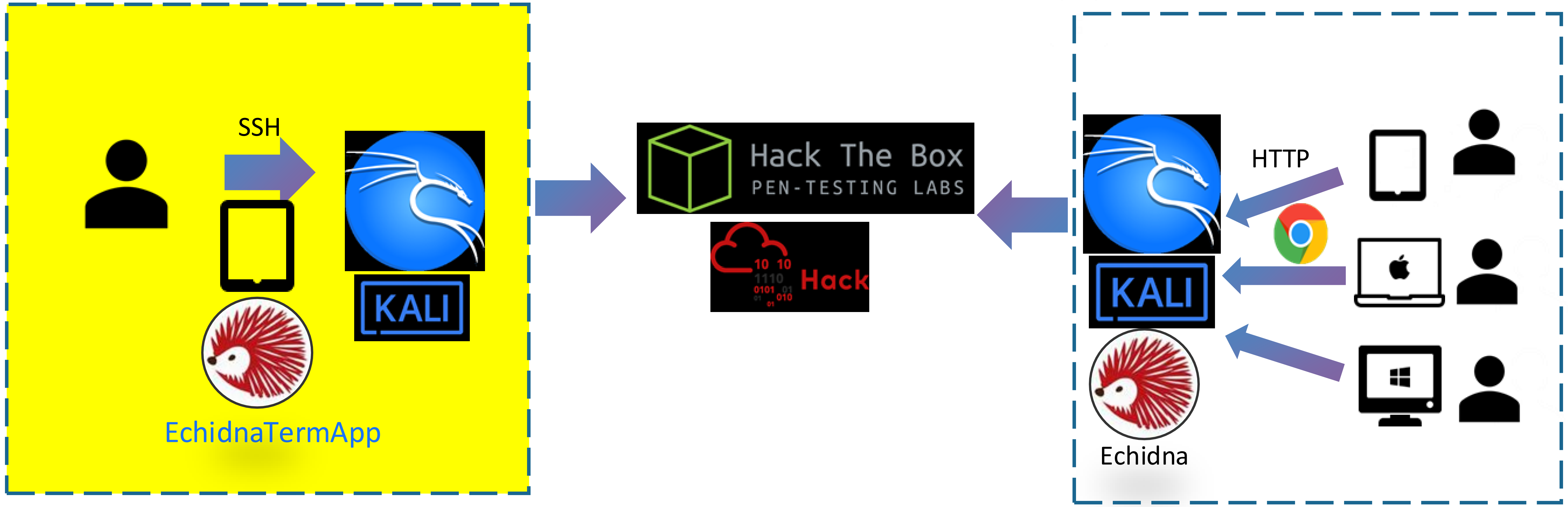
- Especially, spreading remote work makes communications more difficult
- Penetration Testing is Blackbox for many people



EchidnaTermApp

Developed tools to solve the issues

- EchidnaTermApp: iOS app, recently implemented and designed for personal use with improved UI and Performance
- Echidna: Web-based and client-server model, supports teams, implemented last year



Demo Movie for EchidnaTermApp

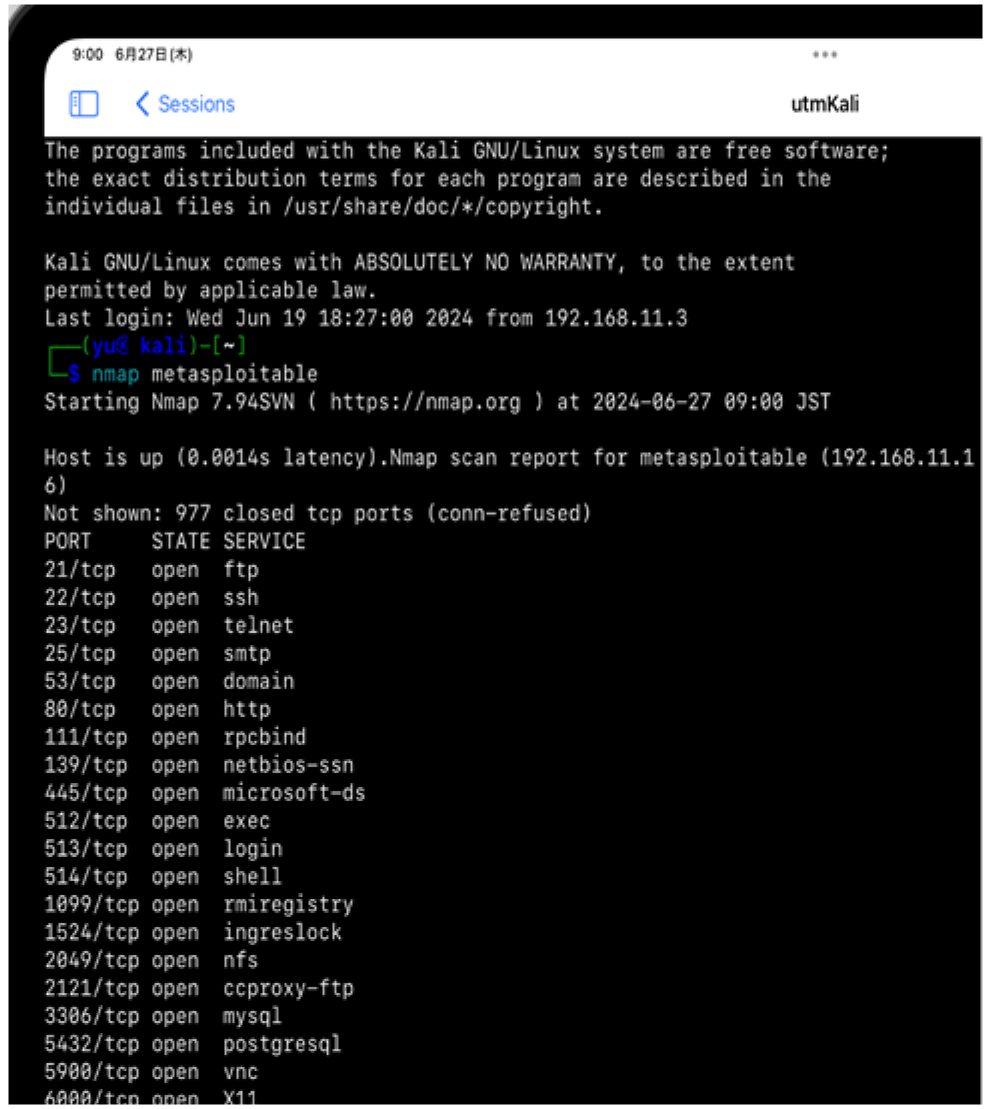
Play Movie

Short Movie for Echidna

Play Movie

How It Works (EchidnaTermApp)

Users install EchidnaTermApp on iPad, and connect to Kali Linux over SSH



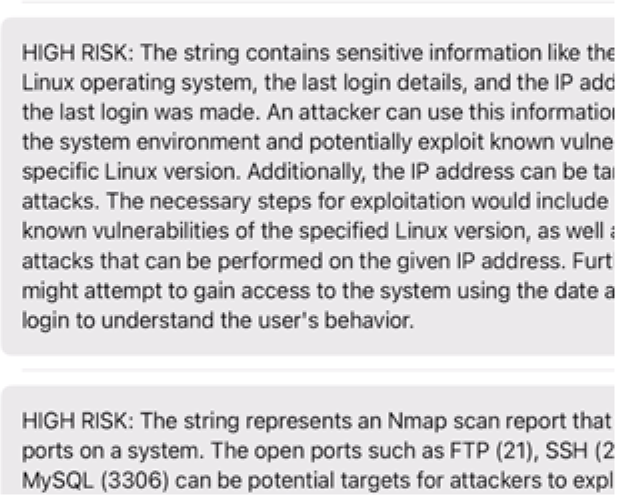
```
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 19 18:27:00 2024 from 192.168.11.3
┌──(yu㉿kali)-[~]
└─$ nmap metasploitable
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 09:00 JST

Host is up (0.0014s latency).Nmap scan report for metasploitable (192.168.11.1
6)
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```

SSH

Terminal Outputs

Parse the terminal outputs and add the results to TargetTree

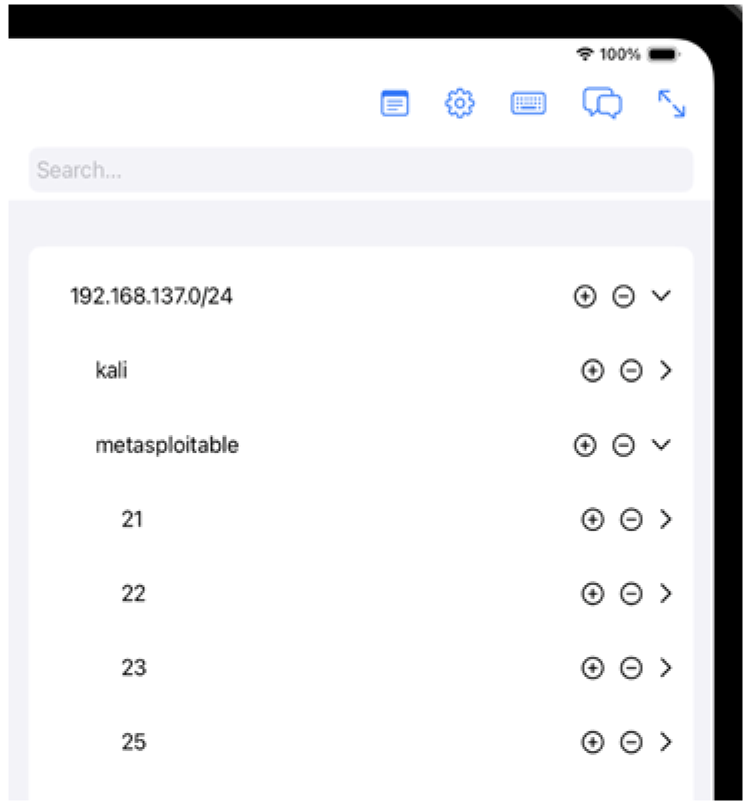
Analyze Terminal Outputs with OpenAI and notify the analysis through Chat Component



HIGH RISK: The string contains sensitive information like the
Linux operating system, the last login details, and the IP add
the last login was made. An attacker can use this informatio
the system environment and potentially exploit known vulne
specific Linux version. Additionally, the IP address can be ta
attacks. The necessary steps for exploitation would include
known vulnerabilities of the specified Linux version, as well a
attacks that can be performed on the given IP address. Furt
might attempt to gain access to the system using the date a
login to understand the user's behavior.

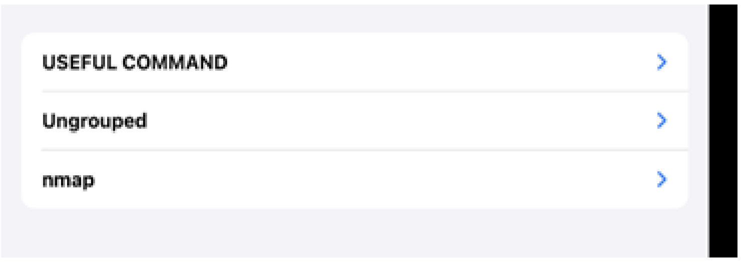
HIGH RISK: The string represents an Nmap scan report that
ports on a system. The open ports such as FTP (21), SSH (2
MySQL (3306) can be potential targets for attackers to expl

Chat Component



TargetTree

Select Target and Update CandidateCommand



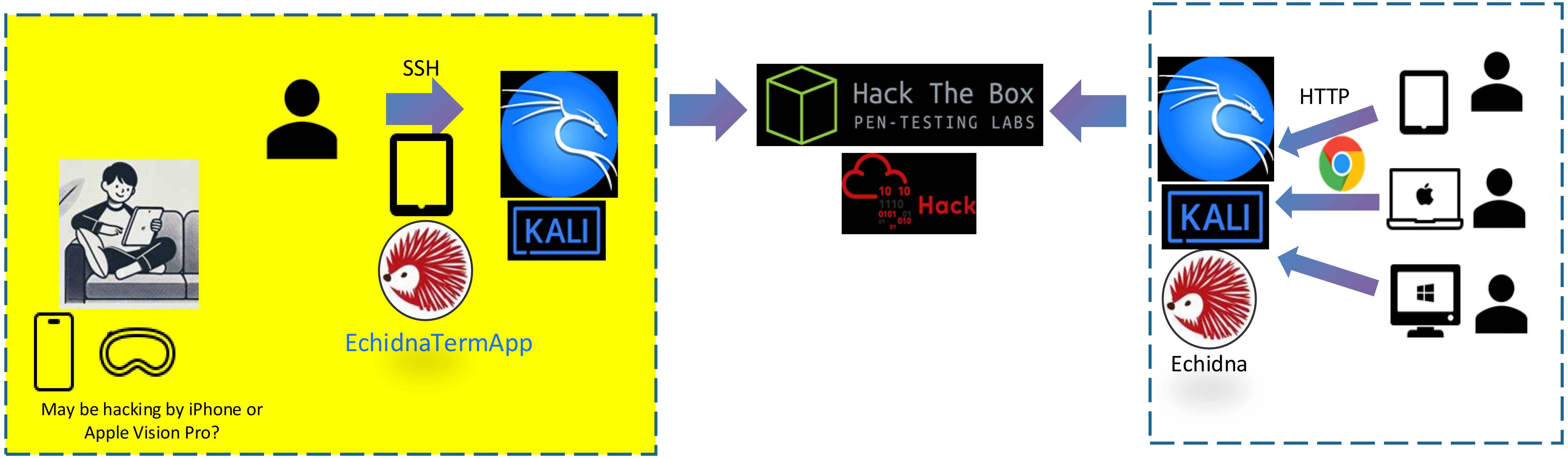
CandidateCommand

Use Cases of EchidnaTermApp

Use case 1: Security beginners utilize EchidnaTermApp to attack vulnerable machines of HTB for training

- Beginners (even students or children) can easily study penetration testing while lounging on a sofa since EchidnaTermApp is iPad app

Use case 2: Security team members within an organization utilize Echidna for penetration tests of internal systems



Use case 1

Use case 2

How to Use EchidnaTermApp

EchidnaTermApp

- Install EchidnaTermApp from the App Store on a iPad (may be iPhone)

  (git clone EchidnaTermApp repository to see the source codes)

Echidna

- git clone Echidna repository on your Github repository on Kali Linux
- Execute install script (install.sh) and access to Echidna web server by Chrome (localhost:8080)

EchidnaTermApp

https://apps.apple.com/jp/app/echidnatermapp/id6520381307?uo=2

https://github.com/Echidna-Pentest/EchidnaTermApp

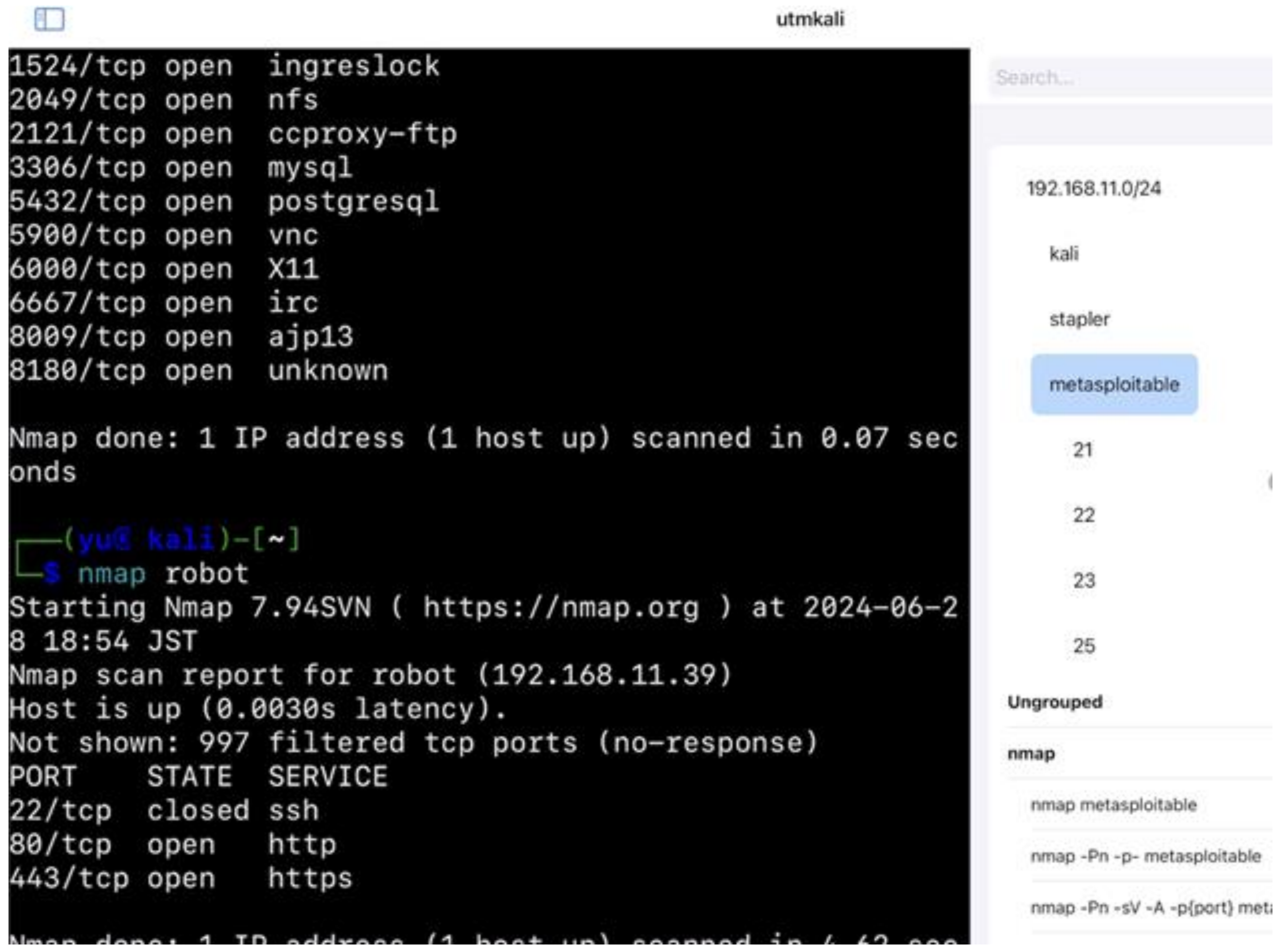
Echidna

https://github.com/Echidna-Pentest/Echidna

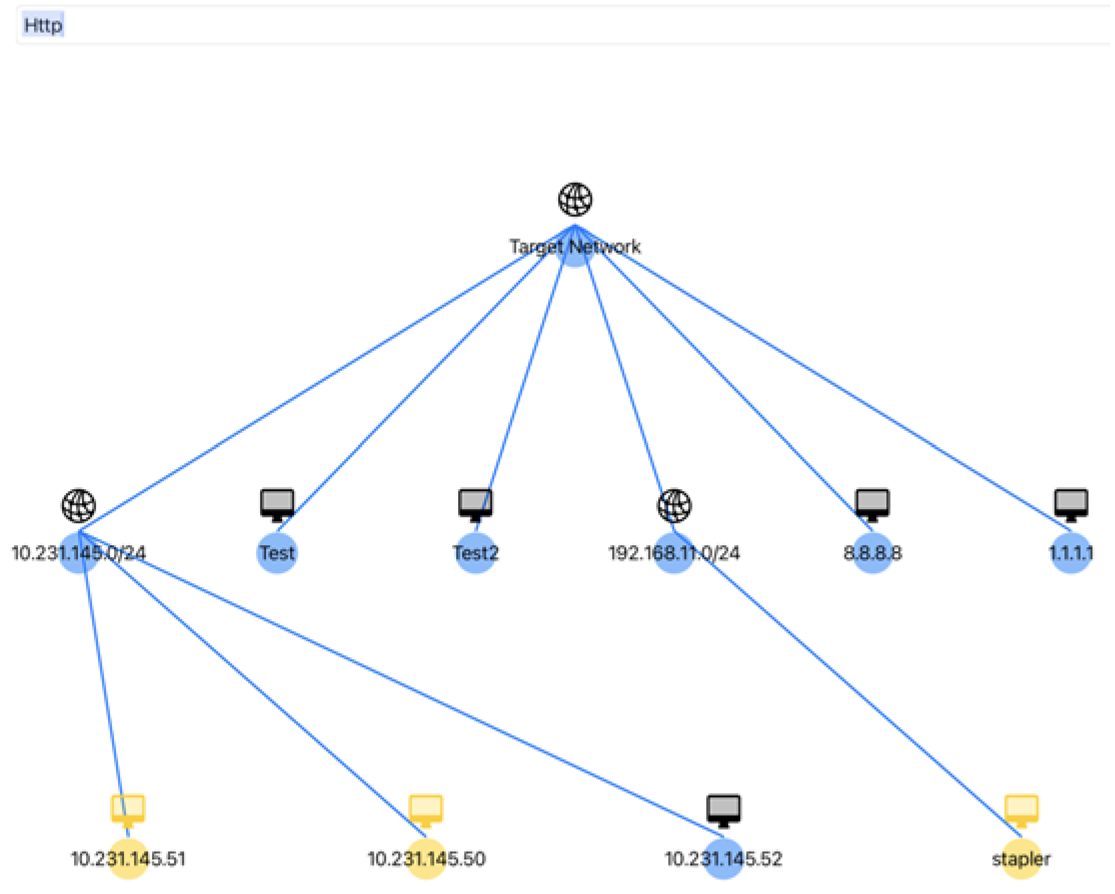
Takeaways

EchidnaTermApp is an iPad app designed to assist beginners in learning attack techniques

- It assists beginners by suggesting candidate commands based on each situation and highlighting important information from the command output
- It organizes target information and visualizes it in a graph, making it user-friendly for beginners.
    - Beginners can exploit vulnerable machines just a few taps by the iPad app.



```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.07 sec
onds

┌──(yu㉿ kali)-[~]
└─$ nmap robot
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-2
8 18:54 JST
Nmap scan report for robot (192.168.11.39)
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
443/tcp  open   https

Nmap done: 1 IP address (1 host up) scanned in 4.62 sec
```



Slide Title

Slide Title

Insert Text Here