netSPI
RISK COMPLIANCE SECURITY

WTF is **Penetration Testing**

v.2

Who are we?

Eric Gruber
@egru
http://github.com/egru
http://github.com/netspi
http://netspi.com/blog

Karl Fosaaen
@kfosaaen
http://github.com/kfosaaen
http://slideshare.com/kfosaaen

Scott Sutherland
@_nullbind
http://github.com/nullbind
http://slideshare.com/nullbind

netSPI
RISK COMPLIANCE SECURITY

Demo

Common Escalation Paths:

- Enumerate live systems and open ports with nmap
- Brute force database account with SQLPingv3
- Get a shell on the database server with the mssql_payload Metasploit module
- Dump domain admin passwords in clear text with mimikatz
- Log into high value database to access data
- Log into domain controller to find and access everything else

netSPI
RISK COMPLIANCE SECURITY

Overview

- What is a penetration test?
- Why do companies pay for them?
- Types of penetration testing
- What are the rules of engagement?
- Who does penetration testing?
- What skills do they have?
- What tools do they use?
- Penetration testing as a Career
- Questions

netSPI
RISK COMPLIANCE SECURITY

What is a Penetration Test?

What is Penetration Testing?

Our Definition:

"The process of evaluating ***systems***, ***applications,*** and ***protocols*** with the intent of identifying vulnerabilities *usually* from the perspective of an unprivileged or anonymous user to **determine potential real world impacts**…"

"…legally and under contract"

netSPI
RISK COMPLIANCE SECURITY

What is Penetration Testing?

In short…

netSPI
RISK COMPLIANCE SECURITY

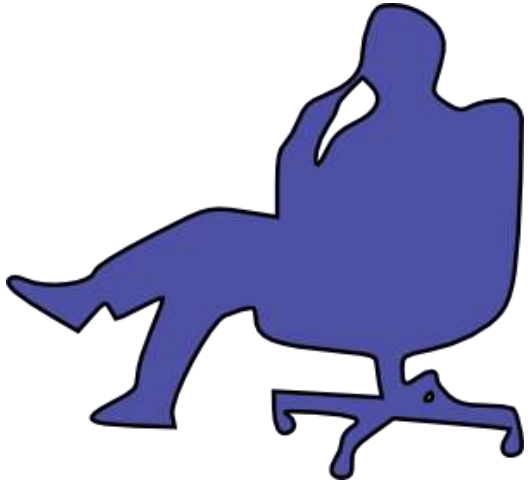
What is Penetration Testing?

…we try to break into stuff

before the bad guys do

netSPI
RISK COMPLIANCE SECURITY

Why do companies buy Penetration Tests?

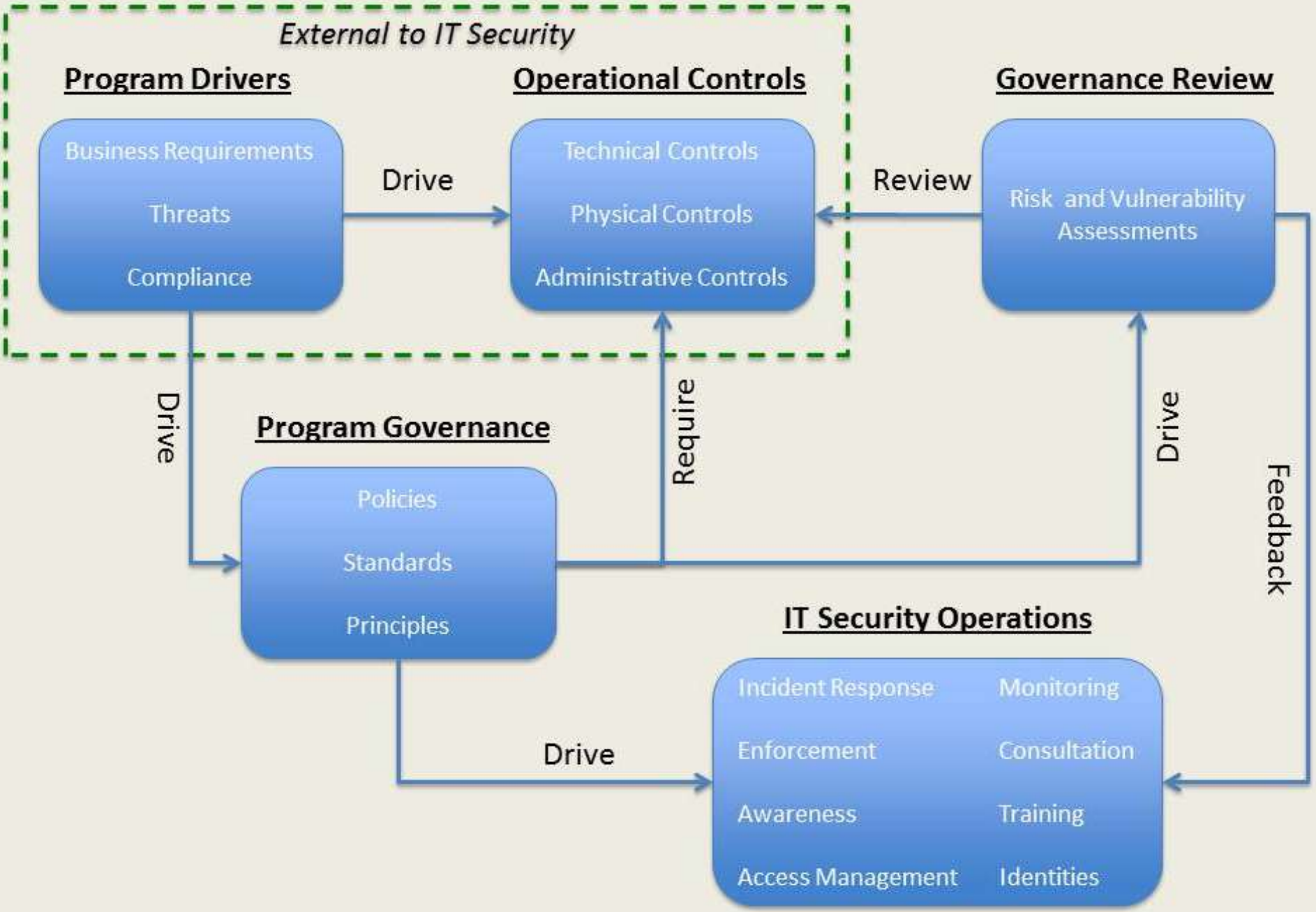


Why do companies buy pentests?

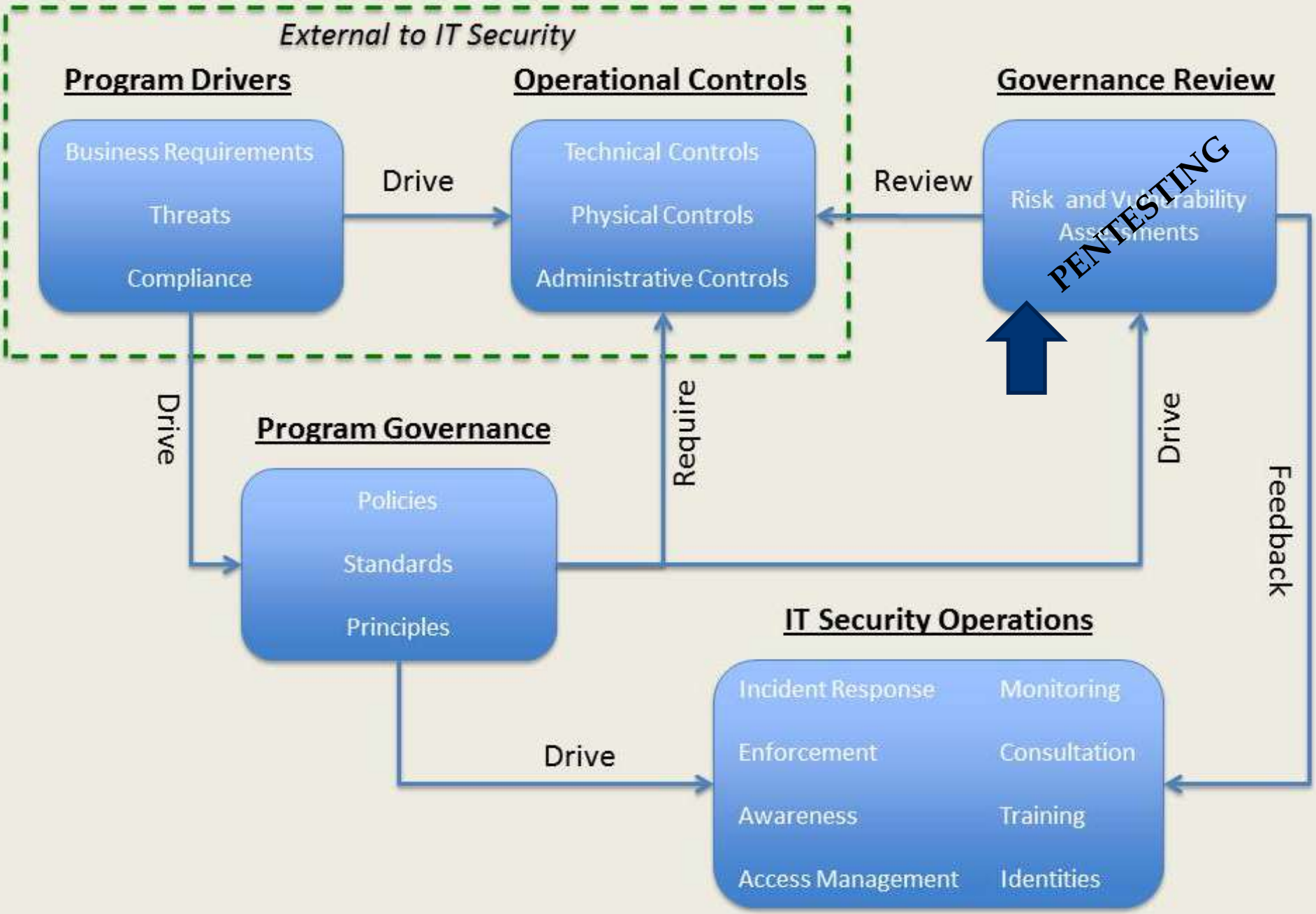
- Meet compliance requirements
- Evaluate risks associated with an acquisition or partnership
- Validate preventative controls
- Validate detective controls
- Prioritize internal security initiatives
- Proactively prevent breaches

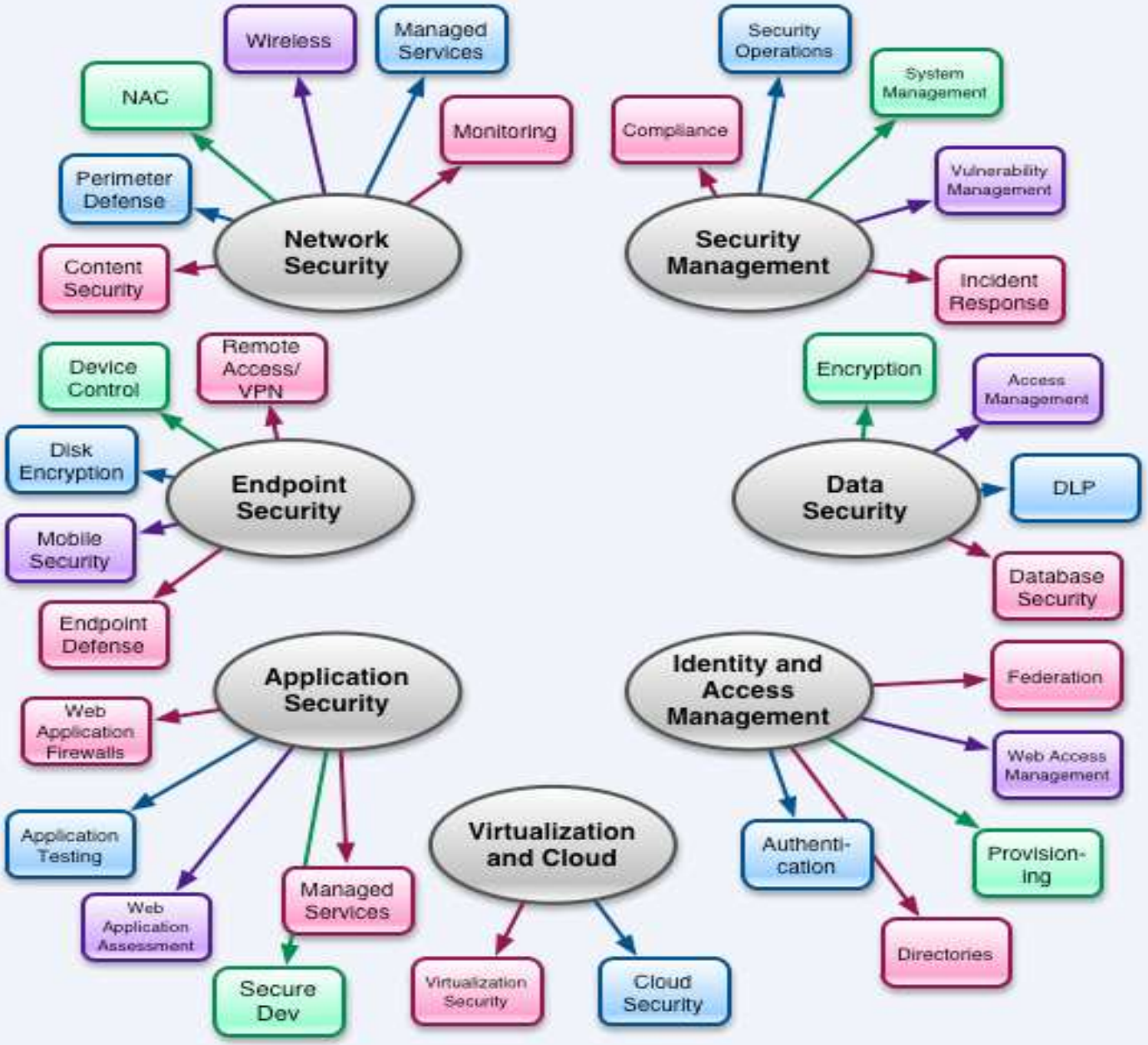
netSPI
RISK COMPLIANCE SECURITY

IT Security Program Overview



IT Security Program Overview




Network Security
Wireless
Managed Services
NAC
Monitoring
Perimeter Defense
Content Security
Security Management
Security Operations
System Management
Compliance
Vulnerability Management
Incident Response
Endpoint Security
Device Control
Remote Access/ VPN
Disk Encryption
Mobile Security
Endpoint Defense
Data Security
Encryption
Access Management
DLP
Database Security
Application Security
Web Application Firewalls
Application Testing
Web Application Assessment
Managed Services
Secure Dev
Virtualization and Cloud
Virtualization Security
Cloud Security
Identity and Access Management
Federation
Web Access Management
Authenti-cation
Provision-ing
Directories


Wireless
Managed Services
NAC
Monitoring
Perimeter Defense
Network Security
Content Security
Security Operations
Compliance
Vulnerability Management
Incident Response
Device Control
Remote Access/ VPN
Disk Encryption
Endpoint Security
Mobile Security
Endpoint Defense
Encryption
Access Management
Data Security
DLP
Database Security
Application Security
Web Application Assessment
Secure Dev
Managed Services
Virtualization and Cloud
Virtualization Security
Cloud Security
Identity and Access Management
Federation
Web Access Management
Authenti-cation
Provision-ing
Directories
PENTESTING

What types of Penetration Tests are there?

Hats and Boxes?

Types of Penetration Testers

Black Hat

Independent research and exploitation with *no collaboration* with vendor.

Gray Hat

Independent research and exploitation with *some collaboration* with vendor.

White Hat

Collaborative research, assessment, and exploitation *with vendor*.

netSPI
RISK COMPLIANCE SECURITY

Types of Penetration Tests

Black Box

Zero knowledge of target.

Gray Box

User knowledge of target. Sometimes as an anonymous user.

White Box

Administrative or development knowledge of target.

netSPI
RISK COMPLIANCE SECURITY

Types of Penetration Tests

Information	Black Box	Gray Box	White Box
Network Ranges		x	x
IP Addresses		x	x
Domains		x	x
Network Documentation		x	x
Application Documentation		x	x
API Documentation		x	x
Application Credentials			x
Database Credentials			x
Server Credentials			x

netSPI
RISK COMPLIANCE SECURITY

Types of Penetration Tests

- **Technical** Control Layer
  - Network
  - Application (mobile, web, desktop etc)
  - Server
  - Wireless
  - Embedded Device
- **Physical** Control Layer
  - Client specific site
  - Data centers
- **Administrative** Control Layer
  - Email phishing
  - Phone and onsite social engineering

netSPI
RISK COMPLIANCE SECURITY

What are the
Rules of Engagement?

Rules of Engagement

- **Hack Responsibly!**
- Written permission
- Clear communication
- Stay in scope
- No Denial-of-Service
- Don’t change major state
- Restore state
- Use native technologies
- Stay off disk

netSPI
RISK COMPLIANCE SECURITY

Are there any Penetration Testing methodologies?

Common Approach

- Kickoff: Scope, test windows, risks, contacts
- Information Gathering
- Vulnerability Enumeration
- Penetration
- Escalation
- Evidence Gathering
- Clean up
- Report Creation
- Report Delivery and Review

netSPI
RISK COMPLIANCE SECURITY

Common Approach: Standards

Methodologies

- Ptes
- OSSTM
- ISSAF
- NIST
- OWASP

Certifications

- SANS
- OSCP
- CREST

netSPI
RISK COMPLIANCE SECURITY

Penetration Test vs.
Vulnerability Assessment

Assessment VS. Penetration

What can both an assessment or pentest answer?

- *What* are my system layer vulnerabilities?
- *Where* are my system layer vulnerabilities?
- Will we know if we are being scanned?
- How do I fix my vulnerabilities?
- Are we fixing things over time?

netSPI
RISK COMPLIANCE SECURITY

Assessment VS. Penetration

What else can a pentest answer?

- What vulnerabilities represent the most risk?
- What are my high impact **system**, **network**, and **application** layer issues?
- Can an attacker gain unauthorized access to *critical infrastructure, application functionality,* and *sensitive data*
- Can attackers bypass multiple layers of detective and preventative controls?
- Can attackers pivot between environments?
- Are procedures being enforced

netSPI
RISK COMPLIANCE SECURITY

Who conducts Penetration Testing?

Who Conducts Penetration Testing?

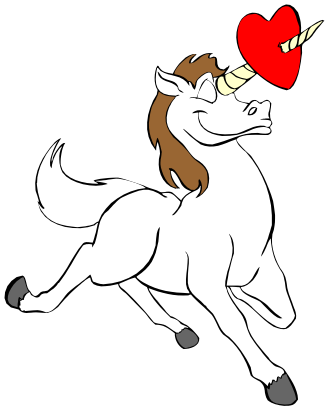
People that can pass a background check

netSPI
RISK COMPLIANCE SECURITY

Who Conducts Penetration Testing?

- Internal Employees
  - Security analysts
  - Security consultants
- Third Parties
  - Audit Firms
  - Value-Added Reseller (VAR)
  - Manage Services
  - Software as a Service (SaaS)
  - Software Vendors
  - Security Consultants

netSPI
RISK COMPLIANCE SECURITY



What skills are required?

What Skills are Needed?

- Non Technical
- Basic Technical
- Offensive
- Defensive

netSPI
RISK COMPLIANCE SECURITY

Non Technical Skillsets

- Written and Verbal Communications
  - Emails/phone calls
  - Report development
  - Small and large group presentations
- Professionalism
  - Respecting others, setting, and meeting expectations

netSPI
RISK COMPLIANCE SECURITY

Non Technical Skillsets

- Troubleshooting Mindset
  - **Never give up, never surrender!**
  - Where there is a will, there is a way
- Ethics
  - Don't do bad things
  - Pros (career) vs. Cons (jail)
  - Hack responsibly

netSPI
RISK COMPLIANCE SECURITY

Basic Technical Skillsets

- Windows Desktop Administration
- Windows Domain Administration
- Linux and Unix Administration
- Network Infrastructure Administration
- Application Development
  - Scripting (Ruby, Python, PHP, Bash, PS, Batch)
  - Managed languages (.Net, Java, Davlik)
  - Unmanaged languages (C, C++)

netSPI
RISK COMPLIANCE SECURITY

Offensive and Defensive **Knowledge**

- System enumeration and service fingerprinting
- Linux system exploitation and escalation
- Windows system exploitation and escalation
- Network system exploitation and escalation
- Protocol exploitation
- Web application exploitation
- Reverse engineering
- Anti-virus Evasion
- Social engineering techniques

netSPI
RISK COMPLIANCE SECURITY

What are some of the common tools?

Common **Tools**

There are **hundreds** of “hacker” tools.

Generally, you need to have enough knowledge to know **what tool** or tool(s) is right **for the task** at hand….

…and if one doesn’t exist, then **create it**.

netSPI
RISK COMPLIANCE SECURITY

Common **Tools**

That being said…

netSPI
RISK COMPLIANCE SECURITY

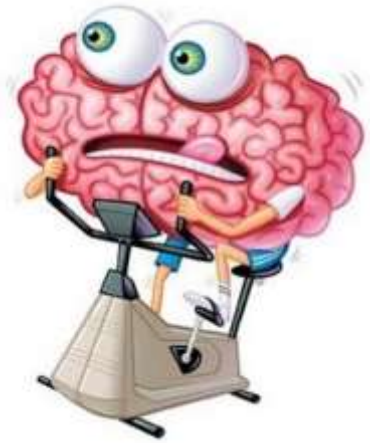
Common **Tools**

Knowledge > Tools = Train your brain!

Understand the core technologies

Understand basic offensive techniques

Understand basic defensive techniques



netSPI
RISK COMPLIANCE SECURITY

Common Tools: Info Gathering

Find online resources owned by target including:

- Subsidiaries (companies)
- Systems (live IP addresses)
- Services
- Domains
- Web applications
- Email addresses

Tool Examples:

- Public registries: IP, DNS, SEC Filings, etc.
- Nmap
- Recon-ng
- Google
- BackTrack / Kali tool sets (many discovery tools)

netSPI
RISK COMPLIANCE SECURITY

Common Tools: Identify Vulnerabilities

Find vulnerabilities:

- Missing patches
- Weak configurations
  - system, application, network
- Application issues

Tool Examples:

- Patches/Configurations: OpenVAS, Nessus, NeXpose, Qualys, IP360 etc
- Applications: Burp, Zap, w3af, Nikto, DirBuster, SQLMap, Web Inspect, Appscan etc

netSPI
RISK COMPLIANCE SECURITY

Common Tools: Penetration

Common penetration methods:

- Buffer overflows
- Default and weak passwords
- SQL Injection
- Insecure Protocols

Tool Examples:

- Patches: Metasploit, Canvas, Core Impact
- Configurations: Native tools, Responder, Metasploit, Yersinia, Cain, Loki, Medusa
- Applications: SQLMap, Metasploit, Burp, Zap etc

netSPI
RISK COMPLIANCE SECURITY

Common Tools: Privilege Escalation

Exploit trust relationships to access to everything!

Tool Examples:

- Local Exploits & Weak Configurations
  - Metasploit, Core Impact, Canvas,
  - exploit-db.com
- Password Hash Cracking
  - John the ripper, Hashcat, Rainbow Tables
- Pass-the-Hash
  - Metasploit, PTH toolkits, WCE
- Token stealing
  - Metasploit and Incognito
- Credential dumping
  - Mimikatz, LSA Secrets, Credential Manager, groups.xml, unattend.xml etc

netSPI
RISK COMPLIANCE SECURITY

Common Tools

Tools output a TON of data!

netSPI
RISK COMPLIANCE SECURITY

How do people manage all that data?

Common Pentest CMS Options

Managing penetration test data:

- Storing files in organized folders
- Writing reports from word/excel templates
- Storing information in databases and XML
- Open source CMS projects
- Commercial CMS products
- Examples:
  - Dradis
  - Threadfix
  - CorrelatedVM
  - Risk IO

netSPI
RISK COMPLIANCE SECURITY

Penetration Testing as a Career?

Pen Testing as a Career: **How to Start**

- Read and learn! – There is no “end”
- Tap into the community!
- Research and development
  - Contribute to/start open source projects
  - Present research at conferences
- Training and Certifications
  - Community: DC612, OWASP, Conferences, etc
  - Professional ($): SANS, OffSec, CISSP, CREST, etc
- Volunteer
- Internships

netSPI
RISK COMPLIANCE SECURITY

Pen Testing as a Career: **Common Paths**

- **Internal Paths**
  - Help Desk
  - IT Support
  - IT Admin
  - Security Analyst
  - IRP Team
  - Senior Security Analyst
  - Internal Consultant
  - CISO

- **Security Consulting Paths**
  - Internship
  - Consultant
  - Senior Consultant
  - Principal Consultant
  - Team Lead
  - Director

Corporate employees tend to stay corporate.

Security consultants often end up in malware research and exploit development.

netSPI
RISK COMPLIANCE SECURITY

What we covered…

- What is a penetration test?
- Why do companies pay for them?
- Types of penetration testing
- What are the rules of engagement?
- Who does penetration testing?
- What skills do they have?
- What tools do they use?
- Penetration testing as a Career
- Questions

netSPI
RISK COMPLIANCE SECURITY

Questions, comments, curses?

netSPI
RISK COMPLIANCE SECURITY

BE SAFE and

HACK RESPONSIBLY

netSPI
RISK COMPLIANCE SECURITY