Submitted By:Iqra Jawad Ahmed

# Part 1: Ettercap: Credential Sniffing

## 1. Objective

To use Ettercap for sniffing login credentials on unencrypted (HTTP) websites within a LAN environment.

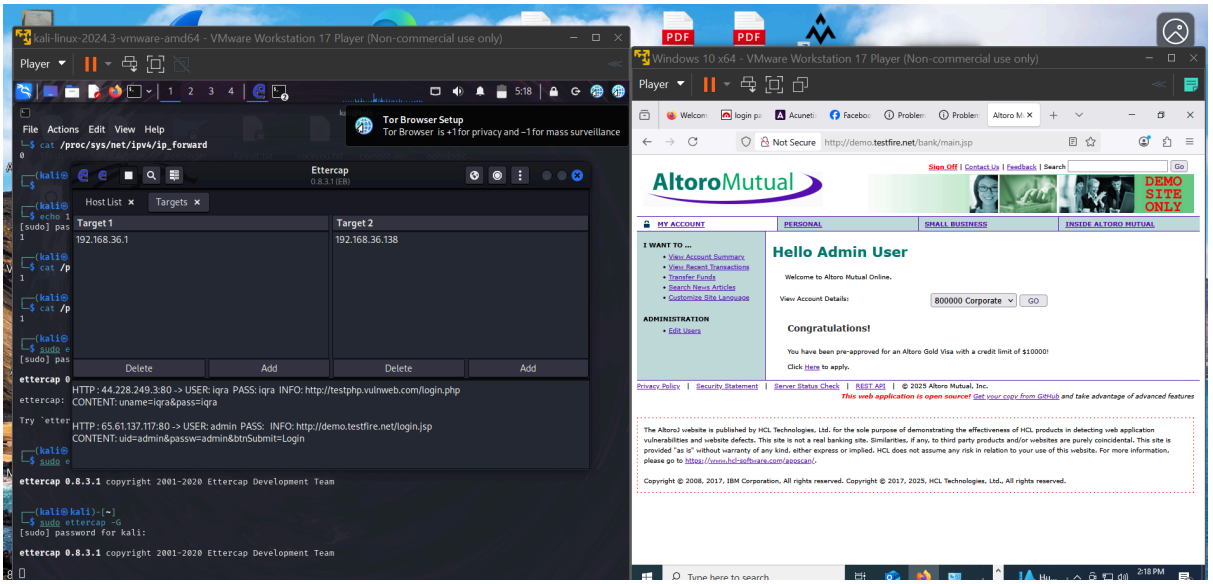
## 2. Tools Used

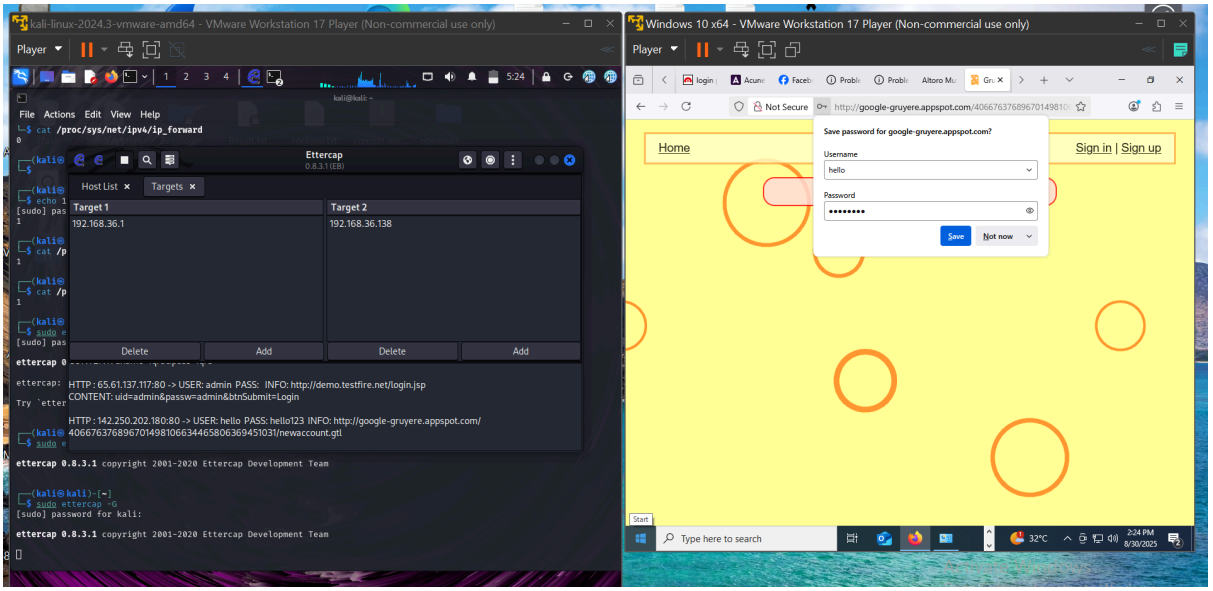
- VMware Workstation
- Ettercap (Linux/Kali machine)
- Test websites:
    1. **vulnweb.com (Sign-up page)**
    2. **testfire.net (Demo bank login page)**
    3. **Google Gruyere (Sign-up page)**

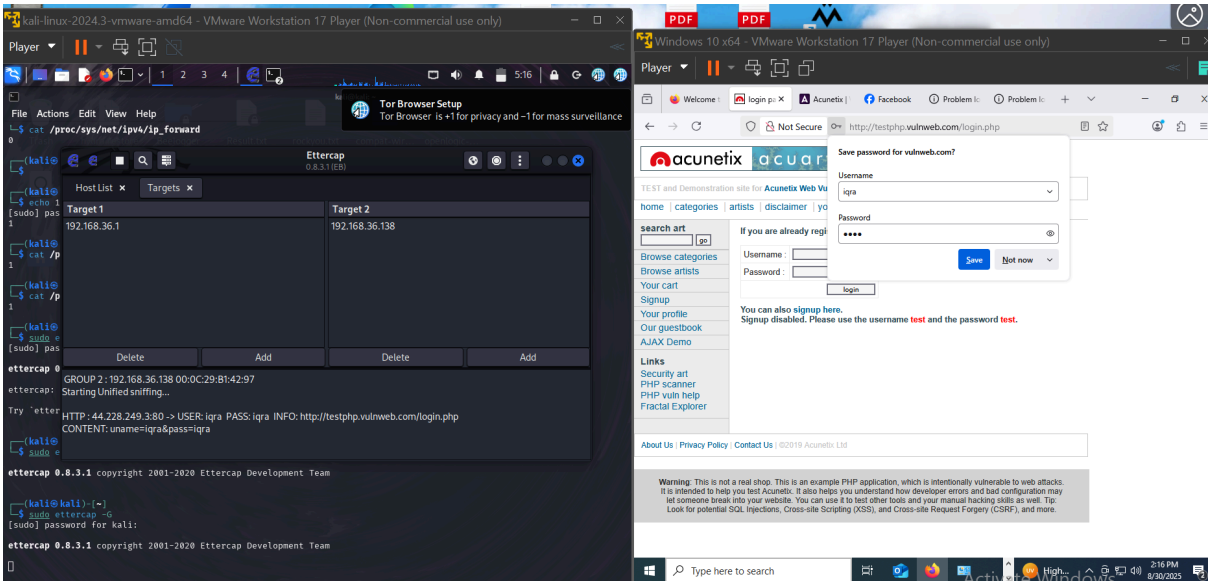
## 3. Implementation Steps

1. Start VMware and run Ettercap in Kali Linux.
2. Enable IP forwarding.
3. Perform ARP poisoning on the victim VM + gateway.
4. Run sniffing in unified sniffing mode.
5. Visit HTTP websites from the victim machine (Windows VM).
6. Ettercap captures login credentials in clear text.

# ScreenShots




kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
Tor Browser Setup
Tor Browser is +1 for privacy and −1 for mass surveillance
Ettercap
Host List
Targets
Target 1
192.168.36.1
Target 2
192.168.36.138
Delete
Add
Delete
Add
GROUP 2 : 192.168.36.138 00:0C:29:B1:42:97
Starting Unified sniffing...
HTTP : 44.228.249.3:80 -> USER: iqra PASS: iqra INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=iqra&pass=iqra
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
[sudo] password for kali:
Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Not Secure
http://testphp.vulnweb.com/login.php
Save password for vulnweb.com?
Username
iqra
Password
Save
Not now
acunetix
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Username :
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.
It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may
let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip:
Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
Type here to search
2:16 PM
8/30/2025

# Part 2:  Keyloggers in Windows VM

## 1. Objective

To demonstrate how keyloggers can capture keystrokes inside a Windows 10 Virtual Machine.

## 2. Tools Used

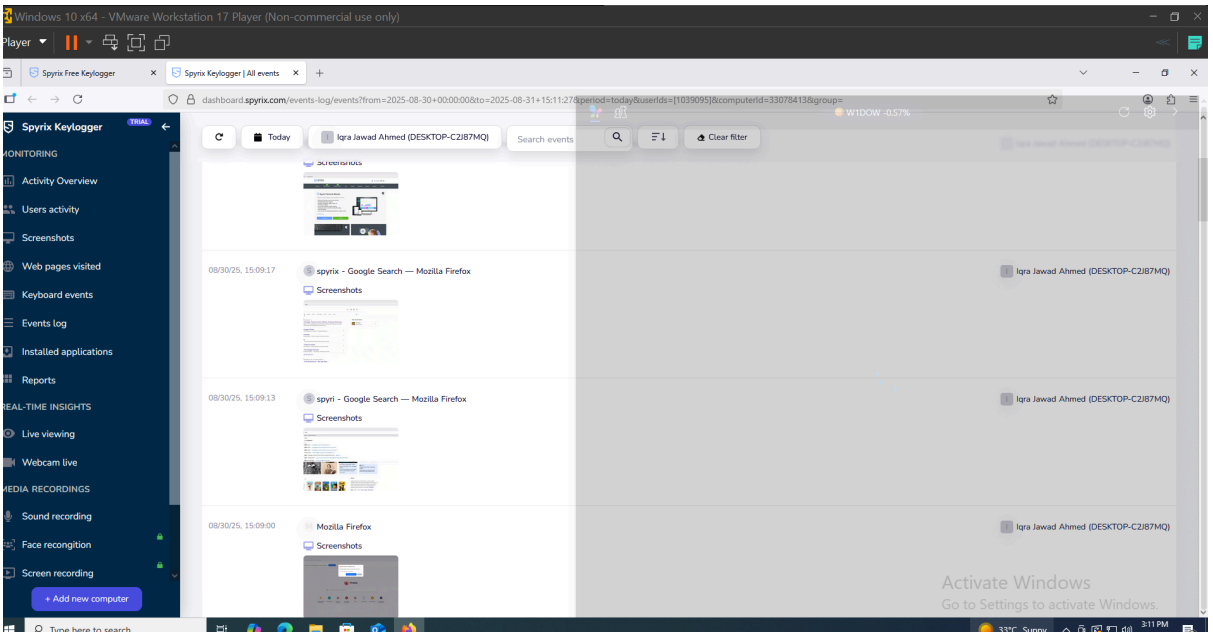
- **Spyrix Free Keylogger**
- **Revealer Keylogger Free**
- Windows 11 (VMware)

## 3. Implementation Steps

1. Installed each keylogger inside Windows 11 VM.
2. Configured the keylogger to run in the background.
3. Typed test credentials/messages (dummy data) in Notepad & browser.
4. Checked keylogger logs.

# ScreenShots

Spyrix Keylogger:




Revealer Keylogger: