

Linux Security:
Application Security

This material is based on work supported by the National Science Foundation under Grant No. 0802551

National Science Foundation
WHERE DISCOVERIES BEGIN

Lesson Overview

This lesson is designed to introduce you to general security risks faced by network administrators. In addition to information on protecting public-facing services and exploring techniques to protect valued applications, this lesson also includes additional day-to-day security tips to keep your systems secure.

Moreover, this lesson will explore additional security concepts that have not been covered elsewhere in the Linux curriculum. In our experience, these additional security concerns are often discussed in job interviews. Therefore, you will be well advised to understand and review this material regularly to maintain a competitive advantage within the IT industry.

Select **PLAY** below for introductory videos:

View Video VideoLesson10Intro (C5L10V1).mp4

Intro

View Video VideoLesson10Reason (C5L10S2v2).mp4

Why study this lesson?

Objective

You should know what will be expected of you when you complete this lesson. These expectations are presented as objectives. Objectives are short statements of expectations that tell you what you must be able to do, perform, learn, or adjust after reviewing the lesson.

Lesson Objective:

Given the need to secure public-facing servers, the student will be able to construct a DMZ subnet containing chrooted DNS and mail or web servers as per industry standards.

Lesson Outline

In this lesson, you will explore:

- Important Terms
- Identifying Risks
- NMAP
- Security Policies
- DMZ
- Chroot
- Summary

Resources and Notes

This lesson uses Ubuntu Linux for demonstration. To complete this lesson successfully, you must have access to:

- Ubuntu Linux on bare metal or as a virtual install
- 10 Gb of hard drive space dedicated to the operating system's use
- A command shell
- Internet for research
- Word processor

Use the resources on the right to configure your system for Ubuntu.

Resources:

- Download Virtualbox
- Using Virtualbox with Ubuntu
- Virtualbox for Linux Hosts
- Virtualbox manual

Glossary of Terms

- **Access control** - Ensures that legitimate traffic is allowed in and out of your network
- **Asset** - Any person, place or thing for which extra security protections are needed
- **Availability** - The continuous operation of network resources
- **Botnets** - A system of hundreds or thousands of computers remotely controlled by a single user. The user routes commands through each of the computers in order to perform system attacks such as DDOS or SPAM messaging. See Zombie Computers and Botnets.
- **Chroot** – A command used to "jail" (confine) users to a particular area of the file system. This would restrict the user(s) from gaining access to and modifying essential system files and folders.
- **Confidentiality** - The protection of data from unauthorized disclosure to others that should not have access.
- **DMZ** - Demilitarized Zone - An area of a network that is normally on the public facing side of a network firewall and provides services such as Web hosting and email. A DMZ can also be configured to take public requests from regular Internet users and forward them to more secured services on the "internal" side of the LAN while remaining seamless to the end user.

Recommended Reading:

- Proxy & DMZ
- Tech Tips & Best Practice

Glossary of Terms

- **Due Diligence** – A legal term that means you have done everything within your immediate power/area of responsibility in order to do what is legally and morally correct
- **Firewall** – System designed to prevent unauthorized access to/from private networks. Can be software, hardware or a combination of both
- **Integrity** – The assurance that data has not been altered or destroyed through process or delivery.
- **Malicious software** – (malware) – A term covering programs such as viruses, worms, Trojan horses and backdoor programs
- **NMAP** – www.nmap.org – NMAP is an open source application used for security auditing.
- **Privilege escalation** – Using a weakness in an application or operating system to gain access to system resources to which the user would not normally have access
- **Script Kiddie** – A malicious person on the Internet who uses programs and applications to gain access to system resources. Script kiddies are not normally considered technically savvy (beginning hackers).
- **Social Engineering** – The ability of an unwanted user (hacker) to gain access to internal resources by pretending to be an authorized user
- **Software exploitation** – Gaining access to system resources through a vulnerability in software.
- **Trusted Networks** – Networks within your network security perimeter/firewall.
- **Untrusted Networks** – Networks that are known to be outside your security perimeter (external to your firewall)
- **Vulnerability** – A weakness associated with any asset or condition of a system. This includes hardware, software, administrative or human weaknesses.

Links and Resources

Review the following links before proceeding with this lesson:

- Practice Security Checklist
- Data Center Physical Security Checklist
- PC Checklist
- Information Security Checklist
- Computer Security Checklist
- CompTIA Security Assessment Tools

Identifying and Eliminating Risks

The responsibilities of the network administrator include:

- **Eliminating Theft** - This includes theft of information, data, employee and personal information, technology, trade secrets and the physical hardware. Items such as hard drives, memory, and licensed software are high loss items.
- **Authentication** – Are users who they really say they are and what level of access do they really need?
- **Identifying Assumptions** - For the network administrator, always assume the worst and finds ways to prevent it.
- **Controlling Secrets** - Protect upcoming and previous trade secrets. Research and development information and new product information are extremely important to your team as well as competitors.
- **Identify risks and prevent threats** - You are at the center of protecting your system resources.

Select the links below to watch the associated videos:

Required Viewing:

- Viruses, Worms & Botnets

View Video http://www.youtube.com/watch?v=LJAb7unURho&feature=related

- Computer Weaknesses

View Video VideoLesson10ComputerWeakness(C5L10S9v2).mp4

- Technology Risks

View Video VideoLesson10TechRisks(C5L10S9V3).mp4

- Spoofing

View Video VideoLesson10Spoofing(C5L10S9v4).mp4

- Security Tips

View Video VideoLesson10SecurityTips(C5L10S9v5).mp4

Security Tools

And Policies

NMAP

NMAP is a popular, open source tool used to identify open ports and services. NMAP has advantages and disadvantages for the system administrator. NMAP allows the administrator to scan networks in a proactive manner looking for unsuspecting services and open ports. This method of identifying services is easy to run and can help harden network resources.

NMAP can also be used by potential hackers to identify the very services hackers wish to exploit!

Since NMAP is open source, anyone can use it, and I assure you everyone does—admins, hackers, students, script kiddies. Anyone and everyone can use NMAP!

Select the links below to view the associated videos on NMAP:

Using NMAP Part I
Using NMAP Part 2

Select **PLAY** below for introductory videos:

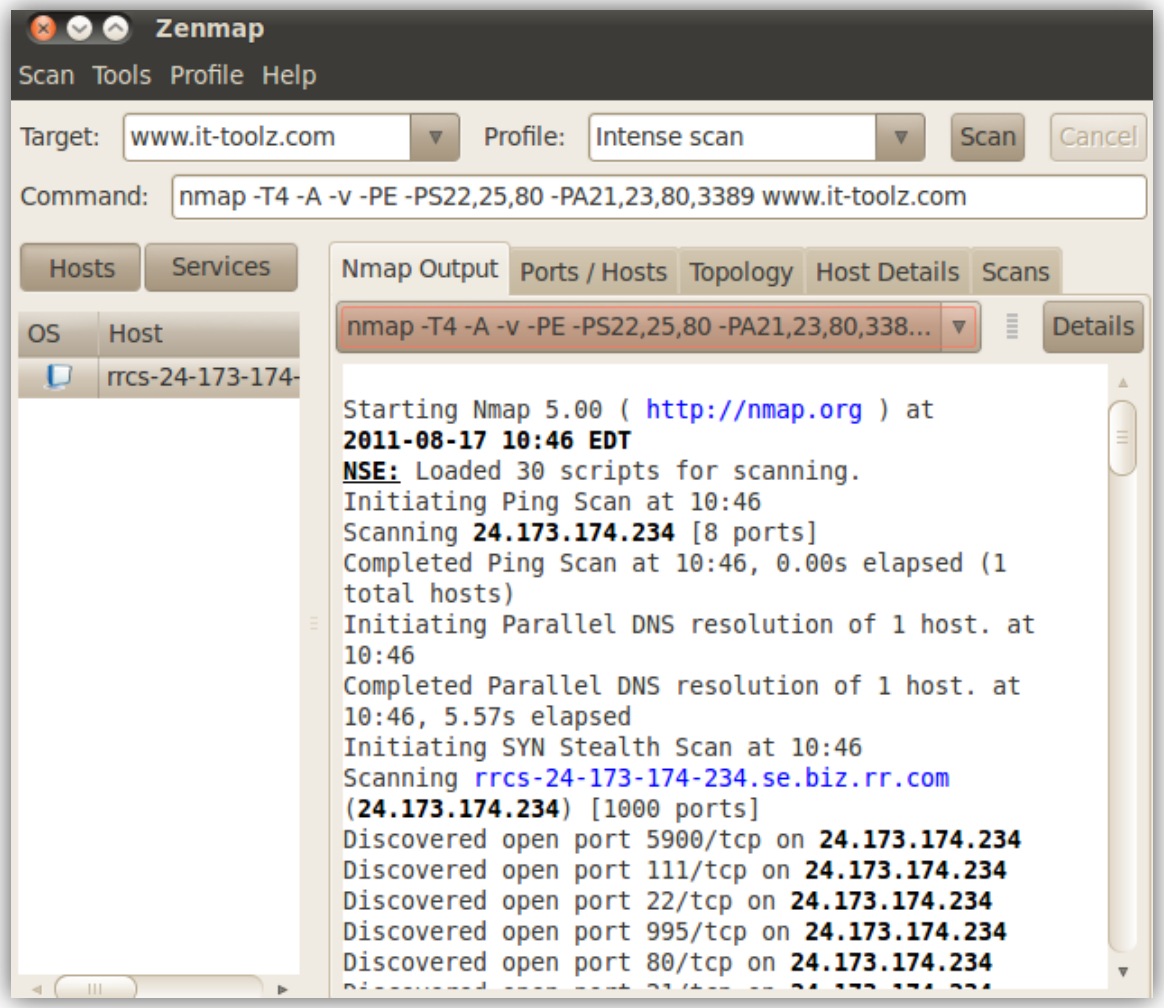
View Video VideoLesson10NMAPWarning(C5L10S11v1).mp4

NMAP Warning

View Video VideoLesson10NMAP(C5L10S11v2).mp4

NMAP

NMAP Tool



Screenshot of the NMAP Tool

Policy

A good security policy is worth its weight in gold. Many companies often overlook good, written security and network policies which can help prevent serious data breaches or accidents.

What are the components of a good security/network policy? A good policy must allow for services that are required for the company to do business while protecting the network from potential risk and attacks.

Your first step in writing a good policy is to understand fully the potential network security risks to you and your company's computer services.

Select **PLAY** below for videos on security risks

View Video
VideoLesson10Authenticate
(C5L10S13v1).mp4

Authentication

View Video
VideoLesson10SecurityRisk
(C5L10S13v2).mp4

Security Risks

Security Policies

Consider the following as you create or contemplate security policies:

- Authentication methods - username and password policies, biometrics
- What services are needed - DNS, HTTP, FTP, Remote access
- What services and applications are not needed - MYSQL, BootP, Broadcast services
- Who needs to know – Users should only be given enough information to do their jobs and nothing more.
- Who needs access – Users should only be given enough access to do their jobs and nothing more.
- Physical security (locks, doors, fences, swipe cards, cameras, video surveillance, guards)
- Wireless access - Who needs wireless network access and why. How is the service configured?
- Wireless devices (cell phones, Blackberry, Smart phones) What is allowed and what is not?
- External Media - Thumb drives, external hard drives, and data cards. Are they really needed and what options are in place to protect both employees and resources?

Recommended Reading

- Policy Templates
- Policy Categories & Types
- Network Security Policy

Tools for Success

For the security conscious network administrator, you should implement the seven-step approach below:

1. Setup physical security access to your network systems
2. Use NMAP to probe the network and then eliminate unused or unnecessary services to minimize external threats.
3. Configure a DMZ—forward inbound traffic to a DMZ running required services to get business done. This action will minimize the risk to your internal network.
4. Configure a Chroot environment. Create a jailed environment from which to run services in order to protect your main system files.
5. Establish a honeypot;- setup a Honeypot to act as a decoy for script kiddies and new hackers.
6. Develop company policy around security - Create a practical, yet protective, company policy that allows you to do business while protecting company information, data and resources.
7. Provide ongoing training - Create and implement proper training for all levels of your corporation. This action is one of the least expensive and probably the most overlooked security tool in your arsenal.

Select **PLAY** below for videos on security options.

View Video
VideoLesson10PhysicalSecurity (C5L10S15v1).mp4

Physical Security

View Video
http://www.youtube.com/watch?v=8FhDVhVUOS4

NMAP

DMZ

DMZ – (Demilitarized Zone) is an area of a network normally located on the public facing side of a network firewall and provides services such as Web hosting and email.

A DMZ can also be configured to take public requests from regular Internet users and forward them to more secured services on the "internal" side of the LAN, while remaining seamless to the end user (act as a proxy).

Take note of designated TCP/IP Ports !!
Be sure to always verify your information by referencing more then one source !!
List of TCP and UDP IP Address Ports.

Select **PLAY** below for a video on DMZ.

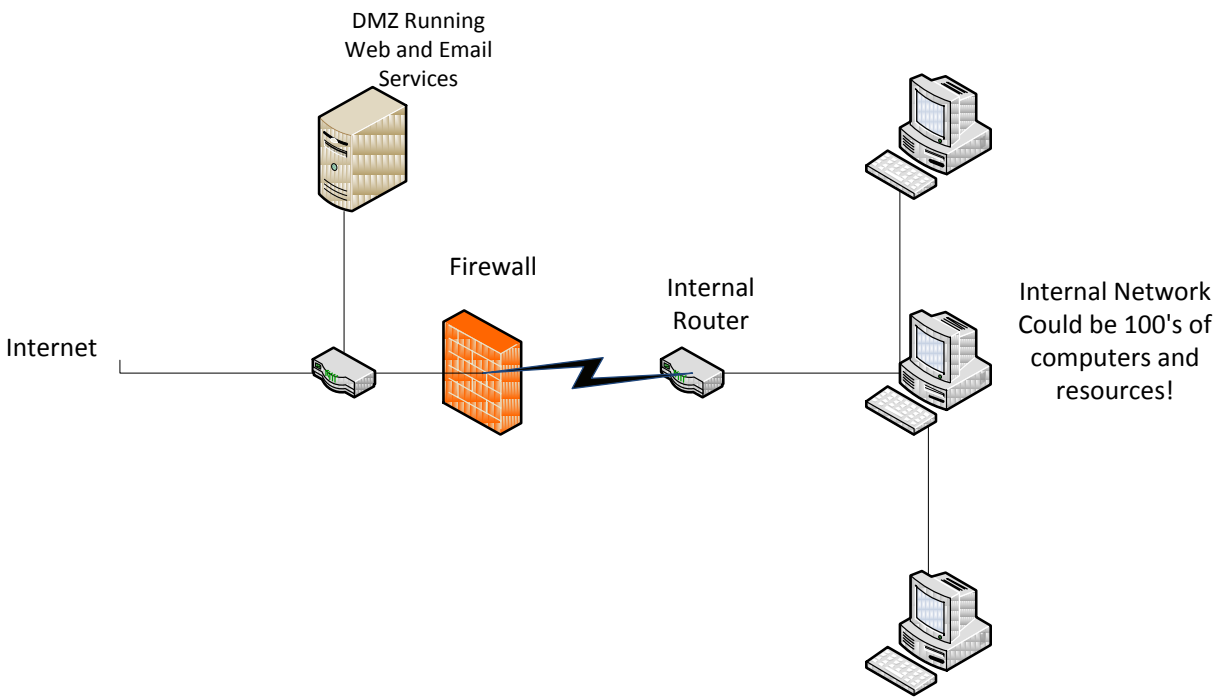
View Video
http://www.youtube.com/watch?v=xgCyDEUTQQk

CompTIA

Recommended Reading

- Configure a DMZ
- DMS Configuration

DMZ Setup

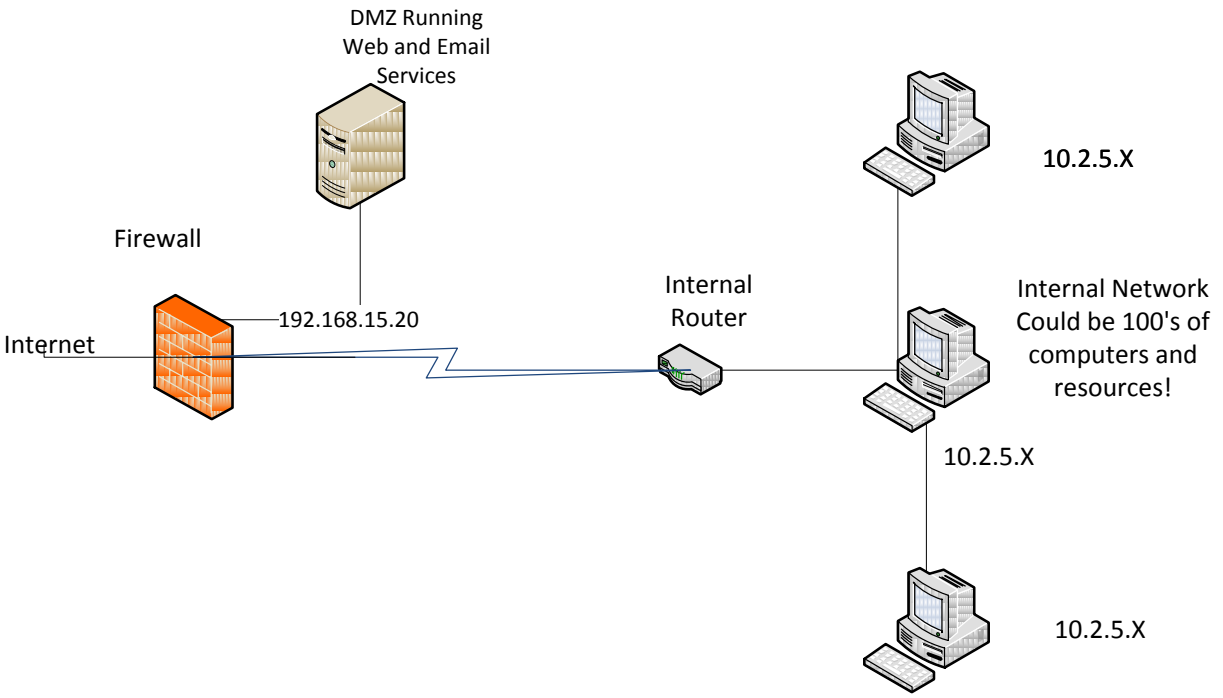


In the setup above, the DMZ would have a different subnet from the internal resources and is probably the most preferred implementation of a DMZ. The DMZ serves both to isolate the server from the internal network while providing required services to external users (the Internet).

Recommended Reading

- Debian Linux
- Make DMZ

DMZ Setup 2



The setup above is another popular setup where the DMZ is isolated from both the Internal network and external networks by a firewall. Note that the DMZ is also on a different subnet from the Internal Network. In this setup, the firewall has explicit rules configuring it to allow and pass data from the requesting client. The firewall can also reject specified service and port requests based on the rules.

Select **PLAY** below for a video on DMZ.

View Video
VideoLesson10DMZ
(C5L10S18).mp4

Recommended Reading

- Installing a DMZ

Chroot

Chroot allows computer administrators to create a "jailed" environment in which applications and services may run. In other words, a new directory structure is set up that includes all the resources required to run a service or application. Anyone accessing that service or resource is then confined to that immediate file structure and removed from the root file system.

Applications and services that are chrooted may include services such as DNS, Web, email services, web hosting, DHCP, and database applications. Implementing a chrooted environment captures and restricts users to a specific, confined environment and protects valuable system files and resources.

Recommended Reading

- Chroot to jail users

Lesson Summary

A network administrator has many responsibilities. You will be the go to person for anything relating to your computer systems including (but not limited to) the following:

- Creating and implementing security and use policies
- Developing or approving training
- Identifying and eliminating risk
- Eliminating theft of data and equipment
- Providing network services required to do business
- Reducing or eliminating unnecessary network services
- Configuring a DMZ
- Isolating services by creating a jailed environment for each
- Reviewing logs
- Keeping yourself trained and knowledgeable on current technologies, risks, and threats.

This lesson served as a basic introduction and review of some of these responsibilities. While this lesson explores limited aspects of application and system security, it does provide minimum approaches to security concerns and will learn you learn what to expect in your work place or during job interviews.

Select **PLAY** below for a summary video application security

View Video
http://www.youtube.com/watch?v=q4Waaq1rcuQ

Computer Policy

View Video
http://www.youtube.com/watch?v=zn-eLR3KiJY&feature=relmfu

Log Analysis