NETSPI

WHAT IS PENETRATION TESTING?

MARCH 21ST, 2018

INTRODUCTION

NETSPI

- Ben Tindell
  - Security Consultant

- Will Strei
  - Security Consultant

NETSPI BACKGROUND

NETSPI

- Founded in 2001
- Headquartered in Minneapolis
- National presence
- Approximately 85 employees (and continuing to grow!)
- Primary clients: Financial Services, Healthcare, Technology, Retail

NETSPI

WHAT IS PENETRATION TESTING?

AND WHY DO COMPANIES DO IT?

WHAT IS PENETRATION TESTING?

NETSPI

Our Definition:

- "The process of evaluating systems, applications and protocols with the intent of identifying vulnerabilities from the perspective of an unprivileged or anonymous user to determine the real world impact…"
- "…legally and under contract"

WHAT IS PENETRATION TESTING?

NETSPI

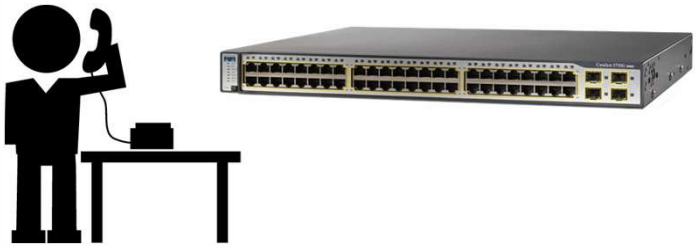
- Also known as…

"Getting paid to break into someone's systems before a bad guy does."

TYPES OF PENETRATION TESTS

NETSPI

- 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



WHY DO COMPANIES PENTEST?

NETSPI

- Compliance Requirements
- Identify Unknown Security Gaps
- Prioritize Existing Security Initiatives
- Prevent Data Breaches
- Validate Existing Controls

WHAT ARE THE TECHNICAL OBJECTIVES?

NETSPI

- Client specific objectives first
- Identify and verify all entry points
- Identify critical escalation paths
- Gain unauthorized access to:
  - Application functionality
  - Critical systems
  - Sensitive data

NETSPI

WHAT GOES INTO PENTESTING?

NON-TECHNICAL, BASIC TECHNICAL, OFFENSIVE & DEFENSIVE KNOWLEDGE, TOOLS

NON-TECHNICAL SKILLS

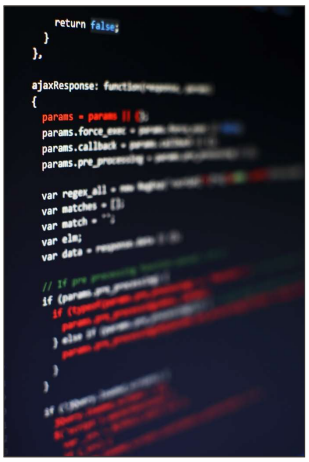
NETSPI

- Written and Verbal Communication
  - Emails/phone calls
  - Report development
  - Small and large group presentations
- Ethics
  - Don't do bad things
  - Pros (career) vs. Cons (jail)
  - Hack responsibly
- Professionalism
  - Respecting others
  - Setting and meeting expectations
- Troubleshooting Mindset
  - Never give up, never surrender
  - Where there is a will, there is a way

BASIC TECHNICAL SKILLS

NETSPI

- System Administration
  - Windows Desktop
  - Active Directory
  - Linux & UNIX
- Network Infrastructure Administration
- Application Development
  - Scripting (Ruby, Python, PowerShell)
  - Managed languages (.Net, Java)
  - Unmanaged languages (C, C++)



OFFENSIVE & DEFENSIVE KNOWLEDGE

NETSPI

- System enumeration and service fingerprinting
- Windows system exploitation and escalation
- Linux system exploitation and escalation
- Protocol exploitation
- Web application exploitation (OWASP)
- Reverse engineering client-server applications + AV evasion
- Social engineering techniques (onsite, phone, email)
- Certificate pinning, root checking

TOOLS

NETSPI

- There are **hundreds** of "hacker" tools:
  - Nessus, nmap
  - Metasploit, Kali Linux
  - Burp
- Generally, you need to have enough knowledge to know **what tool** (or tools) is right **for the task at hand**... and if one doesn't exist, then create it.
  - PowerUpSQL https://github.com/NetSPI/PowerUpSQL
  - SQL Injection Wiki https://github.com/NetSPI/SQLInjectionWiki.
  - https://github.com/NetSPI

TOOLS

NETSPI

- But… Knowledge > Tools
  - Understand the core technologies
  - Understand the core offensive techniques
  - Understand the core defensive techniques

NETSPI

PENTESTING AS A CAREER

COMMON PATHS, HOW TO START, WHY?

PENTESTING AS A CAREER | COMMON PATHS

NETSPI

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

Internal employees often stay internal.

- Security Consulting Paths
  - Associate Consultant
  - Consultant
  - Senior Consultant
  - Principal Consultant
  - Practice Director

Security Consultants often end up in malware research or exploit development, but some go corporate.

PENTESTING AS A CAREER | HOW TO START

NETSPI

- Read and learn!
  - Web Application Hacker's Handbook
  - OWASP.org
  - Vulnhub, DVWA
- Research and development
  - Contribute to open source projects
  - Present research at conferences
- Training and certifications
  - Community: DC612, OWASP, Conferences
  - Professional ($): SANS, OffSec, CISSP
- Bug bounties
- Volunteer
- Internships

OWASP Open Web Application Security Project

BSIDES

DEFCON

PENTESTING AS A CAREER | WHY BE A PENTESTER?

NETSPI

- It's fun ☺
- Every day is different
- Job security
- Competitive compensation
- Important work

NETSPI

OPPORTUNITIES AT NETSPI

OPPORTUNITIES AT NETSPI | NETSPI UNIVERSITY

- Full time, Associate level program for recent graduates
  - Starting in January and June each year
- 6 month program
  - Classroom and hands on training
  - Shadowing Senior Consultants
  - Tapping kegs
- Objective:
  - Promotion to Security Consultant

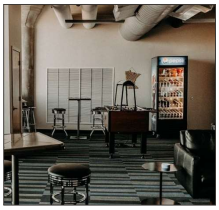
OPPORTUNITIES AT NETSPI | WHAT DO WE LOOK FOR?

- A passion for security
- Involvement in extra curricular activities outside of school
- The ability to creatively solve technical problems
- A good fit with NetSPI's culture

OPPORTUNITIES AT NETSPI | WHY NETSPI?

NETSPI

- Work hard
  - Test clients both locally and nationally
  - Collaborative and supportive environment
  - Work and research within the security community
- Play hard
  - In the office - pinball, Friday lunches, video games
  - Out of the office – dinners, company events, etc.
- Team environment
  - Small company = close knit and tons of fun
  - Expertise in many different areas
  - Constantly bouncing new ideas around



NETSPI

QUESTIONS?


NETSPI
MINNEAPOLIS | NEW YORK | PORTLAND | DENVER | DALLAS
Empowering enterprises to scale & operationalize their security programs, globally.