PENETRATION TESTING VS RED TEAMING, AND HOW TO MAKE BETTER REPORTS

Sampson Chandler
Senior Engineer – RSA Security
Handle – Rusty Shackleford (also GitHub)
Twitter - @SecuritySampson

NOT SURE IF PENETRATION TEST
OR RED TEAM ENGAGEMENT
memegenerator.net

My Infosec Career

- Interning in high school
- Help Desk
- Software Development
- Infosec

OVERVIEW

Issues We Face

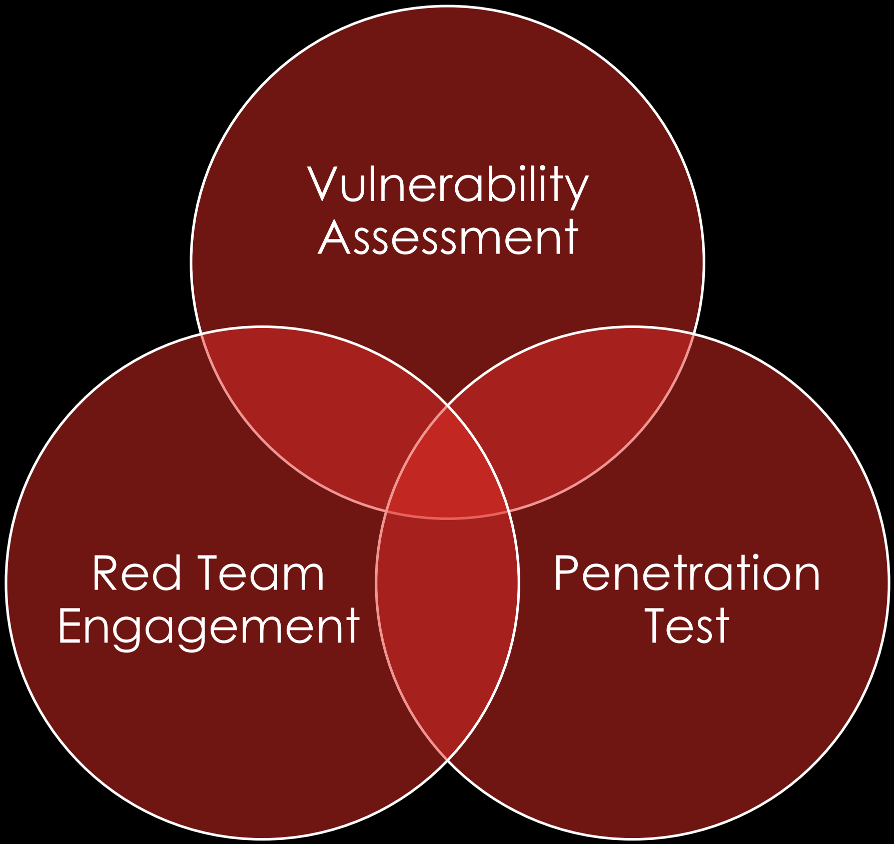
Penetration Testing

Red Teaming

Reports

Conclusion

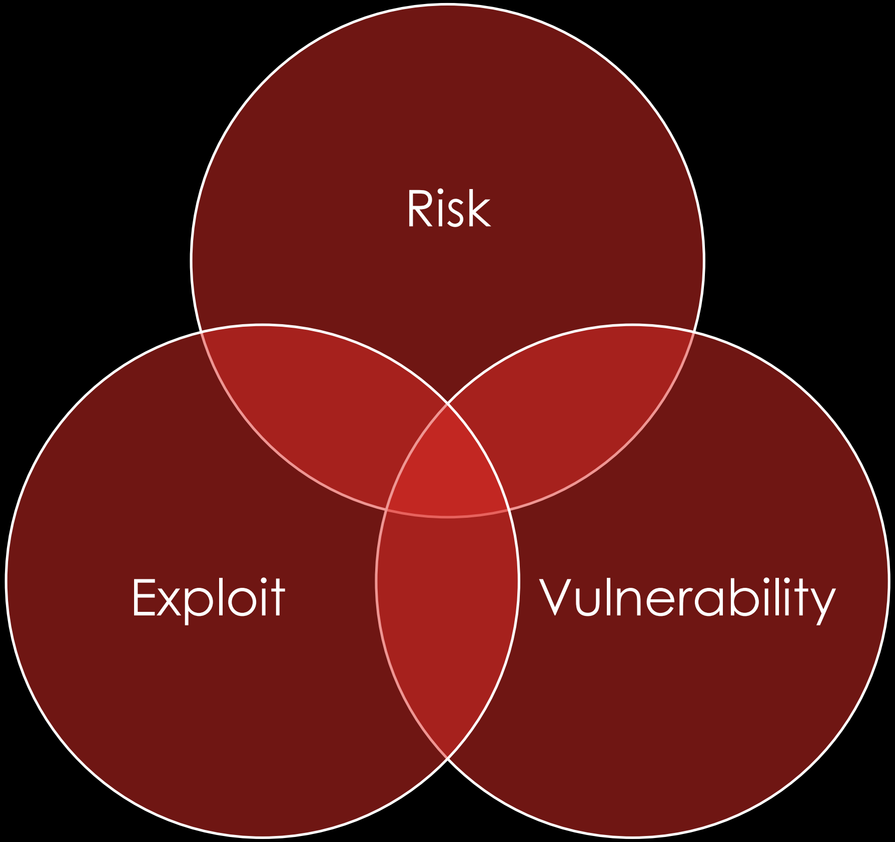
THE ISSUE – KEY TERMS



Vulnerability Assessment

Red Team Engagement

Penetration Test

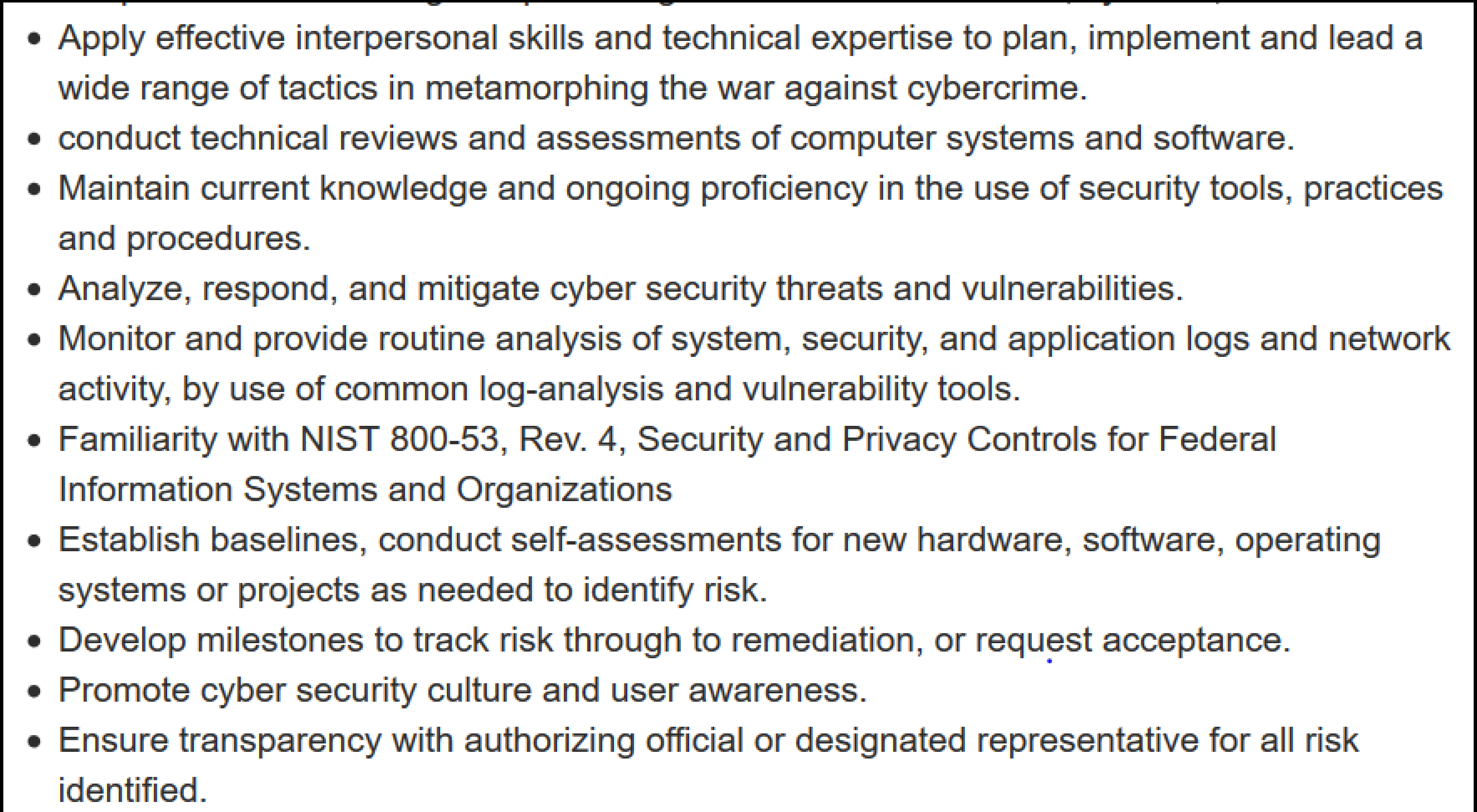


Risk

Exploit

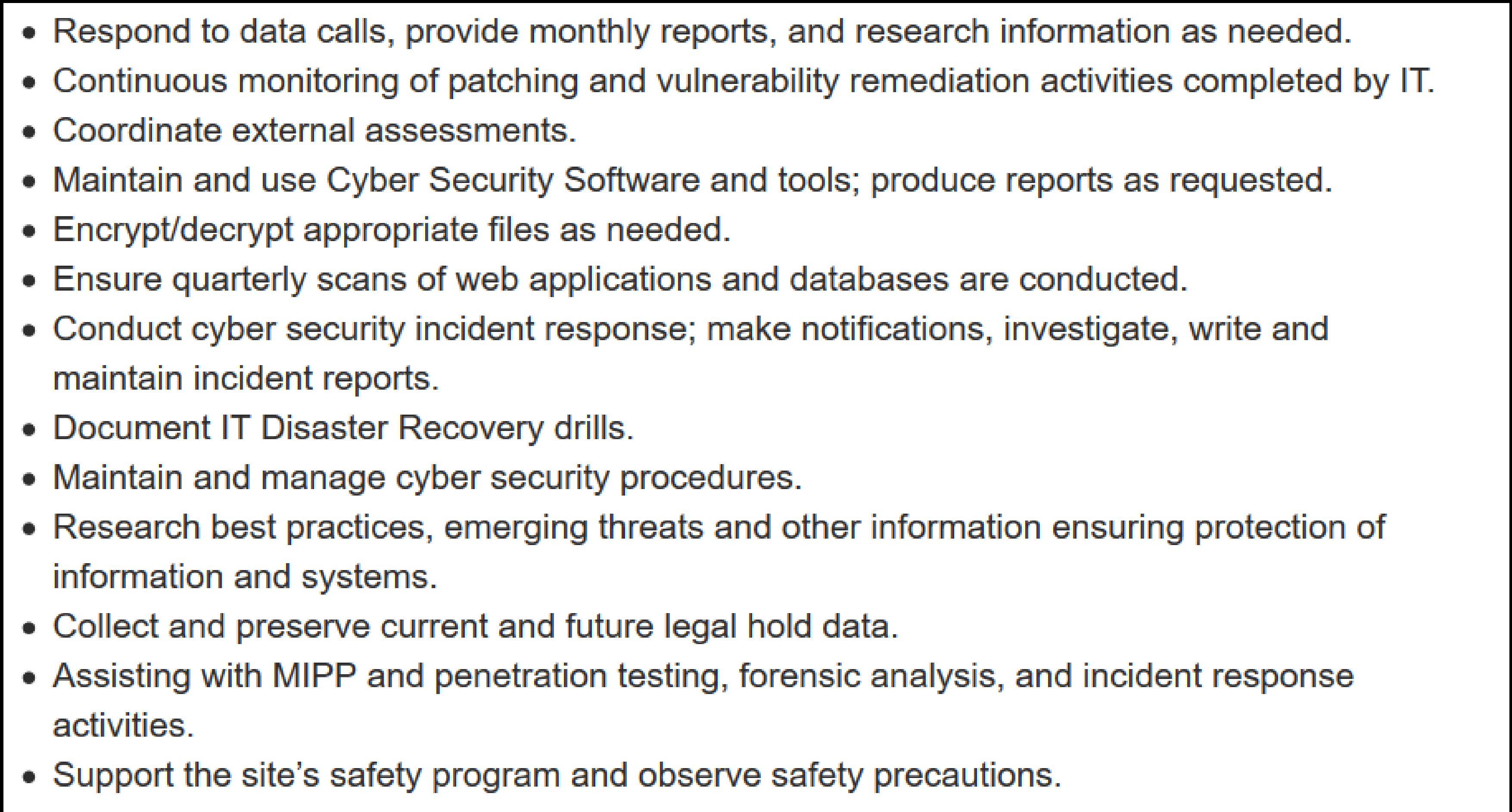
Vulnerability

CYBER SECURITY ANALYST



- Apply effective interpersonal skills and technical expertise to plan, implement and lead a wide range of tactics in metamorphing the war against cybercrime.
- conduct technical reviews and assessments of computer systems and software.
- Maintain current knowledge and ongoing proficiency in the use of security tools, practices and procedures.
- Analyze, respond, and mitigate cyber security threats and vulnerabilities.
- Monitor and provide routine analysis of system, security, and application logs and network activity, by use of common log-analysis and vulnerability tools.
- Familiarity with NIST 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Establish baselines, conduct self-assessments for new hardware, software, operating systems or projects as needed to identify risk.
- Develop milestones to track risk through to remediation, or request acceptance.
- Promote cyber security culture and user awareness.
- Ensure transparency with authorizing official or designated representative for all risk identified.

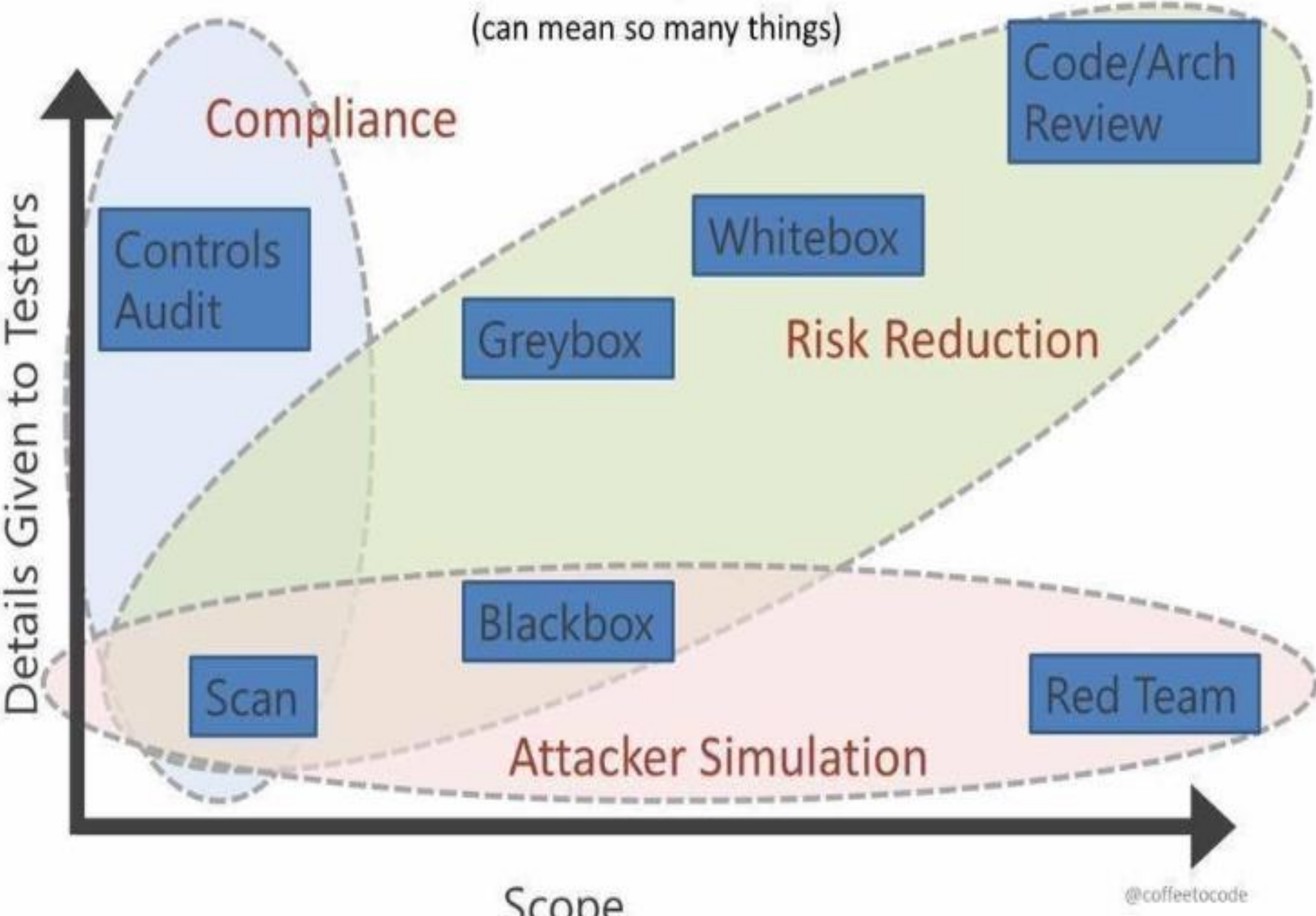
CONTINUED…



- Respond to data calls, provide monthly reports, and research information as needed.
- Continuous monitoring of patching and vulnerability remediation activities completed by IT.
- Coordinate external assessments.
- Maintain and use Cyber Security Software and tools; produce reports as requested.
- Encrypt/decrypt appropriate files as needed.
- Ensure quarterly scans of web applications and databases are conducted.
- Conduct cyber security incident response; make notifications, investigate, write and maintain incident reports.
- Document IT Disaster Recovery drills.
- Maintain and manage cyber security procedures.
- Research best practices, emerging threats and other information ensuring protection of information and systems.
- Collect and preserve current and future legal hold data.
- Assisting with MIPP and penetration testing, forensic analysis, and incident response activities.
- Support the site’s safety program and observe safety precautions.

"I want a pentest"

(can mean so many things)



PENETRATION TESTING

- Definition & Goals
- Penetration Testing VS Vulnerability Assessment
- Different types of penetration testing
- Scope and RoE
- Deciding which is best for your organization
- How each type provides value

PENETRATION TESTING

Goal

- Compromise target systems and gain access to information to determine business impact

Formal Definition

- "Penetration testing involves modeling the techniques used by real-world computer attackers;
    - To find vulnerabilities
    - To exploit those flaws under controlled circumstances
    - Done in a professional, and safe manner. According to carefully designed scope and Rule of Engagement
    - Determine business risk and potential impact, all with the goal of helping organizations improve their security practices“ - Ed Skoudis

Vulnerability Assessment

Frequency

- At least quarterly
- Anytime new equipment or software is added to environment

Reports

- Baseline but usually contains false positives
- Might have incorrect risk rating

Value

- Detects possible vulnerabilities that could be exploited

PENETRATION TESTING

Frequency

- Annually

Reports

- Depends on the type of pen test

Focus

- Discovers known (and possibly unknown) exploitable weaknesses in normal business processes

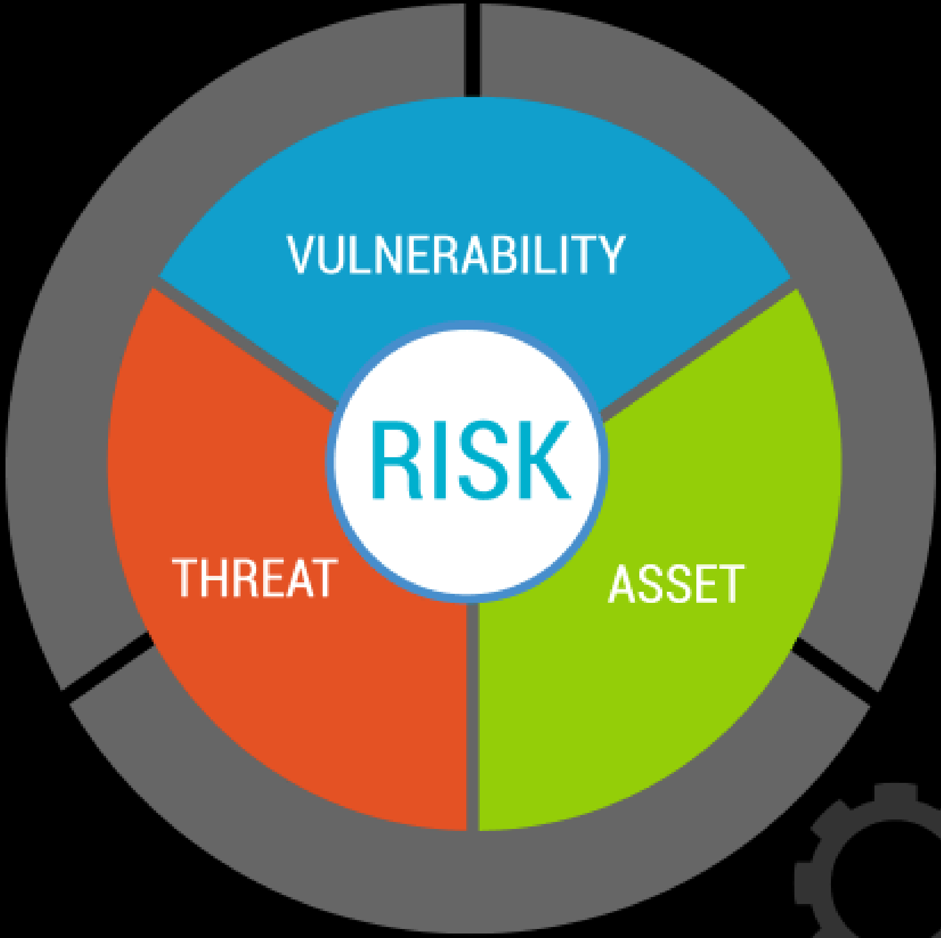
Performed By

- Best to use a third party service

Value

- Detects possible vulnerabilities that could be exploited, tests the blue team, and business impact

EXPLOITS, VULNERABILITIES, THREATS, AND RISK



Vulnerabilities

- A flaw in the measures you take to secure an asset, or anything that exposes your assets to harm.

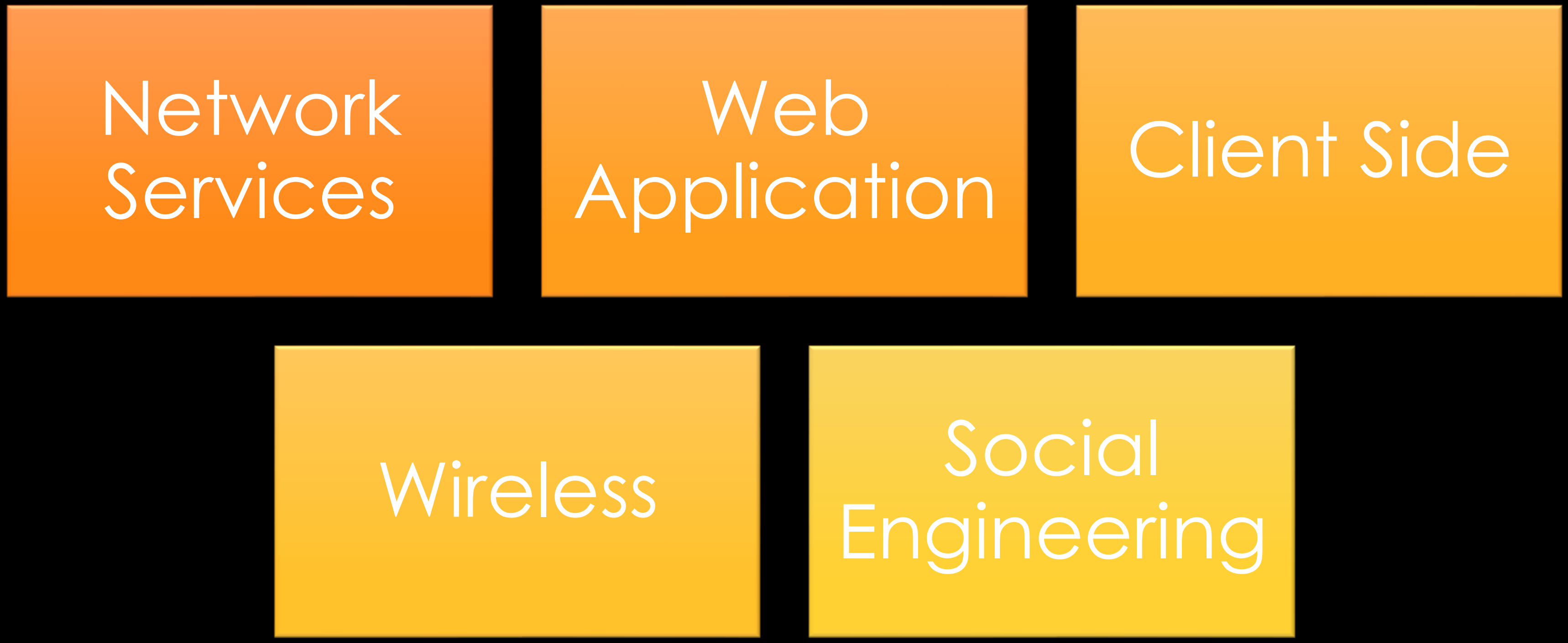
Threats

- Expressed or demonstrated intent to harm an asset or cause it to be come unavailable.

Risk

- “the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability” - Tag

TYPES OF PENETRATION TESTS



Network Services

Web Application

Client Side

Wireless

Social Engineering

DIFFERENCES IN PENETRATION TESTS

Black Box	White Box/Clear Box/Crystal Box	Gray Box
• No knowledge of network architecture, or software used. • Simulates real world attack • determines the vulnerabilities in a system that are exploitable from outside the network	• Tester knows the network infrastructure • Access to software source code • penetration testers are able to perform static code analysis,	• Provide a more focused and efficient assessment of a network's security than a black-box assessment • Can focus their assessment efforts on the systems with the greatest risk and value from the start, rather than spending time determining this information on their own

STEPS OF A PEN TEST

Information Gathering

- The stage of reconnaissance against the target.

Threat Modeling

- Identifying and categorizing assets, threats, and threats communities.

Vulnerability Analysis

- Discovering flaws in systems and applications using a set of tools, both commercially available tools and internally developed.

Exploitation

- Simulating a real-world attack to document any vulnerabilities.

Post-Exploitation

- Determining the value of compromise, considering data or network sensitivity.

Reporting

- Outlining the findings with suggestions for prioritizing fixes. For us, that means walking through the results with you hand-in-hand.

Value of a Pen Test

- Determine
- Identify
- Highlight
- Assess
- Test
- Provide
- Meet
- PrImplement and validate

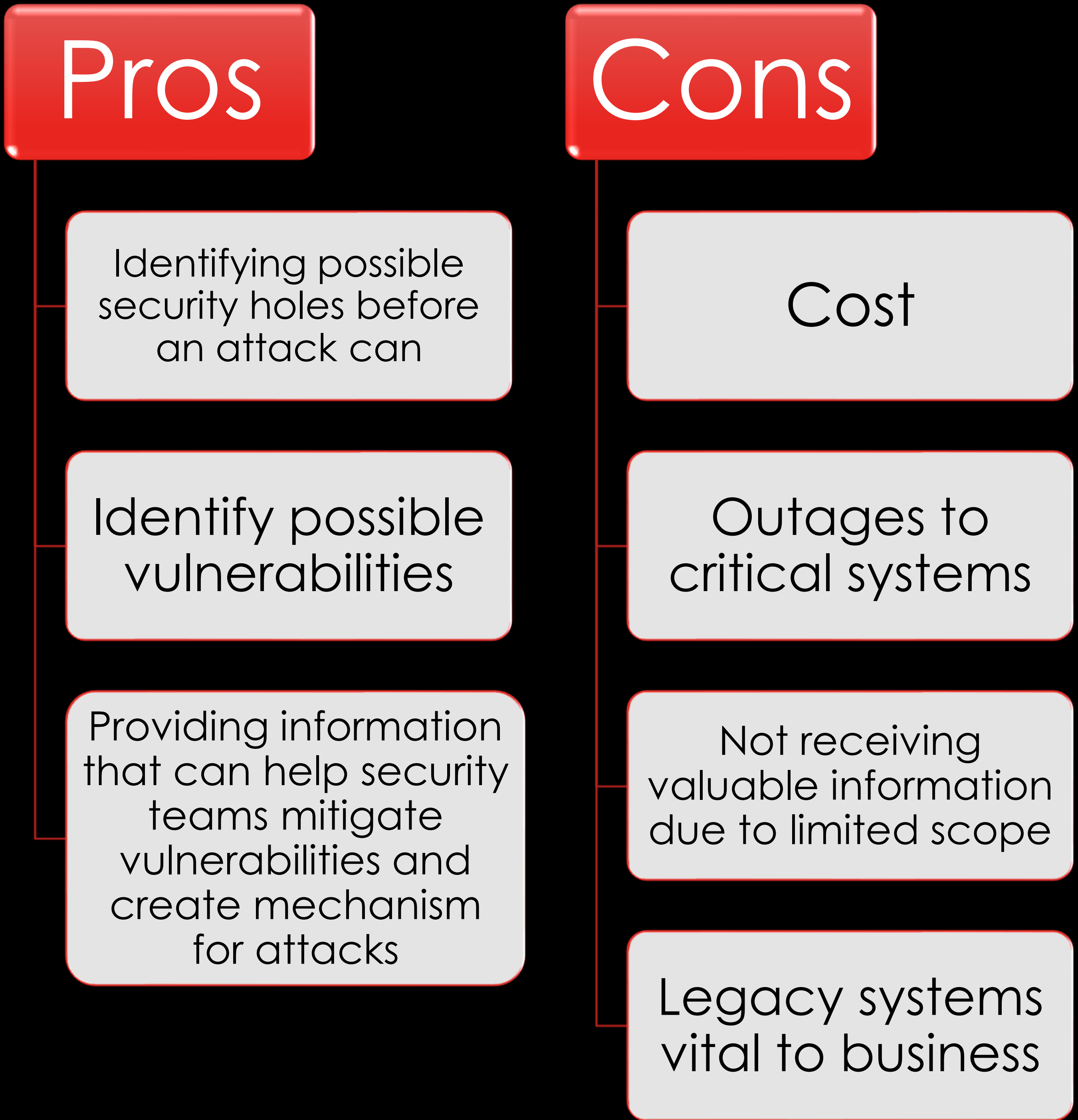
VALUE OF A PEN TEST

- Findings need to be presented in a business sense with data the client will understand.

(For any given risk, decision makers may conclude that, for business purposes, they will accept a given risk identified during a test, rather than mitigate the associated vulnerability. In the end, it’s a business decision)

DEFINING SCOPE & ROE

- Each needs to be defined thoroughly
- What are your security concerns?
- What is to be tested?
- What should be avoided?



Pros

- Identifying possible security holes before an attack can
- Identify possible vulnerabilities
- Providing information that can help security teams mitigate vulnerabilities and create mechanism for attacks

Cons

- Cost
- Outages to critical systems
- Not receiving valuable information due to limited scope
- Legacy systems vital to business

"…one who knows the enemy and knows himself will not be endangered in a hundred engagements."

- Sun Tzu

Originated in the U.S. Military during the 1960s during the height of the Cold War with the Soviet Union

Emerged from game-theory approaches applied to war-gaming and scenario simulations designed to evaluate strategic decisions

From https://www.nuharborsecurity.com/red-teaming-vs-penetration-testing/

RED TEAM

- Definition/Goal
- Misconceptions
- Method & Examples
- Does your company need it?
- Deciding which is best for your organization
- Building a team

PEN TEST = PIRATES
RED TEAM = NINJAS

RED TEAM

Goal-Based adversarial testing process

Identify physical, hardware, software, and human vulnerabilities

Obtain a more realistic understanding of risk for your organization

Help address and fix all identified security weaknesses

Measures how an organization will respond to an attack

Incorporates many elements of an organization's overall security posture

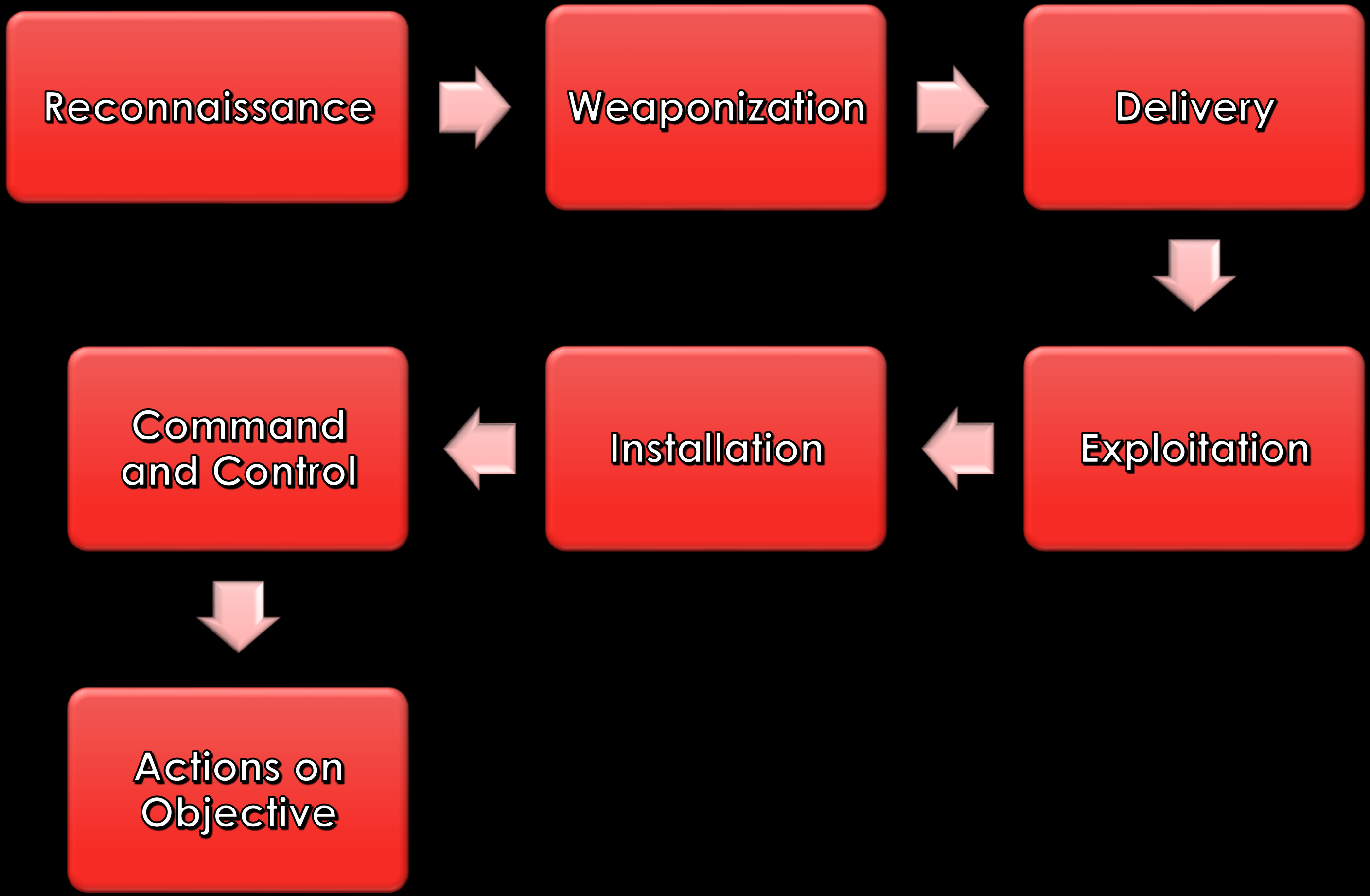
WHAT IS A RED TEAM ENGAGEMENT?

"A red team engagement consists of a full scope, multi-layered adversarial attack simulation created to measure how well an organizations staff, networks, applications and physical security controls can withstand a real-life attack"

WHAT'S THE DIFFERENCE?

- Supporting the Blue team!
- Goals
- Length of engagement
- Members have a more clearly defined role
- Knowledge and experience of team members

Red team Methodology



Reconnaissance

Weaponization

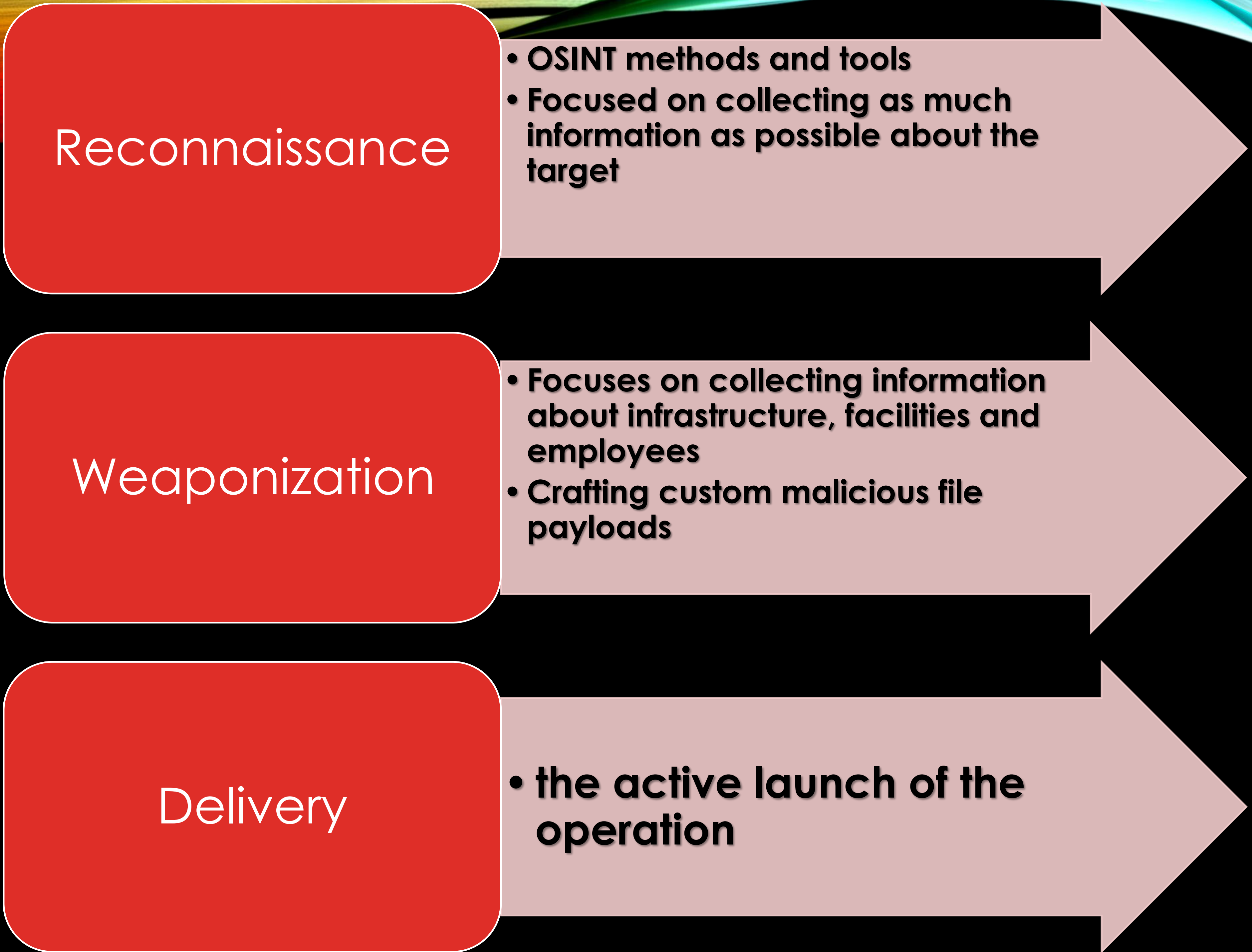
Delivery

Exploitation

Installation

Command and Control

Actions on Objective



Reconnaissance

- OSINT methods and tools
- Focused on collecting as much information as possible about the target

Weaponization

- Focuses on collecting information about infrastructure, facilities and employees
- Crafting custom malicious file payloads

Delivery

- the active launch of the operation

Exploitation	Compromise or “break in”
Installation	Cyber or physical
C&C	Maintaining persistence is the goal
Actions on Objective	The team aims to complete the mission and realize the agreed-upon objectives set by the client

SO WHICH DO I NEED?

Vulnerability Assessment

Scan and enumeration

Penetration Test

Are you looking to test your systems?

Do you want to know which vulnerabilities exists in those systems and more importantly can those vulnerabilities be exploited?

Red Team Engagement

Do you want to learn more about your organization as a whole?

What if we were attacked? How would we respond?

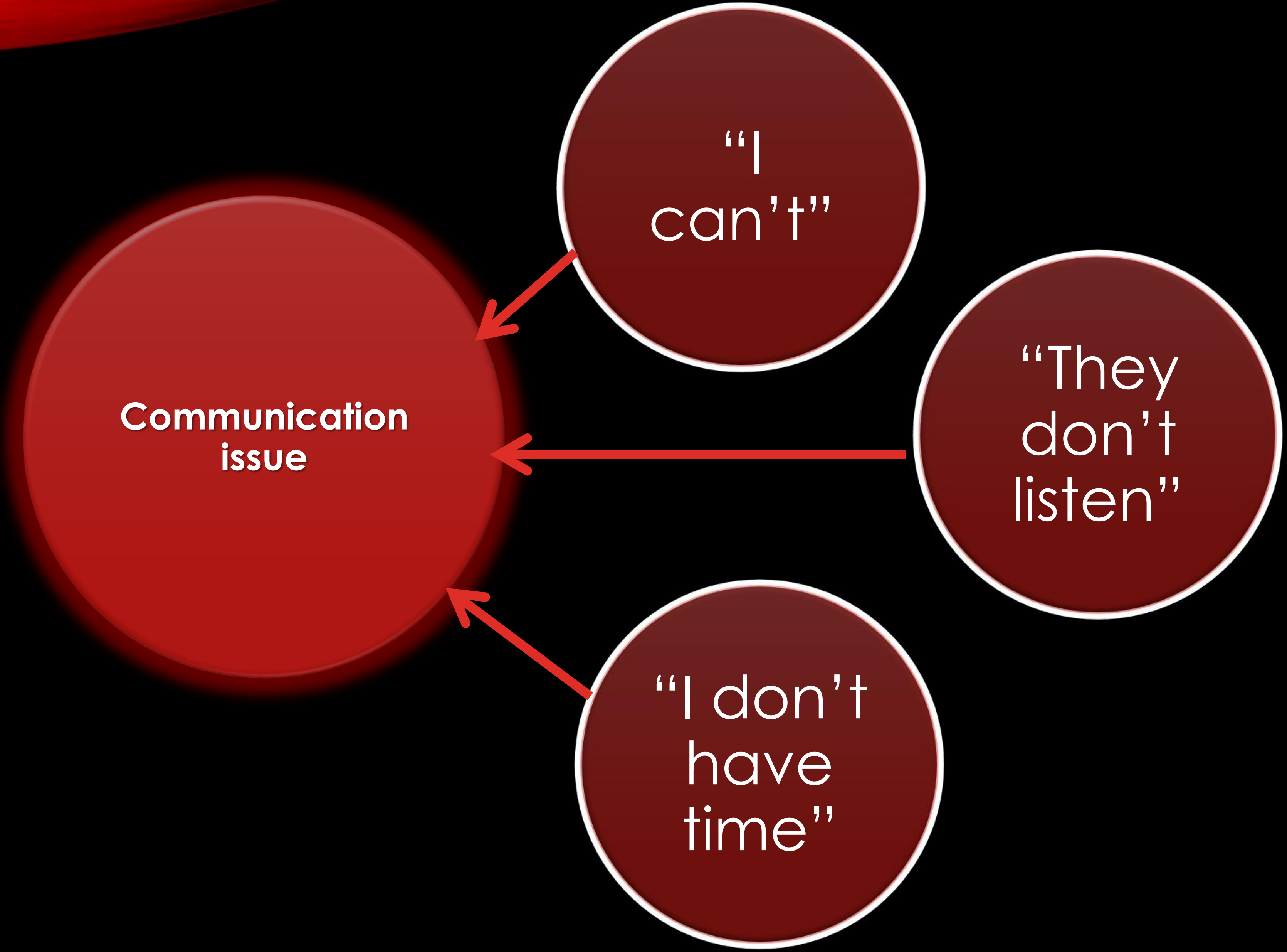
How quickly can we recover from something like ransomware?

Penetration testing can be limited due to time and scope constraints.

In comparison, Red Team campaigns seek to remove this limitation by providing a service that recreates actual attack scenarios and expose attack surfaces

REPORTS

- Effective Writing
- Purpose/Objective & Your Audience
- Preparation
- Structure & Components
- Extra items to set yourself apart



Communication issue

“I can’t”

“They don’t listen”

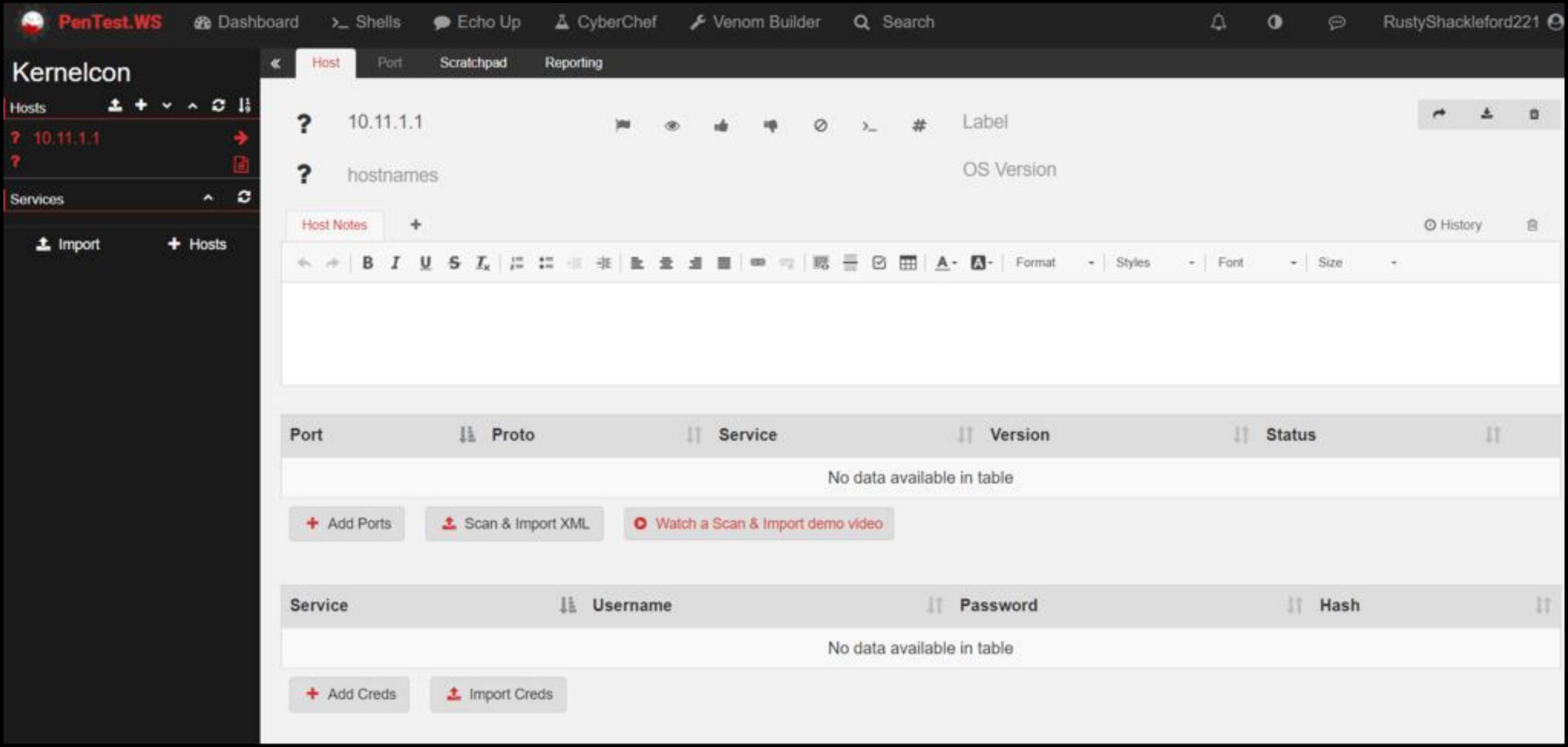
“I don’t have time”

REPORTS ARE THE MOST IMPORTANT PART

- Definition:
  - "A report is a statement of the results of an investigation or of any matter on which definite information is required"
- They last a while
- Others will see them
- Bad reports reflect badly on you and our industry
- It's our end product and how we justify our positions

PREPARATION

- Use shared resources
- Screenshots, screenshots, screenshots
- Notable items
  - Processes, findings, systems, etc..
    - And screenshots



Port	Proto	Service	Version	Status
No data available in table				

Service	Username	Password	Hash
No data available in table			

REPORT STRUCTURE

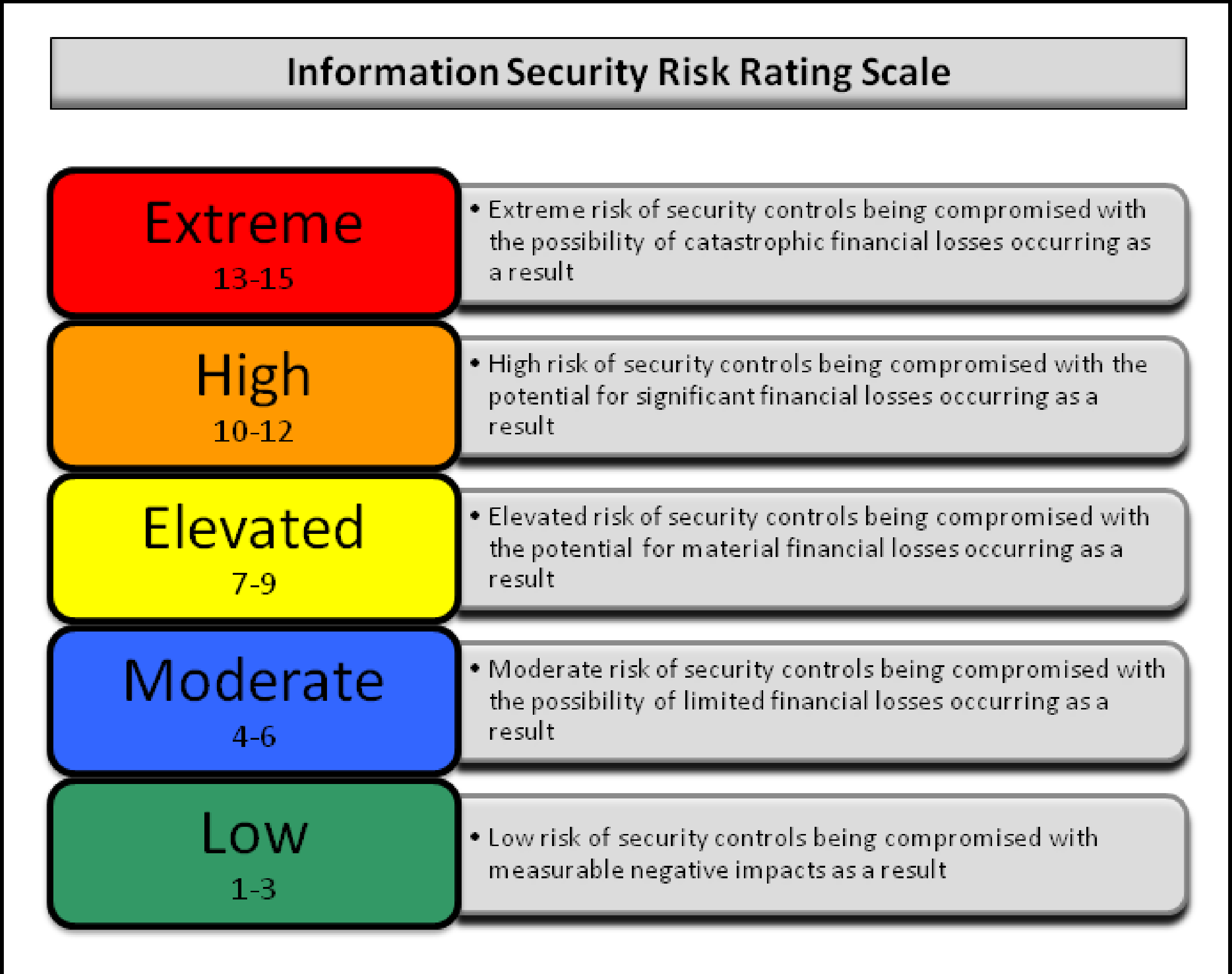
- Executive Summary for Strategic Direction
- Scope
- Methodology
- Attack
- Findings
- Recommendations
- Future Considerations
- References
- Appendices

FINDINGS

- Overview – The vulnerability, risk, probability, and impact.
  - $ amount if possible
- Affected Hosts
  - Use external and internal IPs
  - Use DNS name AND IP addresses

RISK SCORE

- Risk = Impact + Probability



Information Security Risk Rating Scale

Extreme 13-15	• Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result
High 10-12	• High risk of security controls being compromised with the potential for significant financial losses occurring as a result
Elevated 7-9	• Elevated risk of security controls being compromised with the potential for material financial losses occurring as a result
Moderate 4-6	• Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result
Low 1-3	• Low risk of security controls being compromised with measurable negative impacts as a result

RECOMMENDATIONS

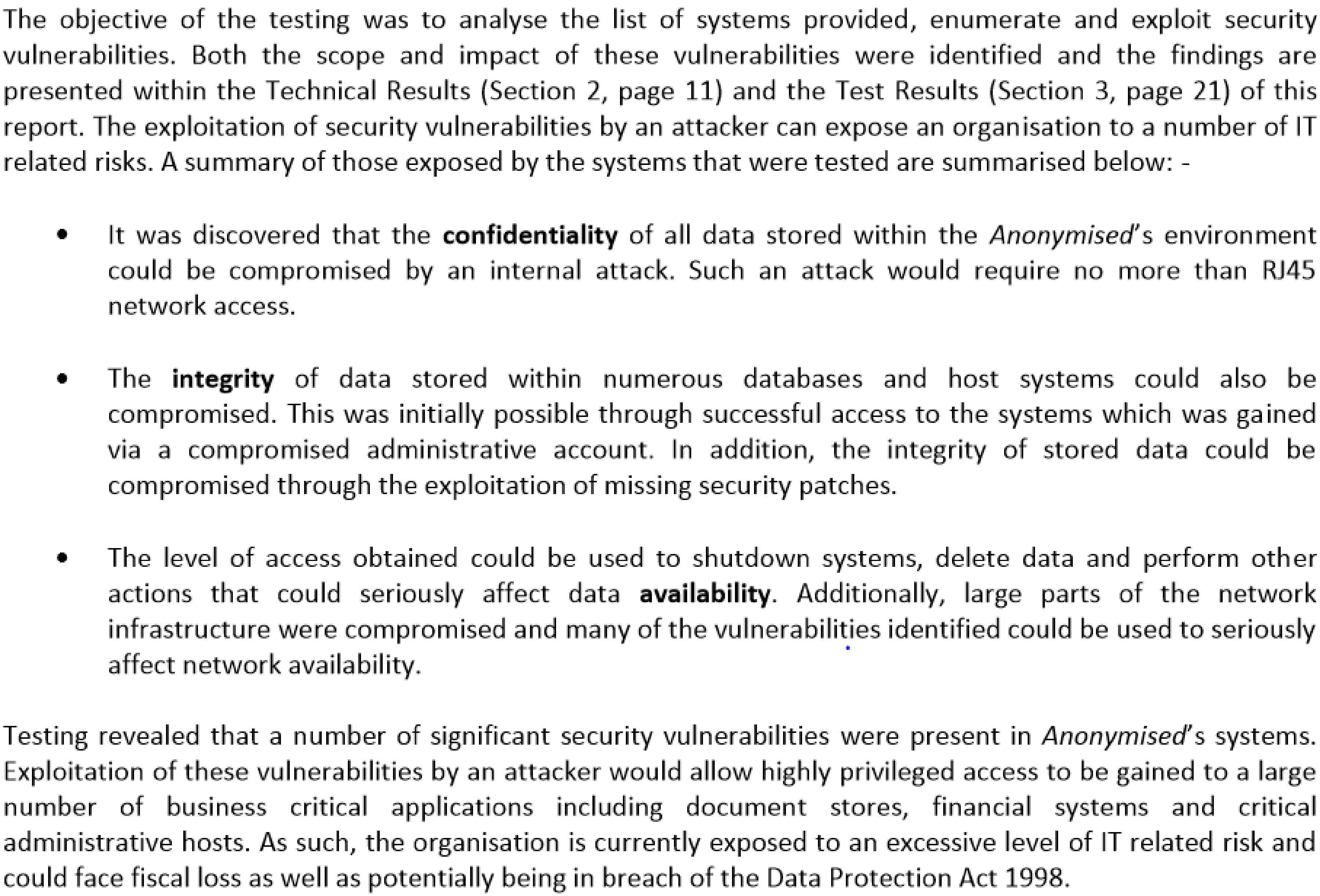
- Protection
  - How should the organization protect itself
- Detection
- Create maturity model
- Give how to guides instead of step by step instructions

VALIDATION & FINDINGS

- How to verify
- Validation **DOES NOT** equal explanation
- Keep it simple
  - Tools
  - Commands
  - Scripts?
- Findings:
  - Store findings in easily accessible spot
  - New findings take a while to write up
  - OneNote, Google Docs, etc..

EXECUTIVE SUMMARY

- Most important part of the report
- Write it for someone who is non-technical
- Should include:
  - Time & duration
  - Scope
  - Project Objective(s)
  - Timeline
  - Method
  - Brief overview of critical findings
  - Risk
  - Recommendations
  - Appendices/References



The objective of the testing was to analyse the list of systems provided, enumerate and exploit security vulnerabilities. Both the scope and impact of these vulnerabilities were identified and the findings are presented within the Technical Results (Section 2, page 11) and the Test Results (Section 3, page 21) of this report. The exploitation of security vulnerabilities by an attacker can expose an organisation to a number of IT related risks. A summary of those exposed by the systems that were tested are summarised below: -

- It was discovered that the **confidentiality** of all data stored within the *Anonymised*'s environment could be compromised by an internal attack. Such an attack would require no more than RJ45 network access.

- The **integrity** of data stored within numerous databases and host systems could also be compromised. This was initially possible through successful access to the systems which was gained via a compromised administrative account. In addition, the integrity of stored data could be compromised through the exploitation of missing security patches.

- The level of access obtained could be used to shutdown systems, delete data and perform other actions that could seriously affect data **availability**. Additionally, large parts of the network infrastructure were compromised and many of the vulnerabilities identified could be used to seriously affect network availability.

Testing revealed that a number of significant security vulnerabilities were present in *Anonymised*'s systems. Exploitation of these vulnerabilities by an attacker would allow highly privileged access to be gained to a large number of business critical applications including document stores, financial systems and critical administrative hosts. As such, the organisation is currently exposed to an excessive level of IT related risk and could face fiscal loss as well as potentially being in breach of the Data Protection Act 1998.

EXTRA

- Possible threats for org
- Tool recommendations
  - Only recommend, do not talk negatively about a tool
- Key metrics and way to track them

TAKE AWAYS

- Pen test != Red team engagement
  - What is your clients goal? Does either of these actually meet that
- Having clearly defined objectives and taking good notes will make your job a lot easier
- Reports are our end product and last a while. They need to be as good as we can make them. It’s how we justify our positions.
- Doing little things will provide substantial value and set you apart
- The best IDS/IPS is people
- If you are blue team, learn offense. If you are offense, learn defense. It goes a long way

RESOURCES

- https://github.com/juliocesarfort/public-pentesting-reports
- https://github.com/rustyshackleford221
- https://github.com/onlurking/awesome-infosec
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://www.peerlyst.com/posts/peerlyst-community-ebook-the-red-team-guide-peerlyst