

This pdf shows the installation of nmap, basic nmap operation, and saving nmap output. Remember you must have permission from the network owner before running this program. You must have non repudiation level permission.

YaST Control Center @ linux-msctc

Search

- Software
- Hardware
- System
- Network Devices
- Network Services
- Novell AppArmor
- Security and Users
- Virtualization
- Support
- Miscellaneous

Ready

Software

- Add-On Products
Install or remove add-on products
- FACTORY Update
- Media Check
- Online Update
- Online Update Configuration
- Package Search (webpin)
- Software Management

YaST Control Center @ linux-msctc

Search

- Software
- Hardware
- System
- Network Devices
- Network Services
- Novell AppArmor
- Security and Users
- Virtualization
- Support
- Miscellaneous

Ready

Software

- Add-On Products
- FACTORY Update
- Media Check
- Online Update
- Online Update Configuration
- Package Search (webpin)
- Software Management

YaST2

File Package Configuration Dependencies Options Extras Help

View Search RPM Groups Installation Summary Package Groups

nmap Search

Search in

- Name
- Keywords
- Summary
- Description
- RPM "Provides"
- RPM "Requires"
- File list

Search Mode:

Contains

Case Sensitive

Package	Summary	Installed (Availab: Size

Description Technical Data Dependencies Versions File

Cancel Accept

Search

-
-
-
-
-
-
-
-
-
-

YaST2

File Package Configuration Dependencies Options Extras Help

View Search RPM Groups Installation Summary Package Groups

nmap Search

Search in

- Name
- Keywords
- Summary
- Description
- RPM "Provides"
- RPM "Requires"
- File list

Search Mode:

Contains

Case Sensitive

Package Summary		Installed	Size
<input type="checkbox"/>	ndiff Compare Results of Nmap Scans	(5.00-7.2)	39.0 KiB
<input checked="" type="checkbox"/>	nmap Portscanner	(5.00-7.2)	5.6 MiB
<input checked="" type="checkbox"/>	zenmap A Graphical Front-End for Nmap	(5.00-7.2)	1.7 MiB

Description Technical Data Dependencies Versions File < >

zenmap - A Graphical Front-End for Nmap

zenmap is a graphical front-end for the nmap network scanner

Authors:

Fyodor <fyodor@dhp.com>

Cancel Accept

YaST2

Perform Installation

Actions performed:

Downloading nmap (download size 1.13 MB)

Downloading nmap - 563.30 kB/s (on average 356.40 kB/s) (download size 1.13 MB)

48%

Installing Packages...

0%

Help Abort Back Next

Search

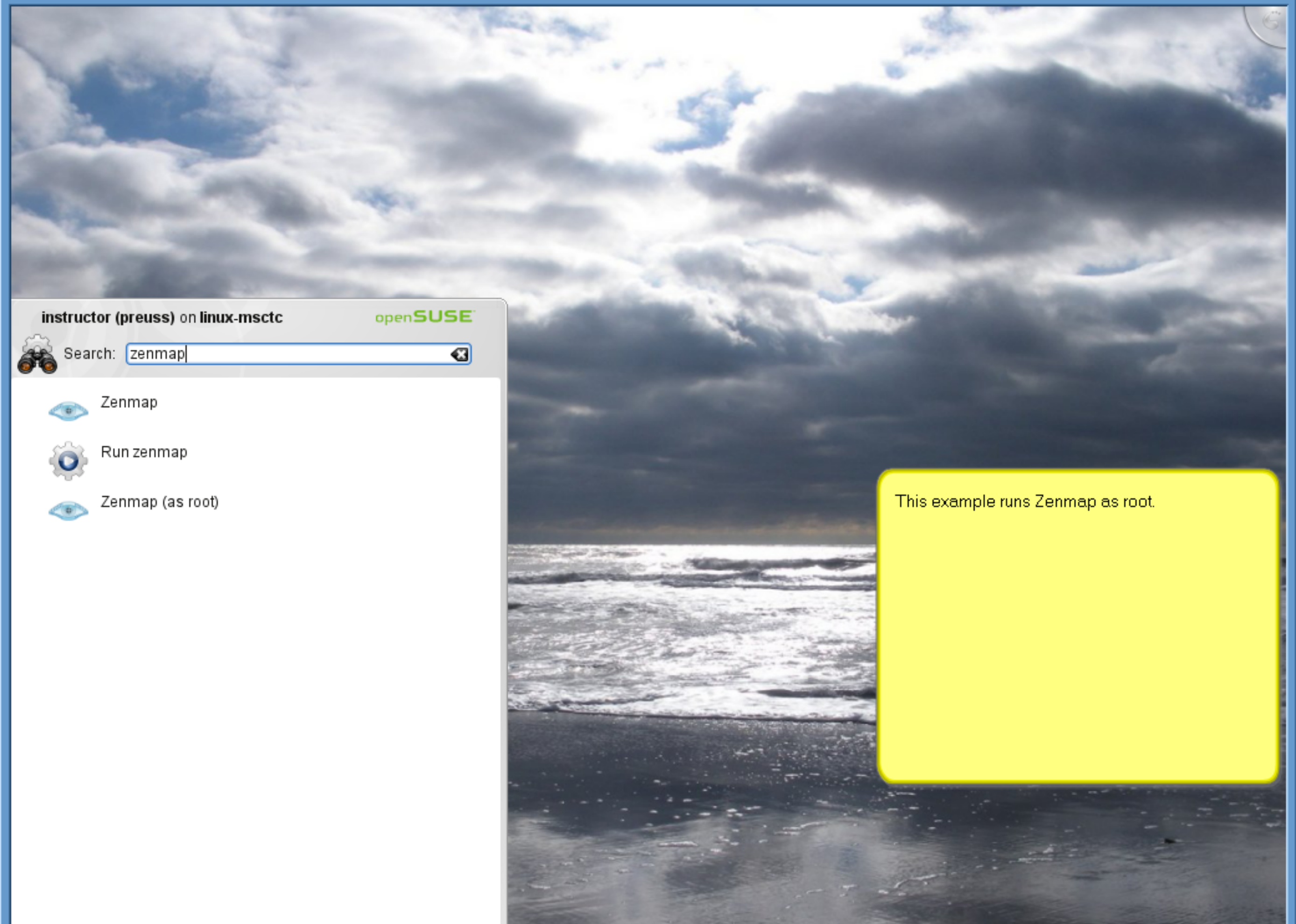
YaST Control Center @ linux-msctc

Search

- Software
- Hardware
- System
- Network Devices
- Network Services
- Novell AppArmor
- Security and Users
- Virtualization
- Support
- Miscellaneous

Software

- Add-On Products
- FACTORY Update
- Media Check
- Online Update
- Online Update Configuration
- Package Search (webpin)
- Software Management**
Install or remove software packages an...



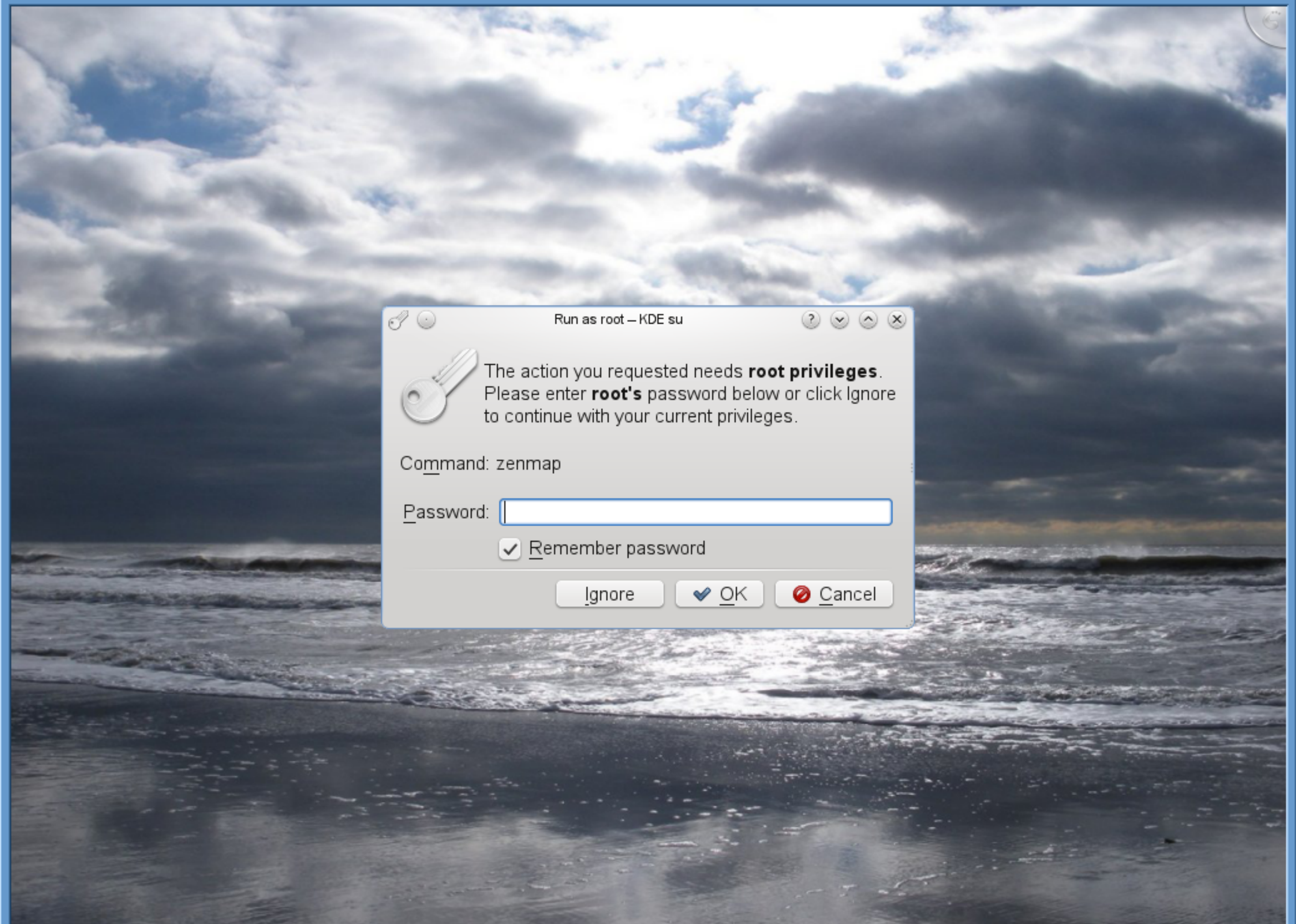
instructor (preuss) on linux-msctc

openSUSE


Search: zenmap

- Zenmap
- Run zenmap
- Zenmap (as root)

This example runs Zenmap as root.



Run as root – KDE su

 The action you requested needs **root privileges**. Please enter **root's** password below or click Ignore to continue with your current privileges.

Command: zenmap

Password:

Remember password

Zenmap

Scan Tools Profile Help

Target: Profile: Intense scan

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host

Details

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

Details

The example only scans one machine. You may put a subnet range in target box.

Zenmap

Scan Tools Profile Help

Target: 192.168.5.4 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.5.4

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.5.4 Details

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-03-23 16:45 CDT
NSE: Loaded 30 scripts for scanning.
Initiating ARP Ping Scan at 16:45
Scanning 192.168.5.4 [1 port]
Completed ARP Ping Scan at 16:45, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:45
Completed Parallel DNS resolution of 1 host. at 16:45, 0.08s elapsed
Initiating SYN Stealth Scan at 16:45
Scanning 192.168.5.4 [1000 ports]
  discovered open port 21/tcp on 192.168.5.4
  discovered open port 22/tcp on 192.168.5.4
  discovered open port 37/tcp on 192.168.5.4
  discovered open port 113/tcp on 192.168.5.4
Completed SYN Stealth Scan at 16:45, 1.11s elapsed (1000 total ports)
Initiating Service scan at 16:45
```

The example selected the scan button and the scan is underway.

Zenmap

Scan Tools Profile Help

Target: 192.168.5.4 Profile: Intense scan [Scan] [Cancel]

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.5.4

Hosts Services

OS	Host
	192.168.5.4

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.5.4 [Details]

```

(NCP, 4, "\xd14\xe8")%r (NotesRPC, 4, "\xd14\xe8")%r
(WMSRequest, 4,
SF: "\xd14\xe8")%r (oracle-tns, 4, "\xd14\xe8");
MAC Address: 00:0F:B0:FF:64:22 (Compal Electronics)
OS fingerprint not ideal because: Didn't receive UDP
response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Unix

data files from: /usr/share/nmap
and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
done: 1 IP address (1 host up) scanned in 86.88 seconds
Raw packets sent: 1156 (56.878KB) | Rcvd: 1001
(058KB)

```

The scan is done.

Please select the Scan menu.

Please select Save Scan.

Name: nmap_scan1

Save in folder: Documents

Browse for other folders

home preuss Documents

Create Folder

- Places
- Search
- Recently Used
- root
- File System

Name	Size	Modified
tmp		03/08/2011

The example uses the name nmap_scan1 as the file name. The file will be an XML file, which you may edit according to the lab.

+ Add - Remove

Nmap XML files (*.xml)

Cancel Save