Trainee Program
SOC path final evaluation, CTF

Windows Event Logs Collected

Disclaimer

By proceeding with this vulnerability assessment, the owner confirms a signed waiver grants permission for testing aimed at identifying vulnerabilities and assessing application security. The owner assumes all business continuity risks.

Document Revision History

Version	Modification	Date	Author	Organization
1.0	Assessment	29th April 2025	Joshua Ortiz	Contractor
TBD	Reviewed and updated the report	TBD	Joshua Ortiz	Contractor

Executive Summary

The CIRT Team performed a vulnerability assessment on an isolated machine, following the cyber kill chain methodology. The purpose of this assessment is to evaluate the overall security posture of the system, analyzed from a grey-box perspective. This includes determining common attack patterns and identifying vulnerable areas in the internal and external interfaces that threat actors might compromise.

Assessment checklist

Vulnerability Name	Affected Status
Denial of Service (DoS)	Not Vulnerable
Brute-Force Attacks:	Not Vulnerable
SQL Injection (SQLi)	Not Vulnerable
IANA (Internet Assigned Numbers Authority) Port 200	Not Vulnerable

Detection & Analysis

1. **What is the username of the local account that is being targeted? (Format: Username)**
    - administrator

2. **What is the failure reason related to the Audit Failure logs? (Format: String)**
   - Unknown user name or bad password.
3. **What is the Windows Event ID associated with these logon failures? (Format: ID)**
   - **4625:** Account logon failure (local computer).
   - **4776:** Domain controller failed to validate credentials (NTLM).
   - **4771:** Kerberos pre-authentication failure (domain controller).
   - **4624:** (Successful Logon): Useful with failure
4. **What is the source IP conducting this attack? (Format: X.X.X.X) (3 points)**
   - 113.161.192.227
5. **What country is this IP address associated with? (Format: Country)**
   - **Country | City**: Vietnam | Phan Thiết
   - **Organization:** Vietnam Posts and Telecommunications Group
6. **How many successful logons are there? (Format: Count of Events)**

4624	2/12/2022 7:11:39 AM	Logon: An account was successfully logged on.
4624	2/12/2022 6:51:38 AM	Logon: An account was successfully logged on.
4624	2/12/2022 6:11:27 AM	Logon: An account was successfully logged on.
4624	2/12/2022 6:06:14 AM	Logon: An account was successfully logged on.

7. **What is the account involved with the successful logons? (Format: String)**

Security ID:	System
Account Name:	EC2AMAZ-UUEMPAU$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

8. What is the user account that performed a read operation on stored credentials?

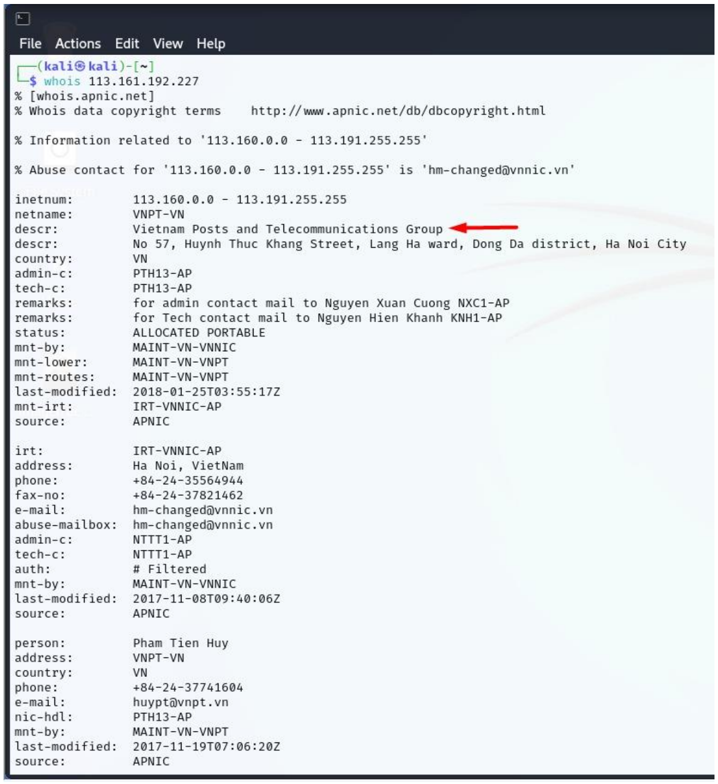
Security ID:	EC2AMAZ-UUEMPAU\BTLO
Account Name:	BTLO
Account Domain:	EC2AMAZ-UUEMPAU
Logon ID:	0xA533B

9. What is the event ID associated with the action of read operation on stored credentials?

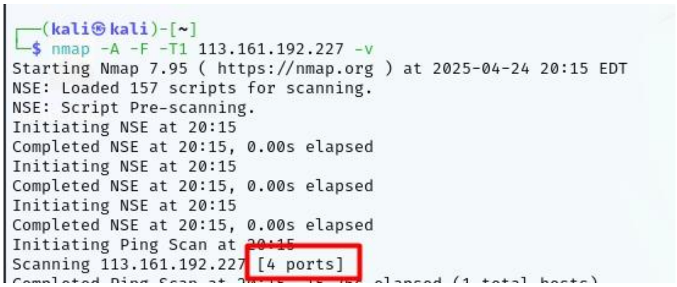
5379	Read Operation	Enumerate Credentials

Finding Details:

○



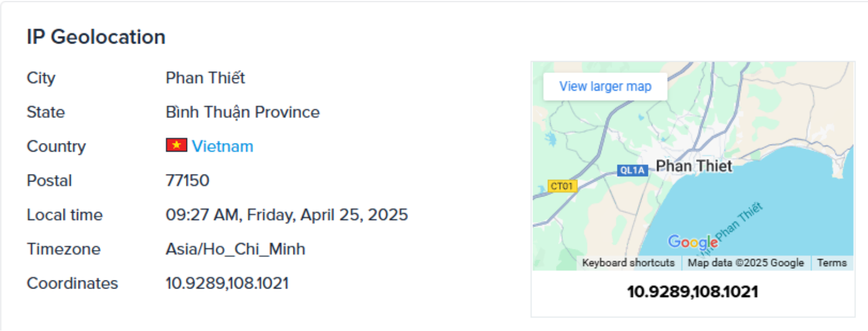
```
┌──(kali㉿kali)-[~]
└─$ whois 113.161.192.227
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '113.160.0.0 - 113.191.255.255'

% Abuse contact for '113.160.0.0 - 113.191.255.255' is 'hm-changed@vnnic.vn'

inetnum:        113.160.0.0 - 113.191.255.255
netname:        VNPT-VN
descr:          Vietnam Posts and Telecommunications Group
descr:          No 57, Huynh Thuc Khang Street, Lang Ha ward, Dong Da district, Ha Noi City
country:        VN
admin-c:        PTH13-AP
tech-c:         PTH13-AP
remarks:        for admin contact mail to Nguyen Xuan Cuong NXC1-AP
remarks:        for Tech contact mail to Nguyen Hien Khanh KNH1-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-VN-VNNIC
mnt-lower:      MAINT-VN-VNPT
mnt-routes:     MAINT-VN-VNPT
last-modified:  2018-01-25T03:55:17Z
mnt-irt:        IRT-VNNIC-AP
source:         APNIC

irt:            IRT-VNNIC-AP
address:        Ha Noi, VietNam
phone:          +84-24-35564944
fax-no:         +84-24-37821462
e-mail:         hm-changed@vnnic.vn
abuse-mailbox:  hm-changed@vnnic.vn
admin-c:        NTTT1-AP
tech-c:         NTTT1-AP
auth:           # Filtered
mnt-by:         MAINT-VN-VNNIC
last-modified:  2017-11-08T09:40:06Z
source:         APNIC

person:         Pham Tien Huy
address:        VNPT-VN
country:        VN
phone:          +84-24-37741604
e-mail:         huypt@vnpt.vn
nic-hdl:        PTH13-AP
mnt-by:         MAINT-VN-VNPT
last-modified:  2017-11-19T07:06:20Z
source:         APNIC
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -F -T1 113.161.192.227 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 20:15 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:15
Completed NSE at 20:15, 0.00s elapsed
Initiating NSE at 20:15
Completed NSE at 20:15, 0.00s elapsed
Initiating NSE at 20:15
Completed NSE at 20:15, 0.00s elapsed
Initiating Ping Scan at 20:15
Scanning 113.161.192.227 [4 ports]
```

Additionally, we identified four open ports:

- Port 1723/tcp
- Port 22/tcp
- Port 1433/tcp
- Port 200/tcp



IP Geolocation

City	Phan Thiết
State	Bình Thuận Province
Country	🇻🇳 Vietnam
Postal	77150
Local time	09:27 AM, Friday, April 25, 2025
Timezone	Asia/Ho_Chi_Minh
Coordinates	10.9289,108.1021

10.9289,108.1021

Containment, Eradication, and Recovery:

1. **What would you do for containment?**

- ○ Block Source IP: Firewall/IPS rule to block 113.161.192.227.
- ○ Isolate Targeted Account (If Needed): Temporarily disable/isolate the administrator account if compromise is suspected (with caution).
- ○ Monitor Affected Systems: Closely watch for other suspicious activity.

2. **What actions would you recommend to eradicate this attack?**

- ○ Analyze All Logs: Examine security logs for intrusions, lateral movement, or related malicious activity.
- ○ Identify Attack Vector: Determine the likely access method (e.g., OWASP Top 10, CVEs, CWEs).
- ○ Check for Compromises: Look for compromised accounts, backdoors, orphan accounts, or malware.

Remediation:

- ○ Password Reset: Force a password reset for the targeted administrator account and any other potentially compromised accounts. Enforce strong password policies.
- ○ Implement Multi-Factor Authentication (MFA): Enable MFA for all critical accounts, especially administrative accounts, to prevent unauthorized access even if passwords are compromised.
- ○ Patching: Ensure all systems are up-to-date with the latest security patches to address known vulnerabilities.
- ○ Network Segmentation: Implement or review network segmentation to limit the potential impact of a breach.

- **Likelihood:** Low
- **Impact:** Low
- **Severity:** Low
- **CVSS score:** 3.5
- **CVSS Link:** Common Vulnerability Scoring System Version 3.1 Calculator (first.org)
- Common Vulnerability Scoring System Version 3.1 Calculator

3. When do you think it would be appropriate to get back to production?

- Containment: Attack source blocked; no further malicious activity.
- Eradication Compromises addressed (passwords reset, malware removed).
- Verification: Affected systems' integrity and security verified.
- Monitoring: Enhanced monitoring for recurrence implemented.
- Business Impact: Security balanced with operational needs.

Post-Incident Actions:

1. What can we do better when dealing with possible future incidents of the same nature?

- Implement MFA to prevent brute-force attacks.
- Enforce strong passwords and regular changes.
- Use aggressive lockout policies and rate limiting on login attempts.
- Keep IDS/IPS rules updated to block brute force and malicious activity.
- Regularly scan for and patch system vulnerabilities.
- Review and update your incident response plan for brute-force attacks
- Activate multifactor authentications for all the network accounts.

TTPs & MITRE ATT&CK Analysis

This report analyzes a security incident using the MITRE ATT&CK framework, identifying a likely brute-force attack and denial-of-service (DoS) originating from IP address 113.161.192.227 (Vietnam).

- Initial Access [TA0001]: Brute Force [T1110] - Multiple failed logon attempts (Event IDs 4625, 4776, 4771) followed by successful logons (Event ID 4624) indicate a brute-force attempt to gain unauthorized access.

- Credential Access [TA0006]: Brute Force [T1110] - Repeated logon failures against local accounts (4625), NTLM (4776), and Kerberos (4771) highlight attempts to compromise credentials. Subsequent successful logons (4624) confirm credential compromise.

- Impact [TA0040]: Denial of Service [T1498] - The identified DoS attack alongside the brute-force suggests an intent to disrupt service availability.

Conclusion

During the recent vulnerability assessment of an isolated machine, log analysis revealed four open ports. While further exploitation was outside the scope of the engagement, we proceeded with remediation steps to strengthen the organization's security posture. This included identifying relevant TTPs using the MITRE ATT&CK framework and pinpointing vulnerable areas in both internal and external interfaces that could be exploited by threat actors.

For more information contact:

Joshua Ortiz
Security Operations Center
E. Joshua.Ortiz@contractor.com | C.+503.6772.4359