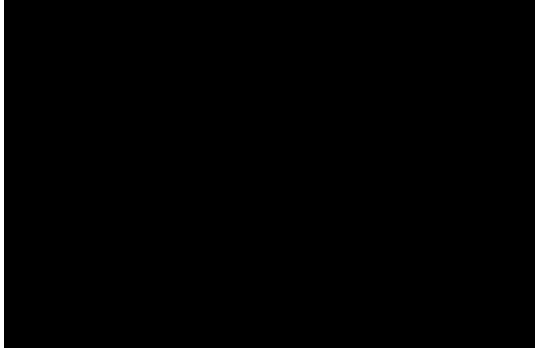


Cybersecurity Management in Organizations II: Security Testing

Meet Tyrus .M. Kamau, a really cool guy :-)

Discussion Topics

- **Vulnerability Management.**
- **Security Testing & Role of Pen testing.**
- **Pen Testing dimension & process.**
- **Ethics of Pen testing.**

Vocabulary 101: Let's define the terms

- **Vulnerability:** The state of being exposed or susceptible to harm or injury
- **Vulnerability Assessment**: The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- **Penetration Test**: A method of evaluating the security of a computer system or network by simulating an attack from a malicious source

Why Perform a Penetration Test?

Penetration testing can help you answer:

- How security aware are my staff?
- How effective are my technical, physical and process based security mechanisms?
- How vulnerable are my home-grown web applications to attack?
- Are there unauthorized/insecure configured wireless/IoT devices present?

Example Tests:

- Social engineering
- Logical & physical attacks (external / internal)
- Web application attacks
- Wireless & IoT scans and attacks

Penetration Tests vs Hackers

What Hackers are not!

- They don't wear masks
- They aren't larger than life movie characters
- They do not have the ability to hack everything
- They don't necessarily have to be computer gurus

What Hackers are:

- Very very patient
- They persevere.
- They are profoundly passionate.
- Love to learn and practice.
- Normal people with one solid objective.

Penetration Tests vs Hackers..cont'd

Hackers exploit “path of least resistance”

– Penetration testers will attempt to find multiple points of entry

- **Hackers use opportunistic approaches**

– Penetration testing is methodical and repeatable allowing easy Verification

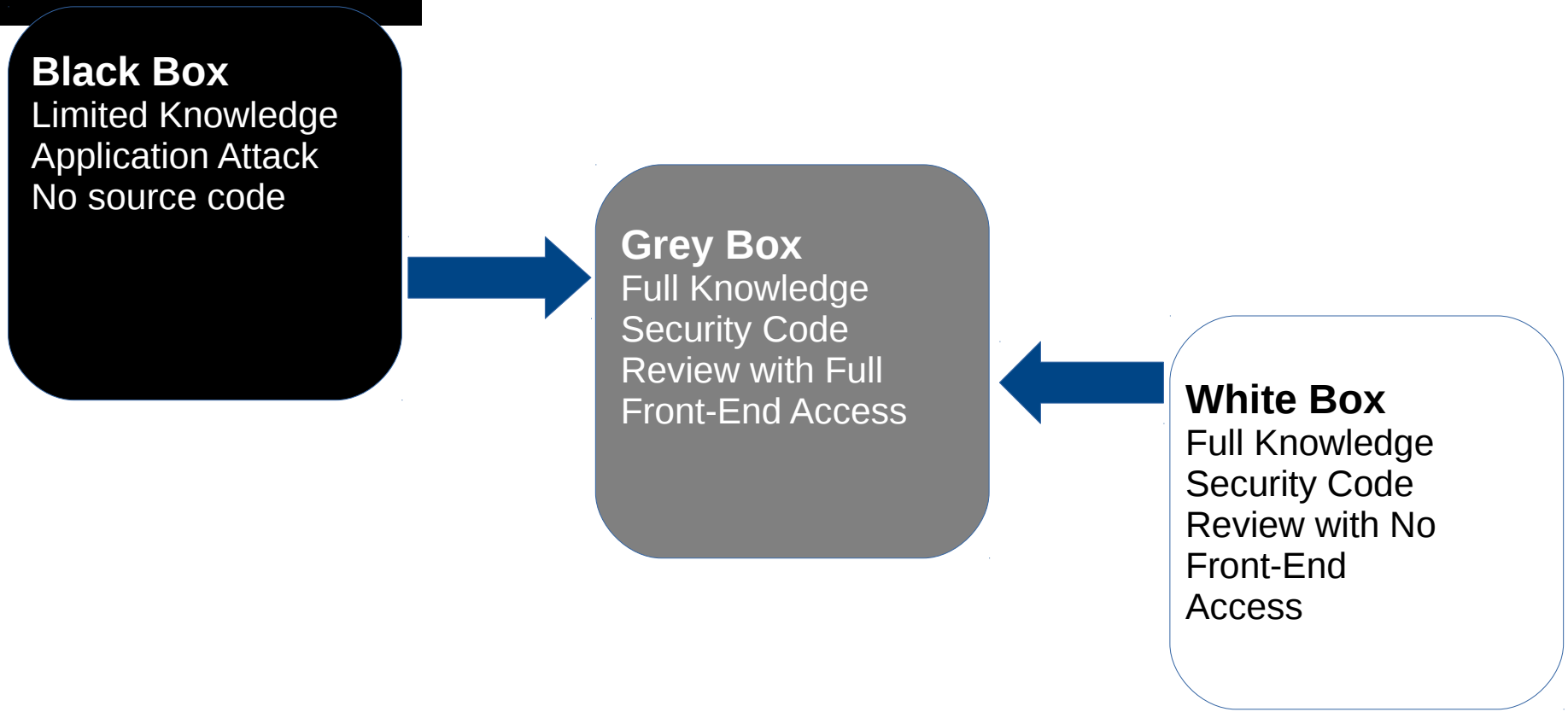
- **Hackers seek to gain information, cause damage**

– Penetration Testers gain sufficient access to illustrate breaches and stop!

- **Penetration Tests bounded by limitations which hackers do not face such as:**

1. Time bounded
2. Sensitive to the environmental restrictions
3. Tests may be narrow in scope, if required by client.

Traditional types of Security Tests



Rules of Engagement

- **Hack responsibly!**
- Written Permission
- Clear Communication
- Stay within scope
- No Denial of Service
- Don't change major state
- Restore state
-
-
-
- ….or should you?

Why traditional testing methods are dead

- It does not focus risk on Business, but on exposure of vulnerability
- Testing that replicates an attacker (sparring partner) has its hands tied.
- Your tester is defined within a .1% of the whole threat surface

Enter the Red Team Assessment

- It goes Beyond compliance
- It simulates the REAL WORLD attacks
- Hackers don’t have scopes.... Why should a test?
- Do you really think testing .1% of your assets makes the COMPANY secure?
- You never know the value of what you have till its gone.

So what's the difference?

Penetration Testing	Red Teaming
Finding, evaluating and exploiting vulnerabilities in **one dimension**	Finding, evaluating and exploiting only **vulnerabilities** that make it possible to **obtain the goals**
Static methodology	**Flexible** Methodology
No matter attacker's profile	**Obtain the attacker's profile**
The security team are normally **warned about the test**	**Without notice**
Office Schedule	**24 hours**
Just finding and exploiting the vulnerability	**Measures business impact** of successful attacks

Case Study

The Sweet Spot

Developers and Auditors

Before

After


THANK YOU!
ANY QUESTIONS?
memegenerator.net