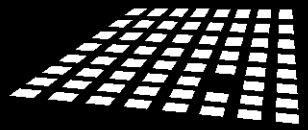
Virtually Pwned
Pentesting Virtualization

Claudio Criscione
@paradoxengine – c.criscione@securenetwork.it

/me

Claudio Criscione



VIRTUALIZATION.INFO

The need for security

Breaking virtualization means…

…hacking ***the underlying layer***

…accessing systems ***locally***

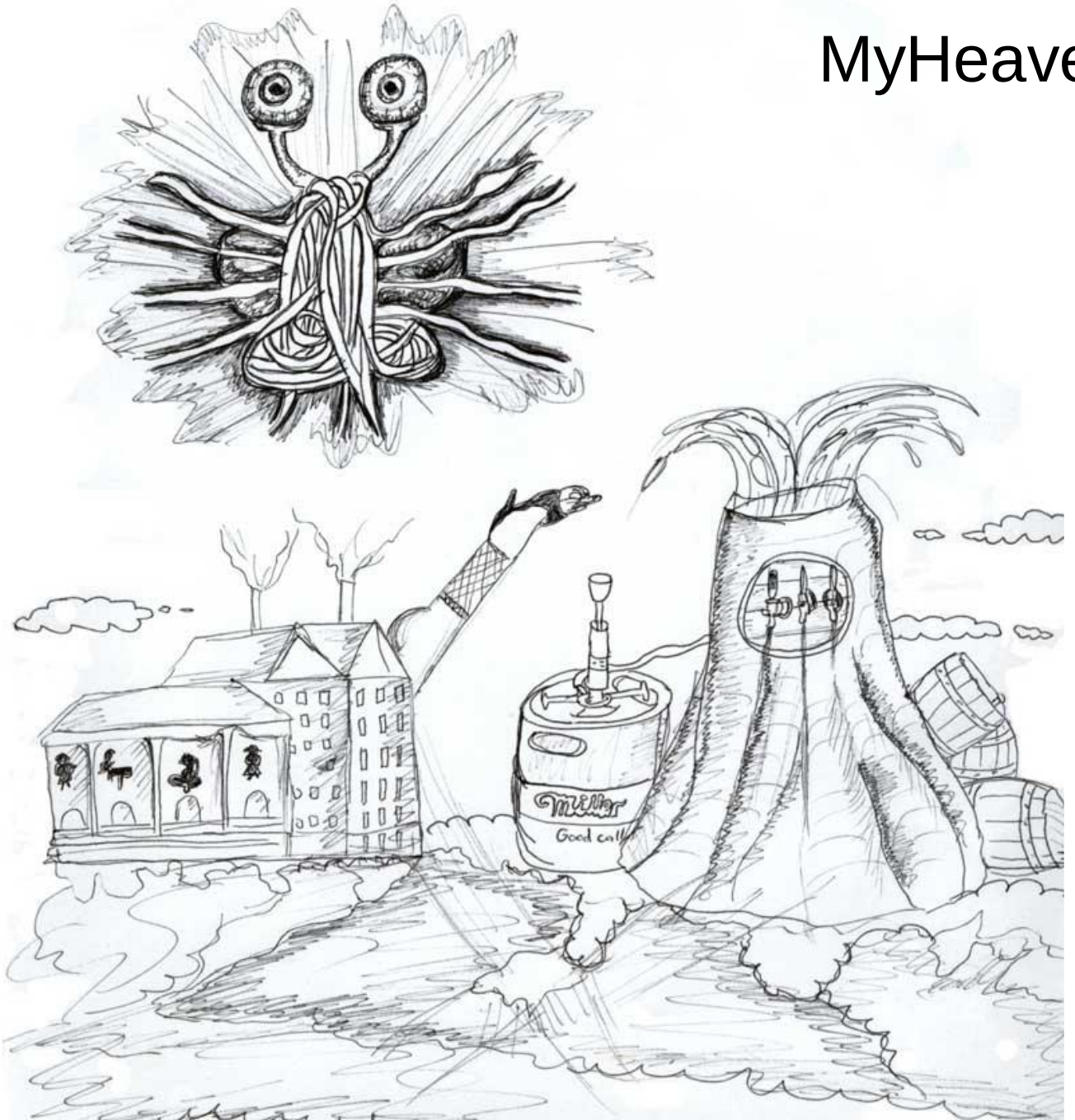
…bypassing access and network ***controls***

…hitting ***multiple targets*** at once

Almost everywhere now

Small number of different solutions deployed

MyHeaven




The elephant in the room

Escaping the VM

Yes, it can be done

Yes, it is (99% up to now) due to an exploit

Yes, it can be patched

Yes, it will happen again

No, it is not something you can easily audit

No, I won't disclose "escape from vm" 0days


1
CAN
249
46
41
66
253
257
229
23
25
603
12
19
92
72
12
17
20
25
12
20
MAIDSTONE
MAYFIELD
HASTINGS
DUNGENESS
HEAD

The Plan

1 - Recon

2 - Attack

3 - Pwn

Tools Of The Trade

VASTO

The Virtualization ASsessment TOolkit

It is an “exploit pack” for **Metasploit** focusing on virtualization and cloud security.

Announcing Beta 0.3 – Featured at The Arsenal… yesterday!

Tnx to Luca Carettoni, Paolo Canaletti, drk1wi for helping with modules!

Our demo target

Security is one of the few fields
where hitting a large target is worth more
than hitting a small one.

How do you notice?

It’s virtual!

Recon

- Local – are you in a VM?
  - Easy – Check MAC address, processes
  - Not so easy – Hardware access
- Remote – where’s the Hypervisor?
  - Network services
  - Fingerprinting

vmware_version

Handy SOAP API to call

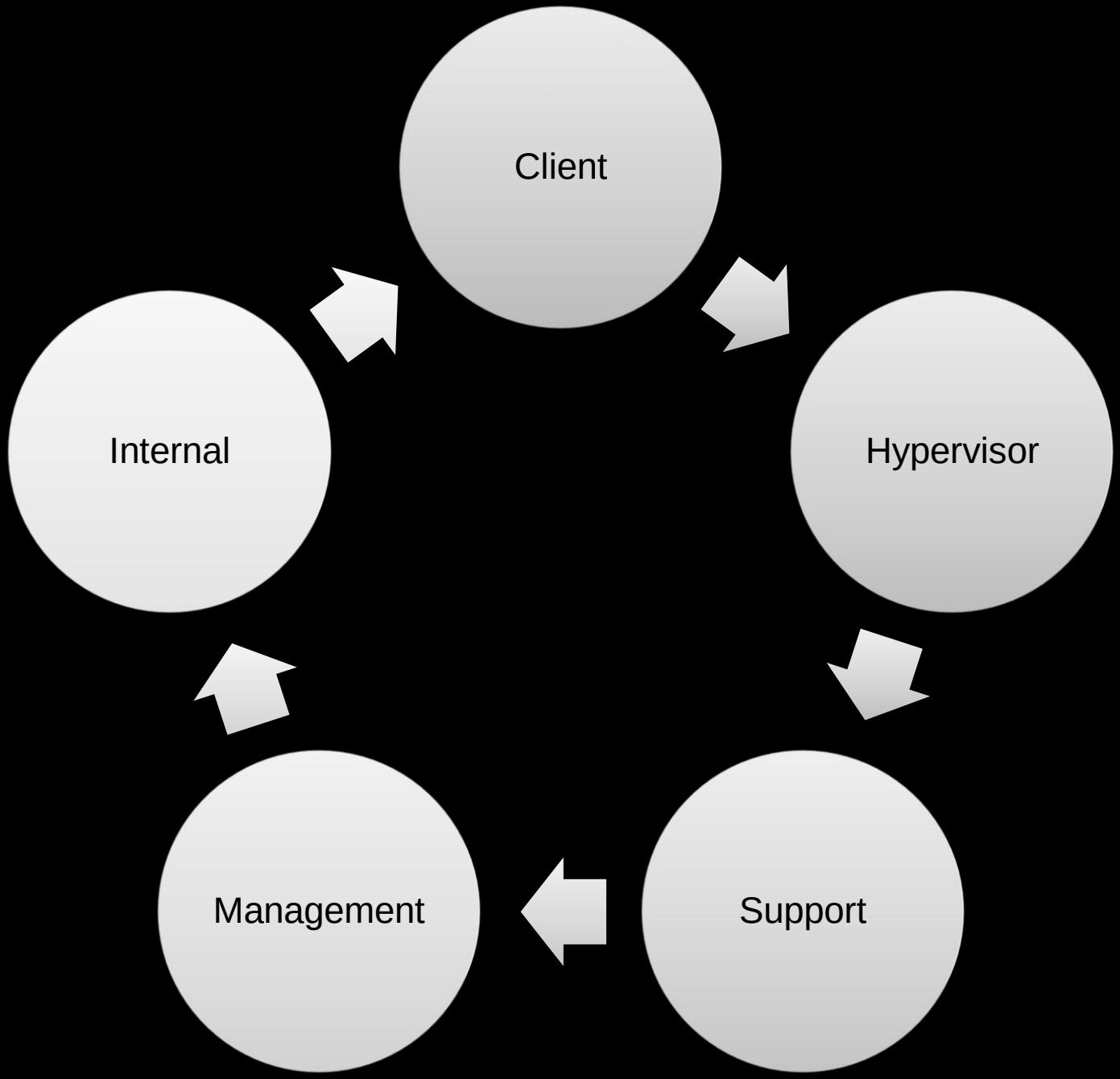
Works on most VMware products

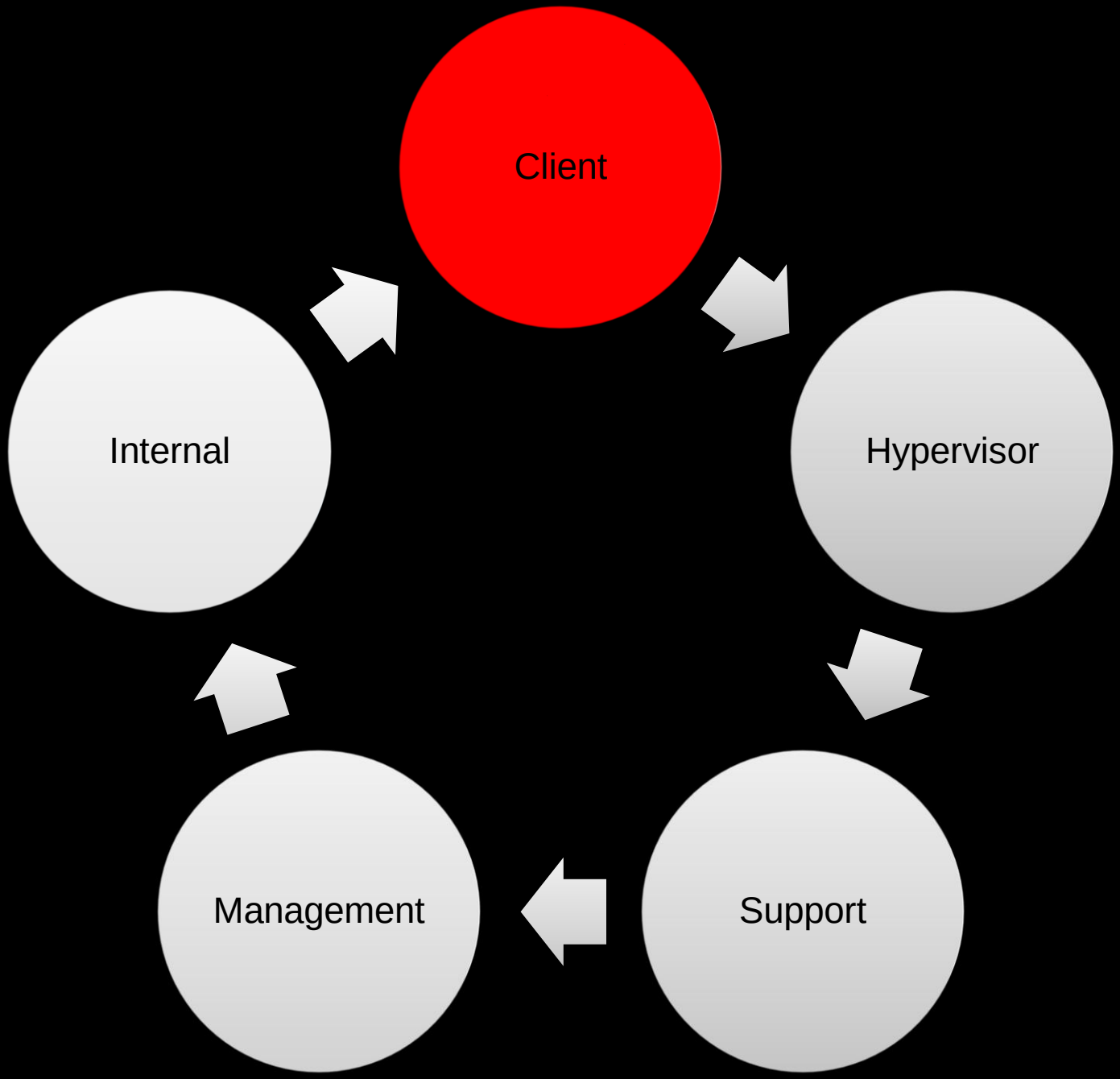
[…]

```
<RetrieveServiceContent xmlns=\"urn:internalvim25\">
            <_this type=\"ServiceInstance\">
                  ServiceInstance
            </_this>
    </RetrieveServiceContent>
```

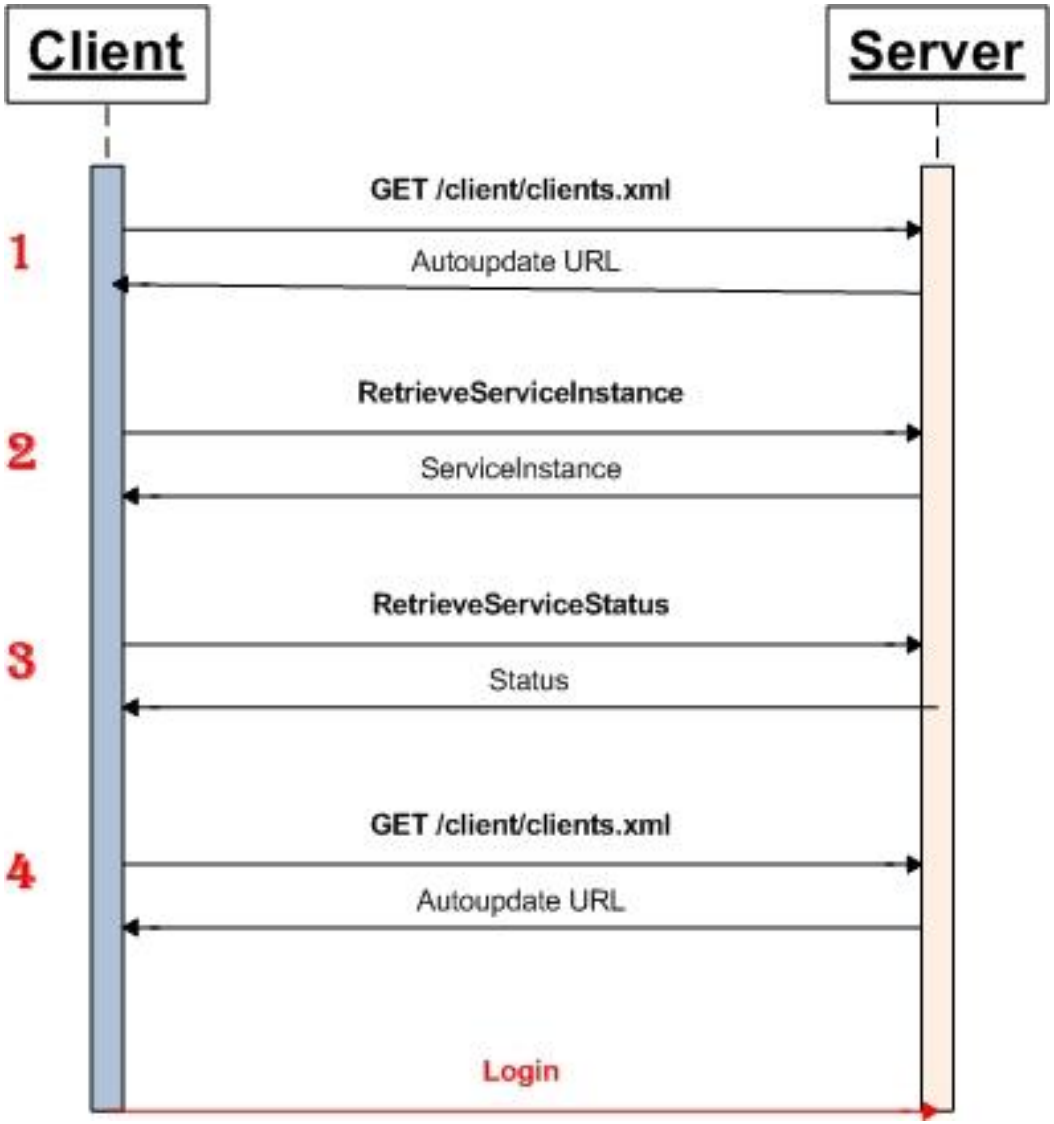
[…]


A multi layered attack


Client
Hypervisor
Support
Management
Internal


Client
Hypervisor
Support
Management
Internal

Client : The Auto Update feature



clients.xml

```
<ConfigRoot>
  <clientConnection id="0000">
    <authdPort>902</authdPort>
    <version>3</version>
    <patchVersion>3.0.0</patchVersion>
    <apiVersion>3.1.0</apiVersion>
    <downloadUrl>https://*/client/VMware-
    viclient.exe</downloadUrl>
  </clientConnection>
</ConfigRoot>
```

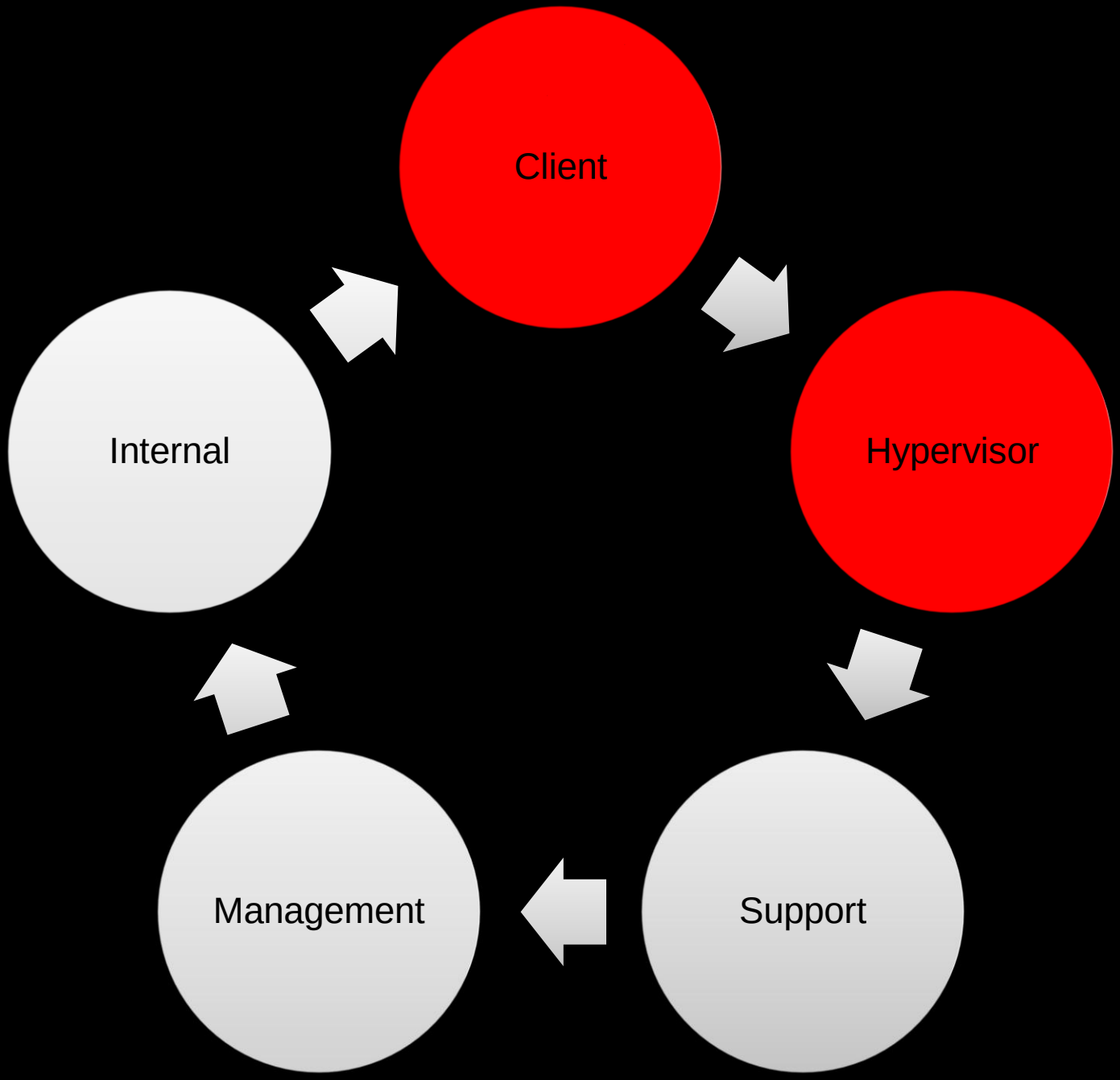
vmware_vilurker

The VIlurker module can perform user-assisted code execution provided you can do MITM on a client.

Almost no one use trusted certificates.

No code signing on updates, but user gets a certificate warning.

BONUS INFO: no SSL check on VMware Server 1.x


Client
Hypervisor
Support
Management
Internal

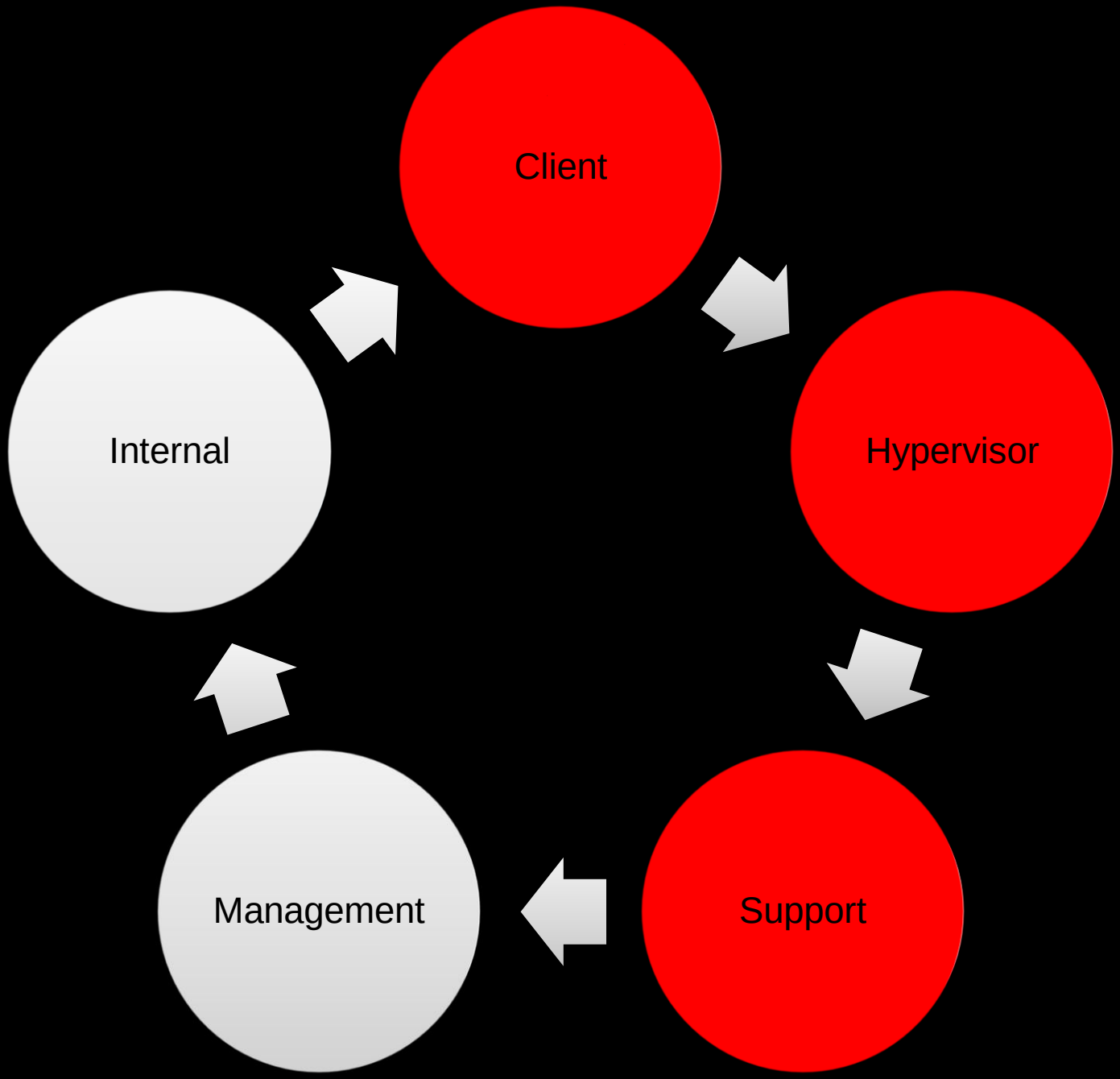
Direct Hit

vmware_guest_stealer

CVE-2009-3733

This path traversal was discovered by Flick and Morehouse and presented last year. Exploit was released as a perl script and it has been ported to VASTO.

It can be used to retrieve any file as the root user, including non-running guests. Works on most outdated VMware Products.


Client
Hypervisor
Support
Management
Internal


Components
Always
Components

vmware_updatemanager_traversal

JETTY-1004

VMware Update Manager includes Jetty 6.1.16

Runs on the vCenter (management) Server

Jetty 6.1.16 is vulnerable to path traversal (again)

Here is the magic string

/vci/downloads/health.xml/%3F/../../../../../../../../../../$FILE


Ok, we can read files on the vCenter, so what?
Follow me!

Introducing vpxd-profiler-*

It is a “debug” file written by vCenter.

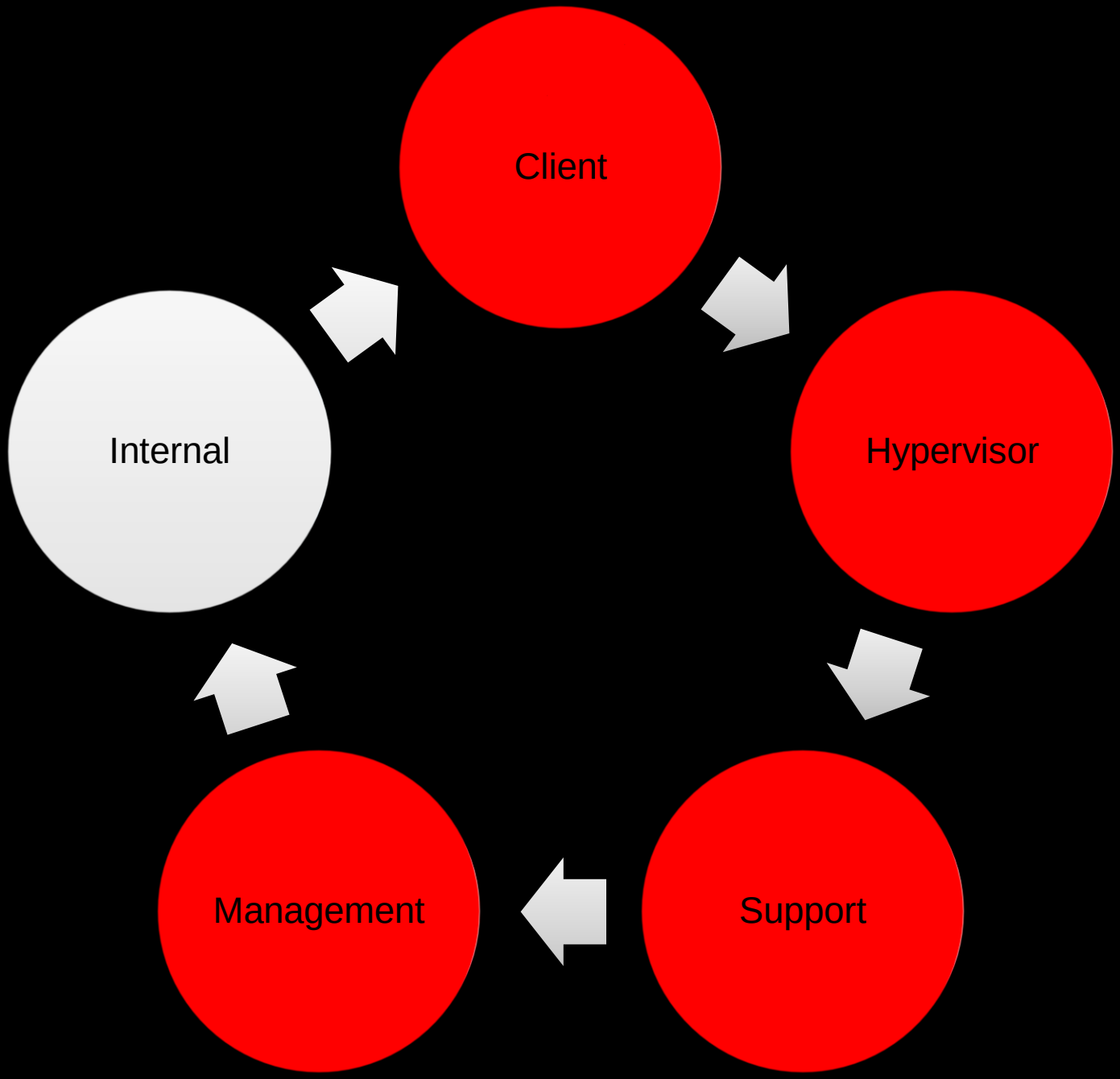
Lots of information inside. Let’s go for low-hanging fruits for now. More to come ☺

/SessionStats/SessionPool/Session/Id='06B90BCB-A0A4-4B9C-B680-FB72656A1DCB'/Username=‘FakeDomain\FakeUser'/SoapSession/Id='AD45B176-63F3-4421-BBF0-FE1603E543F4'/Count/total 1


Ride the session!

vmware_session_rider

- Using the session is non-trivial: VI client has tight timeouts
- The module acts as a proxy to access vCenter using the stolen session.
- Will fake the login to the client and can be easily tweaked to act as a password grabber (unlike VIlurker).


Client
Hypervisor
Support
Management
Internal

The Interface is FUN

Web-based & Complex

XSS

URL Forwarding

BONUS: Shutdown has not been changed, can shutdown local Tomcat on VMware

vmware_webaccess_portscan

CVE-2010-0686

"URL Forwarding" means performing POST requests on remote hosts.

Can be used to exploit IP-based trusts and reach internal networks.

Not just portscan!

Management is not just interface

vCenter connects to ESX server via SSL [SOAP]

Certificates are usually not trusted, but stored.

MITM → Connection Broken

On reconnection, the vCenter will check for the certificate CN

Spoof the CN → Admin gets *usual warning*

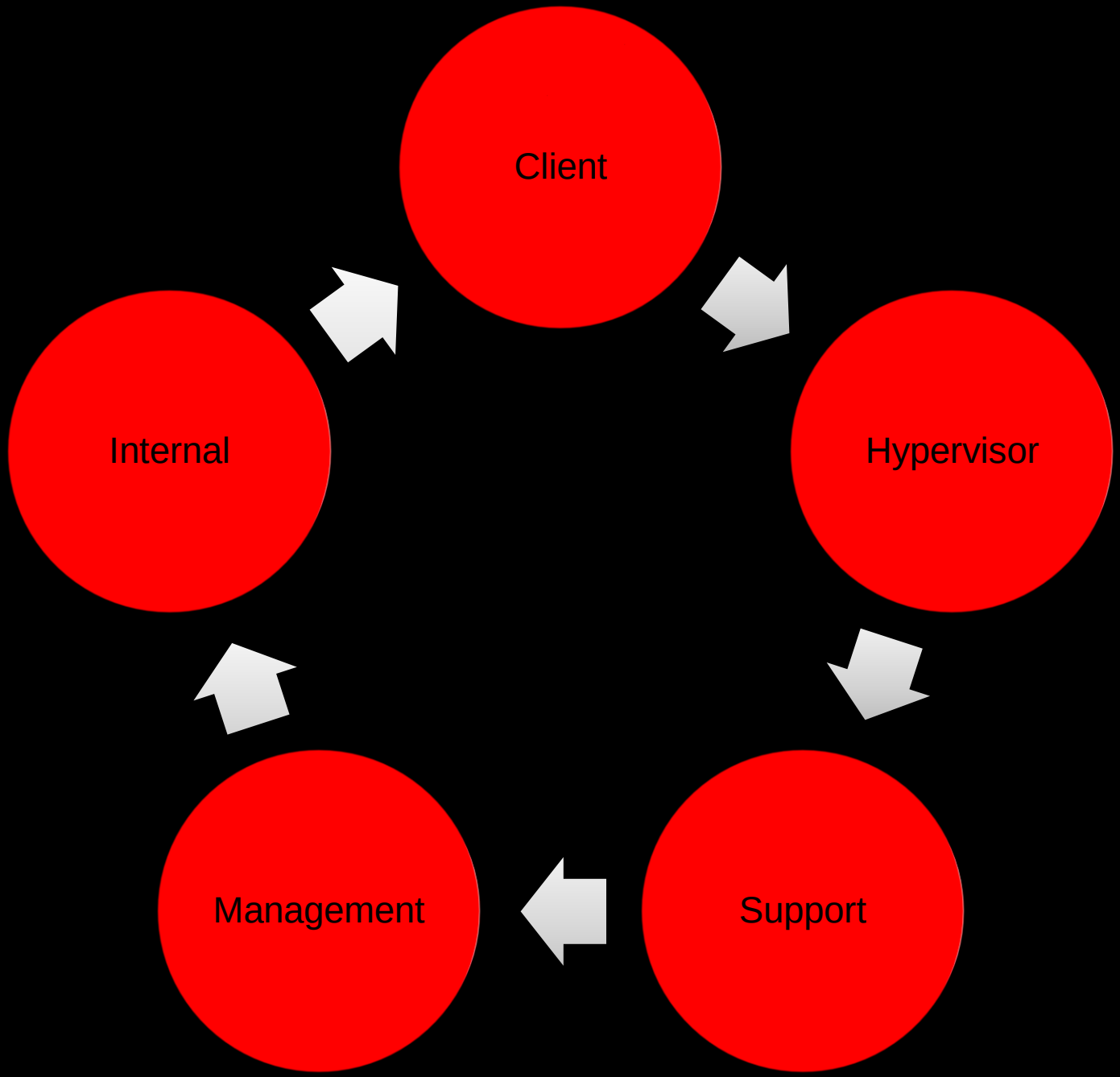
Admin agrees → password sniffed

vmware_login

If nothing works, you can always bruteforce!

Will do standard metasploit bruteforcing

No lockout on standard accounts (unless joined on AD) means a lot of bruteforcing fun


Client
Hypervisor
Support
Management
Internal

What's different?

Multiple local EOP in Virtual Machines

- Will eventually include these as modules as well
- Discovered by great researchers
- Low level attacks, close to the CPU or OS

What else?

Our new Attack surface

Paravirtualization and support tools

vmware_sfcb_exec

CVE-2010-2667

A vulnerability in Virtual Appliance Management Infrastructure resulting in code exec as root

Requires authentication **OR** can be exploited locally without any authentication.

The attack

```
<?xml version="1.0" encoding="UTF-8"?>
    <CIM CIMVERSION="2.0" DTDVERSION="2.0“>
    <MESSAGE ID="13" PROTOCOLVERSION="1.0“>
    <SIMPLEREQ><METHODCALL NAME="SetServerName“>
    <LOCALCLASSPATH> <LOCALNAMESPACEPATH>
       <NAMESPACE NAME="root"/><NAMESPACE NAME="cimv2"/>
    </LOCALNAMESPACEPATH>
     <CLASSNAME NAME="VAMI_NetworkSetting"/>
     </LOCALCLASSPATH>

    <PARAMVALUE NAME="HostName" PARAMTYPE="string“>
    <VALUE>121;$(echo${IFS}ls${IFS}-l)>/tmp/echo</VALUE>

    </PARAMVALUE>
    </METHODCALL>
    </SIMPLEREQ></MESSAGE></CIM>
```

Kudos to Marsh Ray and others for this Twitter-Powered payload ;-)

So, can we attack virtualization?

Summing up

- You can attack the admin client, sniffing the password or owning the administrator
- You can attack the hypervisor and its core modules (by path traversal)
- You can hijack other user's sessions
- You can attack the administration web interface
- You can attack supporting services on the virtual machine

Questions

Pre-made questions to get you started

Q: Do these attacks actually work IRL?

A: Yes, there's a definite patching issue here

Q: What about XEN?

A: Similar issues but… next talk!

Q: They say I have to surrender and be virtualized

A: Not a question. However virtualization can be very good for security!

Thank you

Claudio Criscione

@paradoxengine

c.criscione@securenetwork.it

vasto.nibblesec.org – vasto.securenetwork.it