THOMSON
COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense

Chapter 1
Ethical Hacking Overview

Revised 8-30-17

Objectives

- Describe the role of an ethical hacker
- Describe what you can do legally as an ethical hacker
- Describe what you cannot do as an ethical hacker

Introduction to Ethical Hacking

Introduction to Ethical Hacking

- Ethical hackers
  - Employed by companies to perform penetration tests
- Penetration test
  - Legal attempt to break into a company's network to find its weakest link
  - Tester only reports findings, does not solve problems
- Security test
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Tester offers solutions to secure or protect the network

The Role of Security and Penetration Testers

- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission

The Role of Security and Penetration Testers

- Script kiddies or packet monkeys
  - Young inexperienced hackers
  - Copy codes and techniques from knowledgeable hackers
- Experienced penetration testers write programs or scripts using these languages
  - Practical Extraction and Report Language (Perl), C, C++, Python, JavaScript, Visual Basic, SQL, and many others
- Script
  - Set of instructions that runs in sequence

It Takes Time to Become a Hacker

- This class alone won’t make you a hacker, or an expert
  - It might make you a script kiddie
- It usually takes years of study and experience to earn respect in the hacker community
- It’s a hobby, a lifestyle, and an attitude
  - A drive to figure out how things work

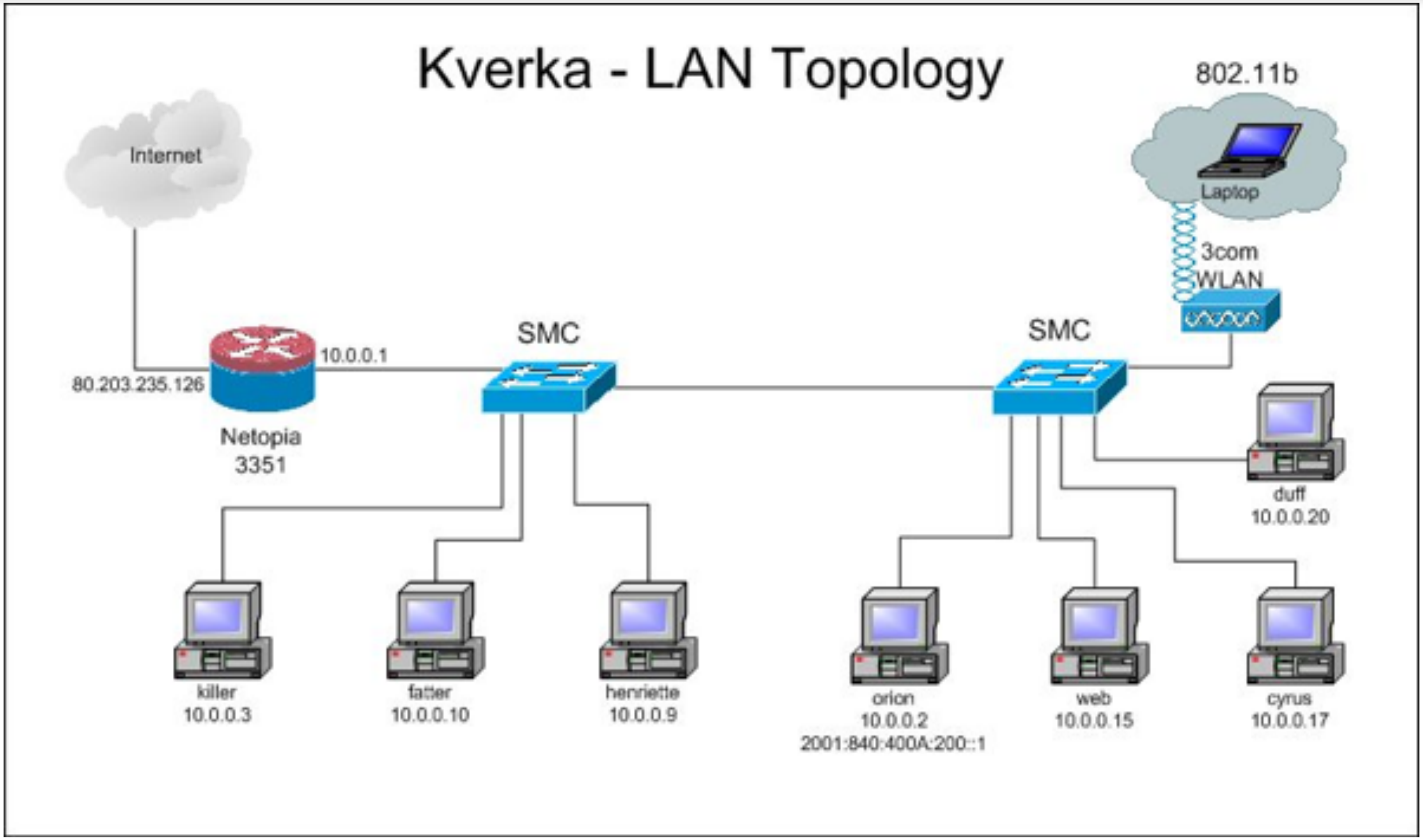
The Role of Security and Penetration Testers

- Tiger box
  - Collection of OSs and hacking tools
  - Usually on a laptop
  - Helps penetration testers and security testers conduct vulnerabilities assessments and attacks

Penetration-Testing Methodologies

- White box model
  - Tester is told everything about the network topology and technology
    - Network diagram
  - Tester is authorized to interview IT personnel and company employees
  - Makes tester's job a little easier

Network Diagram



- From ratemynetworkdiagram.com (Link Ch 1g)

Penetration-Testing Methodologies

- Black box model
  - Company staff does not know about the test
  - Tester is not given details about the network
    - Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

Penetration-Testing Methodologies

- Gray box model
  - Hybrid of the white and black box models
  - Company gives tester partial information

Certification Programs

Certification Programs for Network Security Personnel

- Basics:
  - CompTIA Security+ (CNIT 120)
  - Network+ (CNIT 106 or 201)

CompTIA Web sites : CompTIA Certifications | the Association | CompTIA Members
CompTIA.
the Computing Technology Industry Association
Certification Home
Certification Resources
About CompTIA
News
Customer Support
CompTIA Online Store
Search
CompTIA Certifications
› CompTIA Security+ Home
› CompTIA Security+ at a Glance
› CompTIA Security+ and Your Career
› Download Security+ Objectives
› Prepare for Exam

CompTIA Security+™ Certification

"Benchmarking foundational skills through the CompTIA Security+ certification and then adding progressive layers of expertise seems to us to be absolutely the right thing to do, from both the customer and employee standpoints."
- Steve Jordan
Vice President, System Engineering &Consulting, McAfee, Inc.

Certified Ethical Hacker (CEH)

Meet Sheela. She is a Network Administrator with a difference.
She is a Certified Ethical Hacker.
CEH
TM
Certified Ethical Hacker

- CNIT 123: Ethical Hacking and Network Defense
- CNIT 124: Advanced Ethical Hacking

What is an Offensive Security Certified Professional?

The **Offensive Security Certified Professional (OSCP)** is the companion certification for our Penetration Testing with Kali Linux training course and is the world's first completely hands-on offensive information security certification. The OSCP challenges the students to prove they have a clear and practical **understanding of the penetration testing process and life-cycle** through an arduous twenty-four **(24) hour certification exam**.

An OSCP has demonstrated their ability to be presented with an unknown network, enumerate the targets within their scope, exploit them, and clearly document their results in a penetration test report.

Certified Information Systems Security Professional (CISSP)

- Issued by the International Information Systems Security Certifications Consortium (ISC^2)
  - Usually more concerned with policies and procedures than technical details
- CNIT 125: Information Security Professional Practices
- Web site: www.isc2.org

SANS Institute

- SysAdmin, Audit, Network, Security (SANS)
- Offers certifications through Global Information Assurance Certification (GIAC)
- Top 20 list
  - One of the most popular SANS Institute documents
  - Details the most common network exploits
  - Suggests ways of correcting vulnerabilities
- Web site
  - www.sans.org (links Ch 1i & Ch 1j)

What You Can Do Legally

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
  - Laws change from place to place
- Be aware of what is allowed and what is not allowed

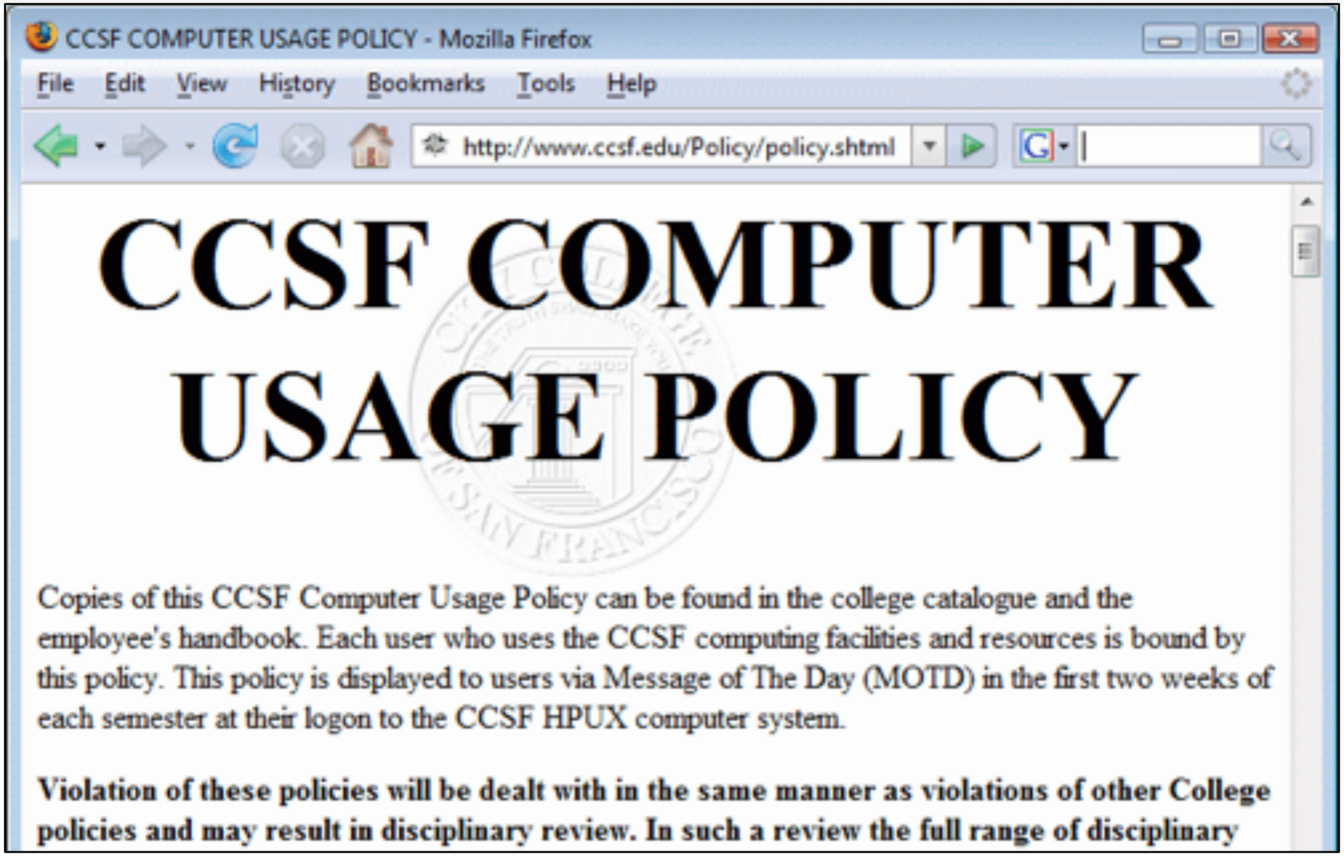
Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Written words are open to interpretation
- Governments are getting more serious about punishment for cybercrimes

Is Port Scanning Legal?

- Some states deem it legal
- Not always the case
- Federal Government does not see it as a violation
  - Allows each state to address it separately
- Read your ISP's "Acceptable Use Policy"
  - IRC "bots" may be forbidden
    - Program that sends automatic responses to users
    - Gives the appearance of a person being present

CCSF Computer Use Policy


CCSF COMPUTER USAGE POLICY - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.ccsf.edu/Policy/policy.shtml

CCSF COMPUTER USAGE POLICY

Copies of this CCSF Computer Usage Policy can be found in the college catalogue and the employee's handbook. Each user who uses the CCSF computing facilities and resources is bound by this policy. This policy is displayed to users via Message of The Day (MOTD) in the first two weeks of each semester at their logon to the CCSF HPUX computer system.

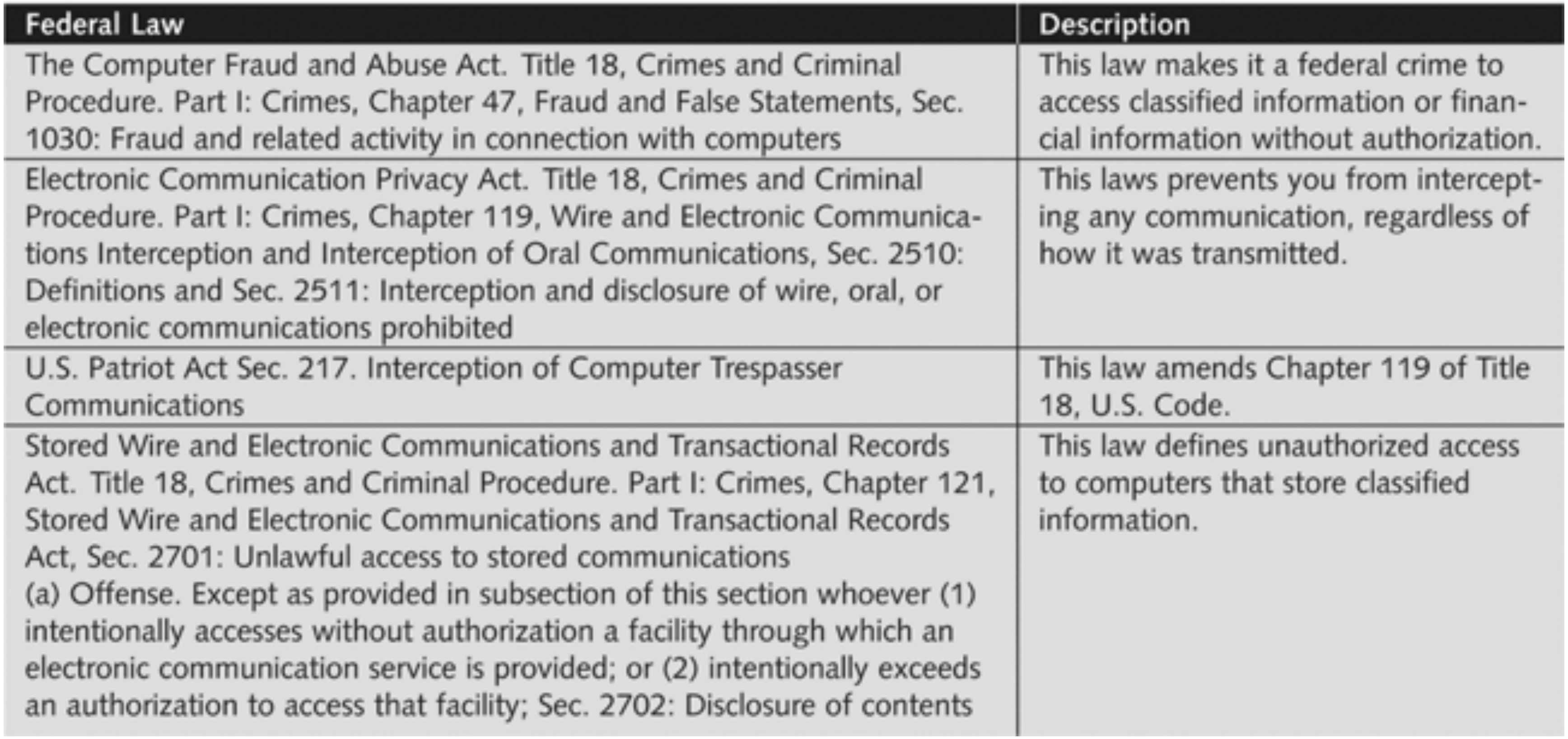
Violation of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review the full range of disciplinary

www.ccsf.edu/Policy/policy.shtml (link Ch 1k)

Federal Laws

- Federal computer crime laws are getting more specific
    - Cover cybercrimes and intellectual property issues
- Computer Hacking and Intellectual Property (CHIP)
    - New government branch to address cybercrimes and intellectual property issues

Table 1-2 Federal computer crime laws



Federal Law	Description
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, Sec. 2510: Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	This laws prevents you from intercepting any communication, regardless of how it was transmitted.
U.S. Patriot Act Sec. 217. Interception of Computer Trespasser Communications	This law amends Chapter 119 of Title 18, U.S. Code.
Stored Wire and Electronic Communications and Transactional Records Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 121, Stored Wire and Electronic Communications and Transactional Records Act, Sec. 2701: Unlawful access to stored communications (a) Offense. Except as provided in subsection of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; Sec. 2702: Disclosure of contents	This law defines unauthorized access to computers that store classified information.

What You Cannot Do Legally

- Accessing a computer without permission is illegal
- Other illegal actions
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs

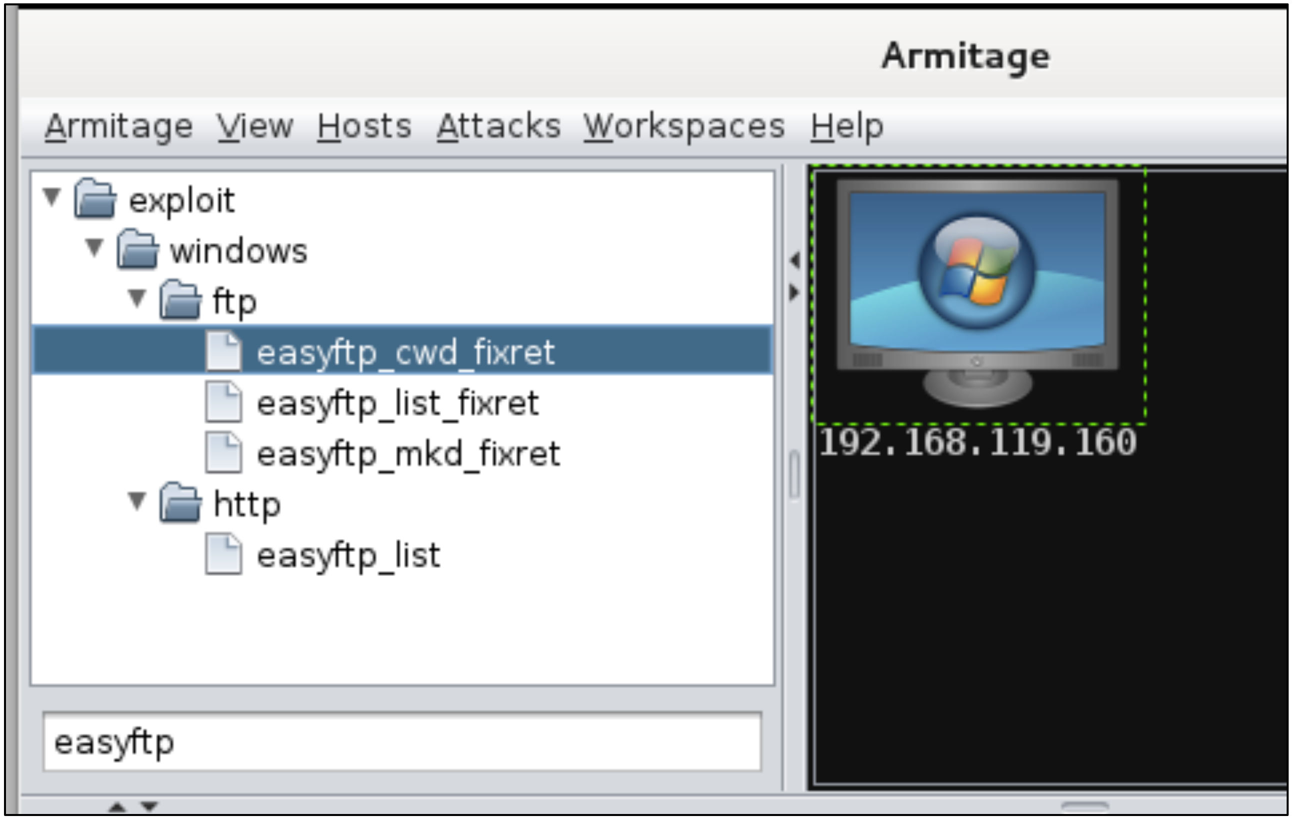
Get It in Writing

- Using a contract is just good business
- Contracts may be useful in court
- Books on working as an independent contractor
  - *The Computer Consultant's Guide* by Janet Ruhl
  - *Getting Started in Computer Consulting* by Peter Meyer
- Internet can also be a useful resource
- Have an attorney read over your contract before sending or signing it

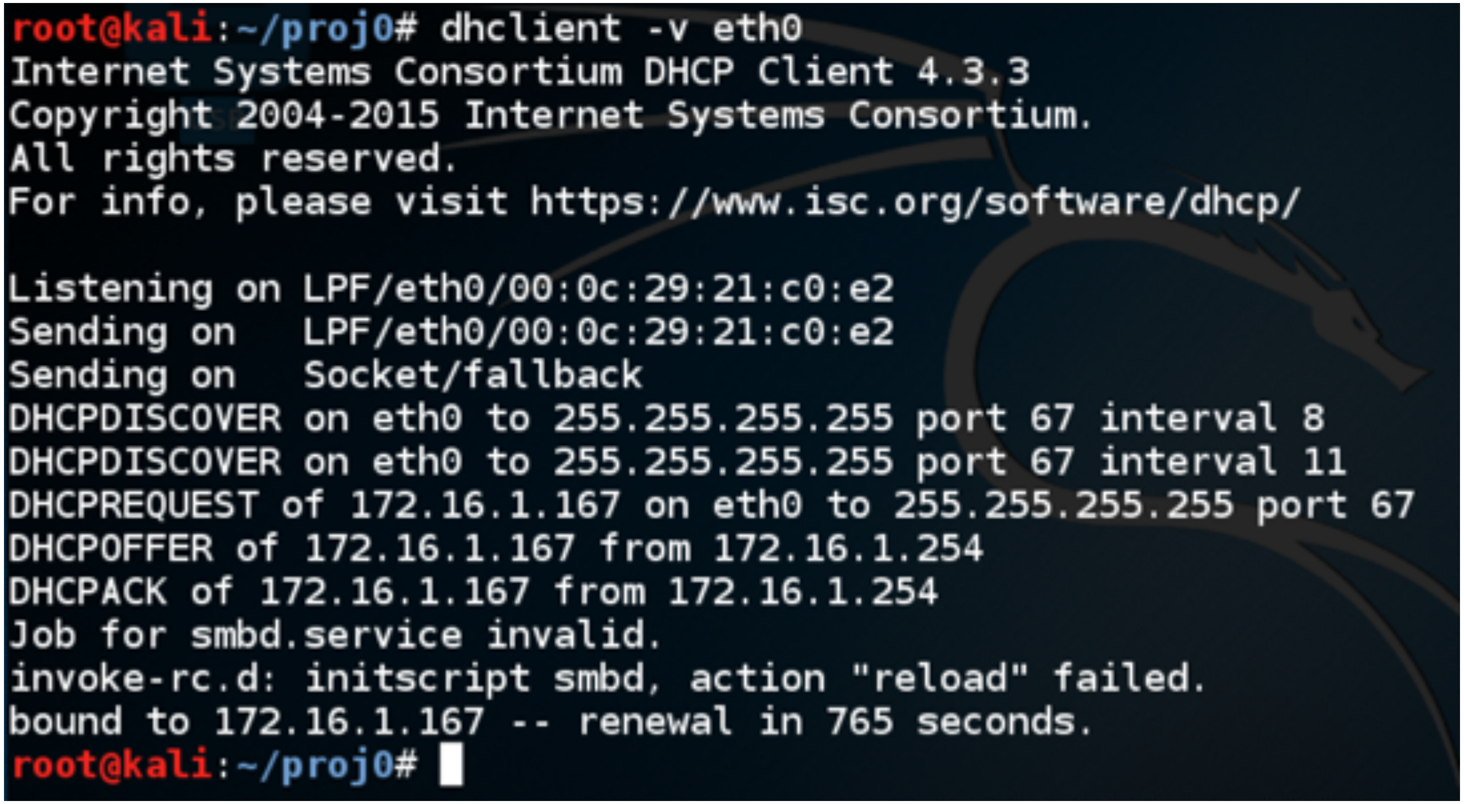
Ethical Hacking in a Nutshell

- What it takes to be a security tester
  - Knowledge of network and computer technology
  - Ability to communicate with management and IT personnel
  - Understanding of the laws
  - Ability to use necessary tools

Project Demo



Linux: Project X0



```
root@kali:~/proj0# dhclient -v eth0
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:21:c0:e2
Sending on   LPF/eth0/00:0c:29:21:c0:e2
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 11
DHCPREQUEST of 172.16.1.167 on eth0 to 255.255.255.255 port 67
DHCPOFFER of 172.16.1.167 from 172.16.1.254
DHCPACK of 172.16.1.167 from 172.16.1.254
Job for smbd.service invalid.
invoke-rc.d: initscript smbd, action "reload" failed.
bound to 172.16.1.167 -- renewal in 765 seconds.
root@kali:~/proj0# 
```