Discovery

CGS - Hugo Miranda

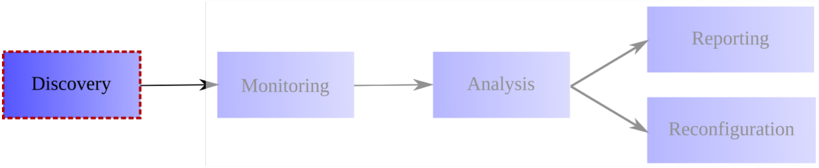
2021

Ciências ULisboa

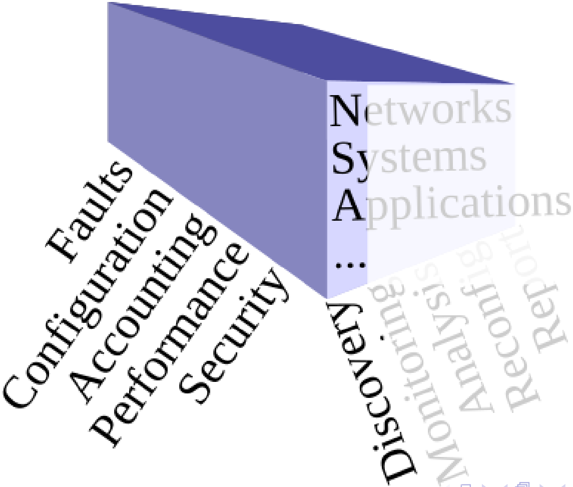
Faculdade de Ciências da Universidade de Lisboa

Activities

- First in the list of activities



What to Discover



Why to Discover

Hardware

- Age
- Planning upgrades
  - Lifetime expectations
  - Prepare replaceable parts
- Compatibility with software upgrades
  - Further discussed in *Configuration class*
- *Ghost* hardware

Why to Discover

Software

- Security
  - Software versions
- Policy enforcement
  - Forbid some applications
- Licensing management

Why to Discover

Users

- Users come and go
  - Outgoing users must have permissions properly removed

Why to Discover

Management/legal issues

- Inventory
- Auditing

When to Discover

- The IT infrastructure is "alive"
  - Hard to keep track of what users and admins
    - do
    - add
    - remove
  - Specially hard when trying to fix problems

Case studies

- The hidden DHCP server
    - Reconfiguration → Fault
- License management
- Laptop management

Case study

Discovery Classes

- Manual Inventory
- Passive Observation
- Active Experimentation
- Agents

Limitations

- Each of the approaches:
  - Does not cover everything
    - Multiple concurrent approaches are required
  - Cannot be applied to all types of components
    - Servers
    - Desktop computers
    - Software
    - Network equipment
    - . . .
- Has distinct
  - impact on the infrastructure
  - efficiency

Manual Inventory

- Walk on the facilities
- Observe services directories/dictionaries
  - DHCP
  - DNS
  - Routing tables
  - Active Directory
  - Firewall logs

Manual Inventory

DHCP

- Inspect lease tables
- Good for hardware in general
  - Servers
  - Network equipment
  - Printers
  - Transient components of the infrastructure
    - Connected at that moment
- Does not cover static (non-DHCP) IP addresses
  - Depends on policies

Manual Inventory

DNS

- Inspect DNS tables
  - Config files
- Covers most of the servers
  - Not necessarily 1-to-1 to servers hardware
- Remaining depends on the DNS policies

Manual Inventory

Routing Tables

- Good for routers and other L3 equipment
- Useless for any other hardware

Passive Observation

- Inspect network traffic flow
  - Port mirroring on switches
  - tcpdump

Passive Observation

Applications

- Network services
- Hardware
  - Clients and Servers
  - Network equipment

Limitations

- Observation is always incomplete
  - Changes with time of day/week
  - Must be made for a sufficient time interval
  - Must be performed in different locations

Passive Observation

- From traffic use:
  - IP/MAC addresses to identify hosts
  - Ports to identify services
- Payload in some protocol messages
  - LLDP/CDP
  - OSPF/RIP

Active experimentation

Ping/Port scan

- Usual approach for detecting network vulnerabilities
- Shows only active applications
  - Not those installed
- Firewalls may block some ports/servers
- Useful for servers, desktops, network equipment and applications

Active experimentation

Traceroute

- Partial view of L3 network equipment
- Only the route in use
    - Not the alternatives

Active experimentation - How traceroute works

Active experimentation

MIBs

- Export information learnt by equipment using it
- Routers
    - Routing table
- Routers/switchs
    - LLDP advertisements from neighbours

Active experimentation

DNS XFER

- Request a full export of DNS servers
- Usual application on DNS mirroring
  - Server must accept the request
- Applicable for hardware/services registered on DNS
  - Policy dependent

Agents

- Look for applications using well known signatures
  - Directories/File names
  - Scan Windows Registry
  - Installed packets on Linux distributions
- Use OS tools to find running processes
  - pstree
  - ...

Agents

- Can be

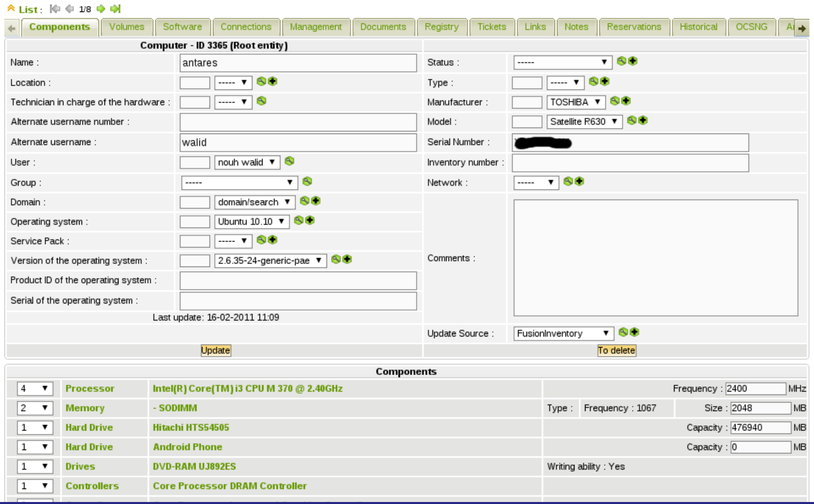
  Active spontaneously report to the management console

  Passive report upon request

Agents

- May not detect all applications
- Consume resources at the host
  - See file indexing when Windows boots
- Can be considered intrusive
  - Must be shielded by organization policy

Agents: FusionInventory



Computer - ID 3365 (Root entity)

Name :	antares	Status :	-----
Location :	-----	Type :	-----
Technician in charge of the hardware :	-----	Manufacturer :	TOSHIBA
Alternate username number :		Model :	Satellite R630
Alternate username :	walid	Serial Number :	[redacted]
User :	nouh walid	Inventory number :	
Group :	-----	Network :	-----
Domain :	domain/search	Comments :	
Operating system :	Ubuntu 10.10		
Service Pack :	-----		
Version of the operating system :	2.6.35-24-generic-pae		
Product ID of the operating system :			
Serial of the operating system :			
Last update: 16-02-2011 11:09			
		Update Source :	FusionInventory

Update   To delete

Components

4	Processor	Intel(R) Core(TM) i3 CPU M 370 @ 2.40GHz		Frequency : 2400 MHz
2	Memory	- SODIMM	Type : Frequency : 1067	Size : 2048 MB
1	Hard Drive	Hitachi HTS54505		Capacity : 476940 MB
1	Hard Drive	Android Phone		Capacity : 0 MB
1	Drives	DVD-RAM UJ892ES	Writing ability : Yes	
1	Controllers	Core Processor DRAM Controller		

Challenge #1: Store Information

- Information is a graph
- Map a graph in a DB in a easy to use way
  - Who has version N of software X installed-
  - Which desktops are connected to switch X?
  - Which applications are running on server X?

Challenge #2: Policies and Utilization

- The thin line between management information and user privacy
- What if you find something you shouldn't
  - To be discussed in ethics class
- Be protected by publicly advertised policies
- Link what is relevant to the monitoring system and knowledge base

Wrap Up

- Discovery is a permanent/cyclic activity
    - Understand it as part of the daily activities
- Care must be taken on the resources consumed for it

What's next

- This lesson on Moodle lessons
  - Additional pointers
- Lab assignment on discovery using a libpcap file