



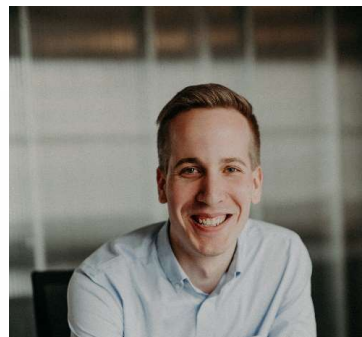
NETSPI

WHAT IS PENETRATION TESTING?

OCTOBER 4TH, 2018

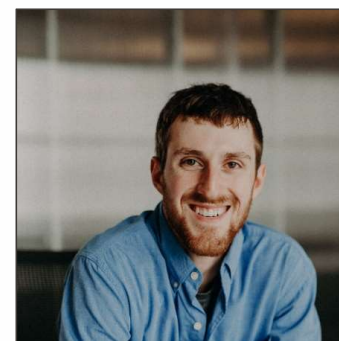
◆ Jake Reynolds

- ◆ Sr. Security Consultant



◆ Will Strei

- ◆ Security Consultant



- ◆ Founded in 2001
- ◆ Headquartered in Minneapolis
- ◆ National presence
- ◆ Approximately 100 employees (and continuing to grow!)
- ◆ Primary clients: Financial Services, Healthcare, Technology, Retail



WHAT IS PENETRATION TESTING?

AND WHY DO COMPANIES DO IT?

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?

◆ Also known as...

“Getting paid to break into someone’s systems before a bad guy does.”



◆ 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?



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



WHAT ARE THE TECHNICAL OBJECTIVES?

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



WHAT GOES INTO PENTESTING?

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

- ◆ Written and Verbal Communication
 - ◆ Emails/phone calls
 - ◆ Report development
 - ◆ Small and large group presentations
- ◆ Professionalism
 - ◆ Respecting others
 - ◆ Setting and meeting expectations

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



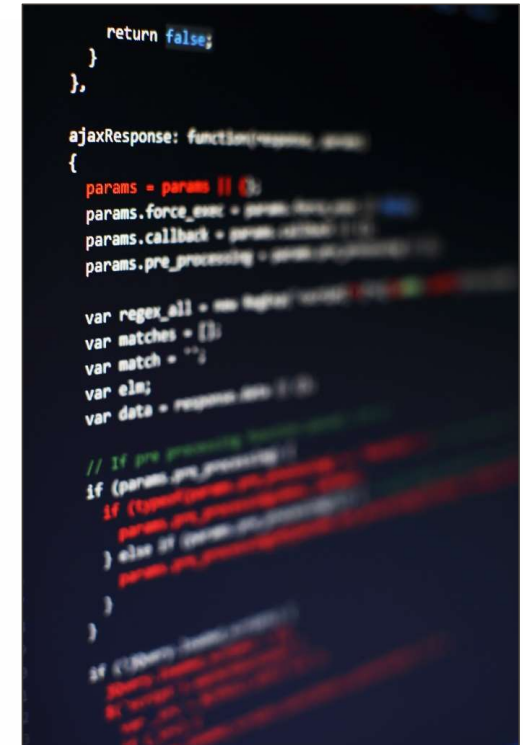
◆ System Administration

- ◆ Windows Desktop
- ◆ Active Directory
- ◆ Linux & UNIX

◆ Network Infrastructure Administration

◆ Application Development

- ◆ Scripting (Ruby, Python, PowerShell)
- ◆ Managed languages (.Net, Java)
- ◆ Unmanaged languages (C, C++)
- ◆ SQL



```
return false;
}
},

ajaxResponse: function(response, status)
{
    params = params || {};
    params.force_exec = params.force_exec || true;
    params.callback = params.callback || function(){};
    params.pre_processing = params.pre_processing || function(){};

    var regex_all = new RegExp(');
    var matches = {};
    var match = {};
    var elm;
    var data = response.data || {};

    // If pre_processing is defined
    if (params.pre_processing)
    {
        if (typeof params.pre_processing == 'function')
        {
            params.pre_processing(params);
        }
        else if (typeof params.pre_processing == 'string')
        {
            // ...
        }
    }

    if (typeof params.callback == 'function')
    {
        params.callback(response, status);
    }
}
```

Offensive

- ◆ System and service fingerprinting
- ◆ OS privilege escalation
- ◆ Protocol exploitation
 - ◆ HTTP/TCP/UDP
- ◆ Social engineering (email, phone, onsite)
- ◆ Critical thinking (business logic bypasses)

Defensive

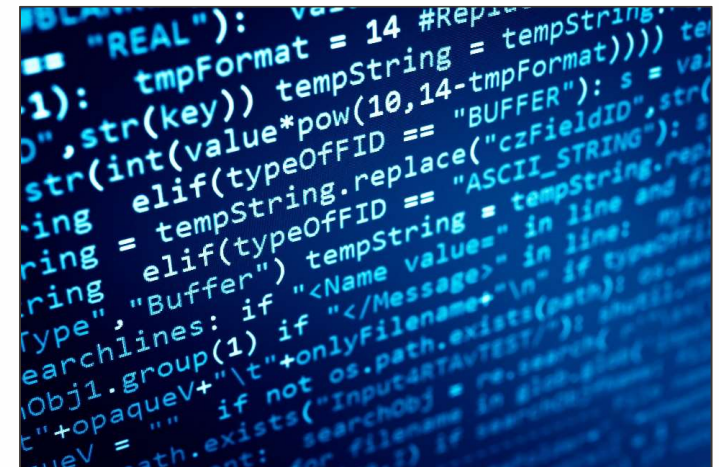
- ◆ Web application firewalls
- ◆ Secure development
- ◆ Parameterized SQL queries
- ◆ Input validation/sanitization

- ◆ 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>
 - ◆ <https://blog.netspi.com>

◆ But... Knowledge > Tools

- ◆ Understand the core technologies
- ◆ Understand the core offensive techniques
- ◆ Understand the core defensive techniques



PENTESTING AS A CAREER

COMMON PATHS, HOW TO START, WHY?

◆ 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.

- ◆ 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



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



OPPORTUNITIES AT NETSPI

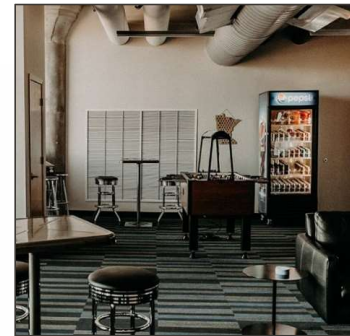
- ◆ Full time, Associate level program for recent graduates
 - ◆ Starting in January and June each year

- ◆ 6 month program
 - ◆ Classroom and hands on training
 - ◆ Shadowing Senior Consultants
 - ◆ Tapping keys

- ◆ Objective:
 - ◆ Promotion to Security Consultant

- ◆ 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

- ◆ 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



QUESTIONS?

<https://github.com/netspi/collegepresentation/>



MINNEAPOLIS | NEW YORK | PORTLAND | DENVER | DALLAS

Empowering enterprises to scale & operationalize their
security programs, globally.