LPIC-3 Exam 303: Security

About this Course

Regarding Linux Professional Institute

- LPI is Non-Profit.
- According to their website, LPI is the world's first and largest vendor-neutral Linux certification body.
- LPI provides a number of Linux focused certificates.

Course Pre-requisites

- LPI will not award the LPIC3-303 certificate unless you have successfully completed the LPIC2 certification.
- LPIC2 requires LPIC1 certification.
- No formal requirements to sit for exam.

- You should have extensive experience with Linux systems prior to attempting the LPIC3-303.
- This is an advanced level professional certification.
- Should have one of the following or equivalent experience at a minimum:
    - LPIC-2: Linux Engineer
    - Red Hat Certified Engineer (RHCE)
    - Linux Foundation Certified SysAdmin (LFCS)

Exam 303-200

- Exam 303-200 is the exam affiliated with the LPIC3-303 certificate.
- The exam is focuses on the security of a system through many facets.
- This course is designed to aid you in preparation for the exam.
- This course will follow the detailed objective list published by LPI.

Keys to Success

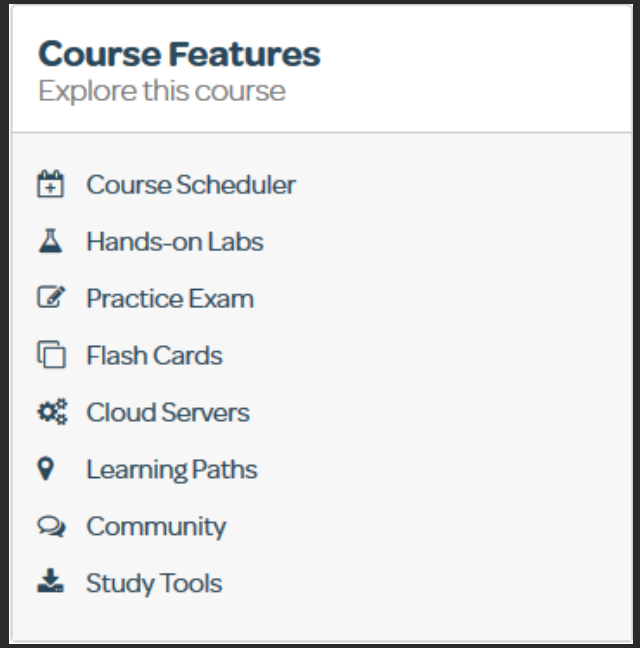
- Thoroughly review the video content.
- Study the flash cards.
- Practice the learning activities.
- Master the practice test!

LPIC-3 Exam 303: Security

Course Features and Tools

Course Features and Tools

- Video Lectures
- Flash Cards
- Study Guide
- Learning Activities
- Practice Test



LPIC-3 Exam 303: Security

325.1 X.509 Certificates and Public Key Infrastructures

Overview

- Cryptography Concepts
- PKI and Trust Chains
- Creating and Working with Certificates
- Operating a Certificate Authority

What is Cryptography?

- According to the Wikipedia article, cryptography is "the practice and study of techniques for secure communication in the presence of third parties called adversaries."
- When we are talking about cryptography in a computational context, we are generally referring to either symmetric or asymmetric encryption.
- Encryption is how we can pass information across public channels without compromising the content or integrity of the data.

Cryptography Concepts

Uses of Cryptography:

- Data Encryption
- Integrity
- Authentication

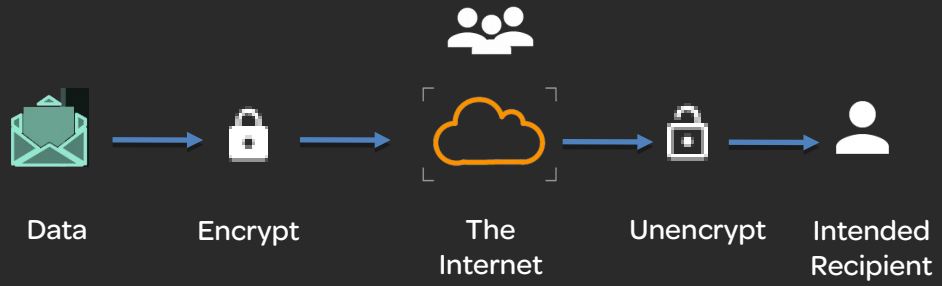
Cryptography Concepts: Encryption

There are two primary elements to cryptography:

- Key:
  - Used to encrypt data
  - Must be secret
- Algorithm:
  - Method of encryption
  - May be public
  - Examples: 3DES (old), blowfish, AES

Cryptography Concepts: Encryption

- A cipher (or algorithm) is used to scramble information
- The ciphertext may be deciphered (or unencrypted) with a key
- There are two types of encryption in modern cryptography:
  - Symmetric
  - Asymmetric



Symmetric and Asymmetric Encryption

Symmetric Encryption:

- There is only one encryption key:
  - Both parties must know the key
- Generally faster than asymmetric encryption
- Example algorithms: Blowfish, AES

Asymmetric Encryption:

- Uses 2 keys:
  - Encryption key is public
  - Decryption key is private
- Example algorithms: RSA, DSA, PKCS
- Good for digital signatures, key distribution, and digital certificates

Cryptography Concepts: Data Integrity through Hashes

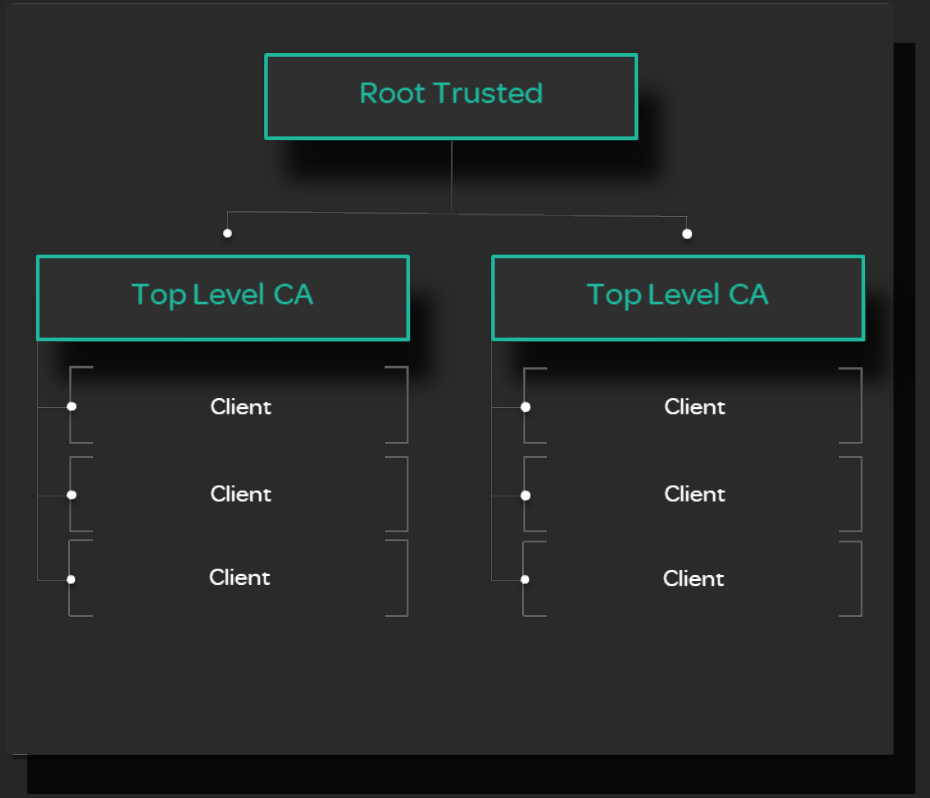
- A hash converts a string of any length to an output string of fixed length.
- Each string provides a unique hash.
- Hashing is generally one way.

- A salt may be used to improve security.
- A salt is an additional text value (typically random text) added to the ciphertext to improve security.
- Common hashing algorithms include crc-32 (insecure), md5, sha-1 (most common).

PKI and Trust Chains

PKI and Trust Chains

- Public Key Infrastructure is made up of a hierarchy of Certificate Authorities and a Certificate Signing Request process.
- CA or Certificate Authority:
    - A CA is a trusted third party that validates the authenticity of a public key.
    - There is a root trusted CA that has signs vetted CA certificates.
    - By trusting a CA certificate, you trust all certificates signed by that CA.
- Certificate Signing Requests (CSR) are essentially public keys that are generated and may be submitted to a CA to be signed:
    - When a CA signs a CSR, it produces a certificate that is trusted by the signing CA.
    - The CA can invalidate the certificate if need be by using either OCSP (Online Certificate Status Protocol) or by using a CRL (Certificate Revocation List).
    - CRL is almost entirely deprecated in favor of OCSP.



Creating and Working with Certificates

Creating a private key

openssl genrsa –<algorithm> -out <key_filename> <key_size>

openssl genrsa –aes128 –out mykey.pem 2048

Generating a self-signed certificate (public key)

openssl req –utf8 –new –key <key_filename> -x509 –days <cert_lifespan> -out <cert_filename>

Display Certificate

openssl x509 –in mycert.crt –text -noout

Creating a CSR

openssl req –new –key <priv_key.pem> -out <output.csr>

Creating and Working with Certificates: File formats

- The openssl command creates PEM formatted files by default.
- There are a few other formats, of which, you should be aware.
  - DER - A binary form of ASCII PEM.
  - P7B/PKCS#7 - Base64 encoded ASCII popular in windows.
  - PFX/PKCS#12 - A binary format capable of storing keys, certs, and intermediary certs together.
- The openssl command is capable of doing conversion.

Operating a Certificate Authority: Understanding CAs

- What makes a CA is really a unique key pair.
- A CA public key has typically been signed by another CA that is trusted.
- The CA has three primary responsibilities:
  - Sign valid CSRs
  - Maintain security of their private key
  - Revoke compromised or misused certificates

Operating a CA

Creating a private key

openssl genrsa –<algorithm> -out <key_filename> <key_size>

openssl genrsa –aes128 –out mykey.key 2048

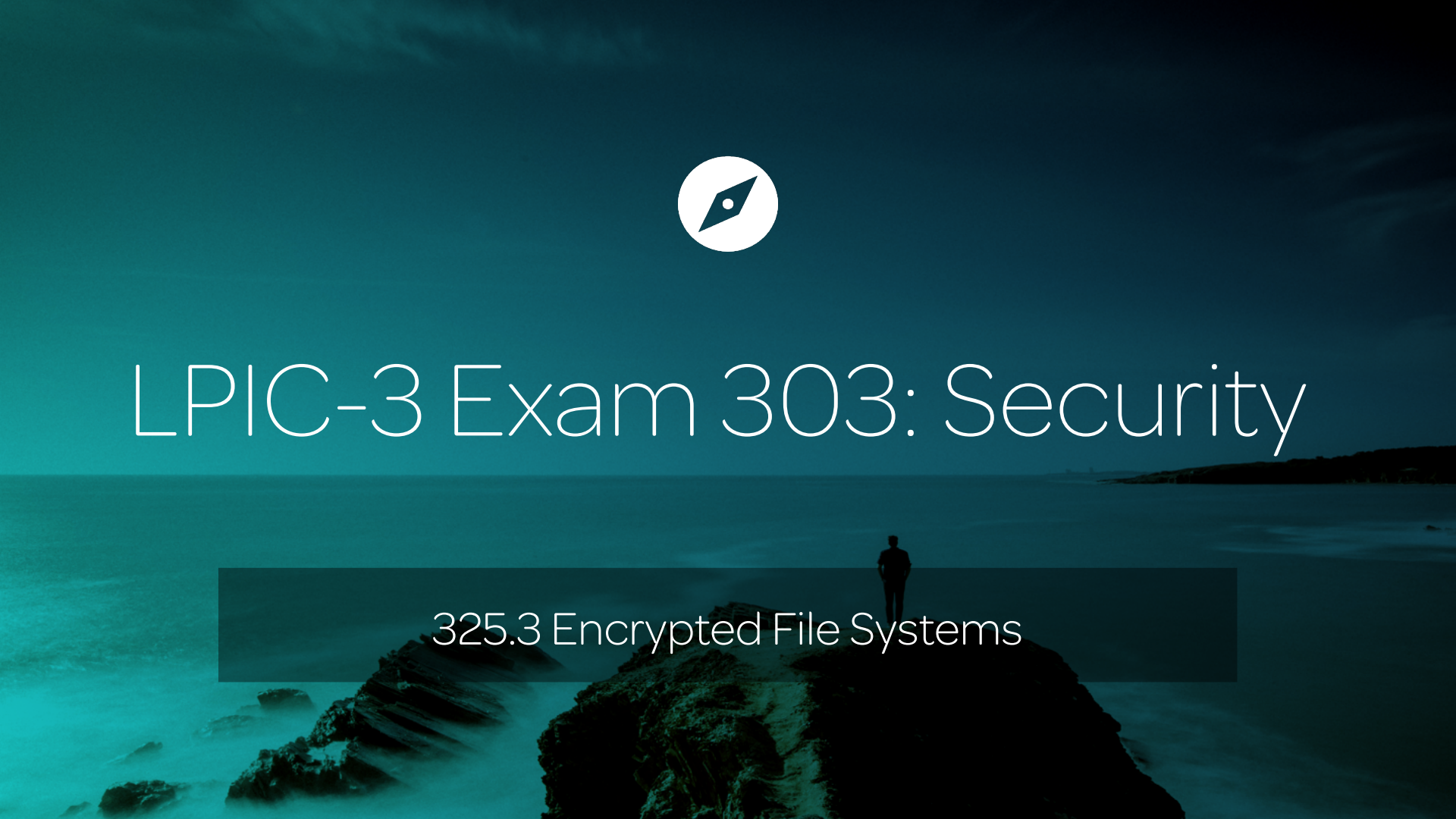
Generating a self-signed certificate (public key)

openssl req –utf8 –new –key <key_filename> -x509 –days <cert_lifespan> -out <cert_filename>

You would add –set_serial <serial_num> for a CA certificate

Signing a CSR as a CA (requires CA keys)

openssl ca –in <csr> -out <crt>



LPIC-3 Exam 303: Security

325.3 Encrypted File Systems

Overview

- Disk Encryption Concepts
- File System Encryption with eCryptfs
- Working with LUKS

Disk Encryption Concepts

- Use cases of disk encryption
  - Protect removable media
  - Add additional data security
- Methods of disk encryption
  - Block Device
  - File System Level
- Disk encryption tools
  - dm-encrypt and LUKS
  - cryptmount
  - eCryptfs
  - EncFS

Disk Encryption with eCryptfs and EncFS

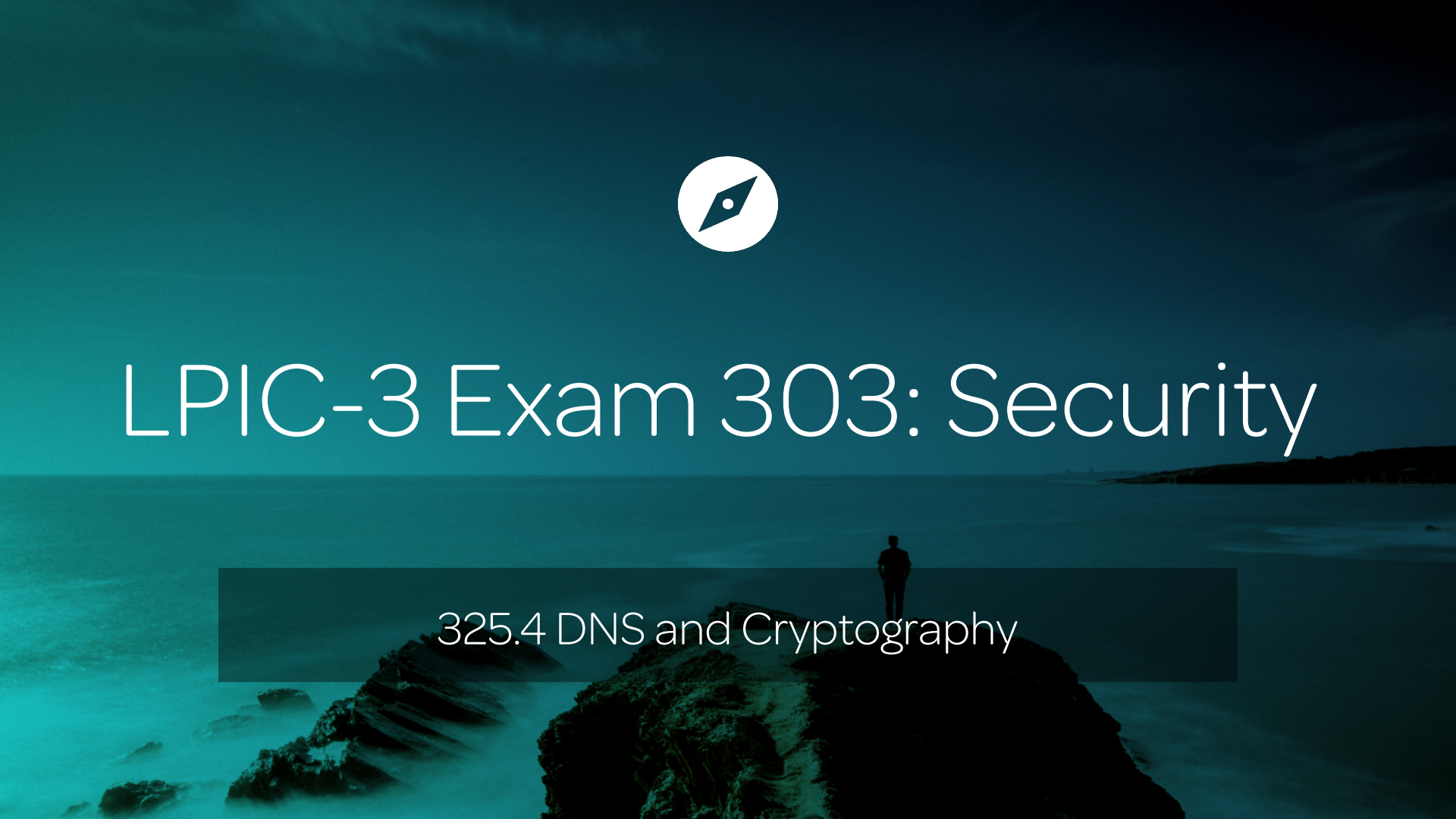
- eCryptfs provides file system level encryption:
  - Uses **ecryptfs** package
  - Mount a new directory using the **ecryptfs** type
  - PAM module provided for automatic mounting options
  - **ecryptfs-utils** package provides helper utilities
- EncFS is similar to eCryptfs but targets non-superusers:
  - Allows for the creation of encrypted repositories by standard users

Working with LUKS

Create encrypted volume
cryptsetup luksFormat dev
cryptsetup luksOpen dev mapping

Luks Keys
cryptsetup luksAddKey dev keyfile

Mount on boot with Crypttab
/etc/crypttab
/etc/fstab



LPIC-3 Exam 303: Security

325.4 DNS and Cryptography

Overview

- Working with DNS
- Securing DNS with DNSSEC

DNS Overview

- DNS is short for Domain Name System:
  - DNS is a hierarchical system used to resolve hostnames.
  - The hierarchy starts with a root server that branches.
  - Resolvers attempt to lookup hostnames against local forwarders if configured.
  - Otherwise, the resolvers will go directly to the root name server which will delegate to an appropriate intermediary.
- Zones and Resource Records:
  - DNS configurations are made up of zones and Resource Records (RRs).
  - RRs consist of a type and a series of labels that make up domains, subdomains, hosts, etc.
- With the development of DNS technology, EDNS was purposed:
  - The extension mechanism for DNS.
  - Documented in RFC 2671.
  - The goal of EDNS is to address backward compatibility for older versions of DNS.
- BIND is a popular implementation of a DNS server:
  - The primary configuration file is located in `/etc/named.conf`.
  - The objectives on LPIC exam 303-200 cover securing DNS with BIND in particular.

Securing BIND

- Means of securing DNS
  - TSIGs – A method of digitally signing data provided to a resolver or data sent in a zone transfer.
  - Running a named server in a `chroot` jail.
  - Configuration directives:
    - Allow query
    - Recursion
    - Allow Transfer
- RNDC stands for Remote Name server Daemon Control
  - Allows for remote name server management.
  - Must be secured using a secret key that is shared with the BIND server.
  - See study guide for more detail.

BIND Configuration

Directives:

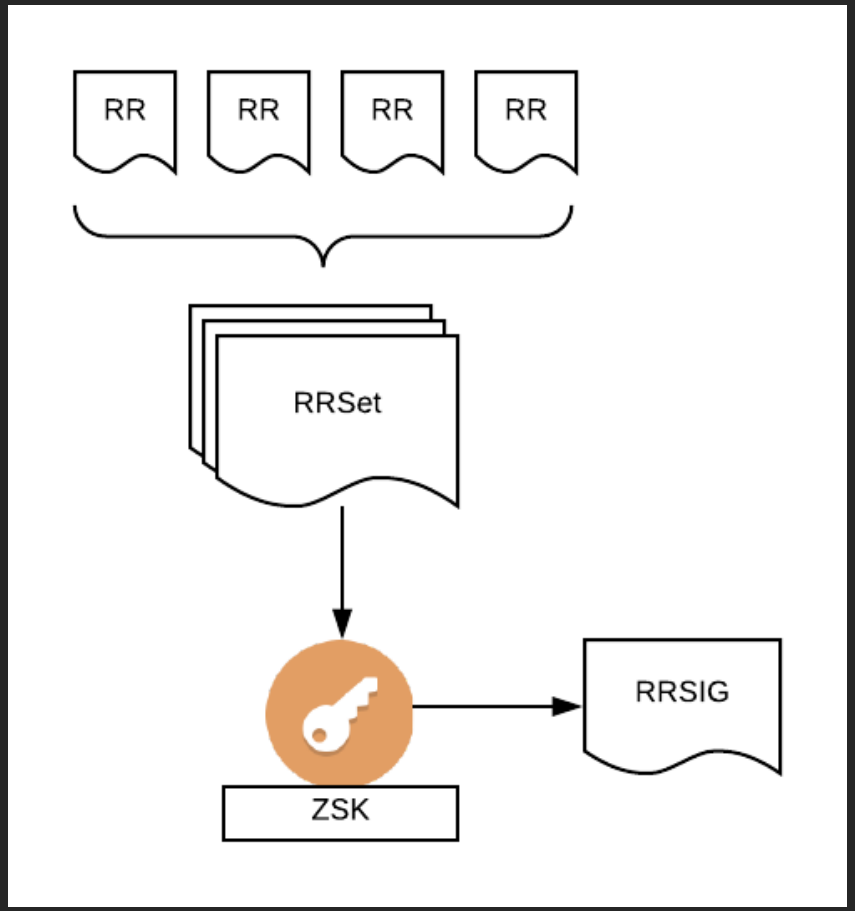
```
allow query
recursion
allow transfer
```

DNS utilities:

```
dig
```

DNS security with DNSSEC

- What is DNSSEC?
  - Domain Name System Security Extension.
  - DNSSEC guarantees the authenticity of Zone Transfers and RR lookups.
  - Security is achieved by digitally signing zone files to ensure they have not been altered or spoofed.
- Enabling DNSSEC
  - `Dnssec-enable` and `dnssec-validation` directives in `namd.conf`.
  - Must create Zone Singing Keys (ZSKs), Key Signing Keys (KSKs), and have your registration publish a Delegation Signer (DS) record for your domain.
  - Must also sign zone files using the `dnssec-signzone` command.



DNSSEC

Zone Signing Keys (ZSK)

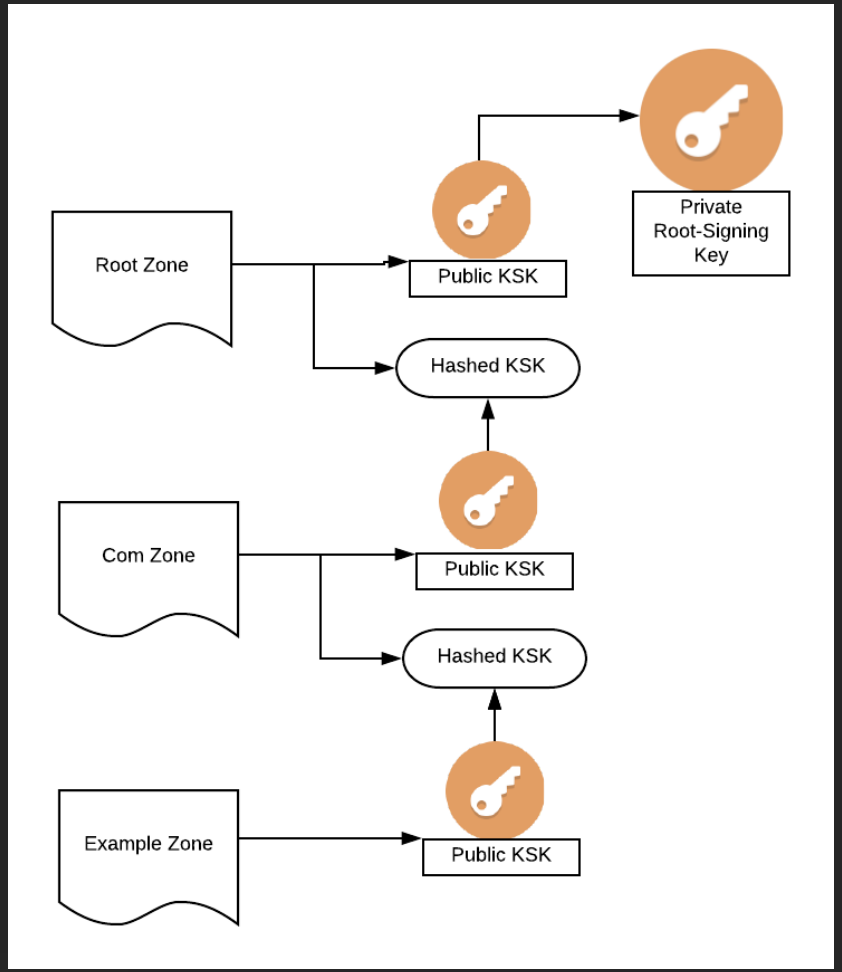
- Signs a particular zone file.
- Generated using `dnssec-keygen`.
- Should be rotated on a monthly interval for optimal security.

Key Signing Keys (KSK)

- KSKs are what authenticate your server's ZSKs.
- Created using `dnssec-keygen` but with `-f` KSK parameter.

Dnssec-signzone

- Generated key records are placed in a zone file.
- `dnssec-signzone` creates a signed zone file for use with BIND.



DNSSEC

Zone Signing Keys (ZSK)

- Signs a particular zone file.
- Generated using `dnssec-keygen`.
- Should be rotated on a monthly interval for optimal security.

Key Signing Keys (KSK)

- KSKs are what authenticate your server's ZSKs.
- Created using `dnssec-keygen` but with `-f` KSK parameter.

Dnssec-signzone

- Generated key records are placed in a zone file.
- `dnssec-signzone` creates a signed zone file for use with BIND.

More on DNSSEC

- Chain of Trust
  - KSKs are provided and published by the parent of a child zone.
  - This continues all the way to the `root dns` servers which have their KSK signed in a key signing ceremony.
- Other commands to understand
  - `dnssec-settime` – Manages the validity period of a given key.
  - `dnssec-dsfromkey` – Used to generate the DS RR for a given KSK.
  - Review the man pages.
- DO and AD bits
  - The DO and AD bits are contained in DNS queries and responses.
  - DO stands for DNSSEC OK and indicates that a client will understand a NDSSEC response.
  - AD stands for Authenticated Data and is set when data returned by a server that is authenticated with DNSSEC.

What is DANE?

- DANE stands for DNS-Based Authentication of Named Entities:
  - Domain Name System Security Extension.
  - DNSSEC guarantees the authenticity of Zone Transfers and RR lookups.
  - Security is achieved by digitally signing zone files to ensure they have not been altered or spoofed.

- The TLSA Resource Record:

```
_443._tcp.www.example.com. IN TLSA (
      1 1 2 92003ba34942dc74152e2f2c408d29ec
            a5a520e7f2e06bb944f4dca346baf63c
            1b177615d466f6c4b71c216a50292bd5
            8c9ebdd2f74e38fe51ffd48c43326cbc )
```

  - Note the port and protocol designation in the label.
  - TLSA Records are not limited to https.

LPIC-3 Exam 303: Security

326.1 Host Hardening

Overview

- Kernel Security
- Securing Grub

Kernel Security

- Disabling unnecessary software:
  - Every running program presents a possible security threat.
  - Disabling unused services is a good security practice.
  - Use systemctl and chkconfig to disable services.
  - Commonly disabled services include atd, avahi-daemon, cups.
- Limiting resource usage:
  - The user may limit system resources such as threads, open files, and memory.
  - The `pam_limits.so` module allows operators to control how much of any one resource a user may access through hard and soft limits.
  - Most systems come with `pam_limits.so` preloaded.
  - The `ulimit` command may be used to adjust these limits at runtime.
  - Limits may be set persistently in `/etc/security/limits.conf`.

Kernel Security

- Tuning kernel parameters:
  - The `sysctl` command is capable of displaying and setting kernel parameters.
  - Parameters map to the `procfs` filesystem.
  - Kernel parameters set persistently in the file `/etc/sysctl.conf`.
  - See kernel-docs for additional information.
- Managing ASLR:
  - ASLR stands for Address Space Layout Randomization.
  - It ensures that every time a program loads, it loads into a different place in memory.
- The NX bit:
  - The NX bit is a CPU feature.
  - It prevents execution from protected memory areas.
  - Exec-Shield is a software solution for the same problem designed to support CPUs without this feature.
- ICMP security settings:
  - Network security may be enhanced through kernel parameter tuning.
  - Disabling ICMP is a common security measure that may be achieved by setting the parameter `net.ipv4.icmp_echo_ignore_all` to `1`.

Sysctl Review

View Settings:

```
sysctl -a
```

```
sysctl -ar <search_pattern>
```

```
procfs
```

Setting parameters:

```
sysctl -w <param>=<value>
```

Persist changes:

```
/etc/sysctl.conf
```

Kernel Security

- Chroot Environments
  - A chroot environment is a 'fake root' that is set for a specific user and process.
  - The chroot command is used by root to create the environment using a pre-configured area in the filesystem.
  - An unprivileged process is unable to access files outside of a chroot environment.
  - Be mindful of hard links in chroot environments.
- Virtualization
  - Virtualization is similar to a chroot environment but at a much more advanced level.
  - Containerization is similar in nature when it comes to resource segmentation and process isolation.

Securing Grub

Boot parameters present a security threat:

- Booting a system with specific options may allow unauthorized access to a system.
- Grub is capable of password protection for menu entries:
  - Grub 1 was only able to support passwords and not unique user accounts.
  - Grub 2 has more robust security.

Securing Grub

Configuring users in `/etc/grub.d/01_users`:

```
set superusers="bob"

Password bob somepw

Password notsuper otherpw
```

Configuring menu entries `grep menuentry /boot/grub2/grub.cfg` in `/etc/grub.d/40_custom`:

```
menuentry "menu item"
--usersnotsuper
```

Building `grub` configuration:

```
grub2-mkconfig -o
/boot/grub2/grub.cfg
```

LPIC-3 Exam 303: Security

326.2 Host Intrusion Detection

Overview

- Threat Detection Tools
- System Auditing with Auditd

Threat Detection

- The important thing about threat detection
  - These tools are post-incident tools.
  - You are alerted once your system has already been compromised!
- The tools you need to know about
  - AIDE
  - OpenSCAP
  - Linux Malware Detect
  - Rkhunter
  - Chkrootkit

- Important for the test
  - Know commands and options.
  - Understand broad concepts.
  - Know configuration directives!

AIDE

Commands:
aide --init
aide --check

Configuration
/etc/aide.conf

A Brief Word on OpenSCAP

- SCAP
  - Security Content Automation Protocol .
  - Community project started by Red Hat.
- OpenSCAP
  - An implementation of SCAP.
  - Vulnerability Assessment.
  - Security Compliance.
  - Be aware of what it is.

Linux Malware Detect

Commands:
maldet -a
maldet -e
systemctl cat maldet

Configuration
/usr/local/maldet/conf.maldet
/usr/local/maldet/monitor_paths

Rootkit detection

Chkrootkit

- chkrootkit -q

Rkhunter

- rkhunter -c --cronjob -rwo
- /var/log/rkhunter/rkhunter.log
-

Other notes

- AIDE may also detect rootkits
- Kernel modules are popular places to hide rootkits

System Auditing with Auditd

- Auditing vs Logging
  - Logs vary by system and software.
  - Audit runs at OS level.
- Auditd
  - Built into Red Hat distributions.
  - May be installed in Debian.
  - Customizable rules.

Working with Auditd

Commands:
ausearch
aureport
auditctl

Configuration
/etc/audit/auditd.conf
/etc/audit/rules.d
/etc/audit/audit.rules

Files
/var/log/audit.log
/etc/pam.d/system-auth

LPIC-3 Exam 303: Security

326.3 User Management and Authentication

Overview

- Linux Login Basics
- PAM Concepts and Configuration
- Kerberos
- Understanding SSSD

Linux Login Basics

- /etc/login.defs:
  - Used to be main login configuration.
  - Replaced over time by PAM.
  - MAIL_DIR.
  - UID and GID settings.
  - UMASK.
- The chage command:
  - Requires root for most functionality.
  - User must have entry in /etc/shadow.
  - -E <YYYY-MM-DD> LOGIN
  - -I <days> LOGIN
  - -W <days> LOGIN
  - A value of -1 may be used to inactivate many options.
- NSS Concepts:
  - The Name Service Switch.
  - Connects calls for information from a system database to a back-end service.
  - Know contents of /etc/nsswitch.conf.

/etc/nsswitch.conf

Databases:
passwd
shadow
group
hosts

Services:
files
sss
dns

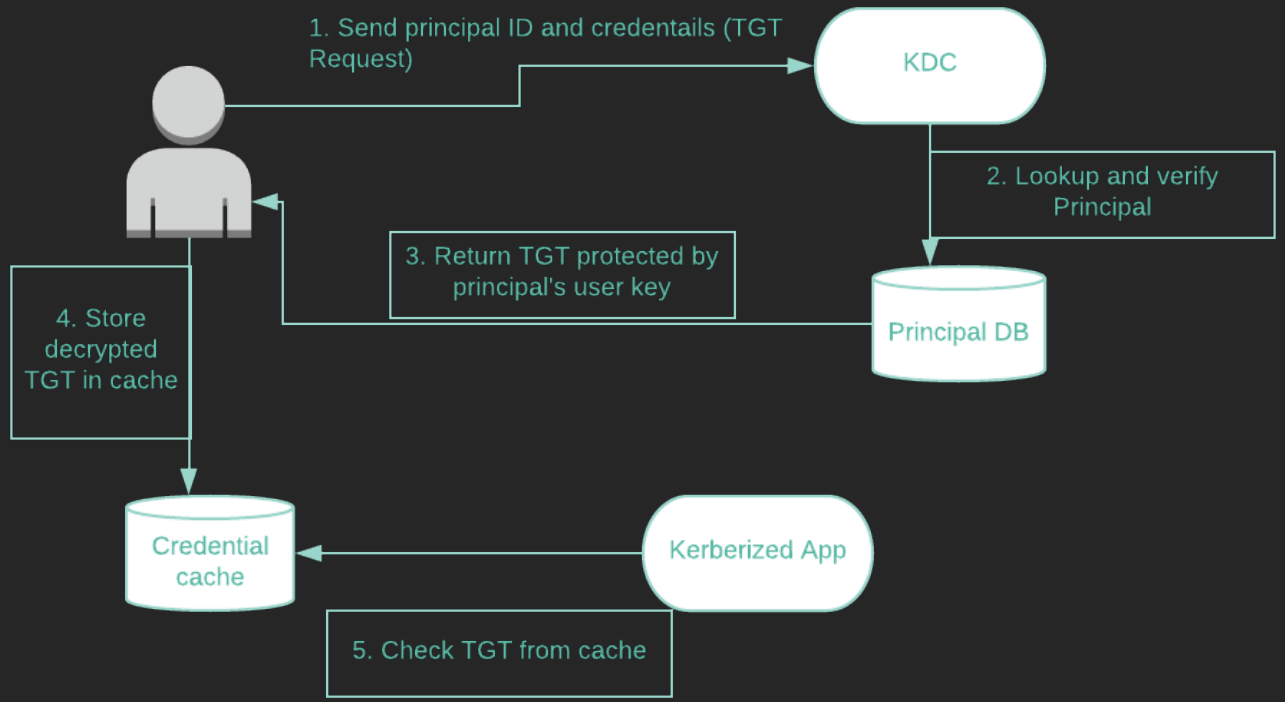
PAM Concepts

- Pluggable Authentication Module
  - Has become a core part of the login process on modern Linux distributions.
  - Made up of a number of modules each handling a unique function regarding authentication and authorization.
- Pam is divided into four management groups:
  - Auth: Used for authentication purposes
  - Account: Deals with account related work such as verifying account details.
  - Password: Modules in this class work with passwords.
  - Session: Interacts with user session properties.

PAM

Configuration:
/etc/pam.d/*

Modules:
pam_tally2.so
pam_cracklib.so



Kerberos

Terms:

- Key Distribution Center
- Realm
- Principal
- Ticket
- TGT
- TGS

Important Files:

- /etc/krb5.conf

Commands:

- kinit
- klist
- kdestroy

System Security Services Daemon

- SSSD provides a set of daemons to manage access to remote directories and authentication mechanisms.
- Key Integrations
  - Active Directory
  - FreeIPA
  - LDAP
  - Kerberos
  - Local Domain

SSSD

Integrations:
Active Directory
IPA
LDAP
Kerberos
Local
NSS
pam_sss.so

Configuration:
/etc/sssd.conf

Utitlities:
sss_useradd
sss_userdel
sss_usermod
sss_groupadd
sss_cache
sss_obfuscate

LPIC-3 Exam 303: Security

326.4 FreeIPA Installation and Samba Integration

Overview

- FreeIPA Overview
- Installing and Configuring FreeIPA
- Working with FreeIPA

Overview of FreeIPA

- What it?
  - FreeIPA is a suite of tools that provides identity and authentication services
  - FreeIPA is similar to Microsoft Active Directory but it is not a replacement
- What can it do?
  - Provide a user directory via LDAP
  - Provide Kerberos Authentication
  - Maintain a central sudo rule set
  - Keep autofs configurations
  - Hold SELinux user mapping data
- The FreeIPA Suite:
  - 389 Directory Server
  - MIT Kerberos
  - DNS (BIND)
  - NTP
  - Dogtag

A word on Certmonger

- The certmonger daemon monitors certificates for impending expiration.
- It can optionally refresh soon-to-be-expired certificates with the help of a CA.
- Working with certmonger:
  - `ipa-getcert list`
  - `ipa-getcert request -f /path/to/server.crt -k /path/to/private.key -r`
  - By default, certmonger works with the CA configured for the IPA noted in `/etc/ipa/default.conf`

FreeIPA Prerequisites

- Local DNS configuration
  - Any IPA server must have a static hostname configured in `/etc/hosts` that matches the system hostname and is in the planned DNS domain.
  - The installation utility verifies DNS resolution prior to starting installation.
- Firewall Considerations
  - Though it is not required for install, there are a number of ports that must be open for proper operation of an IPA server.
  - Services: HTTP/S (tcp/80, tcp/443), Kerberos (tcp/88, tcp/464, udp/88, udp/464), DNS (udp/53), NTP (udp/123), LDAP (tcp 389, tcp/636)

Installing FreeIPA

Packages:

- `ipa-server`
- `Ipa-server-trust-ad`

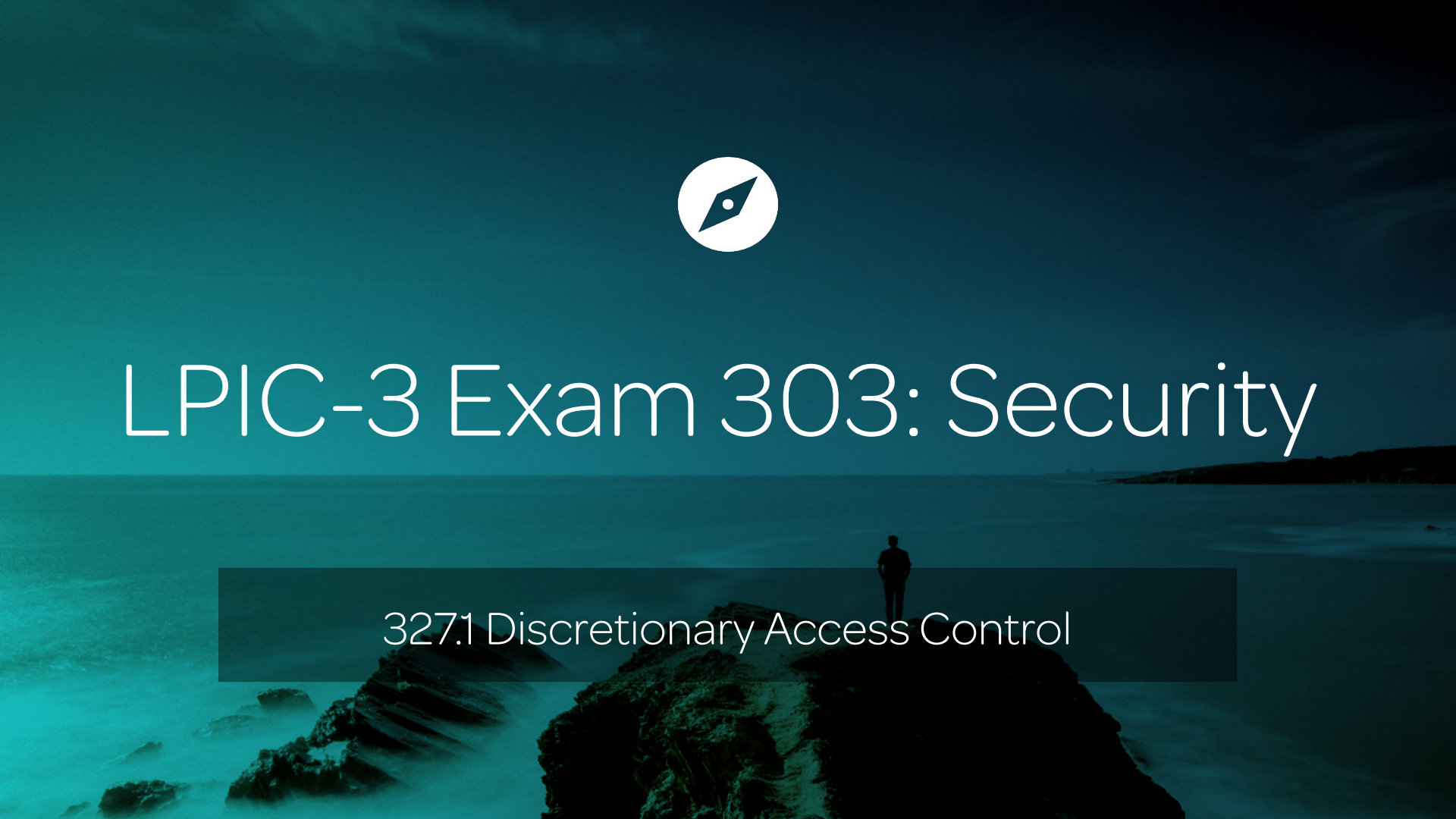
Commands:

- `ipa-server-install`
- `ipa-replica-install`
- `ipa-replica-prepare`
- `ipa-replica-manage`
- `ipa-adtrust-install`

Working with FreeIPA

Packages:
ipa-client

Commands:
- ipa-client-install
- ipa user-add sam --first sam --last j
- ipa group-add staff --desc “staff”
- ipa help



LPIC-3 Exam 303: Security

327.1 Discretionary Access Control

Overview

- Basic System Permissions – DAC Review
- Extended Attributes
- Using ACLs

DAC Review

Commands:

- chown
- chmod

Permissions:

- read / write / execute
- SUID
- SGID
- Sticky Bit

Extended Attributes

- The Concept:
  - Modern Linux Filesystems support extended attributes (abbreviated xattr) if the libattr feature is enabled in the kernel configuration
  - Any regular file may have a list of extended attributes denoted by name

- Xattr namespaces:
  - User
  - Trusted
  - Security
  - System

Xattr

Getting xattrs:

- getfattr
- -n <name>
- -m <pattern>

Setting xattrs:

- setfattr
- -n <name>
- -v <value>
- -x <name>

Access Control Lists

Commands:

- setfacl -m u:lisa:r filename
- setfacl -m m::rx file
- getfacl filename

LPIC-3 Exam 303: Security

327.2 Mandatory Access Control

Overview

- Understanding Mandatory Access Control
- SELinux
- MAC Alternatives

Understanding Mandatory Access Control

The Concept

- **Mandatory Access Control (MAC)** differs from Discretionary Access Control in that access is based on context and not by ownership.
- MAC uses roles and type enforcement (TE) to only allow access to users who are authorized to use resources of a specific type.
- MAC is generally implemented by means of a kernel module and through use of extended attributes.

MAC Systems

- SELinux
- AppArmor
- Smack

SELinux

Commands:

- semanage
- Setsebook, getsebool
- Restorecon
- Newrole
- sealert

Files:

- /etc/selinux/config

MAC Alternatives

AppArmor

- Popular in Ubuntu.
- Known for being less cumbersome to manage than SELinux.
- Works by assigning types to file paths rather than inodes.
- Two modes: Enforcement or Complain.
- The commands `aa-genprof` and `aa-logprof` are used to craft policies.

Smack

- Must be compiled into the kernel.
- Uses extended file attributes for label assignment.
- Uses `-Z` flag like SELinux.
- The `chsmack` command may be used to query and set label information.

LPIC-3 Exam 303: Security

327.3 Network File Systems

Overview

- NFSv4 Improvements
- NFS in Practice
- Understanding NFSv4 ACLs
- CIFS Configuration

NFSv4 Improvements

Access Security

- Kerberos Authentication is built into NFSv4, allowing enhanced security.
- Requires use of additional services to run and tap into GSS (Generic Security Services) API.
- GSS API manages the use of LIPKEY and SPKM public authentication methods.

Pseudo File System

- Allows mounting many exports via parent directory.

Port Mapper Not Required

- NFSv4 may use TPC which eliminates need the for port mapper.

NFS in Practice

Packages:

- nfs
- nfs-utils

Files:

- /etc/exports
- /etc/idmapd.conf

Commands:

- showmount -e

NFSv4 ACLs

Commands:

- nfs4_setfacl
- nfs4_getfacl

CIFS Configuration

Samba

- Popular software suite designed for inter-operation with a Windows domain.
- `smbd` and `nmbd` daemons present file shares for windows hosts.
- CIFS in particular maps windows logins to Linux logins and is part of the Samba suite.
- LPIC-3 303 focuses on security details around CIFS.

Winbind

- Service that allows a CIFS server to integrate with an AD domain.
- Must run the `winbind` daemon.
- May integrate with NSS via the winbind service.
- May integrate with the system login via `pam_winbind`.

CIFS

Commands:

- getcifsacl
- setcifsacl
- mount.cifs

Files:

- /etc/samba/smb.conf

LPIC-3 Exam 303: Security

328.1 Network Hardening

Overview

- FreeRADIUS
- Network Utilities
- Network Threats

FreeRADIUS

Packages:

- freeradius

Files:

- /etc/raddb/radiusd.conf
- /etc/raddb/*

Commands:

- radmin
- radtest
- radwho
- radlast

Network Utilities

Wireshark

- A GUI tool that can perform packet captures
- Provides filtering capability
- Optionally can be ran using tshark CLI utility.
- Be familiar with filters

tcpdump

- A classic CLI utility for capturing network traffic
- Capable of filtering

Capturing Network Traffic

Commands:

- tshark
- tcpdump

Filters:

- host IP
- port PORT
- portrange PORT-PORT
- tcp portrange PORT-PORT

Network Utilities

ndpmon

- Neighbor Discovery Protocol Monitor
- Compiled versions available for BSD, OSX, and Debian
- Used for monitoring ICMPv6 packets
- Writes output to syslog

nmap

- Network Mapper tool
- A utility capable of doing various scans against target networks

nmap

Commands:

- nmap

options:

- -sS
- -T#
- -sN / -sF / -sX

Network Threats

Rogue Router Advertisements

- This is a problem on IPv6 networks where malicious router advertisements may be used to hijack traffic on unsecured networks.
- It can be mitigated by adjusting your kernel to not accept router advertisements:
  - /proc/sys/net/ipv6/conf/<interface>/forwarding
  - /proc/sys/net/ipv6/conf/<interface>/accept_ra

Rouge DHCP Messages

- This is an issue that is best dealt with at the switch level.
- DHCP traffic should be restricted to solely the switch port running the DHCP server that is trusted.
- This is done using DHCP snooping.

LPIC-3 Exam 303: Security

328.2 Network Intrusion Detection

Overview

- Network Monitoring
- Working with Snort
- OpenVas and NASL

Network Utilities

Ntop

- A network traffic probe that provides network usage information.
- To start daemon: `ntop -P /etc/ntop -w4242 -d`
- Reset `ntop` admin password: `ntop --set-admin-password=newpassword`

Cacti

- Another network monitoring tool
- Known for graphic functionality
- More general purpose than `ntop`

Snort

Packages:

- snort
- daq

Files:

- /etc/snort/*

Commands:

- snort
- snort-stat

OpenVAS and NASL

Commands:

- openvas-mkcert
- openvas-nvt-sync

Files:

- /etc/openvas/openvasd.conf

LPIC-3 Exam 303: Security

328.3 Packet Filtering

Overview

- Firewall Review
- Advanced Firewall Concepts
- Nftables

Firewall Review

Files:

- /etc/sysconfig/iptables

Commands:

- iptables
- ip6tables
- Iptables-save
- Iptables-restore

Advanced Firewall Concepts

IP Sets

- Depending on the type of the set, an IP set may store:
  - IP (v4/v6) addresses
  - (TCP/UDP) port numbers
  - IP and MAC address pairs
  - IP address and port number pairs
- The **ipset** command is used to create and work with IP Sets
- Netfilter is able to use the IP Sets

Firewall DMZ

- Provides additional security for a network
- It is a subnet that is separate from a general LAN
- May be accessed by an external network
- Where services and hosts that require a public face are located on a network
- Typically, the internal LAN is firewalled off from external network access

IP Sets

Files:

- /etc/sysconfig/ipset

Commands:

- ipset create
- ipset add
- ipset save
- ipset list

Advanced Firewall Concepts

Connection Tracking

- Used so that the firewall may track a connection state
- The **conntrackd** daemon does the tracking

Network Address Translation

- Used to load balance service or to translate external to internal addresses
- Handled by firewalls and/or routers
- Makes use of the nat tables in **iptables** and the OUTPUT, PREROUTING and POSTROUTING chains

Network Address Translation

Table:

- nat

Chains:

- OUTPUT
- PREROUTING
- POSTROUTING

Advanced Firewall Concepts

Ebtables

- Used to insert and filter Ethernet frames
- Mostly analogous to the **iptables** command except it works specifically with ethernet frames
- Defaults chains:
  - filter
  - broute
  - nat
- Specific options to ebtables
  - `-Ln` — List line numbers when printing a rule set
  - `-Lc` — List packet and byte counters with each rule

Nftables

The Concept

- An alternative to iptables.
- Aims to provide a simpler interface to netfilter.
- Use the nft command to interact with nftables.
- May use iptables rules but supports a more plain language rule set.
- Only brief familiarity required for the exam.

LPIC-3 Exam 303: Security

328.4 Virtual Private Networks

Overview

- OpenVPN
- Working with IPSec Server and Clients

OpenVPN

Files:

- /etc/openvpn/server.con

Commands:

- openvpn --mlock
- openvpn --push

Working with IPSec Server and Clients

The Concept

- IPSec is used to create a peer to peer secure connection
- Configurations reside /etc/ipsec-tools.conf
- The Kernel maintains two databases for IPSec:
  - Security Association Database:
    - A **Security Association (SA)** describes how entities will use security services to communicate
    - SAD entries contain the key of each IPSec-SA
  - Security Policy Database:
    - Used to determine if IPSec applies to a given packet
    - Also determines how an IPSec Security Association applies to a packet
  - The **setkey** utility may add, update, dump, or flush SAD or SPD entries in the kernel

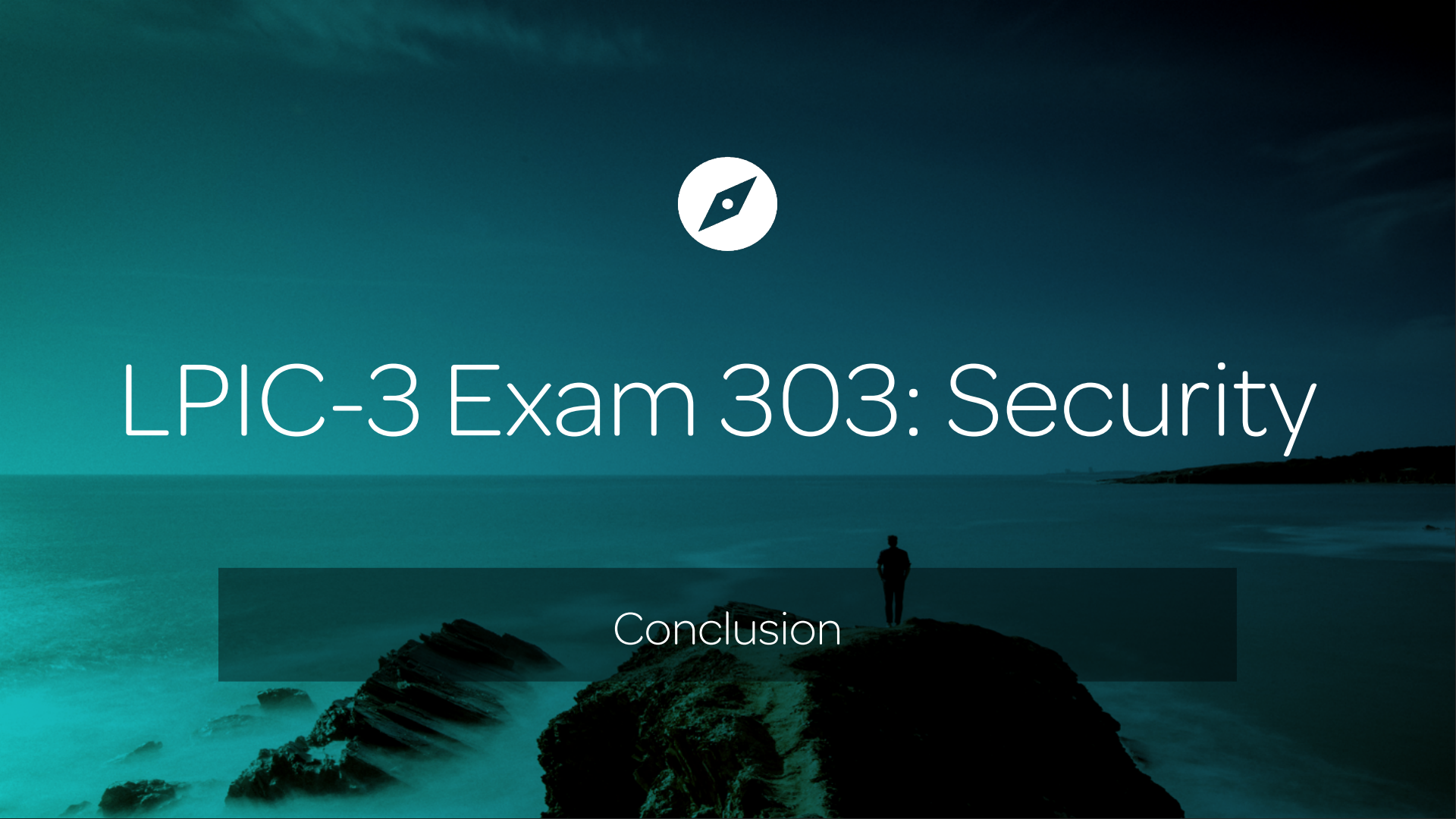
Working with IPSec Server and Clients

Notable setkey directives

- The following are directives that may be used to manipulate the SAD:
  - `add`
  - `get`
  - `delete`
  - `flush`
  - `Dump`
- The directives may be prefaced with '`spd`' (ie `spdadd`) and will work for the SPD.

Racoon and L2TP

- Racoon is an IKEv1 keying daemon.
  - The daemon is configured via `/etc/racoon/racoon.conf`
- L2TP is a VPN technology.
  - By itself, it is insecure.
  - It must be used over an IPSec link due to this.



LPIC-3 Exam 303: Security

Conclusion

Overview

- Exam Review
- Scheduling and Taking the Exam
- After Certification

Exam Review

LPIC-3 303-200

- It is a broad test!
- It hits on commands, options, and configurations particularly hard
- Be able to reliably pass the course practice exam by a wide margin
- Drill the flash cards
- Learning Activities
- Syntax and capitalization are important!

Scheduling and Taking the Exam

LPIC-3 303-200

- Purchase a voucher through the Linux Professional Institute (link in video description).
- Use the Linux Academy discount code (also noted in the video description)!
- The exam is 60 questions and you are given 90 minutes to complete it.
- Most questions are multiple choice.
- Some questions are fill-in-the-blank.

After Certification

Wondering what to study now?

- LPIC3-304 Virtualization
- RHCE / RHCA
- Certified Ethical Hacker