Content

Installing Open-Audit is not even an trivial task. Therefore I've setup an VMWare appliance for straight forward and easy way to try out this very powerful audit solution.

Installation

OpenAudit is installed on an virtual ubuntu server 10. The ubuntu server is up to date (5.5.2012). The appliance is realised as an VMWare guest. Its hardware compatibility level is 4, so it could be run nearly under all VMWare products. It has been tested under VSphere 5, VMServer 2.0 and VMPlayer.

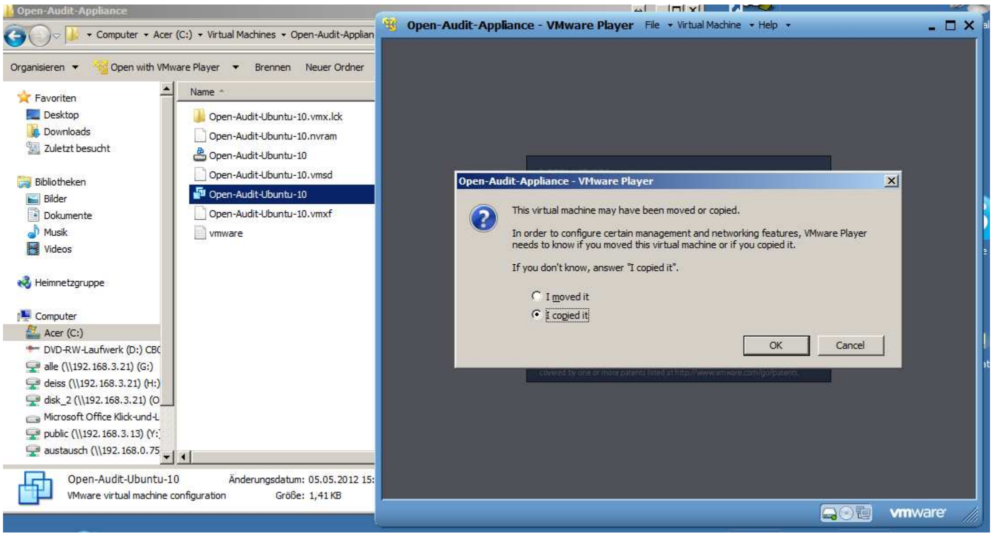
I'll show you how to run it under VMPlayer. You can download VMPlayer for no extra costs from:

http://www.vmware.com/products/player/overview.html

Download and install it. Download and unpack the appliance zip file and copy it's content to an empty directory.

Doubleclick "Open-Audit-Ubuntu-10.vmx". Player comes up and asks if you've moved or copied it.

Important answer "I moved it" !



Open-Audit-Appliance - VMware Player

This virtual machine may have been moved or copied.

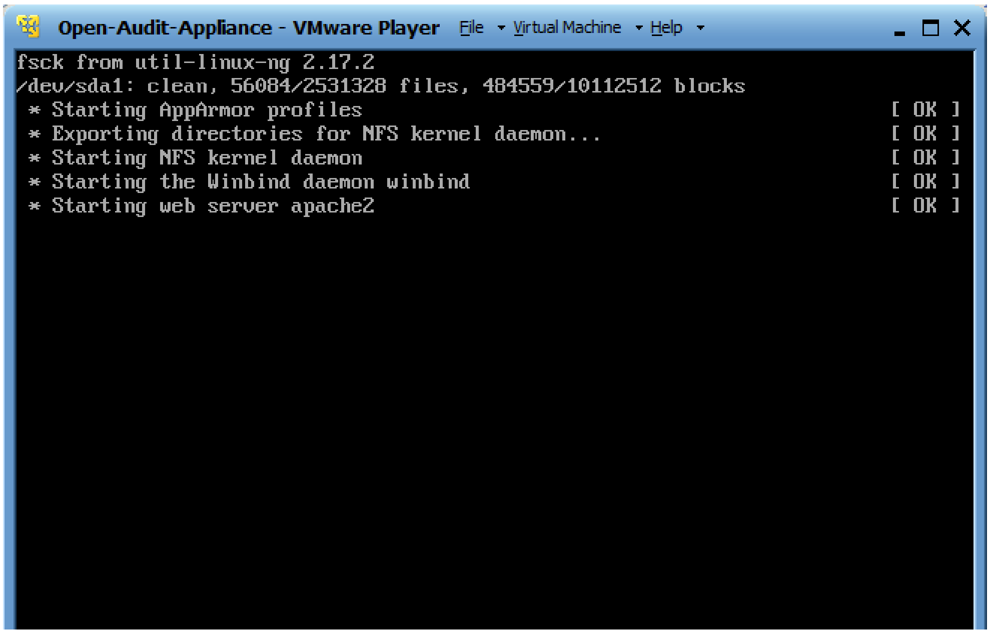
In order to configure certain management and networking features, VMware Player needs to know if you moved this virtual machine or if you copied it.

If you don't know, answer "I copied it".

○ I moved it
● I copied it

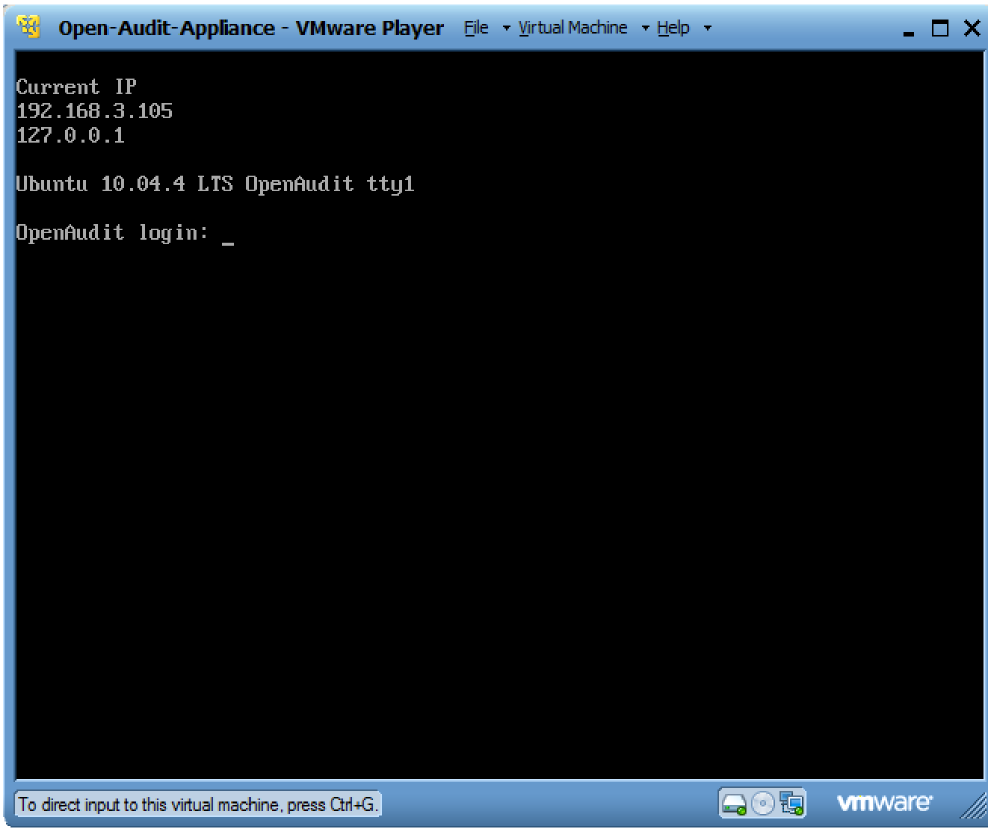
Open-Audit-Appliance
Computer ▸ Acer (C:) ▸ Virtual Machines ▸ Open-Audit-Applian
Organisieren
Open with VMware Player
Brennen
Neuer Ordner
Favoriten
Desktop
Downloads
Zuletzt besucht
Bibliotheken
Bilder
Dokumente
Musik
Videos
Heimnetzgruppe
Computer
Acer (C:)
DVD-RW-Laufwerk (D:) CBC
alle (\\192.168.3.21) (G:)
deiss (\\192.168.3.21) (H:)
disk_2 (\\192.168.3.21) (O
Microsoft Office Klick-und-L
public (\\192.168.3.13) (Y:
austausch (\\192.168.0.75
Name
Open-Audit-Ubuntu-10.vmx.lck
Open-Audit-Ubuntu-10.nvram
Open-Audit-Ubuntu-10
Open-Audit-Ubuntu-10.vmsd
Open-Audit-Ubuntu-10
Open-Audit-Ubuntu-10.vmxf
vmware
Open-Audit-Ubuntu-10
VMware virtual machine configuration
Änderungsdatum: 05.05.2012 15:
Größe: 1,41 KB
Open-Audit-Appliance - VMware Player
File
Virtual Machine
Help
OK
Cancel
vmware

After pressing OK the machine will boot.



```
fsck from util-linux-ng 2.17.2
/dev/sda1: clean, 56084/2531328 files, 484559/10112512 blocks
 * Starting AppArmor profiles                                          [ OK ]
 * Exporting directories for NFS kernel daemon...                      [ OK ]
 * Starting NFS kernel daemon                                          [ OK ]
 * Starting the Winbind daemon winbind                                 [ OK ]
 * Starting web server apache2                                         [ OK ]
```

After booting you should see something like that. Note the Ubuntu machine is configured for DHCP, you should see its current IP on the screen. If you see only 0.0.0.0 DHCP is not working correctly.



Open-Audit-Appliance - VMware Player
File
Virtual Machine
Help
To direct input to this virtual machine, press Ctrl+G.
vmware

```
Current IP
192.168.3.105
127.0.0.1

Ubuntu 10.04.4 LTS OpenAudit tty1

OpenAudit login: _
```

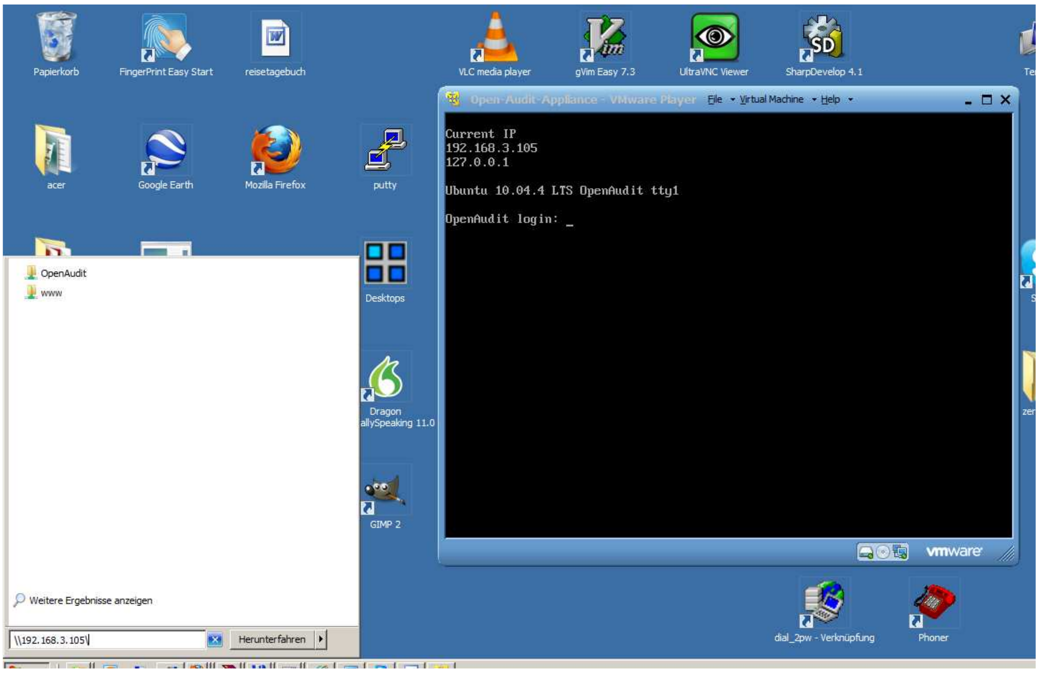
Thats all, now you have an running OpenAudit server.

First Audit

It is time to check your installation. The Ubuntu server comes with a preconfigured samba server. First let us try to access it's smb shares.

Please note: Always change 192.168.xxx.xxx to your IP which you can obtain from the running virtual Ubuntu server !

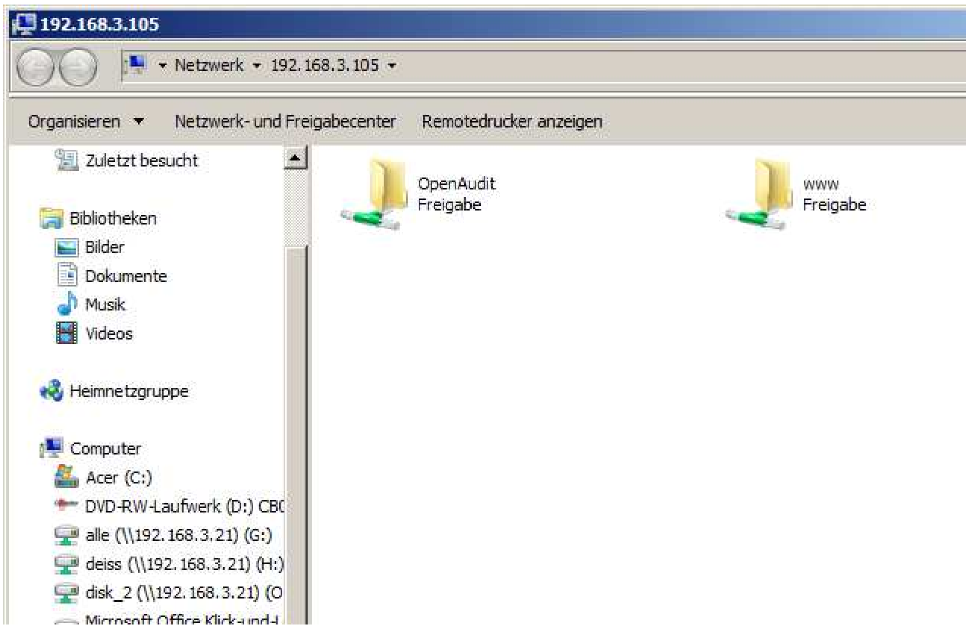
In windows enter now \\192.168.xxx.xxx\



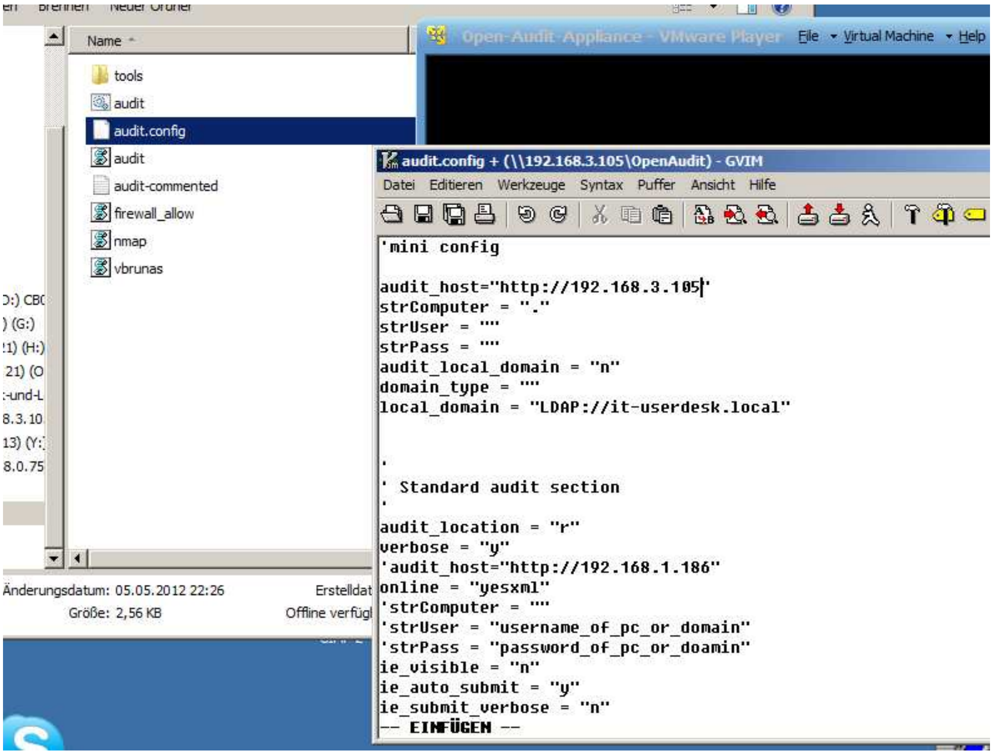
```
Current IP
192.168.3.105
127.0.0.1

Ubuntu 10.04.4 LTS OpenAudit tty1

OpenAudit login: _
```

\\192.168.3.105\

Shares should pop up



Open the OpenAudit share, open audit.config with an editor (e.g. notepad)



```
'mini config

audit_host="http://192.168.3.105"
strComputer = "."
strUser = ""
strPass = ""
audit_local_domain = "n"
domain_type = ""
local_domain = "LDAP://it-userdesk.local"


'
' Standard audit section
'
audit_location = "r"
verbose = "y"
'audit_host="http://192.168.1.186"
online = "yesxml"
'strComputer = ""
'strUser = "username_of_pc_or_domain"
'strPass = "password_of_pc_or_doamin"
ie_visible = "n"
ie_auto_submit = "y"
ie_submit_verbose = "n"
-- EINFÜGEN --
```

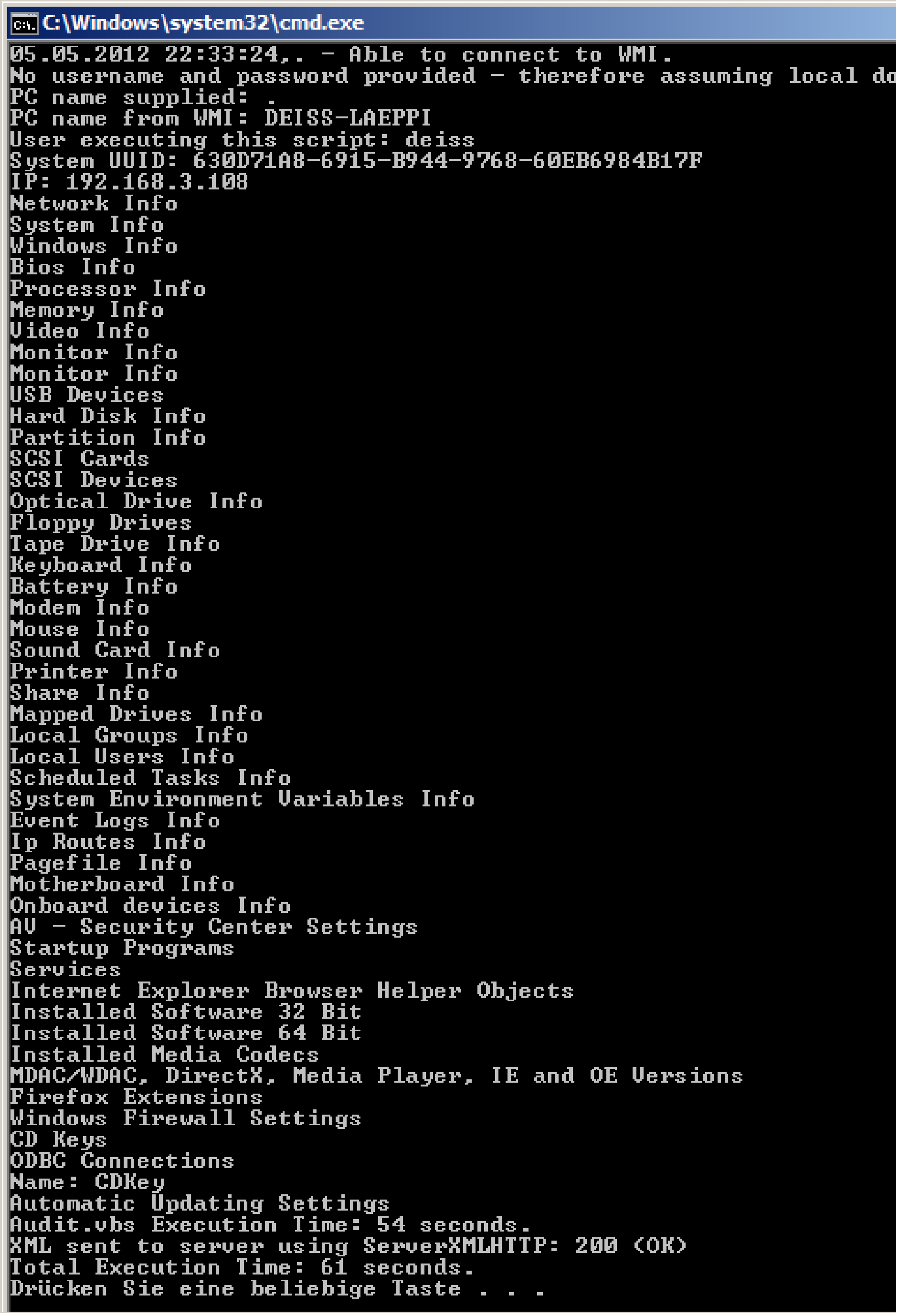
For our first try just change this one line

audit_host=http://192.168.xxx.xxx

Change the IP address to ubuntu's IP address (in our sample this is 192.168.3.105). Save file, close file, then doubleclick audit.cmd.

You should see a dos box, inside running the script which now collects all data from your local pc.

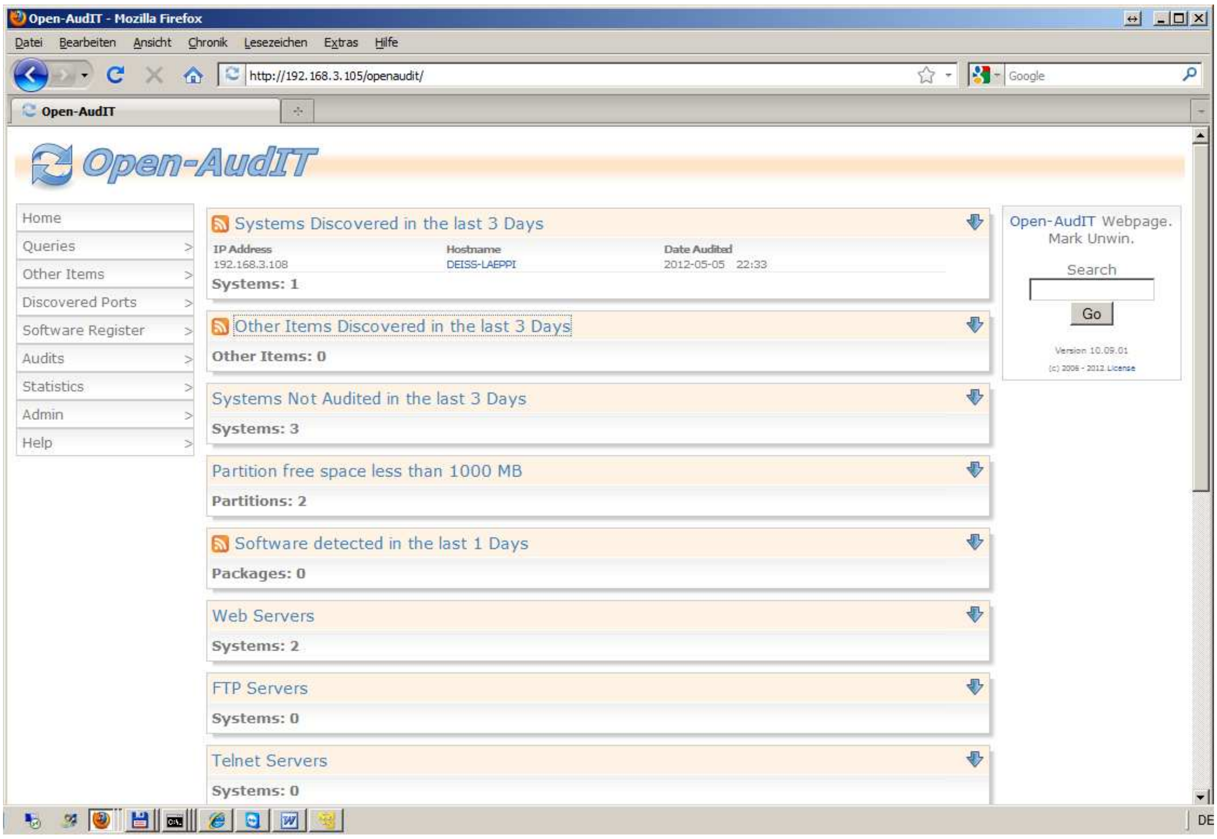
After gathering you should see "XML sent to .... 200 OK"



```
05.05.2012 22:33:24,. - Able to connect to WMI.
No username and password provided - therefore assuming local do
PC name supplied: .
PC name from WMI: DEISS-LAEPPI
User executing this script: deiss
System UUID: 630D71A8-6915-B944-9768-60EB6984B17F
IP: 192.168.3.108
Network Info
System Info
Windows Info
Bios Info
Processor Info
Memory Info
Video Info
Monitor Info
Monitor Info
USB Devices
Hard Disk Info
Partition Info
SCSI Cards
SCSI Devices
Optical Drive Info
Floppy Drives
Tape Drive Info
Keyboard Info
Battery Info
Modem Info
Mouse Info
Sound Card Info
Printer Info
Share Info
Mapped Drives Info
Local Groups Info
Local Users Info
Scheduled Tasks Info
System Environment Variables Info
Event Logs Info
Ip Routes Info
Pagefile Info
Motherboard Info
Onboard devices Info
AV - Security Center Settings
Startup Programs
Services
Internet Explorer Browser Helper Objects
Installed Software 32 Bit
Installed Software 64 Bit
Installed Media Codecs
MDAC/WDAC, DirectX, Media Player, IE and OE Versions
Firefox Extensions
Windows Firewall Settings
CD Keys
ODBC Connections
Name: CDKey
Automatic Updating Settings
Audit.vbs Execution Time: 54 seconds.
XML sent to server using ServerXMLHTTP: 200 (OK)
Total Execution Time: 61 seconds.
Drücken Sie eine beliebige Taste . . .
```

To check the result of this operation it's time to open a browser.

Enter http://192.168.xxx.xxx/openaudit/ in your prefered browser. This should open OpenAudits Website. Now there should be one discovered system.



Systems Discovered in the last 3 Days

IP Address	Hostname	Date Audited
192.168.3.108	DEISS-LAEPPI	2012-05-05 22:33

Systems: 1

Other Items Discovered in the last 3 Days

Other Items: 0

Systems Not Audited in the last 3 Days

Systems: 3

Partition free space less than 1000 MB

Partitions: 2

Software detected in the last 1 Days

Packages: 0

Web Servers

Systems: 2

FTP Servers

Systems: 0

Telnet Servers

Systems: 0

Congratulations !!

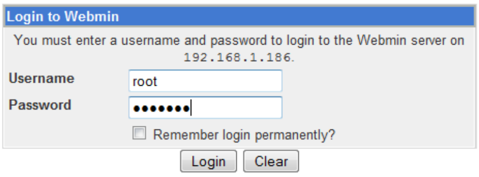
Customizing Installation

The Ubuntu server comes with a preconfigured webmin installation. With webmin you can change settings on linux machines, without knowledge of linux/ubuntu.

Enter

https://192.168.xxx.xxx:10000/

into your Browser. Enter user/password (root/password)



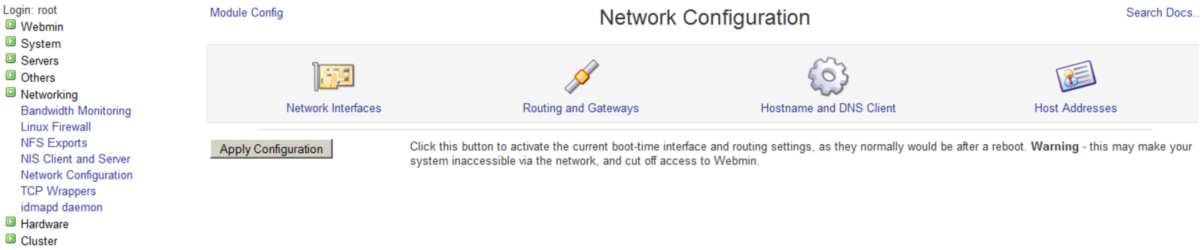
Login to Webmin

You must enter a username and password to login to the Webmin server on 192.168.1.186.

Username	root
Password	●●●●●●●

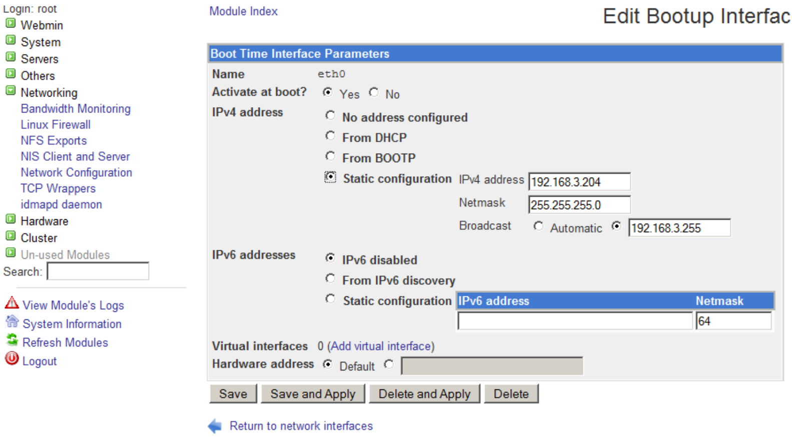
☐ Remember login permanently?

choose "Network Configuration"



Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

- Click network interfaces
- Choose eth0
- Change to static if you prefer fixed IP address for your Ubuntu server (recommended)



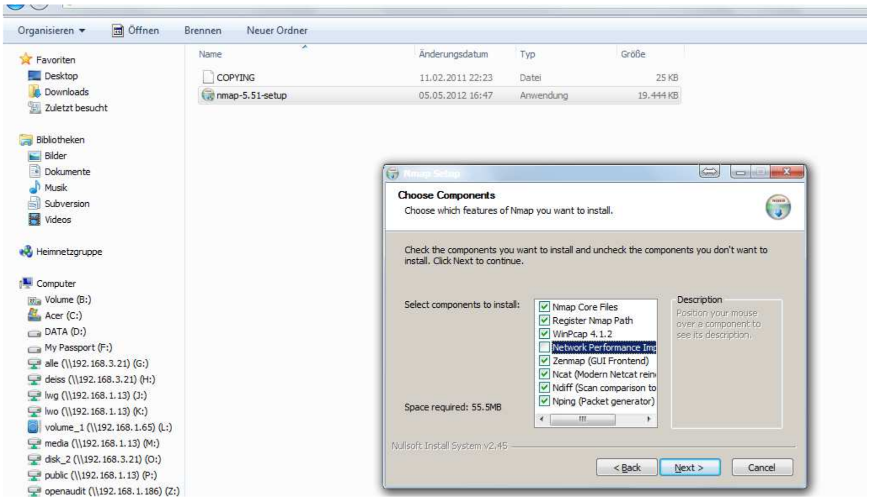
Boot Time Interface Parameters

Name	eth0
Activate at boot?	● Yes ○ No
IPv4 address	○ No address configured ○ From DHCP ○ From BOOTP ● Static configuration IPv4 address 192.168.3.204 Netmask 255.255.255.0 Broadcast ○ Automatic ● 192.168.3.255
IPv6 addresses	● IPv6 disabled ○ From IPv6 discovery ○ Static configuration IPv6 address Netmask 64
Virtual interfaces	0 (Add virtual interface)
Hardware address	● Default ○

Using NMAP

OpenAudit also has an interface to nmap (optional). Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

To use nmap for OpenAudit on windows you first have to install nmap executable. You'll find an installer on the openaudit share on ubuntu server. (\\192.168.xxx.xxx\OpenAudit\installs)



Name	Änderungsdatum	Typ	Größe
COPYING	11.02.2011 22:23	Datei	25 KB
nmap-5.51-setup	05.05.2012 16:47	Anwendung	19.444 KB

Choose Components

Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ Nmap Core Files
- ☑ Register Nmap Path
- ☑ WinPcap 4.1.2
- □ Network Performance Imp
- ☑ Zenmap (GUI Frontend)
- ☑ Ncat (Modern Netcat rein
- ☑ Ndiff (Scan comparison to
- ☑ Nping (Packet generator)

Description

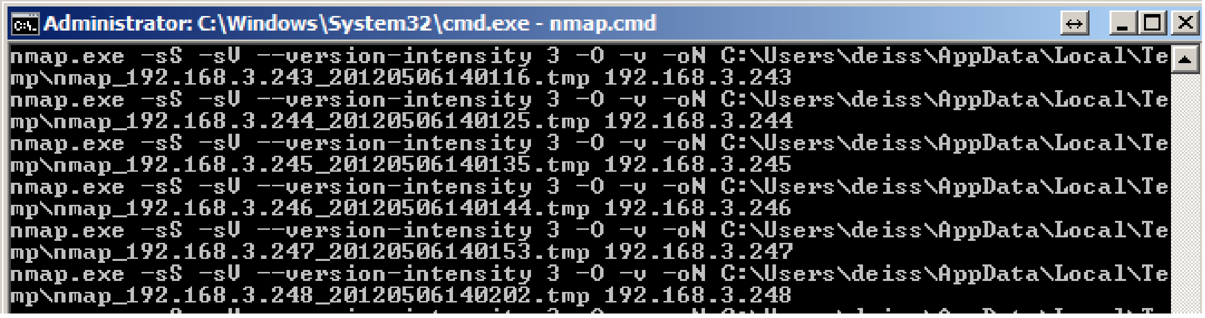
Position your mouse over a component to see its description.

Space required: 55.5MB

Organisieren
Öffnen
Brennen
Neuer Ordner
Favoriten
Desktop
Downloads
Zuletzt besucht
Bibliotheken
Bilder
Dokumente
Musik
Subversion
Videos
Heimnetzgruppe
Computer
Volume (B:)
Acer (C:)
DATA (D:)
My Passport (F:)
alle (\\192.168.3.21) (G:)
deiss (\\192.168.3.21) (H:)
lwg (\\192.168.1.13) (J:)
lwo (\\192.168.1.13) (K:)
volume_1 (\\192.168.1.65) (L:)
media (\\192.168.1.13) (M:)
disk_2 (\\192.168.3.21) (O:)
public (\\192.168.1.13) (P:)
openaudit (\\192.168.1.186) (Z:)
Nullsoft Install System v2.45
< Back
Next >
Cancel

Open the OpenAudit share, open audit.config with an editor (e.g. notepad)
Edit these lines:
nmap_subnet = "192.168.1."   ' The subnet you wish to scan
nmap_subnet_formatted = "192.168.001."   ' The subnet padded with 0's

Save file and doubleclick nmap.cmd. NMAP scans your net, this will take a time .....



Administrator: C:\Windows\System32\cmd.exe - nmap.cmd

```
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.243_20120506140116.tmp 192.168.3.243
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.244_20120506140125.tmp 192.168.3.244
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.245_20120506140135.tmp 192.168.3.245
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.246_20120506140144.tmp 192.168.3.246
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.247_20120506140153.tmp 192.168.3.247
nmap.exe -sS -sV --version-intensity 3 -O -v -oN C:\Users\deiss\AppData\Local\Te
mp\nmap_192.168.3.248_20120506140202.tmp 192.168.3.248
```

After scanning you'll find all scanned items in OpenAudits Webinterface (other items).

Passwords

You can login to Ubuntu server directly (via virtual console)

Valid users are
administrator / password
root / password

You can login to Ubuntu server via ssh (putty)

Valid users are
administrator / password
root / password

mysql login
root / password

webmin login
root / password

Appendix

Installing webmin

- `apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python`
- `wget http://prdownloads.sourceforge.net/webadmin/webmin_1.580_all.deb`
- `dpkg --install webmin_1.580_all.deb`

audit.config

```
strUser = "username_of_pc_or_domain"
strPass = "password_of_pc_or_doamin"
audit_local_domain = "y"
domain_type = "ldap"
local_domain = "LDAP://yourdomain.local"

nmap_subnet = "192.168.1."            ' The subnet you wish to scan
nmap_subnet_formatted = "192.168.001."    ' The subnet padded with 0's
```

Patch to SVN

New objectmodel in IE9 requires to set compatibility mode.

include.php (line 72,added two lines)

```
<title>Open-AudIT</title>
<!-- Mimic Internet Explorer 8 -->
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE8" >
<link rel="icon" href="favicon.ico" type="image/x-icon"/>
```