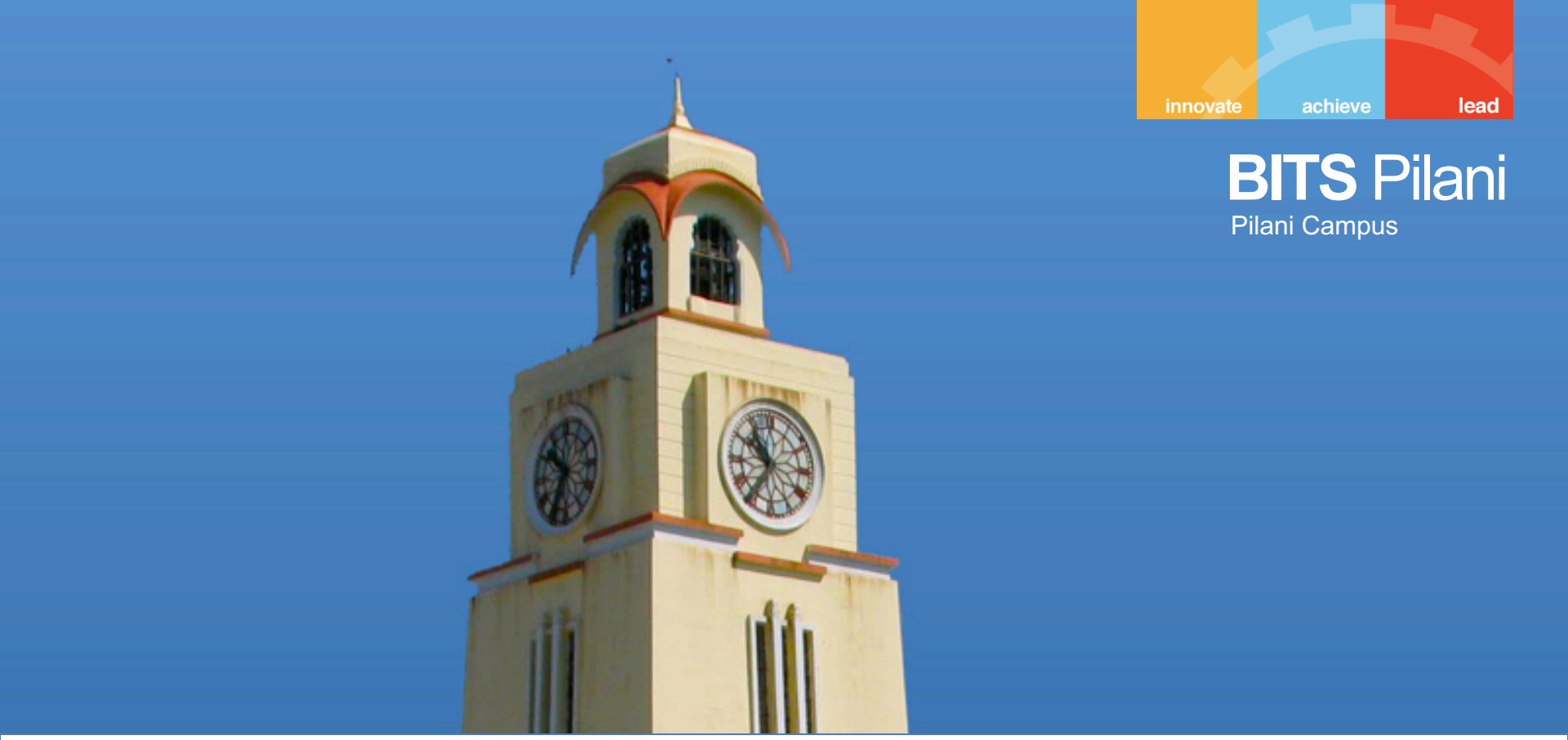
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



SSZG575: Binary Reverse Engineering
Session No: 04

Agenda

innovate achieve lead

- Windows Exploit
  - Presentation by class
- Hacking Database
  - Shodan
  - Exploit-DB
  - Google Hacking Database (GHDB)
- Log analysis
- Privilege Escalation
  - Hands-on Linux Privilege Escalation - Lucideus paper

Windows Exploitation

Trapping Virtual Memory Access

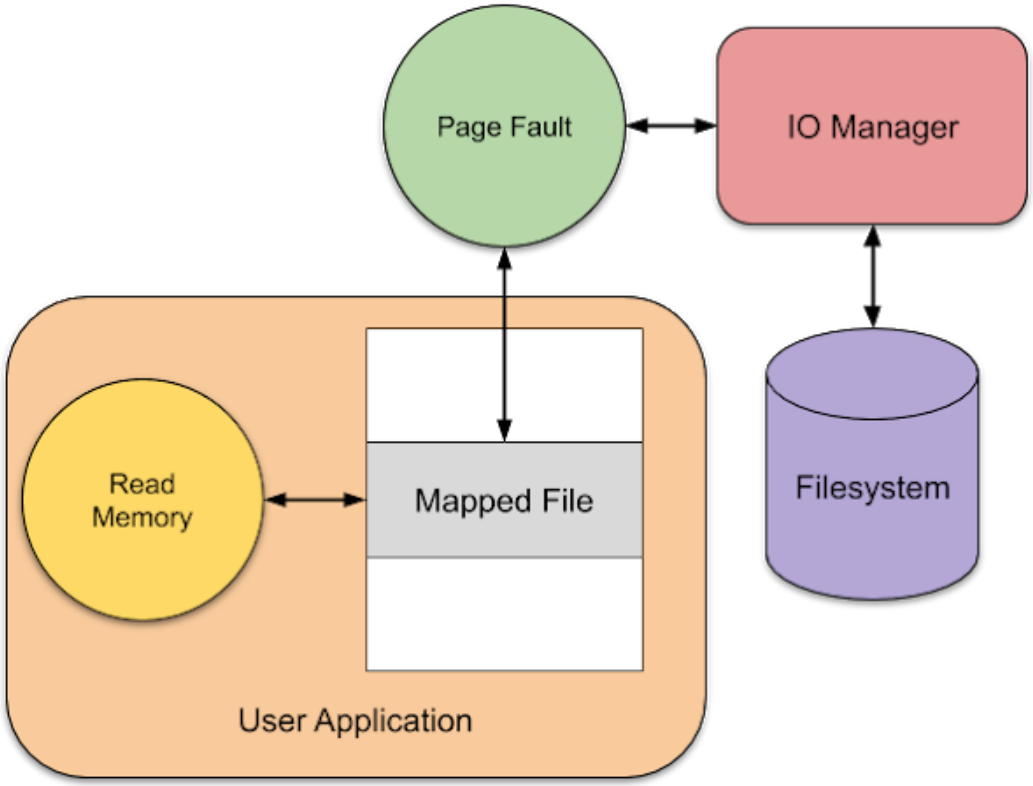
- Method to trap access to Windows virtual memory, get feedback when it occurs and delay access indefinitely.
- Takes advantage of memory double fetches in Windows kernel
- A double-fetch is a type of Time-of-Check Time-of-Use (TOCTOU) vulnerability where code reads a value from memory, such as a buffer length, verifies that value is within bounds and then rereads the value from memory before use.
- By swapping the value in memory between the first and second fetches the verification is bypassed which can lead to security issues such as privilege escalation or information disclosure.

Example Code


```
DWORD* lpInputPtr = // controlled user-mode address
UCHAR  LocalBuffer[256];

if (*lpInputPtr > sizeof(LocalBuffer)) { ①
  return STATUS_INVALID_PARAMETER;
}
RtlCopyMemory(LocalBuffer, lpInputPtr, *lpInputPtr);②
```

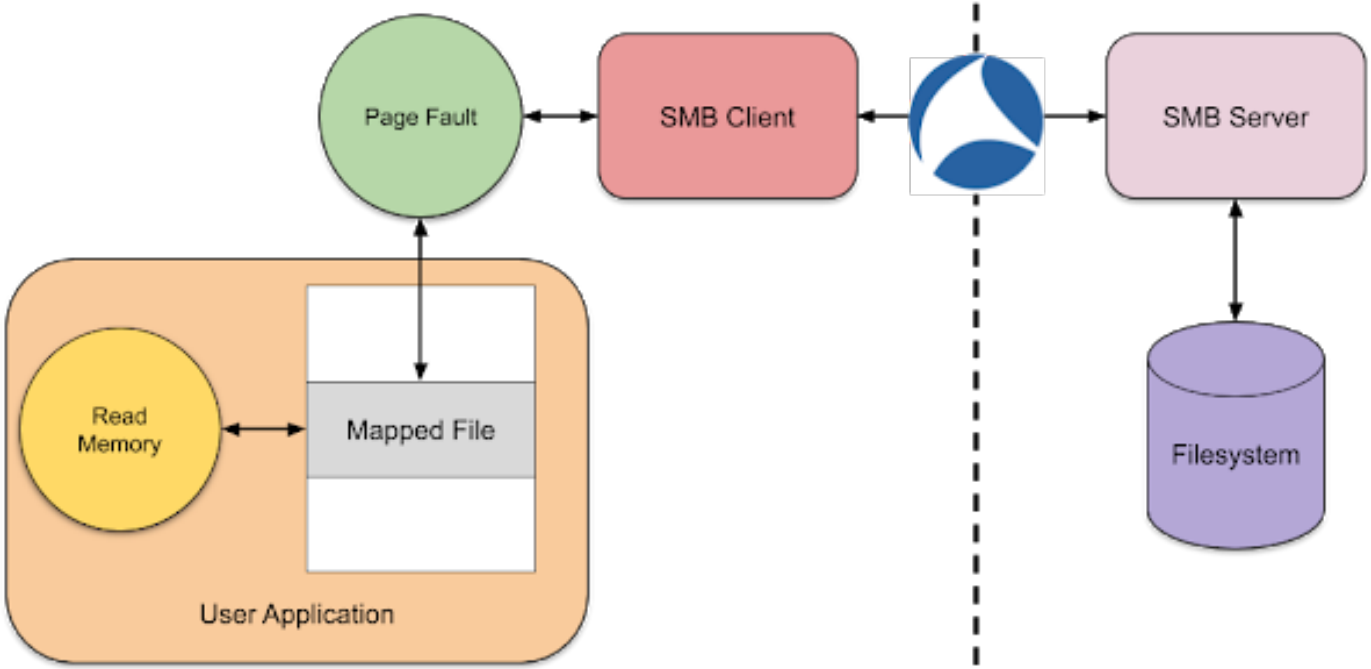
High Level Scenario Diagram



Remote File Systems to be Exploited

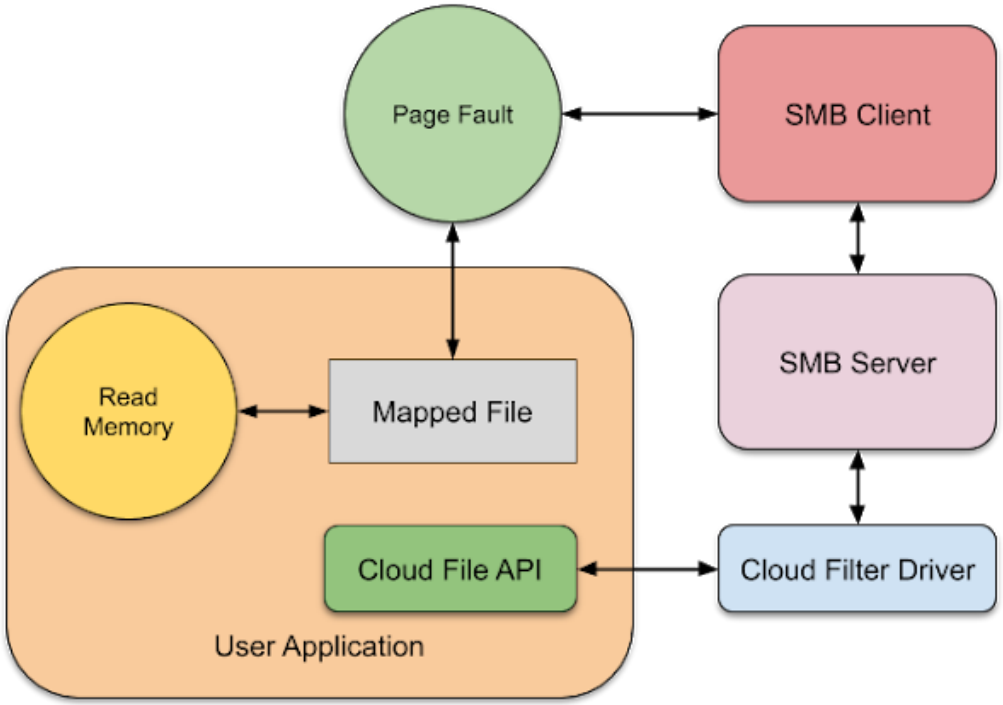
Remote File System	Supported Version	Default?
SMB	Everything	Yes (SMBv1 might be disabled)
WebDAV	Everything	Yes (except Server SKUs)
NFS	Everything	No
P9	Windows 10 1903	No (needs WSL)
Remote Desktop Client	Everything	Yes

Server Message Block (SMB) Approach



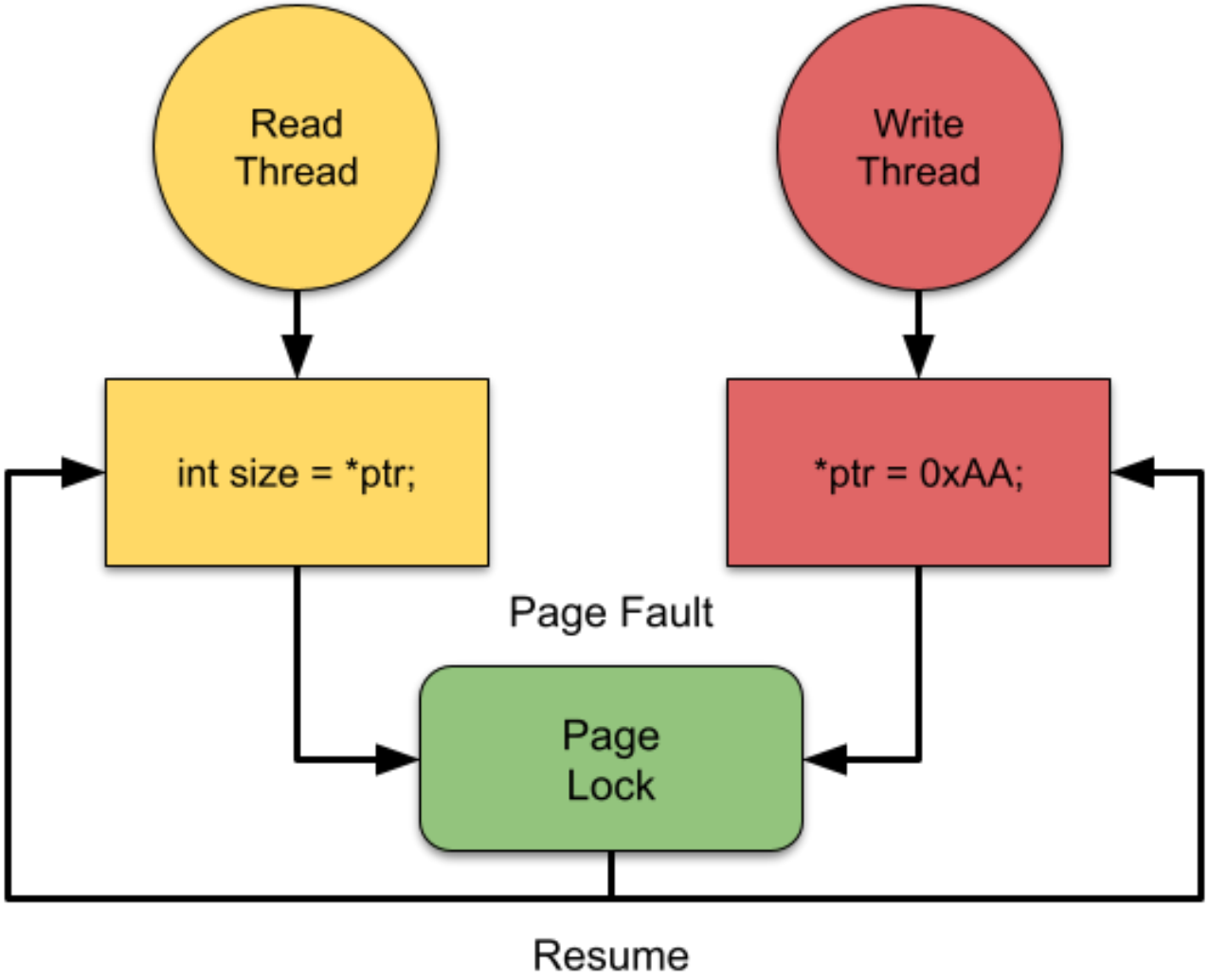
- Hard to use this approach in a sandboxed application.
- This is because MUP restricts access to remote file systems by default from restricted and low IL processes and AppContainer sandboxes need specific capabilities which are unlikely to be granted to the majority of applications.

File System Overlay API



- Cloud Files API is used by OneDrive to provide the local online filesystem
- It can be used to implement any file system overlay you like.
- It works very similar to the Projected File System, with placeholders for files and the concept of hydrating the file on demand.

File System Overlay API



Hacking Database

Shodan Database

- A search engine that can identify a specific device, such as computer, router, server, using a variety of filters, such as metadata from system banners.
- For example, you can search for a specific system, such as a Cisco 3850, running a version of software such as IOS Version 15.0(1)EX.

- Demo Link: https://www.shodan.io

Google Hacking Database (GHDB)

- The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services.
- The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.
- The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
- The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

Google Hacking Database (GHDB)

- The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet.
- The process known as “Google Hacking” was popularized in 2000 by Johnny Long, a professional hacker, who began cataloging these queries in a database known as the Google Hacking Database.
- His initial efforts were amplified by countless hours of community member effort, documented in the book Google Hacking For Penetration Testers

Google Hacking Database (GHDB)

- Johnny coined the term “Googledork” to refer to “a foolish or inept person as revealed by Google“.
- This was meant to draw attention to the fact that this was not a “Google problem” but rather the result of an often unintentional misconfiguration on the part of a user or a program installed by the user.
- Over time, the term “dork” became shorthand for a search query that located sensitive information and “dorks” were included with may web application vulnerability releases to show examples of vulnerable web sites.
- After nearly a decade of hard work by the community, Johnny turned the GHDB over to Offensive Security in November 2010, and it is now maintained as an extension of the Exploit Database.

Log Analysis

Log Analysis

- Log analysis is the process of reviewing, interpreting and understand computer-generated logs.
- Logs are generated by a range of programmable technologies, including networking devices, operating systems, application etc
- A log consists of a series of messages in time-sequence that describe activities going on within a system.
- Log files may be streamed to a log collector through an active network, or they may be stored in files for later review.
- Log analysis is reviewing and interpreting these messages to gain insight into the inner workings of the system.

How to Perform Log Analysis?

- **Instrument and collect:** install a collector to collect data from any part of your stack
- **Centralize and index:** integrate data from all log sources into a centralized platform to streamline the search and analysis process
- **Search and analyze:** Analysis techniques such as pattern recognition, normalization, tagging and correlation analysis can be implemented either manually or using machine learning
- **Monitor and alert:** With machine learning and analytics, IT organizations can implement real-time, automated log monitoring that generates alerts when certain conditions are met
- **Report and dashboard:** Streamlined reports and customized reusable dashboards to ensure confidentiality of security logs

Log Analysis Function

- **Normalization:** normalization is a data management technique wherein parts of a message are converted to the same format.
- **Pattern recognition:** compare incoming messages with a pattern book and distinguish between "interesting" and "uninteresting" log messages
- **Classification and tagging:** group together log entries that are the same type
- **Correlation analysis:** process of gathering log information from a variety of systems and discovering the log entries from each individual system that connect to the known event

Various Logs

- System logs
  - System activity logs
  - Endpoint logs
  - Application logs
  - Authentication logs
  - Physical security logs
- Networking logs
  - Email logs
  - Firewall logs
  - VPN logs
  - Netflow logs
- Technical logs
  - HTTP proxy logs
  - DNS, DHCP and FTP logs
  - Appflow logs
  - Web and SQL server logs
- Cyber security monitoring logs
  - Malware protection software logs
  - Network intrusion detection system (NIDS) logs
  - Network intrusion prevention system (NIPS) logs
  - Data loss protection (DLP) logs

Logs in Linux

- **Application Logs:** Application logs contain records of events, errors, warnings, and other messages that come from applications.
- **Event Logs:** Event logs provide an audit trail, enabling system administrators to understand how the system is behaving and diagnose potential problems.
- **Service Logs:** Linux OS creates a log file **/var/log/daemon.log** tracks important background services that have no graphical output.
- **System Logs:** System log files contain events that are logged by the operating system components. The file **/var/log/syslog** contains most of the typical system activity logs. Users can analyze these logs to discover things like non-kernel boot errors, system start-up messages, and application errors etc.

Logs Analysis Tools

- ELK (Elasticsearch, Logstash and Kibana)
- Splunk
- Loggly
- SumoLogic
- XpoLog

- xplg.com

Hands-On Linux Privilege Escalation

What is Privilege Escalation?

- Privilege escalation is a technique of exploiting a vulnerability, or configuration on a web application or operating system to gain elevated access to permissions (normally root) that should not be available to that user.
- After gaining escalated privileges the attacker can steal confidential data, deploy malware, and potentially do serious damage to an operating system.

How Does Privilege Escalation Work?

- Attacker's start by enumerating the target machine to find information about the services that are running on the target machine.
- Attacker plans for the next steps and lists all the information gathered so far.
- Attacker identifies existing vulnerability based on information gathered and exploits the privilege escalation vulnerability on the target machine which lets them override the limitations of the current user account.
- Now the attacker has access far more than what originally available.

Linux Privilege Escalation

innovate achieve lead

- Privilege Escalation by kernel exploit
- Privilege Escalation by Password Mining
- Privilege Escalation by Sudo
- Privilege Escalation by File Permissions
- Privilege Escalation by Crontab

- Document Link: https://www.exploit-db.com/docs/49411

- 'Dirty.c' code link: https://www.exploit-db.com/exploits/40839

Thank You