



**VIETNAM  
WEB  
SUMMIT**

# IT SECURITY AUDITING

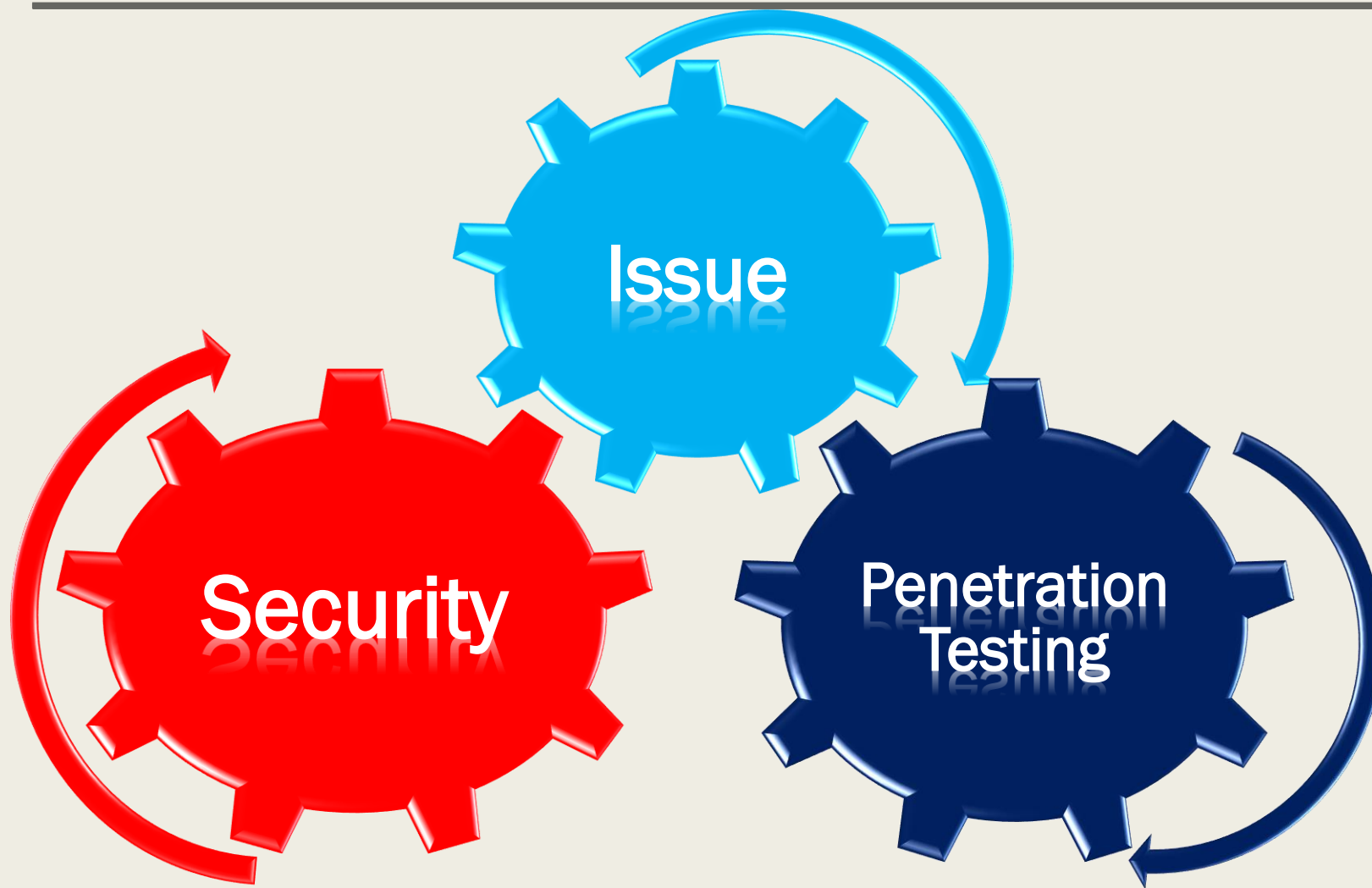
*Speaker: Chuyên gia An toàn thông tin - VCCorp*

*Huỳnh Ngọc Thông - [thonghuynhngoc@vccorp.vn](mailto:thonghuynhngoc@vccorp.vn)*

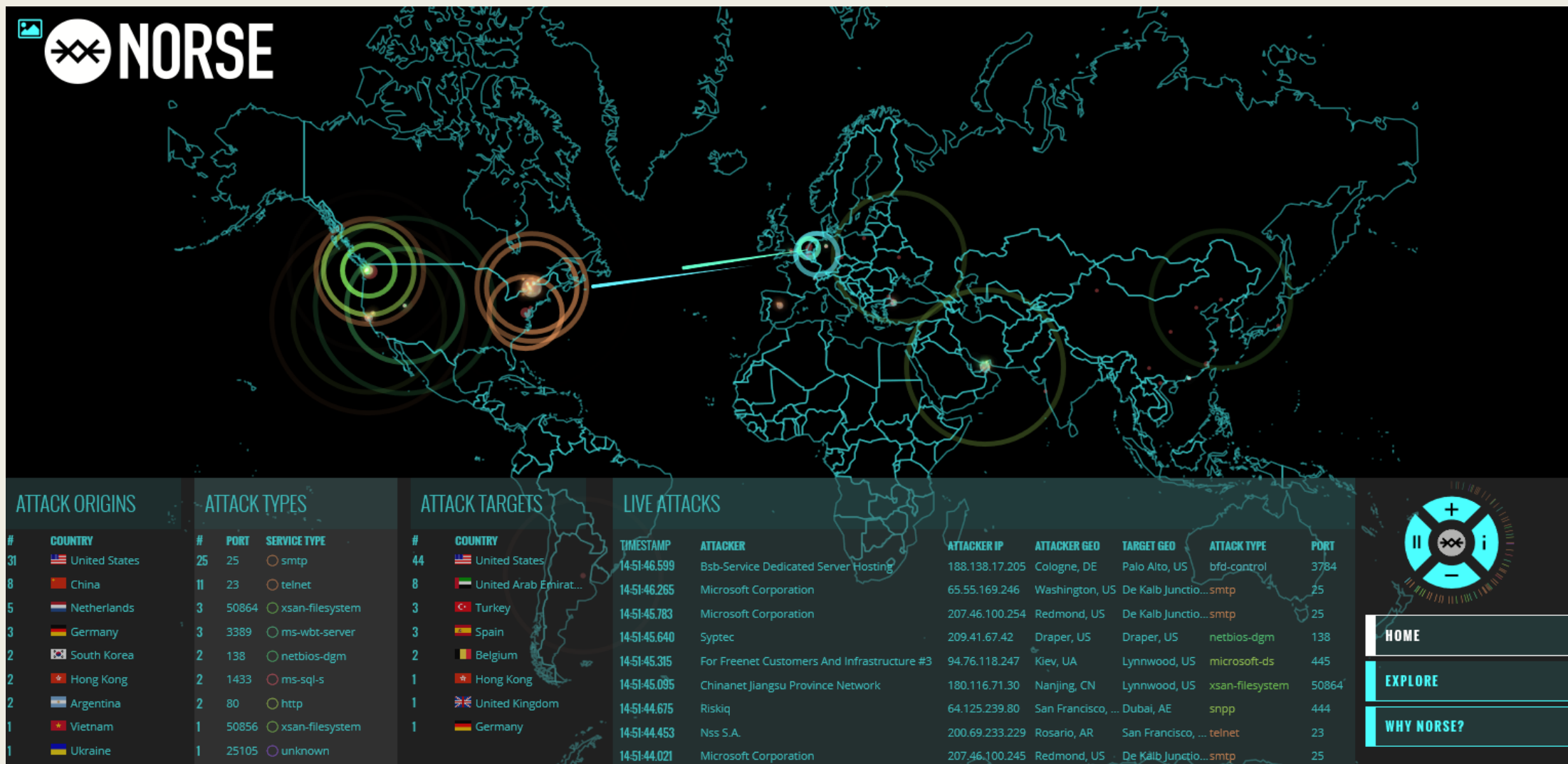
*Nguyễn Đăng Thứ - [thunguyendang@vccorp.vn](mailto:thunguyendang@vccorp.vn)*

# CONTENTS

---



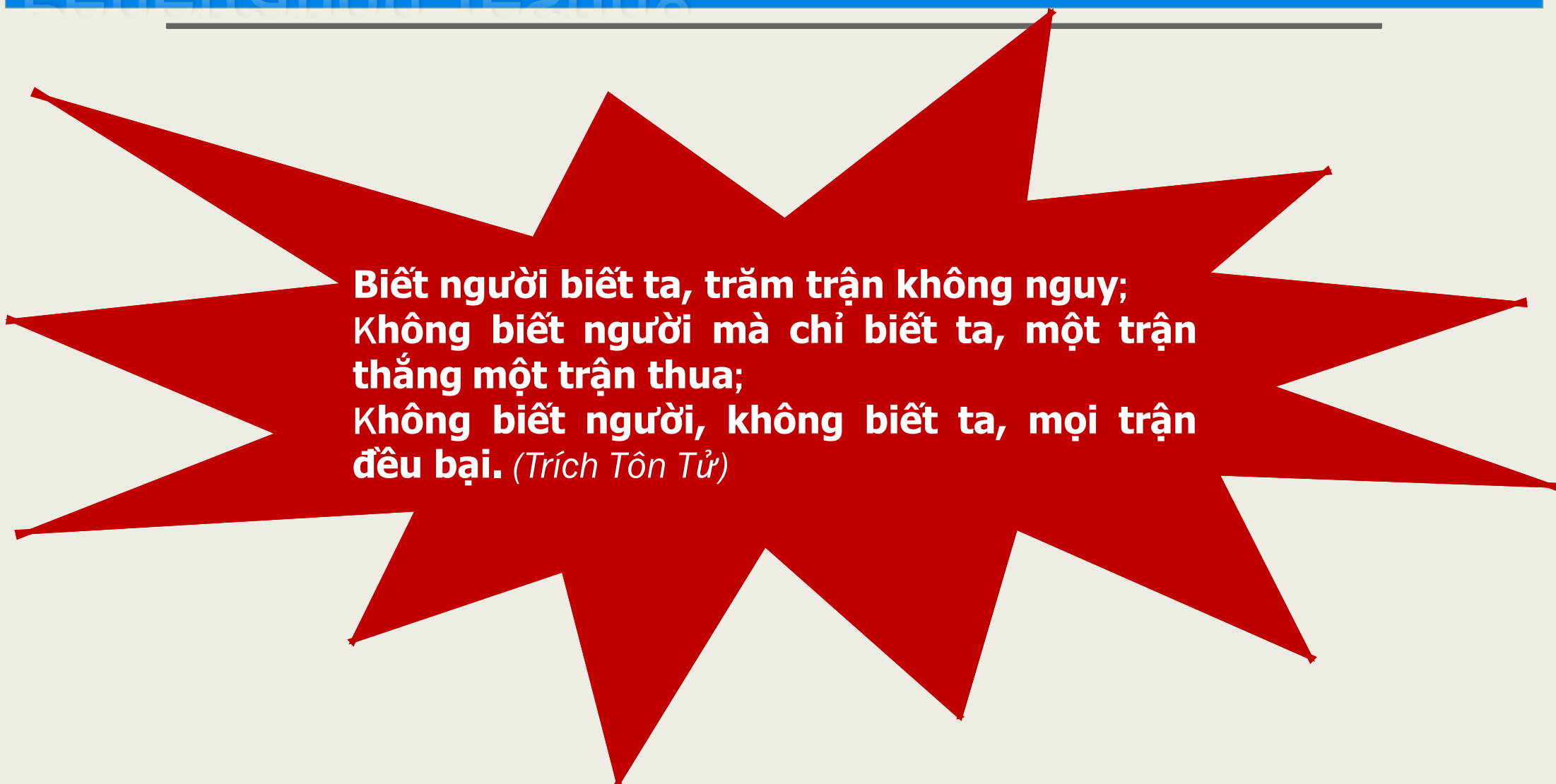
# ISSUES



# ISSUES



# Penetration Testing



**Biết người biết ta, trăm trận không nguy;  
Không biết người mà chỉ biết ta, một trận  
thắng một trận thua;  
Không biết người, không biết ta, mọi trận  
đều bại. (Trích Tôn Tử)**

# Penetration Testing

---

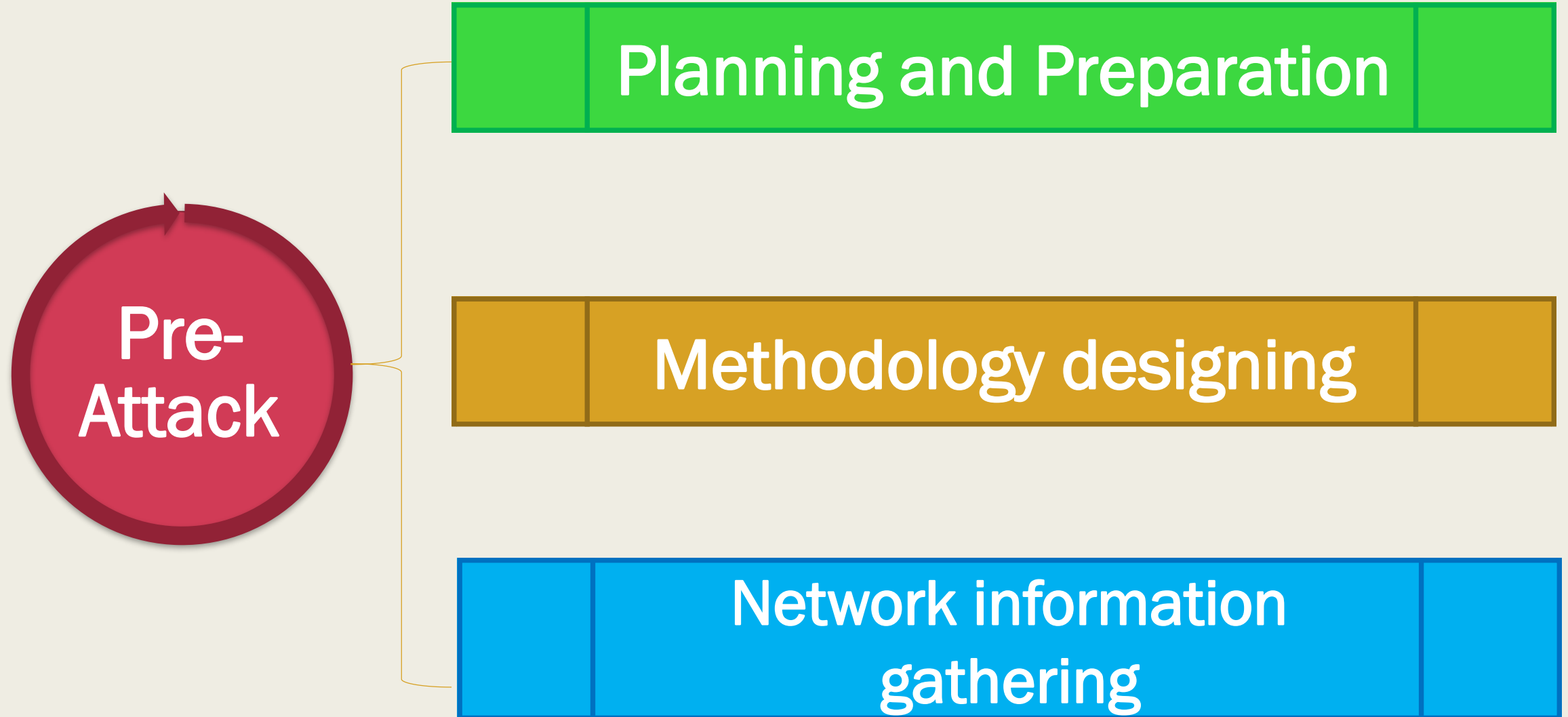
“Biết người”???



# Penetration Testing

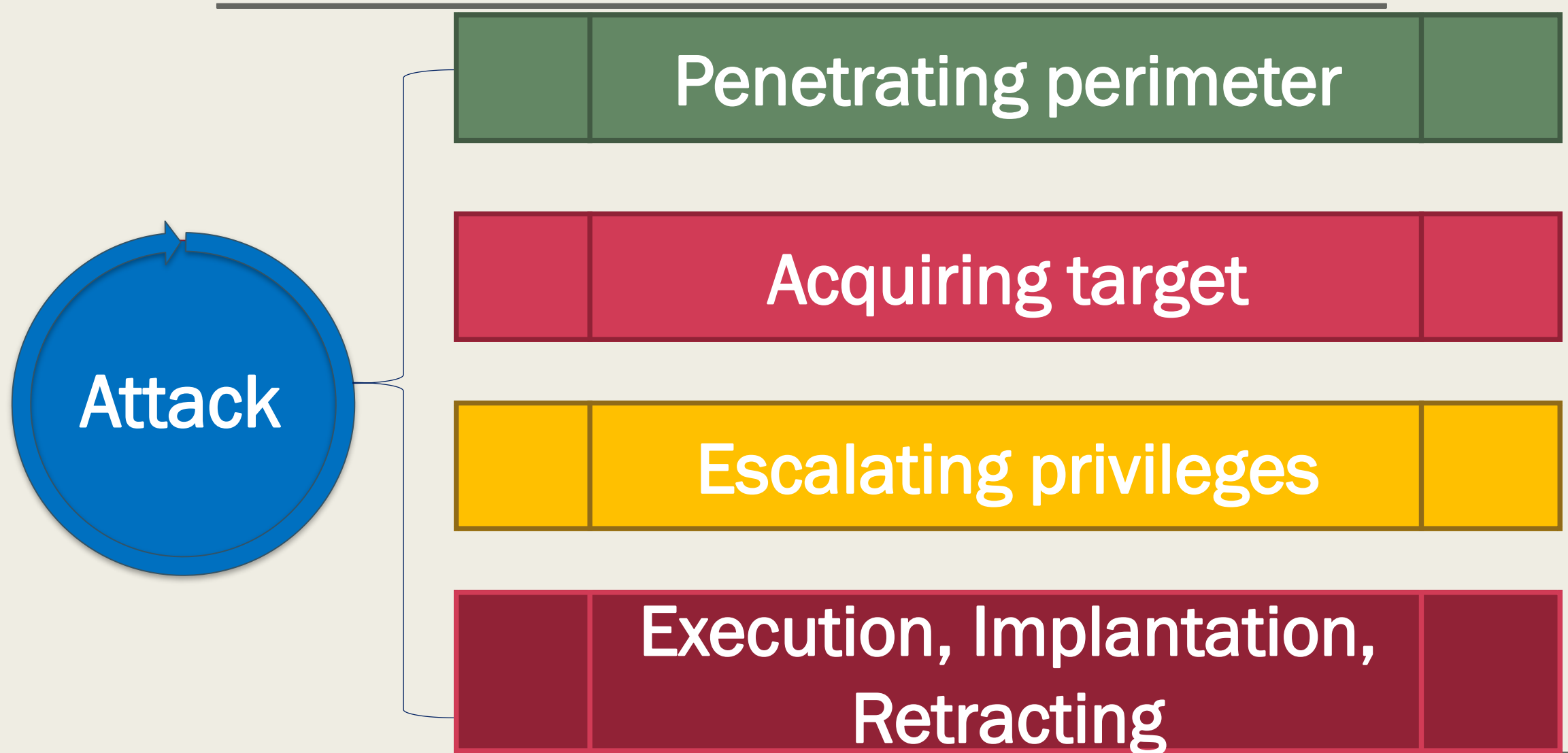


# Penetration Testing

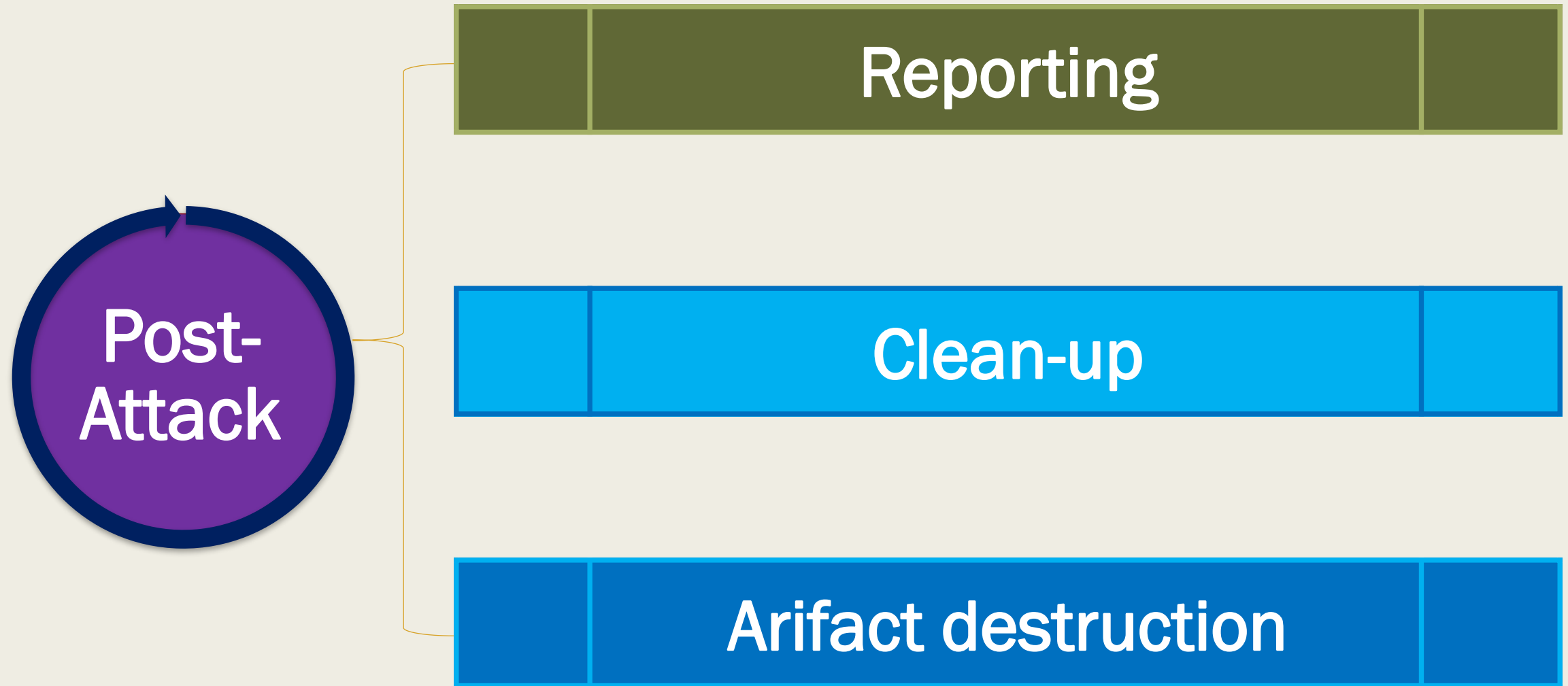




# Penetration Testing



# Penetration Testing



# OWASP TOP 10

---

A1 - Injection	A6 – Sensitive Data Exposure
A2 - Broken Authentication and Session Management	A7 – Missing Function Level Access Control
A3 – Cross-Site-Scripting (XSS)	A8 – Cross-Site-Request Forgery (CSRF)
A4 – Insecure Direct Object References	A9 – Using Components with Known Vulnerabilities
A5 – Security Misconfiguration	A10 – Unvalidated Redirects and Forwards

Báo tiếng Việt nhiều người xem nhất

SỞ HỮU SẢN PHẨM  
"CÔNG NGHỆ ĐỈNH"  
NHẬT BẢN

20

[Thời sự](#)
[Thế giới](#)
[Kinh doanh](#)
[Giải trí](#)
[Thể thao](#)
[Pháp luật](#)
[Giáo dục](#)
[Sức khỏe](#)

[Đời sống số](#)
[Sản phẩm](#)
[Điện tử gia dụng](#)
[Làng game](#)
[Kinh nghiệm](#)

[Sở hữu](#)
[Đời sống số](#)
[Bảo mật](#)

Thứ hai, 1/6/2015 | 21:41 GMT+7

## Hơn 1.000 website Việt Nam bị tấn công hai ngày cuối tháng 5

Chỉ trong hai ngày 30/5 và 31/5, khoảng 1.200 trang web của Việt Nam và Philippines đã bị tin tặc tấn công, thay đổi giao diện và để lại các thông điệp liên quan đến xung đột trên Biển Đông.

Theo diễn đàn bảo mật WhiteHat, trong số này có tới hơn 1.000 website là của Việt Nam. Đáng chú ý là thống kê cho thấy có 15 website có địa chỉ .gov.vn và 50 trang web có đuôi .edu.vn. Thông tin này được đăng trên site của nhóm tin tặc 1937cn.

## Phân tích vụ việc 1000 website của Việt Nam bị Trung Quốc tấn công

[Bài phân tích hay](#)
[Khẩn cấp](#)
[Tin tức](#)

June 2, 2015 10:12 am



Như nhiều báo chí đã đưa tin, nhằm phản hồi lại việc tấn công tên "OpChina" của một số hacker đến từ Việt Nam và Philippines, Trung Quốc đã thực hiện công defacement, chiếm quyền điều khiển, DDOS và các hoạt động tấn công khác. Nhóm hacker 1937cn đã trả đũa bằng cách tấn công 1000 website của Trung Quốc.

FCKEditor

A9 – Using Components with Known Vulnerabilities





SQLi



Details

# Ubuntu Linux Forum Hacked!

A1 - Injection

# 200 Million Hacked YAHOO! Accounts Up On SALE



Yahoo 200M

By peace\_of\_mind ( 100.0% ) ( 14 )

0 3.0000 / BT

weak password  
hashing!

Qty: 0

Buy It Now

Escrow

Yes, escrow by RealDeal is available.

Class

Digital

Ships From

Worldwide

Favorite

Question

## A6 – Sensitive Data Exposure



## FILE 69: VỤ ÁN 3 TRIỆU THÔNG TIN CÁ NHÂN



```
public static ResponseData getUserProfile(String paramString)
{
    new ResponseData();
    return HttpUtils.callGetApi(Common.getXHostByLanguage() +
    "api/customer/profile/id" + "/" + paramString);
}
```

### A4 – Insecure Direct Object References

# Penetration Testing

---

“Biết ta”???





# Secure software development



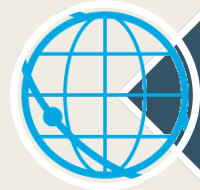
Configuration Policies



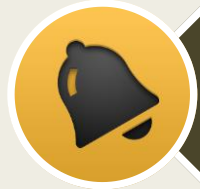
Privacy & Security



Checklists & Rating Scales



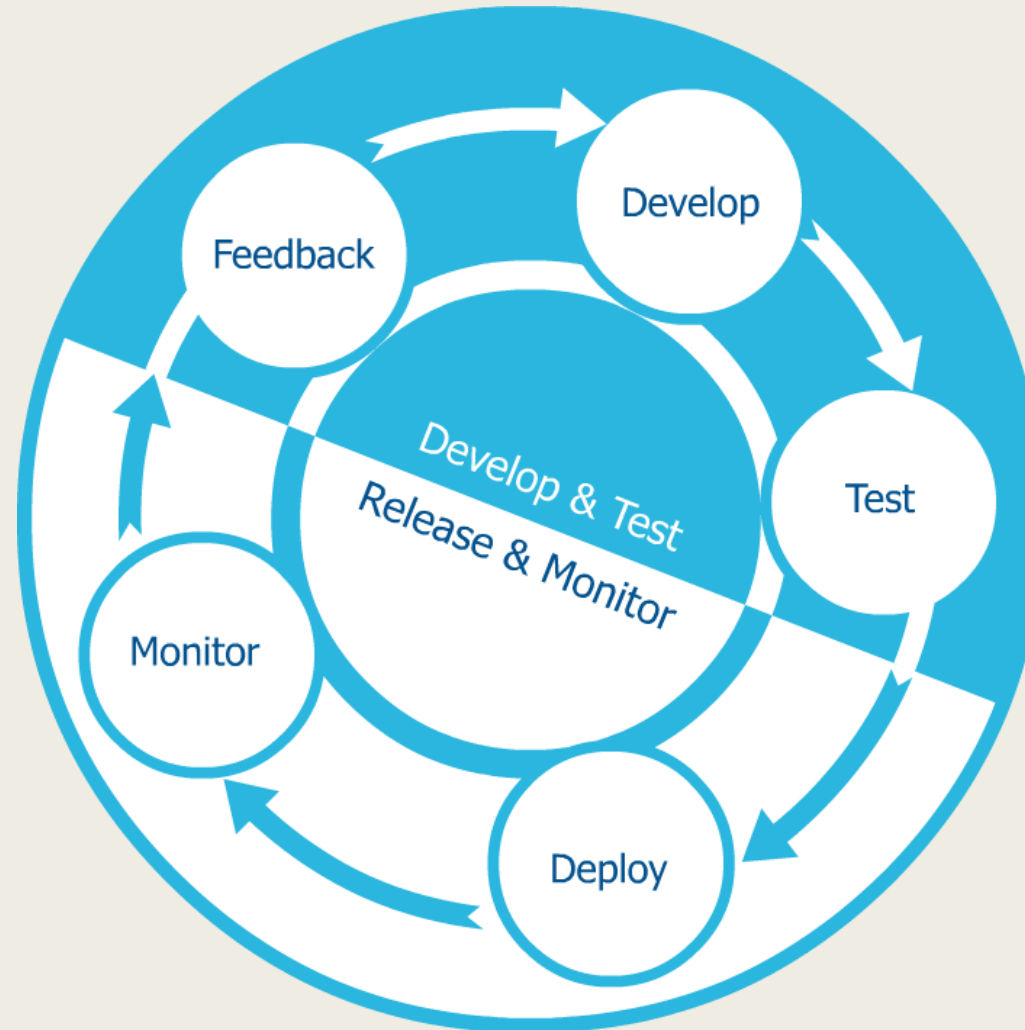
Web Security



Notification Security

# Secure software development

- Lifecycle




# Secure software development



## Configuration Policies

- CPE (Platforms)
- CVE (Vulnerabilities)
- CVSS (Scoring System)
- CCE (Configurations)
- XCCDF (Configuration Checklists)
- OVAL (Assessment Language)

# Configuration Policies

 OpenSCAP Evaluation Report 1.1.0

CharacteristicsCompliance and ScoringRule OverviewResult Details

### Characteristics

Evaluation was performed on a target called **some.target.somewhere.com**.

#### CPE Platforms

cpe:/o:fedora:project:fedora:20


#### Addresses

IPv4 123.123.123.123

IPv4 123.123.123.124

IPv6 0:0:0:0:0:0:1

### Compliance and Scoring

 **The system is not compliant!** Please review rule results and apply remediation.

55% passed

35% failed

10% other

Scoring system	Score	Maximum	%
urn:xccdf:scoring:default	42.71	100.00	<div>42.71%</div>
urn:xccdf:scoring:flat	62.71	100.00	<div>62.71%</div>

### Rule Overview

Showing 1 to 2 of 2 items

Title ^	Identifiers	Severity	Result
<a href="#">gpgcheck Enabled In Main Yum Configuration</a>	-	medium	<div>pass</div>
<a href="#">Prelinking Disabled</a>	<ul style="list-style-type: none"><li>cve 123</li><li>cce 321</li></ul>	low	<div>fail</div>

<< < 1 of 1 > >>

# Configuration Policies

## Result Details

### Prelinking Disabled

Result	fail
Rule ID	xccdf_org.ssgproject.content_rule_disable_prelink
Time	2014-07-09 16:19
Severity	low

The prelinking feature changes binaries in an attempt to decrease their startup time. In order to disable it, change or add the following line inside the file `/etc/sysconfig/prelink`:

```
PRELINKING=no
```

Next, run the following command to return binaries to a normal, non-prelinked state:

```
# /sbin/prelink -ua
```

The prelinking feature can interfere with the operation of checksum integrity tools (e.g. AIDE), because it modifies binaries to speed up their startup time. Also it makes the location of shared libraries very predictable, mitigating the efficiency of address space layout randomization (ASLR) protection mechanism. In addition, each upgrade of an application or a library requires prelink to be run again.

Remediation script:

```
#
# Disable prelinking altogether
#
if grep -q ^PRELINKING /etc/sysconfig/prelink
then
    sed -i 's/PRELINKING.*/PRELINKING=no/g' /etc/sysconfig/prelink
else
    echo -e "\n# Set PRELINKING=no per security requirements" >> /etc/sysconfig/prelink
    echo "PRELINKING=no" >> /etc/sysconfig/prelink
fi

#
# Undo previous prelink changes to binaries
#
/usr/sbin/prelink -ua
```

# Configuration Policies

Rule ID	xccdf_org.ssgproject.content_rule_service_chronyd_or_ntpd_enabled
Result	pass
Time	2015-09-25T11:00:45
Severity	medium
Identifiers and References	<div>identifiers: CCE-RHEL7-CCE-TBD</div> <div>references: AU-8(1), 160, Test attestation on 20121024 by DS</div>
Description	<p>The <code>chronyd</code> service can be enabled with the following command:</p> <pre>\$ sudo systemctl enable chronyd</pre> <p>Note: The <code>chronyd</code> daemon is enabled by default.</p> <p>The <code>ntpd</code> service can be enabled with the following command:</p> <pre>\$ sudo systemctl enable ntpd</pre> <p>Note: The <code>ntpd</code> daemon is not enabled by default. Though as mentioned in the previous sections in certain environments the <code>ntpd</code> daemon might be preferred to be used rather than the <code>chronyd</code> one. Refer to: <a href="https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/ch-Configuring_NTP_Using_the_chrony_Suite.html">https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/ch-Configuring_NTP_Using_the_chrony_Suite.html</a> for guidance which NTP daemon to choose depending on the environment used.</p>
Rationale	<p>Enabling some of <code>chronyd</code> or <code>ntpd</code> services ensures that the NTP daemon will be running and that the system will synchronize its time to any servers specified. This is important whether the system is configured to be a client (and synchronize only its own clock) or it is also acting as an NTP server to other systems. Synchronizing time is essential for authentication services such as Kerberos, but it is also important for maintaining accurate logs and auditing possible security breaches.</p> <p>The <code>chronyd</code> and <code>ntpd</code> NTP daemons offer all of the functionality of <code>ntpdate</code>, which is now deprecated. Additional information on this is available at <a href="http://support.ntp.org/bin/view/Dev/DeprecatingNtpdate">http://support.ntp.org/bin/view/Dev/DeprecatingNtpdate</a></p>

# Secure software development



## Privacy & Security

- Facebook Policy <https://www.facebook.com/policy.php>
- Google Policy <https://www.google.com/policies/privacy/>



# Secure software development



## Checklists & Rating Scales

- Joomla [https://docs.joomla.org/Security\\_Checklist](https://docs.joomla.org/Security_Checklist)
- Wordpress [https://codex.wordpress.org/Main\\_Page](https://codex.wordpress.org/Main_Page)
- Magento <https://magento.com/security/best-practices>
- Closedsource or CMS ???



# Secure software development

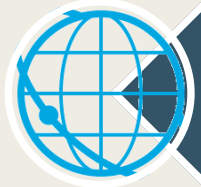


## Checklists & Rating Scales

Item	Description
Secure the Login page	<input type="checkbox"/> Lockdown the <a href="#">login page</a> for repetitive failed login
	<input type="checkbox"/> Activate <a href="#">2 factor authentication</a>
	<input type="checkbox"/> Use <a href="#">email address</a> to login instead of username
	<input type="checkbox"/> Rename wp-login.php file to another name (Optional)
	<input type="checkbox"/> Remove login link from the theme (if there is any)
	<input type="checkbox"/> Use a strong password containing upper and lower alphabet, number and special characters and at least 16 characters long
	<input type="checkbox"/> Change the password regularly
Protecting the Admin dashboard	<input type="checkbox"/> Password protect the “wp-admin” folder
	<input type="checkbox"/> Implement SSL for the WordPress Admin section
	<input type="checkbox"/> Update WordPress to the latest version
	<input type="checkbox"/> Create another administrator account and delete the default “admin” account
	<input type="checkbox"/> Create an Editor account and use it solely for publishing articles.
	<input type="checkbox"/> Install anti-virus plugin like <a href="#">WordFence</a> , <a href="#">WP Security Scan</a> , <a href="#">Sucuri</a> , <a href="#">VIP Scanner</a> , <a href="#">Exploit Scanner</a>
	<input type="checkbox"/> Scan the site for viruses, malware and security loopholes

Protecting the Theme	<input type="checkbox"/> Update the active theme to the latest version
	<input type="checkbox"/> Delete and remove unused themes
	<input type="checkbox"/> Download and use theme only from reputable sources
	<input type="checkbox"/> Remove WordPress version from the theme
Improving the Plugins	<input type="checkbox"/> Update all plugins to the latest version
	<input type="checkbox"/> Delete unused plugins
	<input type="checkbox"/> Only install plugin from a reputable source
	<input type="checkbox"/> Replace outdated plugins with alternative newer plugin
Protect the Database	<input type="checkbox"/> Upload a blank index.html file to the plugin folder to prevent unauthorized viewing of your plugins
	<input type="checkbox"/> <a href="#">Change the default table prefix</a>
Web host Issues	<input type="checkbox"/> Schedule weekly <a href="#">backup</a> of the database and site
	<input type="checkbox"/> Hire a reliable and trustworthy web host
	<input type="checkbox"/> Access your site only with SFTP (Secure FTP)
	<input type="checkbox"/> Set all files to file permission 644 and all folders to 755
	<input type="checkbox"/> Make sure the <i>wp-config.php</i> file is not accessible by others.

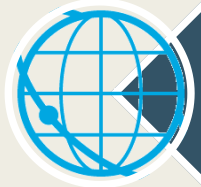
# Secure software development



## Web Security

- W3C Security: <https://www.w3.org/Security/>
- P3P <https://www.w3.org/P3P/>
- Chrome: <https://developers.google.com/web/>
- Firefox: <https://developer.mozilla.org/en-US/docs/Web/>
- Backend Programming Language???

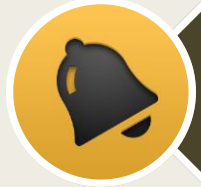
# Secure software development



## Web Security

- Platform: unies/windows
- Protocol: http, ftp, ssh, rdp,
- Database: oracle/mssql/mysql..
- WebUI:html, css, js, media, document,
- Programming language: adobe cfm/php/java/.net/rubyonrails/python
- Plugin: ...
- Framework: ...
- Library: ...
- Opensource: ...

# Secure software development



## Notification Security

- Wordpress <https://wpvulndb.com/>
- Joomla <https://vel.joomla.org/live-vel>
- Magento <https://magento.com/security/vulnerabilities>
- Closesource or CMS???

THANKS FOR YOUR  
LISTENING!



VIETNAM  
WEB  
SUMMIT