NOVEMBER 4 – 5

TexSAW

2016

6th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

Celebrating 30 Years

THE UNIVERSITY OF TEXAS AT DALLAS

Presenting Sponsor

State Farm®

Supporting Sponsor

Raytheon

Penetration Testing

Ian Brown | Ryan Kao | Joel Seida | Devin Wiley

XYZ Bank

What is Penetration Testing?

Process to discover vulnerabilities that exist in a system which already has security policies in place

- Perform sanctioned attacks against a system
- Find and document as many vulnerabilities as possible

Virtual or physical

- **Virtual**: scanning the network to find and exploit vulnerabilities
- **Physical**: picking locks, inserting malicious flash drives, social engineering

Why Should We Care?

Increased focus on security ⟶ more penetration tests

- Required for compliance with a variety of standards
- HIPAA, PCI/DSS, Gramm-Leach-Bliley

Highly marketable skill

- Average salary: $71,660

Great way to learn about the intricacies and weaknesses of many different systems and protocols

Metasploit Framework

Software platform for developing, testing, and executing exploits, using its extensive database of known vulnerabilities.

- Used to create security testing tools and exploit modules
- Acts as a plug-and-play penetration testing system
- Industry standard for penetration testing

Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Scanning

Finding what systems exist within a network and the applications they are running

Goal: Find a machine on the target network that is vulnerable

- Discover network topology
- Discover vulnerable processes

Two types of scanning

- Network scanning
- Port scanning

Scanning

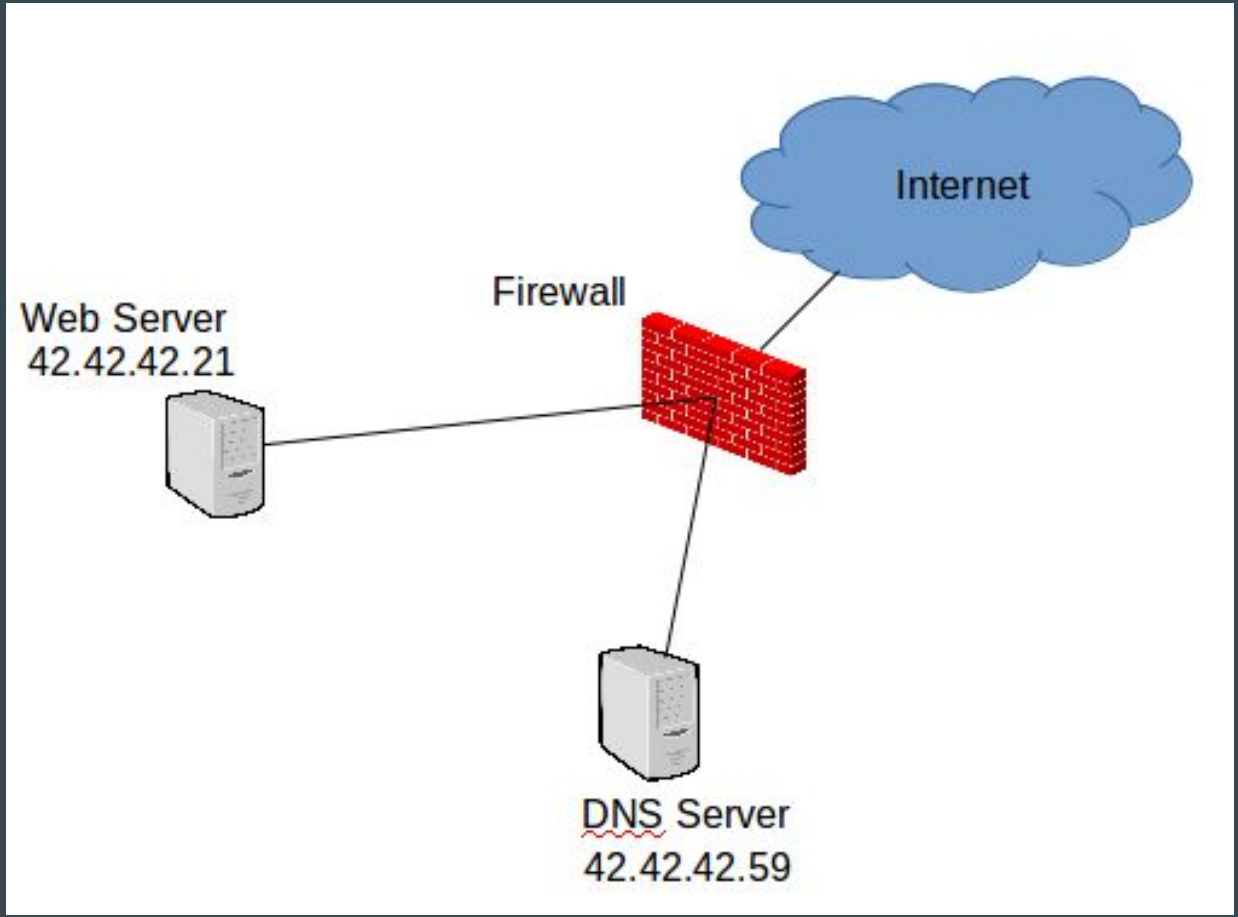
Nmap (db_nmap in Metasploit)

- General purpose network scanning tool

Ways to scan:

- Network scanning
  - IP Ping
  - ICMP Echo
- Port Scanning
  - TCP SYN
  - TCP SYN/ACK
  - UDP

Scanning


Internet
Firewall
Web Server
42.42.42.21
DNS Server
42.42.42.59

Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Initial Exploit

Finding a loophole in the applications that a system is running that will grant access to the internals of the system

Goal: Gain access to a machine on the target network

Access Types:

- Command Line (preferred)
- Code execution
- Physical access

Initial Exploit

Approaches to Exploitation:

- Buffer Overflow
- Command Injection
  - SQL Injection
  - PHP Injection
  - CSRF
- Phishing

Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Escalate Privileges

Gaining access to user with elevated privileges from a less privileged user (e.g. Root or System)

- How does this occur?

Escalating privileges using Metasploit and Meterpreter

- getsystem/getprivs
- steal_token
- Mimikatz (Windows)

Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Establish Persistence

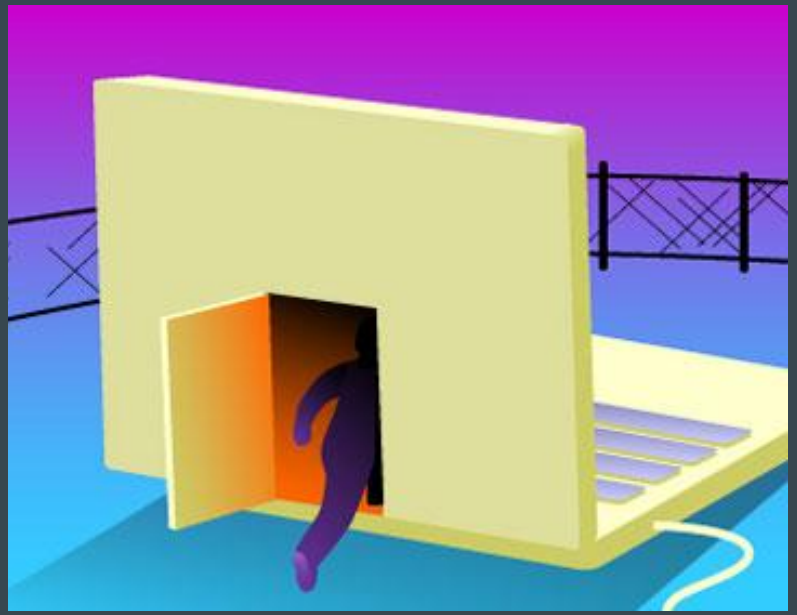
Maintain access to the exploited system(s)

One of the least used steps in a successful penetration test

- How to access if backdoors get patched?

Metasploit options for establishing persistence

- Metsvc
- Persistence module



Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Move Laterally

One computer is great, but what if we want to control the network?

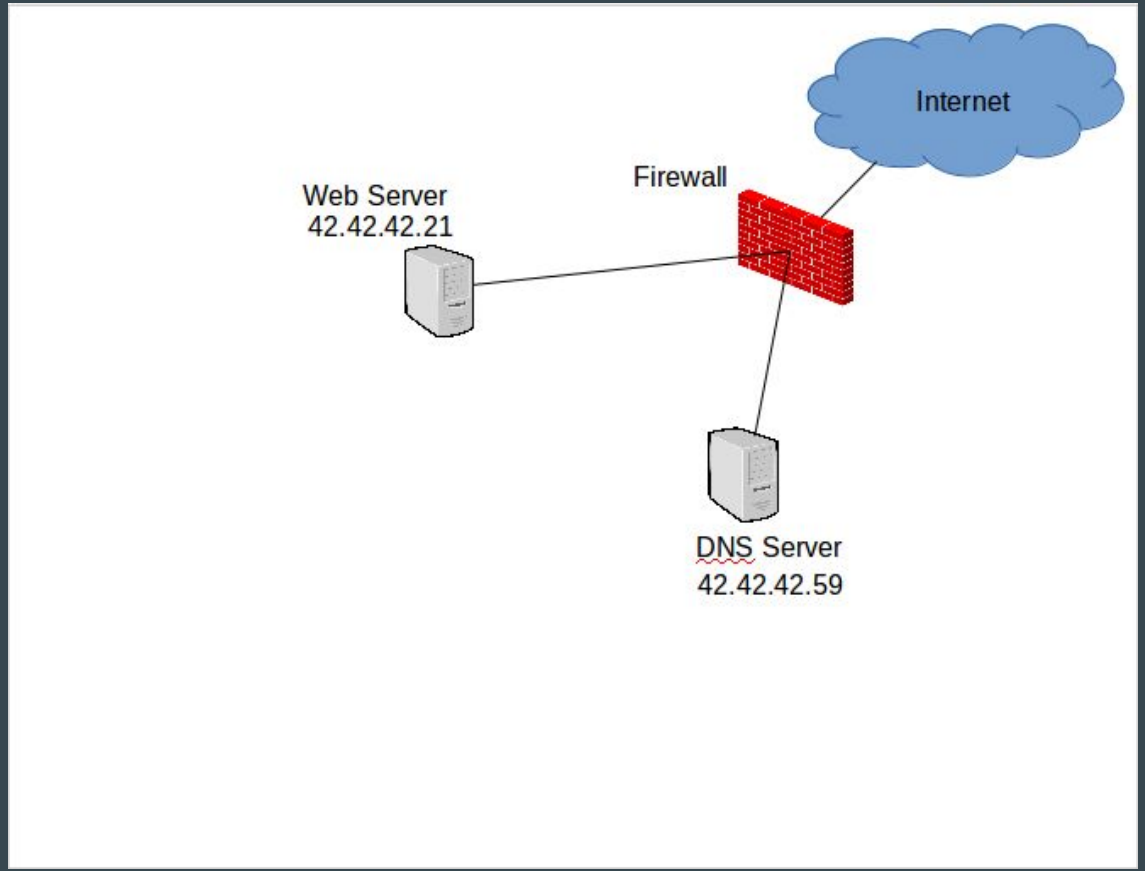
- Unlikely first compromised system contains highest-level credentials
- Must be able to reach other systems in network

Executing commands through compromised host(s)

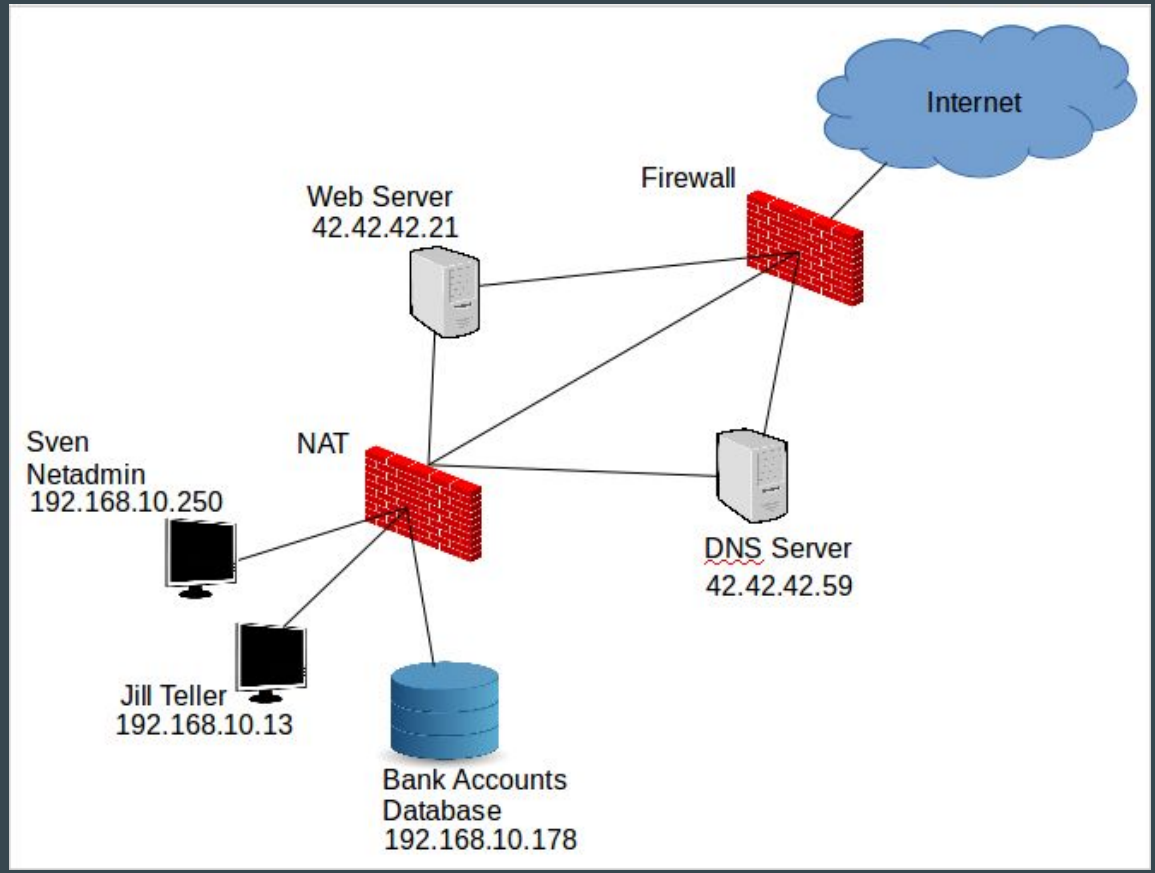
- load auto_add_route
- Port scanning with db_nmap

Shell commands vs. Tunneled commands

Move Laterally



Move Laterally



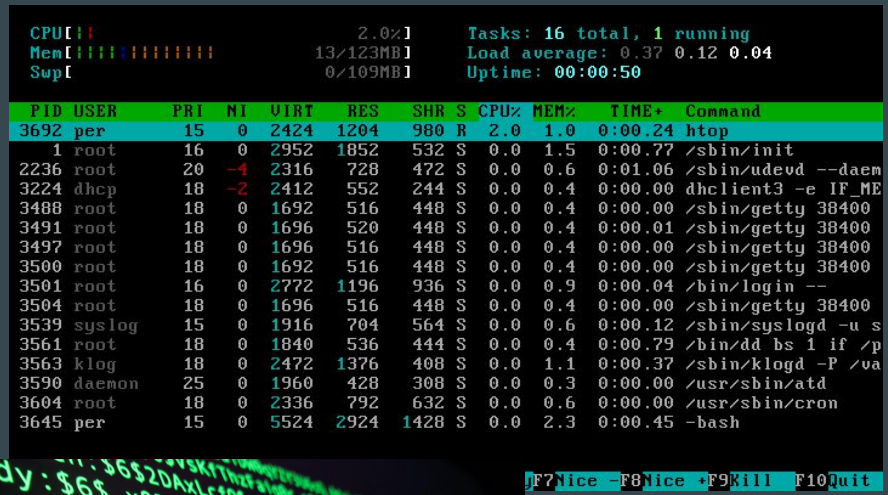
Steps of Penetration Testing

1. Scanning
2. Initial Exploit
3. Escalate Privileges
4. Establish Persistence
5. Move Laterally
6. Obtain “Crown Jewels”

Obtain “Crown Jewels”

What are “Crown Jewels”?

- Passwords (hashdump)
- Private keys
- Kill processes (kill -9)
- Disable anti-virus (killav)



Ethics and Laws

Legal Authority

- 18 USC 1030 - It’s a crime to access a computer without authorization.

Hack-back

- Hacking back is legally the same as hacking; it’s a crime.

Professionalism

- It’s important to document everything, even the lack of findings.

Licensing and Certification

- Some states require the pen tester to be a licensed private investigator

Ethics and Laws

A proper contract would include:

- Statement of Work
  - The test agreement should specifically state exactly what will, and will not be done (the scope of the project), and all the assumptions that underlie the agreement.
- Damage Control
  - Notify the customer in writing about any potential damage that may occur even when the pen test is done perfectly.
- Indemnification
  - Ensure that you are protected from harm caused to third parties.
- Data Ownership
  - The customer owns all the findings to the pen test.

Ethics and Laws

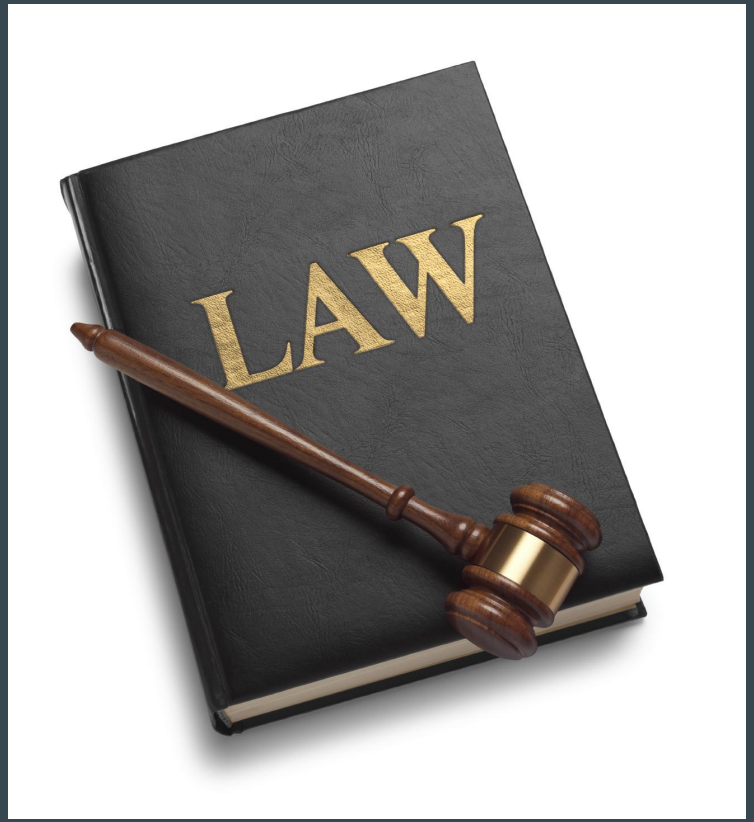
Unauthorized hacking is illegal, so “Get Out of Jail Free”...

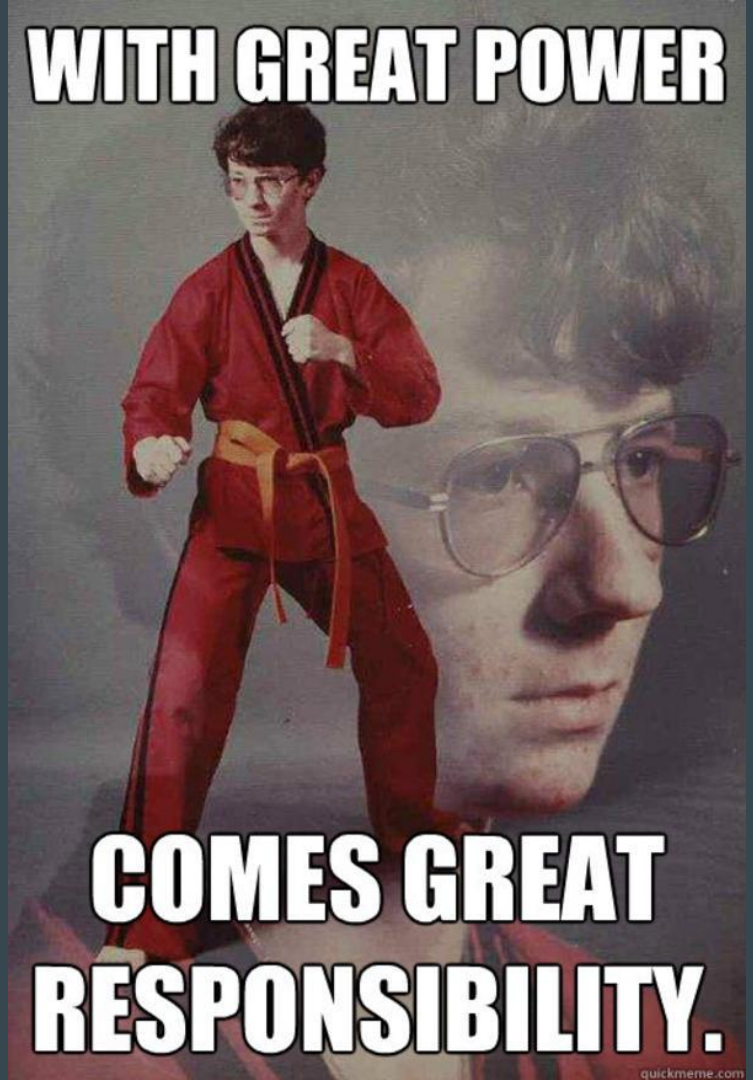
Before starting any test, all parties involved must agree upon a written contract indicating the scope and targets of the pen test.

The customer asking for a pen test must have the authority to authorize a pen test.

Ethics and Laws

- Privacy Issues
- Duty To Warn




WITH GREAT POWER
COMES GREAT
RESPONSIBILITY.
quickmeme.com

Questions?

NOVEMBER 4 – 5

TexSAW

2016

6th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

Celebrating 30 Years

THE UNIVERSITY OF TEXAS AT DALLAS

Presenting Sponsor

State Farm®

Supporting Sponsor

Raytheon