1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCP Wrappers

Finding files with SUID/SGID bit se

Verify Pack

Passwords and Aging

Update binaries with

Basic intro to

References

icense Of This

1.114.1

Perform security administration tasks Weight 4

Linux Professional Institute Certification — 102

Nick Urbanik <nicku@nicku.org>
This document Licensed under GPI —see section ??

2005 November

| Context Objectives Configuring TCP Wrappers Rules for hosts.allow, hosts.deny Format of rules in hosts.{allow, deny} Example Wildcards Patterns Option Fields: Logging EXCEPT operator How is TCP Wrappers enabled? Finding files with SUID/SGID bit set Effect of SUID/SGID permissions | Verify Packages Why Verify Software Packages? Verify Package Files with rpm Verify Installed Packages with rpm Verify Packages with apt/dpkg Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and ipchains iptables tables iptables chains Examples of filtering Viewing firewall rules |
|--|---|
| Specifying Permissions to | Saving and restoring rules |
| find | Reterences |

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Finding files with

erify Package

asswords and Aging afternation

Update binaries with security alerts

Basic intro to iptables and ipchains

References

Document

Topic 114 Security [8] Where we are up to

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCF Wrappers

Finding files with SUID/SGID bit se

Verify Pack

Passwords and Aging

Update binaries with

Basic intro to iptables and

References

License Of This

1.114.1 Perform security administration tasks [4]

- 1.114.2 Setup host security [3]
- 1.114.3 Setup user level security [1]

Candidates should know how to review system configuration to ensure host security in accordance with local security policies. This objective includes how to configure TCP wrappers, find files with SUID/SGID bit set, verify packages, set or change user passwords and password aging information, update binaries as recommended by CERT, BUGTRAQ, and/or distribution's security alerts. Includes basic knowledge of ipchains and iptables.

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCI Wrappers

inding files with

erify Packages

asswords and Agir

formation

Basic intro to

iptables **an** ipchains

References

License Of This Document 1.114.1 Perform security administration tasks [4]

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

ontext

Objectives

Wrappers

SUID/SGID bit se

/erify Packages

Passwords and Aging

Update binaries with security alerts

Basic intro to

References

License Of This

/proc/net/ip_fwchains — Firewall chain linkage (2.2 kernel)

/proc/net/ip_masquerade — Major
 masquerading table (2.2 kernel)

find — We see how to find SUID and SGID programs using find

ipchains — The tool to configure the firewall on a 2.2 kernel

passwd — Discuss how to use to set password aging information

socket — The end point of a network connection iptables — The tool to configure the firewall on a 2.4, 2.6 kernel

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Obiective:

Wrappers

Rules for hosts.allow, hosts.deny

hosts. {allow, de

Wildcards

Patterns
Option Fields: Logging
EXCEPT operator

How is TCP Wrappers mabled?

inding files with UID/SGID bit se

Verify Packages

Passwords and Aging

lpdate binaries w

Basic intro to

References

License Of T

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow,

hosts.deny

Format of rules in

hosts.{allow,deny}

Example

Wildcards

Patterns

Option Fields: Logging

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

Verify Installed Packages with:

Verify Packages with apt/dpkg

Passwords and Aging Information
Update binaries with security alerts
Basic intro to iptables and

ipchain

iptables tables iptables chains

Examples of filtering Viewing firewall rules

Saving and restoring rule

References

License Of This Documer

Rules for hosts.allow, hosts.deny

- Search stops at the first match in this sequence:
- Access will be granted when a (daemon, client) pair matches an entry in the /etc/hosts.allow file.
- Otherwise, access will be denied when a (daemon, client) pair matches an entry in the /etc/hosts.deny file.
- Otherwise, access will be granted.

1.114.1

Perform security administration tasks Weight 4

Nick Hrhanik

Rules for hosts.allow. hosts.deny



More about how tcp_wrappers rules applied

► Because access rules in hosts.allow are applied first, they take precedence over rules specified in hosts.deny.

Therefore, if access to a service is allowed in hosts.allow, a rule denying access to that same service in hosts.deny is ignored.

- ► The rules in each file are read from the top down and the first matching rule for a given service is the only one applied. The order of the rules is extremely important.
- ► If no rules for the service are found in either file, or if neither file exists, access to the service is granted.
- changes to hosts.allow or hosts.deny take effect immediately without restarting network services.

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Context

Objectives

Configuring TCI

Rules for hosts.allow, hosts.deny

Format of rules in

/ildcards

atterns ption Fields: Loggi

EXCEPT operator

How is TCP Wrap

Penabled?

nding files with JID/SGID bit se

erify Packages

Passwords and Agii

Jpdate binaries v

asic intro to ptables and

References

License Of Th Document



1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objective

Configuring TCP Wrappers

Rules for hosts.allow

Format of rules in hosts.{allow,deny}

Example Wildcards

Patterns
Option Fields: Loggin

How is TCP Wrapper enabled?

inding files with

Verify Packages

Passwords and Aging

pdate binaries v

Basic intro to iptables and

References

License Of The Document

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow, hosts.denv

Format of rules in hosts. {allow, deny}

Example Wildcards

Patterns

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm

Verify Packages with apt/dpkg asswords and Aging Information lodate binaries with security alerts

ipchains

iptables tables iptables chains Examples of filtering Viewing firewall rules Saving and restoring ru

References

License Of This Documen

Format of rules in hosts. {allow, deny}

► Each rule is of the form:

```
\langle daemon \ list \rangle: \langle client \ list \rangle [: \langle option \rangle: \langle option \rangle: ...]
```

(daemon list) A comma separated list of process names (not service names) or the ALL wildcard — see § ??.

The daemon list also accepts the EXCEPT operator to allow greater flexibility — see § ??

(client list) A comma separated list of hostnames, host IP addresses, special patterns — see § ??, or special wildcards — see § ?? — which identify the hosts effected by the rule. You can also use the EXCEPT operator.

⟨option⟩ An optional action or colon separated list of actions performed when the rule is triggered. Option fields support % expansions — see \$ man 5 hosts_access ← , launch shell commands, allow or deny access, and alter logging behavior — see § ??

1.114.1

Perform security administration tasks Weight 4

Nick Urbanik

Context

Dojectives Confiaurina TCF

Rules for hosts.allow

Format of rules in hosts.{allow,deny}

Example Wildcards

Option Fields: Loggin EXCEPT operator

enabled? Finding files with

Verify Packages

asswords and Ag

odate binaries wi

ecurity alerts

Basic intro to iptables and ipchains

References

License Of Th Document

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Conte

Objective:

Configuring TCP Wrappers

Rules for hosts.allow

Format of rules in

Example

Wildcards Patterns

Option Fields: Loggin EXCEPT operator

inding files with

Verify Package

Passwords and Agir

lpdate binaries wit

Basic intro to

iptables **an** ipchains

References

License Of To Document

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow hosts.deny
Format of rules in
hosts.(allow.deny)

Example

Wildcards

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permission Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?
Verify Package Files with room

Verify Installed Packages with rp

verify Packages with apt/dpkg asswords and Aging Information

Basic intro to iptables and

ipchain

iptables tables

Examples of filtering

Saving and restoring rul

References

License Of This Documen

Example rule

vsftpd : .example.com

- ▶ watch for connections to the FTP daemon (vsftpd) from any host in the example.com domain.
- ▶ If this rule appears in hosts.allow, the connection is accepted.
- ▶ If this rule appears in hosts.deny, the connection is rejected.

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objectives

onfiguring TCP /rappers

Rules for hosts.allow, hosts.deny

ormat of rules in

Example

Vildcards

atterns

CEPT operator

inding files with

UID/SGID bit s

erify Packages

asswords and Agir

date binaries wi

asic intro to

References

License Of T



1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objective

Configuring TCP

Rules for hosts.allow

Format of rules in

Example

Wildcards

Wildcards Patterns Option Fields: Logg

EXCEPT operator
How is TCP Wrappers

inding files with

Verify Packages

Passwords and Agin

ndate binaries with

ecurity alerts

Basic intro to

References

License Of T Document

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow hosts.deny Format of rules in hosts.{allow,deny}

Wildcards

Patterns

Option Fields: Logging

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permission. Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm

Verify Packages with apt/dpkg

Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

ipchain

iptables chains
iptables chains
Examples of filtering
Viewing firewall rules
Saving and restoring r

References

License Of This Documen

Wildcards

Wildcards allow TCP wrappers to more easily match groups of daemons or hosts. They are used most frequently in the client list field of access rules.

The following wildcards may be used:

ALL Matches everything. It can be used for both the daemon list and the client list.

LOCAL Matches any host that does not contain a period (.), such as localhost

KNOWN Matches any IP address which has a corresponding hostname; also matches usernames when the *ident* service is available (which is usually not)

UNKNOWN Matches any IP address which does *not* have a corresponding hostname; also matches usernames when the *ident* service *not* available

PARANOID Matches any host where a double reverse hostname/IP address lookup fails to match

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Context

Objectives

Configuring T(

ules for hosts.allow

mat of rules in ts.{allow,der

fildoordo

Wildcards

Option Fields: Loggin

EXCEPT operator

How is TCP Wrapper

inding files with SUID/SGID bit se

erity Packages

Update binaries with

security alerts

Basic intro to ptables and

References

License Of TI Document

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objective

onfiguring TCP

Rules for hosts.allow,

hosts.deny
Format of rules in

Example

Wildcards Patterns

Option Fields: Logging EXCEPT operator How is TCP Wrappers

inding files with

Verify Packages

Passwords and Agi

Jpdate binaries wi

Basic intro to iptables and

References

License Of TI Document

Finding SUID or SGID files

Configuring TCP Wronners

Configuring TCP Wrappers

hosts.deny
Format of rules in
hosts.{allow,deny}
Example

Patterns

Option Fields: Logging
EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Specifying Permissions to find Why Verify Software Packages?
Verify Package Files with rpm
Verify Installed Packages with ry
Verify Packages with apt/dpkg
Passwords and Aging Information
Update binaries with security alerts
Basic intro to iptables and

iptables tables
iptables chains
Examples of filtering
Viewing firewall rules
Saving and restoring rules
iferences

eferences

License Of This Document

ALL : .example.com

▶ IP address ending with a period (.) This matches any host in the 192.168.x.x network:

ALL: 192.168.

▶ IP address/netmask pair This matches any host in the address range 192.168.0.0 ... 192.168.1.255:

ALL: 192.168.0.0/255.255.254.0

▶ Note: a pattern of the form 192.168.0.0/23 will not work

The asterisk (*) Asterisks can match entire groups of hostnames or IP addresses. This matches any host in the example.com domain:

ALL: *.example.com

 This asterisk notation is not used anywhere else as far as I know. Context

Objectives

0 - - 6 - - - - - - - -

Vrappers

osts.deny

mple

Vildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers

nding files with JID/SGID bit se

rify Packages

Passwords and Aging Information

> odate binaries w curity alerts

> sic intro to

eferences

License Of The Document

1.114.1 Weight 4

Configuring TCP Wrappers

Option Fields: Logging

Finding SUID or SGID files

Perform security administration tasks

Nick Hrhanik

Option Fields: Logging



Option Fields: Logging with severity

See \$ man 5 hosts options ← for details of other options; just look at severity directive for logging access

▶ Here, connections to the SSH daemon from any host in the example.com domain are logged to the default authpriv syslog facility (because no facility value is specified) with a level of emerg:

```
.example.com : severity emerg
sshd:
```

specifying a facility: The following example logs any SSH connection attempts by hosts from the example.com domain to the local0 facility with a level of alert:

```
.example.com : severity
local0.alert
```

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

Option Fields: Logging



1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objective

Configuring TCP

Rules for hosts.allow

hosts.deny

hosts.{all

Wildcards

Patterns

EXCEPT operator

enabled?

nding files with JID/SGID bit set

Verify Packages

Passwords and Aging

pdate binaries v

Basic intro to iptables and

References

License Of Tourish

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

hosts.{allow.denv}

Example

Wildcards

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Installed Packages with r

asswords and Aging Information

Industry binaries with security alerts

Basic intro to iptables and

ipchain

iptables tables

Examples of filtering

Viewing firewall rules

Saving and restoring i

References

License Of This Documen

EXCEPT operator

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objective

Configuring TCP

Rules for hosts.allow,

ormat of rules in

xample

ldcards tterns

atterns ption Fields: Log

EXCEPT operator

enabled?

inding files with UID/SGID bit s

/erify Packages

Passwords and Aging

odate binaries v

asic intro to

References

License Of This Document

► There is one operator: EXCEPT.

can be used in both the daemon list and the client list of a rule.

allows specific exceptions to broader matches within the same rule.

Example:

ALL: .example.com EXCEPT cracker.example.com

▶ In the another example from a hosts.allow file, clients from the 192.168.0.x network can use all services except for FTP:

ALL EXCEPT vsftpd: 192.168.0.

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objective

Configuring TCP Wrappers

Rules for hosts.allow

hosts.deny
Format of rules in

Example

Wildcards

Patterns Option Fields: Loggin

How is TCP Wrappers enabled?

Finding files with

/erify Packages

remy rackages

Passwords and Agii

odate binaries v

Basic intro to

References

License Of T Document

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

hosts.{allow,denv}

Example

Wildcards

Option Fields: Logging

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?
Verify Package Files with room

Verify Installed Packages with anti-darkages

Passwords and Aging Information
Jydate binaries with security alerts

pchain

iptables tables iptables chains

Viewing firewall rules

Saving and restoring rule

References

License Of This Documen

How is TCP Wrappers enabled?

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

Context

Objectives

Vrappers
Rules for hosts.allow

Format of rules in nosts.{allow,de

xample Vildcards

atterns ption Fields: Log

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit se

erify Packages

asswords and Agii nformation

pdate binaries v ecurity alerts

asic intro to

References

License Of This Document

Recent systems use libwrap, part of the tcp_wrappers package

▶ Red Hat suggest doing \$ strings -f ⟨binary-name⟩ | grep hosts_access ← to see if a program is compiled with libwrap.

► Most programs are dynamically linked against /usr/lib/libwrap.so.0, so you can check for that with \$ 1dd ⟨binary-name⟩ ←

Example:

```
$ /usr/sbin/xinetd | grep libwrap ←
    libwrap.so.0 => /usr/lib/libwrap.so.0 (0x00320000)
```

➤ Older systems used /usr/sbin/tcpd and entered this in /etc/inetd.conf instead of the binary name of the service, but this is no longer necessary

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objectives

Configuring TCP
Wrappers

Finding files with

Effect of SUID/SGID permissions

Specifying Permissions to find

Verify Packages

Passwords and Aging

Update binaries with

ecurity alerts

Basic intro to iptables an ipchains

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm

Verify Installed Packages with my Verify Packages with apt/dpkg

Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

ipchain

iptables tables iptables chains Examples of filtering Viewing firewall rule:

References

License Of This Documen

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow hosts.denv

hosts (allow don

Example

Wildcards

Option Fields: Logging

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions

<ロ > < @ > < き > < き > ・ き · りへ(~)

Objectives

Finding files with

Effect of SUID/SGID

permissions Specifying Permissions

find

Jorify Packages

Passwords and Ad

Passwords and Aging Information

lpdate binaries wit ecurity alerts

Basic intro to

References

License Of Thi

A program with Set User-ID (SUID) permission will execute with the process owned by the owner of the file instead of the user that executed the program.

- A program with Set Group-ID (SGID) permission will execute with the group of the process the same as the group of the file instead of the group of the user that executed the program.
- A serious security risk.

Some History

- ▶ A friend in UNSW in 1985 used to stay in the lab with me till 5 AM many mornings; he had root access on the PDP-11, greatly upsetting the BOFH.
- ► He told me that he gained this through a set user-ID executable owned by root.

Context

Configuring TCP

Finding files with SUID/SGID bit set

Specifying Permissions to

Finding SUID or SGID to

Deserved and Asia

Passwords and Aging Information

Jpdate binaries with

Basic intro to

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm

Verify Packages with apt/dpkg

Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

pchain

iptables tables
iptables chains
Examples of filtering
Viewing firewall rules
Saving and restoring

eferences

License Of This Documen

Context

Objectives

Configuring TCP Wrappers

Rules for hosts.allow, hosts.denv

hosts. {allow, deny

Example

Patterns

Option Fields: Logging

How is TCP Wrappers enabled

Finding files with SUID/SGID bit set

Specifying Permissions to find

Obiectives

Configuring TCP Wrappers

SUID/SGID bit set
Effect of SUID/SGID
permissions

Specifying Permissions to find Finding SUID or SGID file:

orify Bookogoo

Passwords and Aging

Jpdate binaries wit

security alerts

Basic intro to

Poforonoo

References

License Of This

- The find program finds files for which various conditions are true
- The -perm ⟨mode⟩ condition can find files which match the permissions specified in ⟨mode⟩ in various ways:
 - if ⟨mode⟩ starts with '-' then true if all of the permissions in ⟨mode⟩ are present. Any permissions not in ⟨mode⟩ are ignored
 - if \(\langle\) starts with '+' then true if \(\frac{any}{any}\) of the permissions in \(\langle\) are present. Any permissions not in \(\langle\) are ignored
 - if \(\langle mode \rangle \) starts with neither '-' nor '+' then true if permissions are exactly \(\langle mode \rangle \).
- \(mode\)\) can be specified in octal or symbolically: e.g., you can specify -perm +6000 or -perm +ug=s
 - both are true if the file has either SUID or SGID permission set.

Context

OUTILOAL

Configuring TCP

Finding files with SUID/SGID bit set

permissions
Specifying Permissions 1

find

Finding SUID or SGID files

rify Packages

Passwords and Aging

Information Undate binaries with

Jpdate binaries w ecurity alerts

Basic intro to iptables an ipchains

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm

Verify Packages with apt/dpkg

Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

ipchain

iptables tables
iptables chains
Examples of filtering
Viewing firewall rule

References

References

License Of This Document

Contex

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Wildcards

Option Fields: Logging

How is TCP Wran

How is TCP Wrappers enabled

Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions Specifying Permissions to find

finding SUID or SGID files

► Here we can search the entire file system for SUID or SGID files: \$ find / -perm +6000 -ls ←

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Contex

Objectives

Configuring TCF Wrappers

SUID/SGID bit set

Effect of SUID/SGID
permissions

Specifying Permissions to

Finding SUID or SGID files

ify Packages

Passwords and Aging

Update binaries with

security alerts

otables **an** ochains

References

License Of This



1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objectives

Finding files with

SUID/SGID bit se

Verify Package

Why Verify Software Packages?

Verify Package Files with

Verify Installed Packag with rpm

Verify Packages with

apt/dpkg

Information

Update binaries with security alerts

Basic intro to iptables and ipchains

References

License Of Thi Document

Finding SUID or SGID files Verify Packages

Why Verify Software Packages?

Verify Installed Packages with r Verify Packages with apt/dpkg Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

iptables tables
iptables chains
Examples of filtering
Viewing firewall rules
Saving and restoring rules
eferences

License Of This Docume

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Wildcards

Patterns

Option Fields: Logging

How is TCP Wranners enal

Finding files with SUID/SGID bit set

Specifying Permissions to find

Why Verify Software Packages? Main reasons:

- As another tool to check whether trojan executables have been installed by a cracker, replacing the original binary
- As a check that software downloaded from the Internet is from a trusted source and has not been compromised

1.114.1 Perform security

administration tasks Weight 4

Nick Hrhanik

Why Verify Software Packages?

Conte

Objective:

Configuring TCP Wrappers

Finding files with SUID/SGID bit se

/erify Packages Why Verify Software

Packages? Verify Package Files with rpm

Verify Installed Packag with rpm

With rpm
Verify Packages with
apt/dpkq

Passwords and Agii Information

Update binaries with

Basic intro to iptables and

References

License Of Thi

Finding SUID or SGID files Verify Packages

Why Verify Software Packages

Verify Package Files with rpm

Verify Packages with apt/dpkg
Passwords and Aging Information
Update binaries with security alerts
Basic intro to iptables and

iptables tables
iptables chains
Examples of filtering
Viewing firewall rules
Saving and restoring rules
eferences

License Of This Docume

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny}

Example

Wildcards

Patterns

Option Fields: Logging

How is TCP Wrappers enabled

Finding files with SUID/SGID bit set Effect of SUID/SGID permission

Specifying Permissions to find

SUID/SGID bit set

Verify Package Files with

- Ensure have the GPG key of the signer of the software packages, e.g.,
 - \$ sudo rpm --import /media/cdrom/RPM-GPG-KEY*
- Verify that each downloaded software package is signed before installing it: with yum, use the option gpgcheck=1
- ▶ If you have the RPM binary package file, you can check its signature with:
 - \$ rpm -K ⟨complete-package-file-name⟩ ←
- Example:
 - \$ rpm -K httpd-2.0.54-10.2.i386.rpm ← httpd-2.0.54-10.2.i386.rpm: (sha1) dsa shal md5 qpq OK

Verify Installed Packages

with rpm

Finding SUID or SGID files Verify Packages

Verify Installed Packages with rpm

Verify Installed Packages with rpm

- ▶ Do \$ rpm -V ⟨package-name⟩ ←
- ► Ensure that no binary executables have changed; here is an example of an executable that does not match the original installed version: \$ rpm -V spamassassin ← S.5....T /usr/bin/spamc
- This indicates that the size, the MD5sum and the timestamp have changed of this executable file, and it could quite possibly be a trojan
- There are eight characters; a dot indicates original value, a letter shows there is change:
- S file Size differs
- M Mode differs (includes permissions and file type)
- 5 MD5 sum differs
- D Device major/minor number mismatch
 - readLink(2) path mismatch
- U User ownership differs
 - Group ownership differs
- T mTime differs

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Context

Objective

Configuring

Finding files wit SUID/SGID bit

erify Packages

/hy Verify Software ackages? erify Package Files wi

rpm Verify Installed Packages

with rpm
Verify Packages with

erify Packages with pt/dpkg

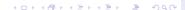
asswords and Agin Iformation

date binaries v curity alerts

asic intro to

References

License Of Thi Document



Objective

Configuring TCP

Finding files with

Verify Packages

Why Verify Software Packages? Verify Package Files with

Verify Installed Packag with rpm

Verify Packages with apt/dpkg

Passwords and Aging Information

Update binaries wi

Basic intro to iptables and

Reference

License Of This

Finding SUID or SGID files Verify Packages

Why Verify Software Packages? Verify Package Files with rpm Verify Installed Packages with rpm

Verify Packages with apt/dpkg Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

iptables tables iptables chains Examples of filtering Viewing firewall rule

References

License Of This Documen

Contex

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny}

Example

Wildcards

Option Field

EXCEPT operator

How is TCP Wranne

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set
Effect of SUID/SGID permission

Specifying Permissions to find

Verify Packages with apt/dpkg

- ► To be done.
- ► There is a way...

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Contex

Objective:

Configuring TCF Wrappers

Finding files with SUID/SGID bit se

erify Packages Vhy Verify Softwar

Packages? /erify Package Files w

rpm Verify Installed Packages

ith rpm

Verify Packages with

asswords and Agin

odate binaries wit

asic intro to

References

License Of Th Document

Password Aging

- ► Limiting the age of passwords can improve security, although users may ping-pong between two passwords
- ▶ Best not to force users to change more than once every few months (page 607, [Gar2003]), else some will write them down

1.114.1 Perform security

administration tasks Weight 4

Nick Urbanik

Context

Objective:

Configuring TCP Vrappers

Finding files with SUID/SGID bit se

erify Packa

Passwords and Aging

Update binaries with

Basic intro to iptables an

eferences

icense Of This

Password Aging options to passwd

- -d This is a quick way to disable a password for an account. It will set the named account passwordless. Available to root only.
- -n This will set the minimum password lifetime, in days, if the user's account supports password lifetimes. Available to root only.
- -x This will set the maximum password lifetime, in days, if the user's account supports password lifetimes. Available to root only.
- —w This will set the number of days in advance the user will begin receiving warnings that her password will expire, if the user's account supports password lifetimes. Available to root only.
- -i This will set the number of days which will pass before an expired password for this account will be taken to mean that the account is inactive and should be disabled, if the user's account supports password lifetimes. Available to root only.

1.114.1

Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Finding files wi SUID/SGID bit

erify Pack

Passwords and Aging Information

Update binaries with security alerts

Basic intro to iptables and ipchains

References

License Of Thi Document

Finding out about security alerts

- The best way to get cracked is to never apply security updates on a machine exposed to the Internet
- Subscribe to the mailing list for your distribution that announces security updates
- Subscribe to http://lwn.net and read their comprehensive security information, in particular from http://lwn.net/security

1.114.1 Perform security

administration tasks Weight 4

Nick Hrhanik

Update binaries with security alerts

Objectives

Configuring TCP Wrappers

SUID/SGID bit

erify Packa

Passwords and Ag

Update binaries with security alerts

Basic intro to iptables and inchains

References

License Of This

- ➤ You can either apply updates automatically: with systems with yum installed, enable yum updates in cron.
- ▶ To update a system with yum:
 - \$ sudo yum -y update \hookleftarrow
- To update a system with apt:
 - \$ sudo apt-get update ←
 - \$ sudo apt-get -y upgrade \hookleftarrow
- If the system is mission critical and especially if it has complex software installed, install updates on a test system first

indina files with

SUID/SGID bit s

erify Pack

Passwords and Agin

Update binaries with

Basic intro to iptables and

iptables tables
iptables chains
Examples of filtering
Viewing firewall rules

iewing firewall rules aving and restoring ru

References

License Of This

 Used to filter network packets coming into, out of and through the system

- Very useful for network security, Internet connection sharing
- ▶ iptables on 2.4, 2.6 kernels, ipchains on 2.2 kernels
- ▶ iptables is easier to use than ipchains
 - Many more things must be considered before you can predict what will happen to a packet passing through an ipchains system, while iptables tends to have a packet dealt with in one spot only, causing less brain pain.
- iptables has support for stateful inspection which allows the system to remember which response is in answer to which packet

Components of iptables

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

Context

Objectives

Vrappers

Finding files wit SUID/SGID bit :

erify Pack

Passwords and Agir

Update binaries with security alerts

Basic intro to iptables and ipchains

iptables tables
iptables chains

/iewing firewall rules

References

icense Of This

► There are four main terms to consider with iptables:

table — a table holds a major category of set of rules.

chain — sets of rules within a table that affect traffic

rule — decides how to send a packet to a target. Next rule checks a packet if this doesn't match.

target — can be ACCEPT, DROP, QUEUE, or RETURN. A matched packet is accepted, dropped, queued on another chain or returned to the parent chain from the current chain.

Nick Hrhanik

iptables tables

Finding SUID or SGID files

Basic intro to iptables and ipchains

iptables tables

iptables tables

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

/rappers

SUID/SGID bi

erify Packa

Passwords and Aging

Update binaries wire security alerts

Basic intro to iptables and ipchains

iptables tables

ptables chains examples of filtering fiewing firewall rules

eferences

License Of This

► There are three *tables* used by iptables:

filter — default table for handling network packets

nat — used to alter packets that create a new connection and used for Network Address Translation (NAT).

mangle — for specific types of packet alteration, including time to live, type of service — for special routing purposes

Contex

Obiectives

Configuring TCP

Finding files with

Verify Packages

Passwords and Aging

Update binaries with

Basic intro to iptables and

pchains

iptables **table**

iptables chains

/iewing firewall rules

Saving and restoring i

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages? Verify Package Files with rpm Verify Installed Packages with rpm

Verify Packages with apt/dpkg Passwords and Aging Information

Basic intro to iptables and ipchains

ipchains

iptables tables iptables chains

Examples of filtering

Viewing firewall rules

eferences

License Of This Documer

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Patterns

Option Fields: Logging

How is TCP Wranners er

Finding files with SUID/SGID bit set

Specifying Permissions to find

iptables filter chains

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

Context

Objective

Configuring TCP Wrappers

Finding files with SUID/SGID bit s

erify Packa

asswords and Agii

Update binaries with

Basic intro to iptables and ipchains

ptables **tab**l

iptables chains

camples of filtering

iewing firewall rules

leferences

License Of This

iptables filter table has three chains:
 INPUT for packets coming into the system, destined for the system itself
 OUTPUT for packets originating from the system, destined for outside the system
 FORWARD for packets entering the system that are meant for other systems on the other side,

where the system is working as a router

Outline

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objectives

Configuring TCP Wrappers

Finding files with

Verify Packages

Passwords and Aging

Update binaries with

Basic intro to iptables and inchains

pchains ptables tables

ptables tables

ptables chains

Examples of filtering

Viewing firewall rules

References

License Of This

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Wildcards

Patterns

Option Fields: Logging

How is TCP Wrappers enable

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions

Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm
Verify Installed Packages with rpm

Passwords and Aging Information

Basic intro to iptables and ipchains

iptables tables iptables chains

Examples of filtering

Viewing firewall rules
Saving and restoring rule

References

License Of This Documer

Examples of filtering

To drop all traffic to this machine from the source IP address 1.2.3.4, do:

\$ sudo iptables -A INPUT -s 1.2.3.4 -j DROP \hookleftarrow

➤ You might do that if there is nuisance traffic from that remote machine.

1.114.1

Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCP Vrappers

Finding files with SUID/SGID bit se

/erify Packa

Passwords and Aging

Update binaries with

Basic intro to

tables **and** chains

ables chains

Examples of filtering

/iewing firewall rules

References

License Of Th

iptables nat chains

► The built-in chains for the nat table:

PREROUTING — Alters network packets when they arrive

OUTPUT — Alters locally-generated network packets before they are sent out

POSTROUTING — Alters network packets before they are sent out

1.114.1

Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCP Vrappers

Finding files with SUID/SGID bit se

Verify Pacl

Passwords and Aging

Update binaries with

Basic intro to iptables an

tables tables

Examples of filtering

xamples of filtering iewing firewall rules

Saving and restoring rule

References

License Of This

Outline

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Contex

Objectives

Finding files with

SUID/SGID bit se

Verify Packages

Passwords and Aging Information

Update binaries with

Basic intro to iptables and inchains

pchains
iptables tables

ptables **chains**

Viewing firewall rules

Saving and restoring re

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?
Verify Package Files with rpm
Verify Installed Packages with rp
Verify Packages with packages with rp

Passwords and Aging Information
Update binaries with security alerts

Basic intro to iptables and ipchains

iptables tables iptables chains

Viewing firewall rules

Saving and restoring rules
References

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Wildcards

Patterns

Option Fields: Logging

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions

Specifying Permissions to find

Finding files with SUID/SGID bit s

Verify Pac

Passwords and Aging Information

Update binaries wit

Basic intro to iptables and ipchains

ptables tables
ptables chains

Viewing firewall rules

oaving and restorn

References

License Of This

▶ To see the firewall rules for the filter table, do:

\$ iptables -L ←

► To avoid the time to look up each IP address, do:

\$ iptables -L -n ←

To see the counters of the number of packets for each rule: \$ iptables -L -n -v ←

▶ To see the exact counters of the number of packets:

\$ iptables -L -n -v -x \hookleftarrow

➤ To view the rules for the nat table without the DNS lookup delay:

\$ iptables -t nat -L -n \hookleftarrow

➤ To view the rules for the mangle table without the DNS lookup delay:

\$ iptables -t mangle -L -n ←

1.114.1 Perform security

administration tasks Weight 4

Nick Hrhanik

Use masquerade where the external Internet address is changed by the ISP:

- ▶ iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o ppp0 -j MASQUERADE
- This is source Network Address Translation where the external address is changing.
- Where the Internet address is fixed, use the SNAT target:
- ▶ iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o ppp0 -j SNAT --to-source 220.233.65.75

Viewing firewall rules

Outline

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Configuring TCP

Finding files with

Verify Packages

Passwords and Aging

Update binaries with

Basic intro to iptables and

ptables **and** pchains iptables **tables**

ptables tables ptables chains examples of filtering

Saving and restoring rules

References

License Of This

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?
Verify Package Files with rpm
Verify Installed Packages with rp
Verify Packages with apt/dokg

Passwords and Aging Information Update binaries with security alerts Basic intro to iptables and

ipchains

iptables tables iptables chains Examples of filtering Viewing firewall rules

Saving and restoring rules

References License Of This Documer

Context

Objectives

Configuring TCP Wrappers

hosts.deny

Format of rules in

hosts.{allow,deny

Example

Wildcards

Option Fields: Logging

How is TCP Wrappers enabled

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions Specifying Permissions to find

Saving and restoring rules

- ▶ the iptables-save command saves the rules;
- ▶ iptabels-restore reads them back in from a file.
 - ► On Debian, need redirect to/from a file
 - ► Red Hat/Fedora systems store them in /etc/sysconfig/firewall

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

Context

Objectives

Configuring TCF Wrappers

Finding files with SUID/SGID bit se

Verify Pack

Passwords and Aging

Update binaries with

Basic intro to iptables and

ptables tables
ptables chains
examples of filtering

Saving and restoring rules

References

License Of Th



Perform security administration tasks I

Resources of interest

The /proc Filesystem

in Documentation/filesystems/proc.txt with Linux Kernel source



Red Hat. Inc.

Red Hat Enterprise Linux 4: Reference Guide

Chapter 17: TCP Wrappers and xinetd http://www.redhat.com/docs/manuals/

enterprise/RHEL-4-Manual/ref-guide/

ch-tcpwrappers.html

Chapter 18: iptables

http:

//www.redhat.com/docs/manuals/enterprise/ RHEL-4-Manual/ref-guide/ch-iptables.html

Simson Garfinkel, Gene Spafford and Alan Schwartz. Practical Unix and Internet Security O'Reilly 2003.

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

References

Perform security administration tasks II

Resources of interest



Info node: Find Permissions

\$ info '(find)Permissions' \hookleftarrow

\$ info '(find)File Permissions' \hookleftarrow

rpm man page

\$ man rpm ←
and search for VERIFY OPTIONS

Eric Foster-Johnson.

RPM Guide

http://fedora.redhat.com/docs/drafts/
rpm-quide-en/

1.114.1 Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectives

Configuring TCP Wrappers

Finding files with SUID/SGID bit set

Verify Pack

Passwords and A

Update binaries with

Basic intro to

References

License Of This

```
Topics Covered
Context
Objectives
Configuring TCP Wra
Rules for hosts.
Format of rules in
Example
Wildcards
Patterns
```

.deny w,deny}

abled? bit set

issions find

ackages? ith rpm

1 apt/dpkg

administration tasks Weight 4 Nick Urbanik

1.114.1

Perform security

Context

Jointont

nfiguring TCF

ding files with ID/SGID bit set

words and Agi

odate binaries w curity alerts

sic intro to tables and chains

References

ense Of This sument

```
Topics Covered
                                                                                           Perform security
                                                                                          administration tasks
 Context
                                                                                            Nick Hrhanik
 Objectives
                                                                                         References
```

4 日) 4 間) 4 目) 4 目) 耳

1.114.1

Weight 4

```
Topics Covered
 Context
 Objectives
```

Configuring TCP Wrappers

Perform security administration tasks Weight 4 Nick Hrhanik

1.114.1

References

イロト イ押ト イヨト イヨト 一選 一

```
Topics Covered
 Context
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
```

イロト イ押ト イヨト イヨト 一選 一

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

References

```
Topics Covered
                                                                           Perform security
                                                                          administration tasks
 Context
                                                                             Weight 4
                                                                            Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
     Rules for hosts.allow, hosts.deny
     Format of rules in hosts. {allow, deny}
                                                                          References
```

1.114.1

```
Topics Covered
                                                                           Perform security
                                                                          administration tasks
 Context
                                                                             Weight 4
                                                                            Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
     Rules for hosts.allow, hosts.deny
     Format of rules in hosts. {allow, deny}
     Example
                                                                         References
```

1.114.1

```
Topics Covered
                                                                          Perform security
                                                                         administration tasks
 Context
                                                                            Weight 4
                                                                           Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
     Rules for hosts.allow, hosts.deny
     Format of rules in hosts. {allow, deny}
     Example
    Wildcards
                                                                         References
```

1.114.1

```
Topics Covered
                                                                         Perform security
                                                                        administration tasks
 Context
                                                                          Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
     Rules for hosts.allow, hosts.deny
     Format of rules in hosts. {allow, deny}
     Example
    Wildcards
    Patterns
                                                                       References
```

1.114.1

Weight 4

Nick Hrhanik

References

Nick Hrhanik

References

Nick Hrhanik

References

Nick Hrhanik

References

How is TCP Wrappers enabled? Finding files with SUID/SGID bit set

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled? Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions

1.114.1 Perform security administration tasks Weight 4

Nick Hrhanik

References

Weight 4 Nick Hrhanik

1.114.1

Perform security

References

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled? Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions

Specifying Permissions to find

```
Topics Covered
Context
Objectives
```

Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

Format of rules in hosts. {allow, deny}

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions

Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

Verify Installed Packages with rpm

leasured and Asian Information

1.114.1 Perform security administration tasks

Weight 4
Nick Urbanik

Contex

Objective

Configuring TCI Vrappers

Finding files with SUID/SGID bit set

Verify Pac

Passwords and Agir Information

Update binaries with security alerts

asic intro to ptables and pchains

References

Document Document

Context

Objectives

Configuring TC Wrappers

Finding files with SUID/SGID bit se

Verify Pac

Passwords and Agi

Update binaries with security alerts

Basic intro to ptables and pchains

References

License Of This

Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

Format of rules in hosts. {allow, deny}

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions

Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

Verify Installed Packages with rpm

Passwords and Aging Information

Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm Verify Installed Packages with rpm Verify Packages with apt/dpkg 1.114.1 Perform security administration tasks

Weight 4

Nick Urbanik

Contex

Objective

onfiguring TCP Irappers

Finding files with SUID/SGID bit set

Verify Pac

Passwords and Agii

Update binaries with security alerts

Basic intro to ptables and pchains

References

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

License Of This Document Rules for hosts.allow, hosts.deny Format of rules in hosts. {allow, deny}

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set Effect of SUID/SGID permissions

Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

1.114.1 Perform security administration tasks

> Weight 4 Nick Hrhanik

References

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

Finding files with SUID/SGID bit se

Verify Pac

Passwords and

Update binaries with security alerts

Basic intro to ptables and pchains

References

License Of This

Objectives
Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

Format of rules in hosts. {allow, deny}

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SCID files

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

Verify Installed Packages with rpm

Verify Packages with apt/dpkg

◆ロト ◆個 ト ◆ 恵 ト ◆ 恵 ・ 夕 Q ○

References

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

Configuring TCP Wrappers

Rules for hosts.allow, hosts.deny

Format of rules in hosts. {allow, deny}

Example

Wildcards

Patterns

Option Fields: Logging

EXCEPT operator

How is TCP Wrappers enabled?

Finding files with SUID/SGID bit set

Effect of SUID/SGID permissions Specifying Permissions to find

Finding SUID or SGID files

Verify Packages

Why Verify Software Packages?

Verify Package Files with rpm

Verify Installed Packages with rpm Verify Packages with apt/dpkg

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

```
Topics Covered
                                                                      Perform security
                                                                     administration tasks
 Context
                                                                        Weight 4
                                                                       Nick Hrhanik
 Objectives
 Configuring TCP Wrappers
    Rules for hosts.allow, hosts.deny
    Format of rules in hosts. {allow, deny}
    Example
    Wildcards
    Patterns
    Option Fields: Logging
    EXCEPT operator
    How is TCP Wrappers enabled?
 Finding files with SUID/SGID bit set
    Effect of SUID/SGID permissions
                                                                    References
    Specifying Permissions to find
    Finding SUID or SGID files
 Verify Packages
    Why Verify Software Packages?
    Verify Package Files with rpm
    Verify Installed Packages with rpm
    Verify Packages with apt/dpkg
```

◆□ ▶ ◆□ ▶ ◆■ ▶ ◆□ ◆ ◆○ ◆

License Of This Document

Copyright © 2005 Nick Urbanik <nicku@nicku.org> You can redistribute modified or unmodified copies of this document provided that this copyright notice and this permission notice are preserved on all copies under the terms of the GNU General Public License as published by the Free Software Foundation—either version 2 of the License or (at your option) any later version.

1.114.1 Perform security

Perform security administration tasks Weight 4

Nick Urbanik

Context

Objectiv

Configuring TCI Vrappers

Finding files with SUID/SGID bit se

Verify Pack

Passwords and Aging

Update binaries with

Basic intro to iptables and ipchains

eferences

License Of This