Security in Organizations (SIO)

Assignment 6 - 2021-2022

Goals:

- Performing a simple Windows and Network IT security audit
- Acquiring experience with drafting an IT security audit report

Instructions:

- This assignment must be completed by a team of two students.
- The assignment must be written with the Times New Roman font, in size 12pt, with normal spacing. The subtitles are in bold, and the margins must be all of size 2.5cm.
- The original numbering of the questions must be indicated for each answer.
- State your answers in a succinct and clear manner.

Deadline:

- Submit the assignment in a PDF document through Brightspace before **2022/01/13 23:59.**

If and only if you do not have a Brightspace access, you can submit your assignment by email to Anna Guinet (see SIO website) in a PDF document.

Introduction:

Treasury Management B.V. (TMBV) is an organization that performs treasury management as a service to international holding companies. A holding is a group of organizations, called subsidiaries, and the holding company is the highest in the hierarchy.

The holding company clients of TMBV have many subsidiaries in many different countries. All these subsidiaries have their own bank accounts in the countries they are based in. In some situations, the subsidiary A of a holding has a (temporary) large surplus of money while the subsidiary B of that organization has a (temporary) lack of money. In that case, it is efficient for the holding to let the subsidiary A lend money to the subsidiary B rather than lending money from a bank, because it is often cheaper for the subsidiary B (and thus for the holding).

The subsidiaries are legal entities of their own, thus although the holding company owns the subsidiaries, the money transfer from A to B is ‘lending’ from an accounting, legal and tax perspective. TMBV facilitates this process by making inventories of the subsidiary needs by communicating with the subsidiaries through phone and email. TMBV is also authorized to perform electronic banking based transactions for these subsidiaries, e.g., to transfer money from the bank account of the subsidiary A to the one of the subsidiary B like in the previous example. To further facilitate this process, TMBV has a single highly sensitive workstation that is used to perform these electronic banking based transactions. This workstation is called SSLF (Specialized Security –

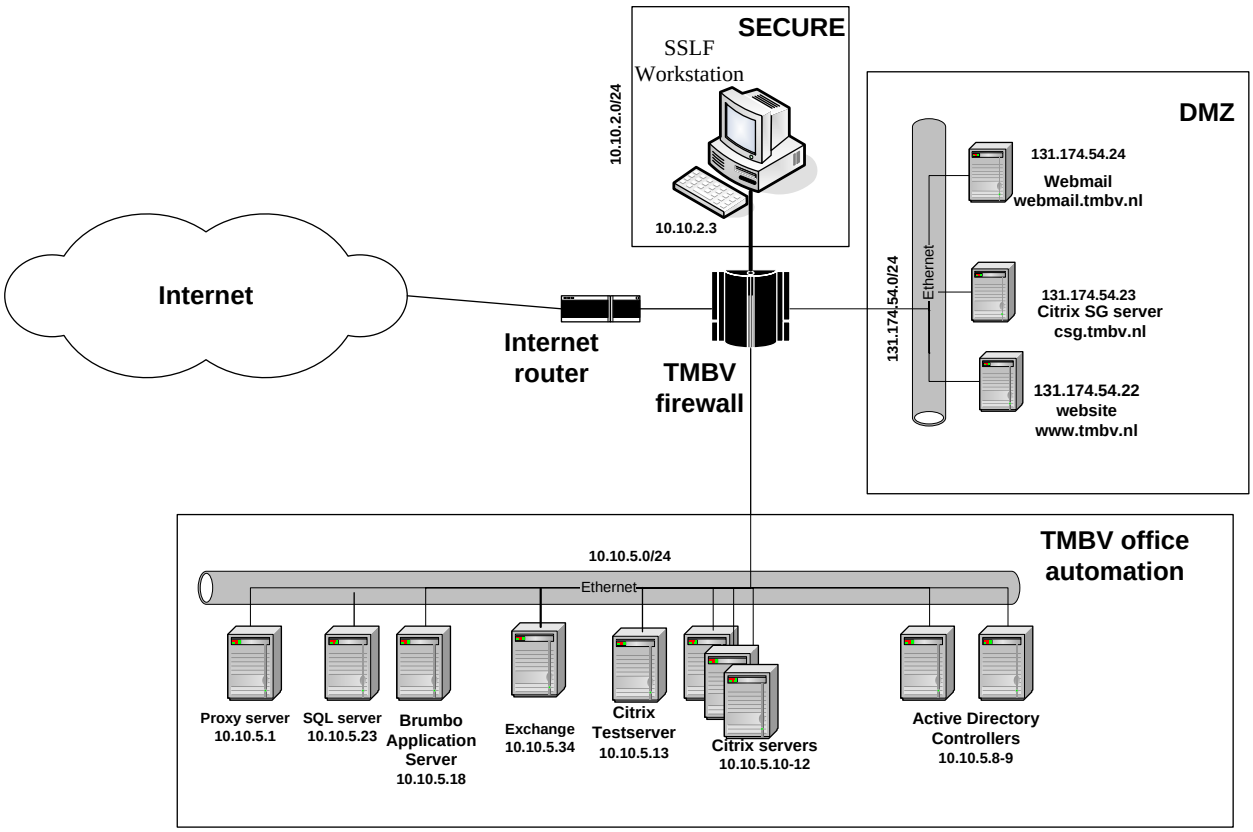
Limited Functionality) and is based on Windows 10 professional. Only the employees of the Treasury department should have access to the SSLF workstation.

Network:

TMBV has three network segments:

- An office automation segment, in which a Windows Active Directory resides with several workstations and various other types of servers. This segment also contains a Citrix farm that makes it possible for TMBV employees to work from home.
- A secure segment in which only the SSLF workstation resides.
- A DMZ that hosts the website of TMBV, a webmail server (Outlook Web Access) and a Citrix secure gateway that makes it possible TMBV employees to connect to through https and –after a successful authentication– are then redirected to the Citrix farm on the OA segment.

These segments are separated by a firewall as is depicted below.



ICT Audit:

The management of TMBV has contracted you as an IT security auditor to perform an IT security audit.

The scope of the audit is the TMBV firewall and the SSLF workstation.

A. Formulate five audit criteria for reviewing the rulebase of the TMBV firewall. Keep in mind the scope of the audit.

B. In the Appendix A, the rulebase of the TMBV firewall is provided. Identify three main negative findings in the rulebase compared to your formulated criteria in the question A. Justify your choice.

C. Examine the Windows Security guide that is provided in both .doc and .pdf format with this assignment. From this document, formulate audit criteria concerning the scope of this audit on:
   a. Password Policy Settings (cf. Table 3.1 of the guide)
   b. Account Lockout Policy (cf. Table 3.2 of the guide)
   c. Audit policy (cf. Table 4.2 of the guide)

D. By running the Windows command *gpedit.msc* [1] in the SSLF workstation, you have access to its settings on Password Policy, Account Lockout Policy and Audit Policy. The result is included in a .pdf file that is enclosed to the assignment. Formulate at least six main negative findings in comparison with your formulated criteria in the question C. Justify your choice.

E. A Windows system contains several groups: the 'Administrator' group that contains the administrative users, and the 'Users' group that contains the regular users. In addition, the employees of the Treasury department have a dedicated group that is called 'Treasury'. Formulate audit criteria for these three groups in at most one sentence for each.

F. In the Appendix B, an excerpt of the TMBV directory is presented. One can use a tool like DUMPSEC tool [2] to get a view of the actual users and group members on the SSLF workstation. The results are included in both a .csv and a .pdf file that is enclosed to the assignment. In your opinion, what is the main negative finding compared to your formulated criteria in the question E? Justify your choice.

G. Examine further the DUMPSEC output that is enclosed to the assignment. Mention at least two other issues compared to your criteria in the question E. Justify your choice.

H. Write a one-page (only) audit report, as part of your opinion. Imagine that this audit report is handled to the upper management of TMBV. Therefore, present your report as discussed in the lecture. Restrict yourself to the criteria and findings you have stated for the previous questions. In addition, include some recommendations for TMBV, and provide a positive or negative assurance.

CALCULATION OF THE GRADE	
Question	Max. points
A. Firewall rulebase audit criteria	1
B. Firewall rulebase negative findings	2
C. Windows Security guide	1
D. *gpedit.msc* negative findings	2
E. Groups audit criteria	1
F. DUMPSEC main negative findings	2
G. DUMPSEC other negative findings	2
H. Audit report	3
SUM	**14**
Grade = (1 + 9*(sum_of_points / 14)) rounded to the nearest 0,5 point.	

#	**Reference**
[1]	Available from http://www.systemtools.com

Appendix A: TMBV rulebase

	RULE	PROTOCOL	PORTS	STATE	SOURCE	DESTINATION	INCOMING ON
1	DENY	*	*	*	#LAN	*	eth2,eth3
2	ACCEPT	UDP	53	*	*	*	eth1,eth2,eth3
3	DENY	*	*	*	#SSLF	*	eth0,eth1,eth3
4	DENY	*	*	*	#LAN	*	eth0,eth1,eth2
5	DENY	ICMP	*	*	*	#DMZBCAST	eth0,eth2,eth3
6	DENY	ICMP	*	*	*	#LANBCAST	eth0,eth1,eth2
7	ACCEPT	TCP	80,443	NEW	*	#DMZ	eth0,eth2.eth3
8	ACCEPT	TCP	*	ESTABL	*	#DMZ	eth0,eth2,eth3
9	ACCEPT	TCP	691,389,1494, 2598,81	NEW	#DMZ	#LAN	eth1
10	ACCEPT	TCP	*	ESTABL	#DMZ	#LAN	eth1
11	ACCEPT	TCP	80,25,21,443	NEW	#LAN	#DMZ	eth3
12	ACCEPT	TCP	*	ESTABL	#LAN	#DMZ	eth3
13	ACCEPT	TCP,UDP	992	*	#WAN	#DMZ	eth0
14	ACCEPT	TCP	80,25,21,443	NEW	131.174.92.89	#SSLF	eth0
15	ACCEPT	TCP	*	ESTABL	131.174.92.89	#SSLF	eth0
16	ACCEPT	TCP	80,25,21,443, 993,110	*	10.10.5.1	#WAN	*
17	ACCEPT	TCP	*	ESTABL	*	#LAN,#SSLF	eth0

eth0 = Interface to WAN
eth1 = Interface to DMZ
eth2 = Interface to SSLF
eth3 = Interface to LAN (TMBV office automation)

#DMZ = 131.174.54.0/24
#DMZBCAST = 131.174.54.255
#SSLF = 10.10.2.0/24
#SSLFBCAST = 10.10.2.255
#LAN = 10.10.5.0/24
#LANBCAST = 10.10.5.255
#WAN = 0/0

NOTE: The SOURCE and DESTINATION columns contain the IP addresses contained in the IP Packet itself. The ‘INCOMING ON’ column indicates the physical interface on which the message comes in.
Thus, for example, the first rule drops packets that come in on eth2 or eth3 and contain a #LAN IP address as source address in the header. This rule enforces users to use the proxy server instead of setting up direct connections to the Internet.

Appendix B: excerpt from the TMBV directory

Name employee	Department/Function	Employment date	Tel. Number
…	…	…	...
…	…	…	...
Jan Klaasen	Treasury	1-1-1998	4523
Piet Pietersen	Treasury	2-4-2003	1256
Marieke Hond	Treasury	*Contract terminated*	-
Jose Petersen	Financial Administration	3-4-2005	1212
Bart Kat	Treasury	*Contract terminated*	-
Tim Korver	Treasury	4-1-2004	7890
Jasper de Vriend	Secretary	5-5-2002	2356
Henk de Bos	ICT Administrator	1-7-1995	1111
Wouter Maat	ICT Administrator	*Contract terminated*	7645
Monique de Snoo	Reception	4-4-1999	1000
…	…	…	...
…	…	…	...