SANGFOR

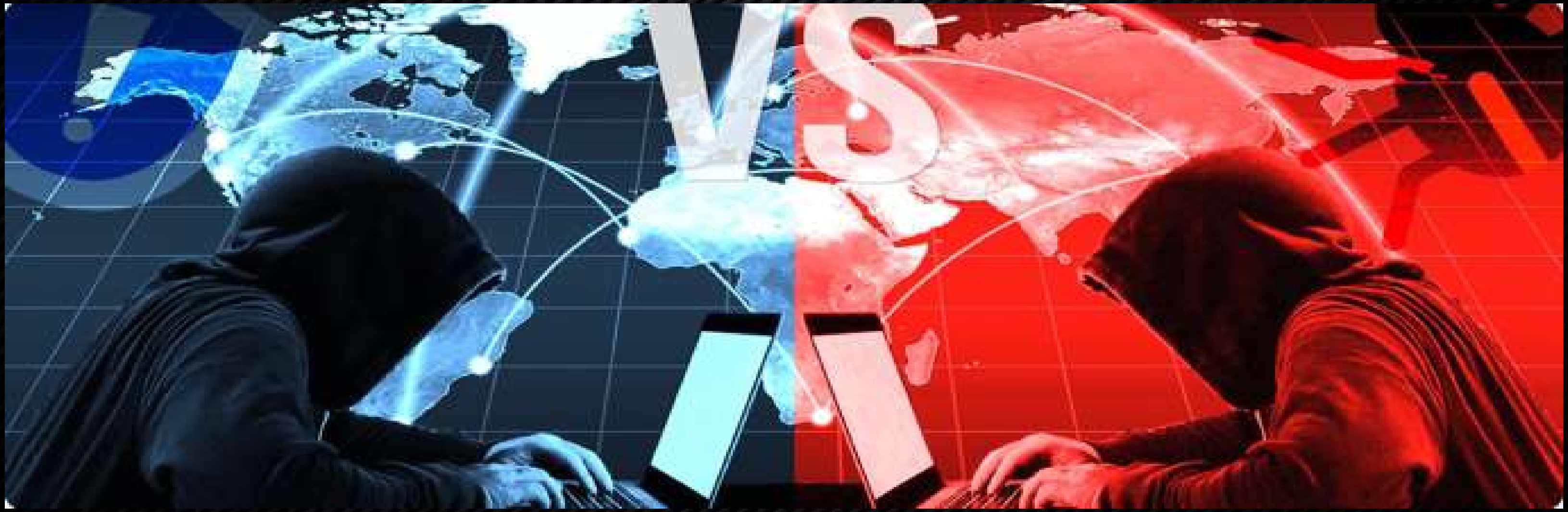
Penetration Test & Red Team Service A Real-Life CTF

Kaiser Lee | Solution Consultant |CEH, OSCP, CISSP
Kaiser.lee@sangfor.com
Sangfor Technologies

Capture-the-flag (CTF)

Capture the Flag (CTF) in computer security is an exercise in which participants attempt to find text strings, called "flags", which are secretly hidden in purposefully-vulnerable programs or websites.

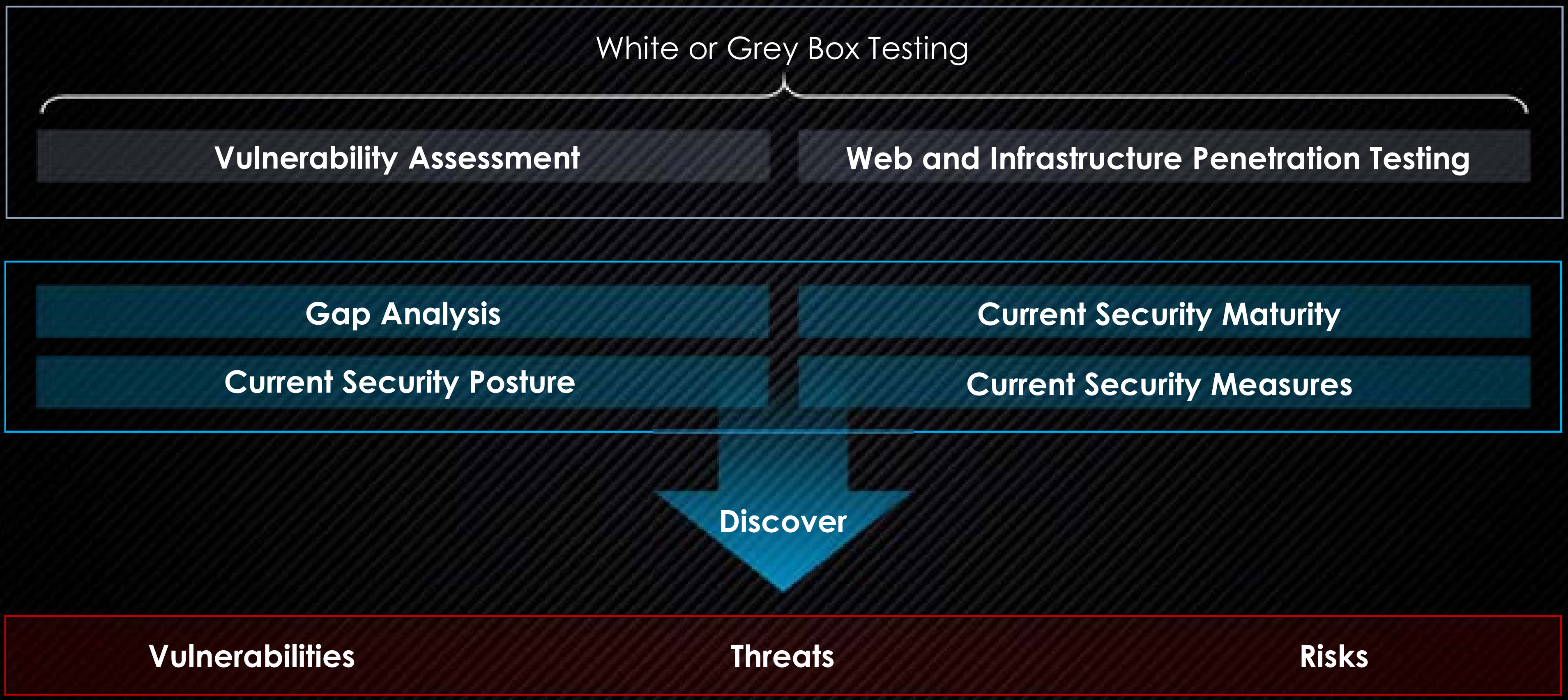
- Jeopardy-style challenges
- Attack-with-Defense (AWD)



Techniques using in CTF

- Forensics
- Cryptography
- Web Exploitation
- Reverse Engineering
- Binary Exploitation

What is Security Assessment & Consultation



White or Grey Box Testing

Vulnerability Assessment

Web and Infrastructure Penetration Testing

Gap Analysis

Current Security Maturity

Current Security Posture

Current Security Measures

Discover

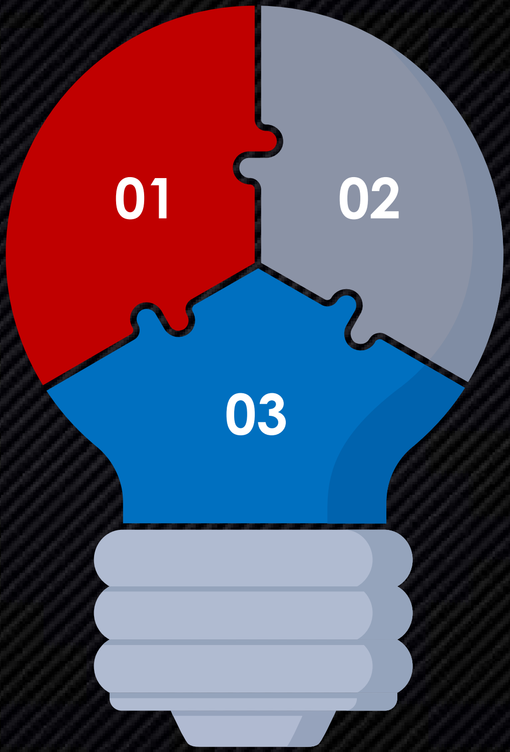
Vulnerabilities

Threats

Risks

Why Security Assessment & Consultation?

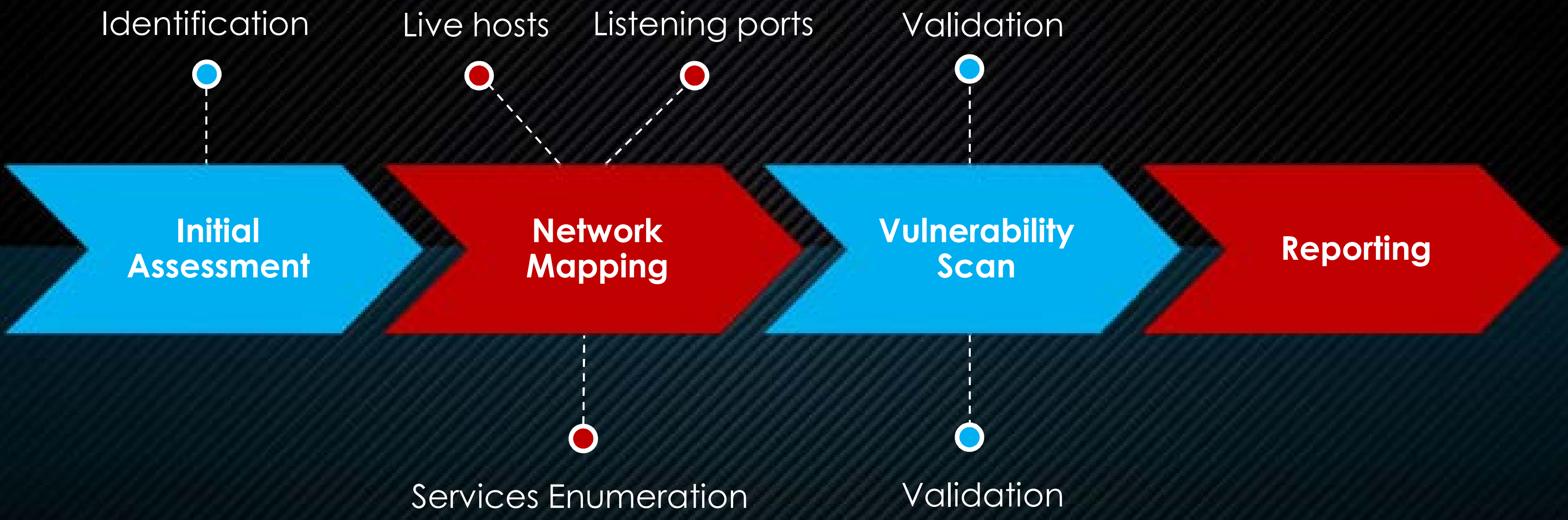
- Identify Security Posture
- Meet Minimum Security Requirements
- Compliance
- Basis for Decision Making
- Identify Vulnerabilities, Threats & Risks
- Asset Protection
- Security Awareness



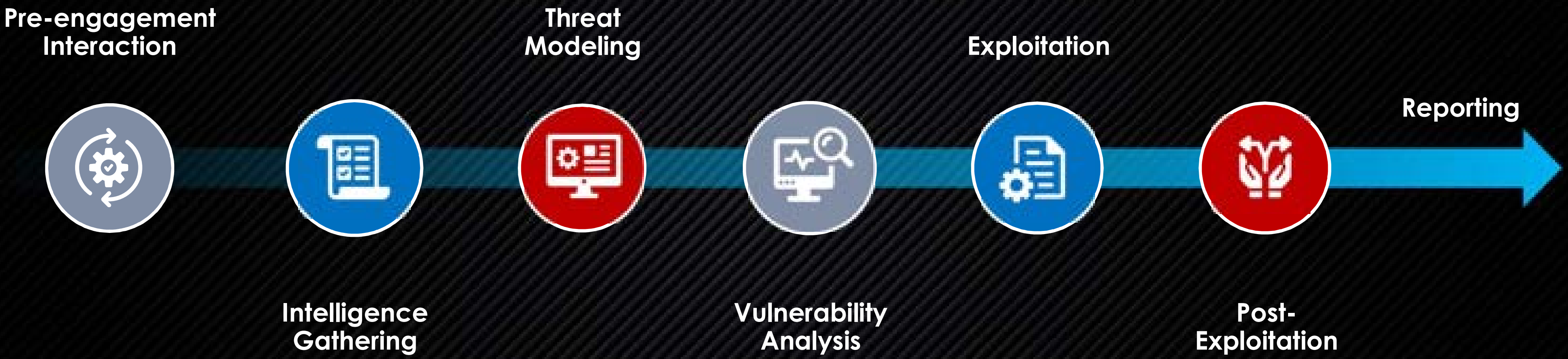
- Business Focus
- Security Status
- Image & Reputation
- User Trust

- Attacks Surfaces & Vectors
- Uncertain on threats & Risks
- Security Incidents
- Worry

Vulnerability Assessment Methodology



Penetration Test Methodology



Pre-engagement Interaction

Intelligence Gathering

Threat Modeling

Vulnerability Analysis

Exploitation

Post-Exploitation

Reporting

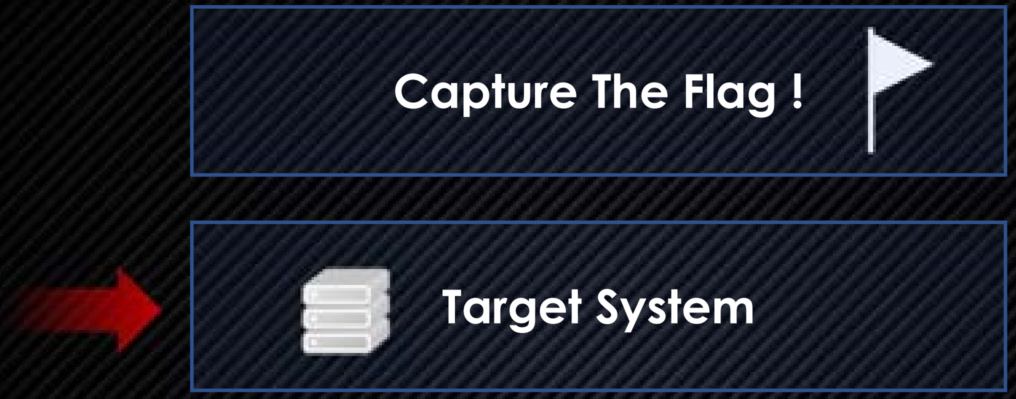
Red Team Services - Prerequisites of a Security Scenario

- **Security self-inspection:** Many organizations are currently facing APT attacks, and it is imperative to simulate the APT attacker's perspective to find out the security problems;
- **Capability verification:** It has become a mainstream practice to verify the cyber security defense capability of an organization's core business systems through red team service.
- **Drills and preparations:** Regulatory agencies and industry competent units will also organize multiple offensive and defensive drills to test the security protection capabilities of relevant units. Once the ranking is poor in the drills, it will affect the security performance of the organization. It is necessary to conduct in-depth security self-regulation during the drill preparation stage.

What is the Target?

Capture The Flag !

What is the Target?



Capture The Flag !

Target System

But, Customer will ask…

How did you do that?

What is the impact?

How do I fix it?

Red Team Service Target

Hacker's Perspective | Target Systems | Personnel | Software/Hardware Equipment | Infrastructure

Identify potential security risks by simulating hacker intrusions

Multi-pronged attack

Multi-dimensional attack

Adversarial attack

Attack Purpose

- ✓ System privilege escalation
- ✓ control business system
- ✓ Collect information

Security Weaknesses

- ✓ Entry point
- ✓ Attack path

Methodology: What will you do & How will you do?

Anything I can do to get the flag !

Methodology: What will you do & How will you do?

Anything I can do to get the target system !

But, in real life…

A complicated network **with 100,000** hosts…

Mindset

- In CTFs, you KNOW there is/are entry points
- In real life, who knows?

- An exposing RDP
- Zero-day vulnerabilities
- A vulnerable web application
- etc….

Mindset: Information gathering (Reconnaissance)

- What is the business nature?
- What application are they using?
- Any exposing attack surfaces?
- etc…

- Scanning
- Search Engines (Google hacking…)
- Browsing related website…

Red Team Attack Methods and Content

Social Engineering (Optional)

Phishing emails, SMS scams, dating scams, watering hole attacks, etc.

Web Security

Detect CMS, user registration, user login, password modification, password reset, verification code bypass, weak password, cookie replay attack, session token analysis, session token leak, session fixation attack, function abuse, vertical privilege escalation, horizontal privilege escalation, SQL injection, file upload, arbitrary file download, etc.

Database

Whether the database has weak passwords, improper permissions configuration, known historical vulnerabilities, etc.

Third-party Applications

Middleware and framework classes test whether the target system has remote code execution vulnerabilities such as Jboss, WebLogic, and Tomcat, and whether there are remote code execution vulnerabilities such as Shiro and Fastjson.

Centralized System

Detect whether there are vulnerabilities in the centralization of systems such as cloud management platforms, IoT management and control platforms, big data platforms, and single sign-on systems

Red Team
Service

Server, Host

Remote code execution test server and host for MS17010, CVE-2019-0708 and other vulnerabilities

Security/Network Equipment

Testing security/networking devices for weak password vulnerabilities and whether there are known historical vulnerabilities

Execution: Time to PWN !

SANGFOR

Any method, Any tools !

But, in real life…

A system with millions of trading per sec

Electricity System on a small town with million people

Application affect the whole organization operation

Execution: Time to PWN !

You can do an attack ≠ You can impact customer

What are the tools you are using? Are they trusted? What can the tools do? ….

Will the exploit cause a Denial-of-Services (DoS) to the customer?

DOES CUSTOMER ALLOW YOU TO TAKE THIS ACTION?

Execution: Time to PWN !

I am Ready ! (Pressed Enter to exploit…)

Execution: Time to PWN !

Security Products have joined the battle.

You do not need to face security products in most Jeopardy-style CTF

But, in real life…

- You are facing a secured (supposed) environment
- Endpoint solutions
- Firewalls
- Security Solutions
- Blue team
- etc…

Reporting Stage: What is a good report?

Similar to CTFs: Write-ups

- ✓ Abstract
- ✓ Purpose
- ✓ Methodology
- ✓ Details of exploitation
- ✓ Discovery
- ✓ Recommendation
- ✓ Clean-ups

Remember our target?

Red Team Service Value

SANGFOR

Discover security risks under current defenses

Red Team personnel simulate the invasion of hackers, cut in from the outside as a whole, and finally fall to a certain threat point and use it, and finally threaten the entire network, so as to promote the organization to speed up security construction based on the deep security hidden danger points under the current security defense situation.

Improve security awareness of all employees

The results of the red team detection can be used as cases of internal security awareness, and these cases can be used in the safety education of relevant managers, which can effectively urge managers to improve security awareness, thereby reducing the overall risk

Reduce risk of regulatory notification

Through the red team service, the security problems of the organization are found in time and rectification is made in time to prevent being notified by the superior competent department or industry supervision department.

Improve the defensive effect of drills

Carry out in-depth security self-inspection through red team service, timely discover and eliminate hidden security risks in the organization, and improve the defense effect of the exercise.

Takeaway

SANGFOR

1

CTFs provide good knowledge and techniques to Cybersecurity.

2

Security Assessment & Consultant are using these experiences to deliver services to customer.

THANK YOU!

Kaiser Lee | Solution Consultant |CEH, OSCP, CISSP
Kaiser.lee@sangfor.com
Sangfor Technologies