

Security in organizations

Assignment 5, 29 November 2010

Goals:

- Performing a simple Windows and Network IT security audit
- Getting some hands-on with drafting an IT security audit report

Introduction

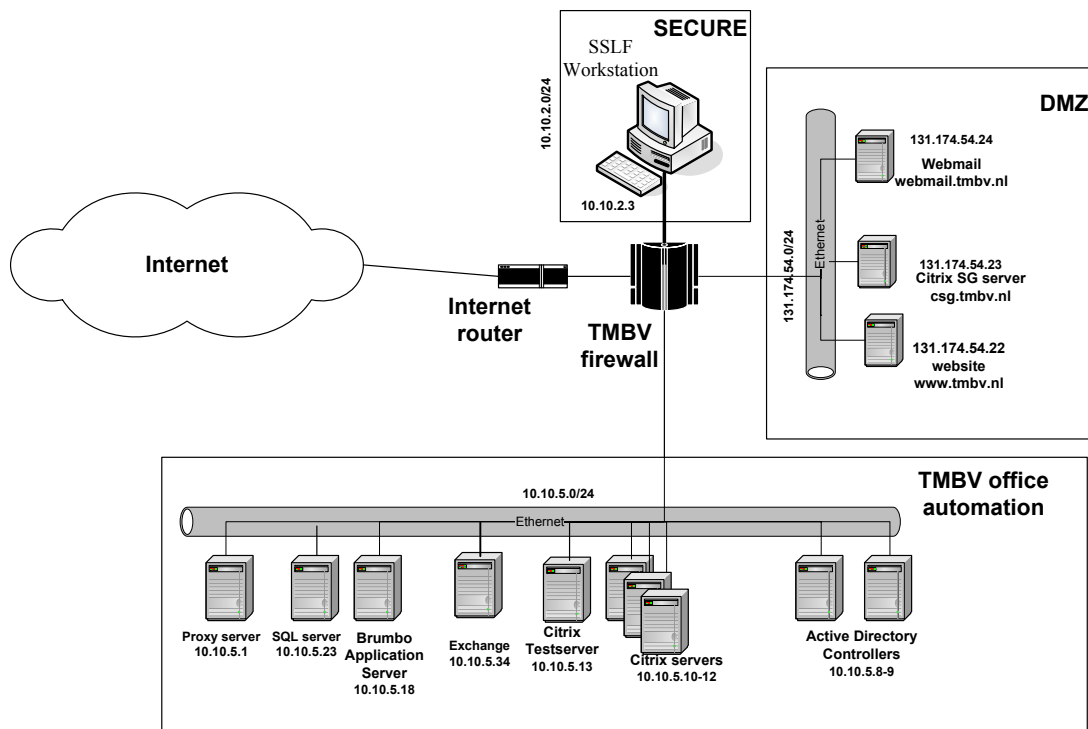
Treasury Management B.V. (TMBV) is an organization that performs treasury management as a service to international holding companies. A holding is a group of organizations, called subsidiaries and the holding company is the highest in the hierarchy: it is the 'boss' of the holding. The holding company 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 subsidiary A of a holding has a (temporary) large surplus of money while subsidiary B of that organization has a (temporary) lack of money. In that case it is efficient for the holding to have subsidiary A lend money to subsidiary B as that is typically cheaper for subsidiary B (and thus for the holding) than to lend it from a bank. The subsidiaries are legal entities of their own, so 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 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. transferring money from the bank account of subsidiary A to that of subsidiary B in the example above. To further facilitate this process, TMBV has one very 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 XP professional. Only the employees of the Treasury department should have access to the SSLF workstation.

TMBV has three network segments:

- An office automation segment, in which a Windows Active Directory resides several workstations as well as various types of servers. This segment also contains a Citrix farm that allows TMBV employees to work from home.
- An 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 allows TMBV employees to connect to through https and – after successful authentication – are then redirected to the Citrix farm on the OA segment.

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



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.

You need to run the VMWARE image provided by Gerard de Koning Gans. The 'Administrator' password is 'tmbv123'.

Questions

1. Formulate audit criteria for reviewing the rulebase of the TMBV firewall
2. In Appendix A the rulebase of the TMBV firewall is provided. What findings do have when comparing the rulebase with these criteria?
3. Formulate audit criteria for reviewing the security patch level of the SSLF workstation.
4. Run MBSA (Microsoft Baseline Security Analyzer, see [http://technet.microsoft.com/nl-nl/security/cc184924\(en-us\).aspx](http://technet.microsoft.com/nl-nl/security/cc184924(en-us).aspx)) on the TMBV workstation (available from the desktop). What findings do have when comparing the security patch level with these criteria?
5. Look at the Windows Security guide (see http://blackboard.ru.nl/webapps/blackboard/execute/content/file?cmd=view&mode=designer&content_id=1217997_1&course_id=41973_1) and formulate audit criteria on
 - Password Policy Settings (cf. Table 3.1 of the guide)
 - Account Lockout Policy (cf. Table 3.2 of the guide)
 - Audit policy (cf. Table 4.2 of the guide)
 - Audit log size (cf. Table 4.27 of the guide)
 - User Rights (cf. Table 4.11 of the guide)
 - Registry settings (cf. Table 4.29 of the guide)
6. By running gpedit.msc in the SSLF workstation what findings do you have when comparing the actual settings with these criteria?

7. A Windows systems has various groups of which the 'Administrator' group contains the administrative users and the 'Users' group the (regular) users. What audit criteria would you formulate for these two groups?
8. In Appendix B an excerpt of the TMBV directory is placed. Run the DUMPSEC tool (available from the desktop) to get a view of the actual users and group members on the SSLF workstation. What findings do you have?
9. Write a one page report on your audit, as part of your opinion make sure the minimal requirements as discussed in the lecture are met. Also include some recommendations.

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.

So, 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 II: excerpt from the TMBV directory

Name employee	Department/Function	Employment date	Tel. Number
...
...
Jan Klaasen	Treasure	1-1-1998	4523
Piet Pietersen	Treasure	2-4-2003	1256
Marieke Hond	Treasure	<i>Contract terminated</i>	-
Jose Petersen	Financial Administration	3-4-2005	1212
Bart Kat	Treasure	<i>Contract terminated</i>	-
Tim Korver	Treasure	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	<i>Contract terminated</i>	7645
Monique Baars	Reception	4-4-1999	1000
...
...