Lab Report 16

1. Assessment Sheet
2. **Why is it recommended to update the antivirus software’s signature database before performing an antivirus scan on your computer?**

The reason why we need to continuously update our antivirus signature database is that the virus varied day to day. If we don’t update our database, we cannot effectively detect fresh virus and might cause huge losses for company.

1. **What are typical indicators that your computer system is compromised?**

The most typical indicators are as followings

* The running speed of browser becomes slow
* Applications behave abnormally
* Operating systems cannot star up normally
* Numerous windows pop-up and hard to close them all.

1. **Where does AVG Anti-Virus Business Edition place viruses, Trojans, worms, and other malicious software when it finds them?**

The AVG stores these detected items in Virus Vault.

1. **What other viruses, Trojans, worms, or malicious software were identified and quarantined by AVG within Virus Vault.**

LSASecretesView.exe, harmful program logger, harmful program Tool, harmful Remote admin

1. **What is the difference between the complete scan and the Resident Shield?**

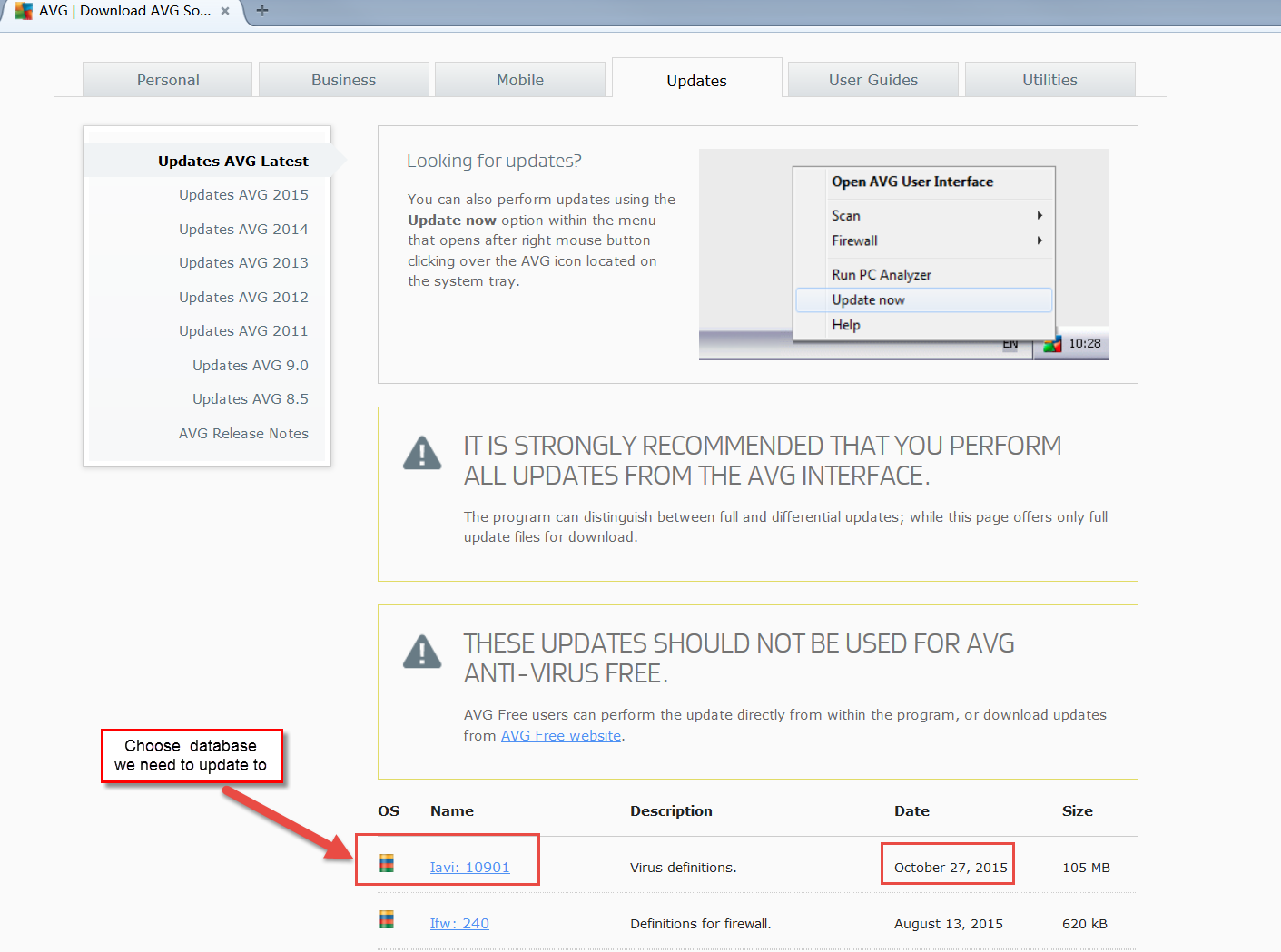
The complete scan will scan the entire files on the operating systems, which will run both manually and automatically by setting up schedules while the Resident Shield runs in the background and it monitors the state, open, copy, save of file/directory. Once the file or directory which contains virus was opened, saved, copied, then the Resident Shield will generate alert to user.

1. Challenge Questions

**Description: 1) Descript the steps needed to update AVG offline and why might someone want to update their antivirus software offline? 2) Assuming that users will be connected to the Internet, what security countermeasures can organizations implement to help mitigate the risk from viruses, malware, and malicious software?**

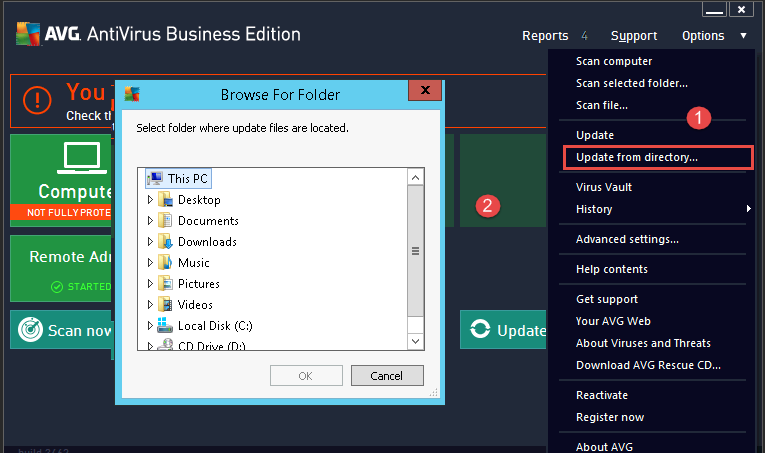
1. Steps to update AVG offline
2. Go to the website to download AVG Virus updated database

Download updates URL: [www.avg.com/update](http://www.avg.com/update)



1. AVG **->** options **->** update from directory

In this step, we choose “update from directory” option in AVG, and choose the updates we downloaded in step 1.



1. Click “OK”

After chosen the update, then click the “Ok”, the AVG will install this update automatically.

1. Why someone want to update AVG offline

In some cases, the host might not be able to connect to Internet – shutting down of the server, but the updating of AVG database is have already scheduled at that time. Once schedule is unable to run, we need to update AVG manually.

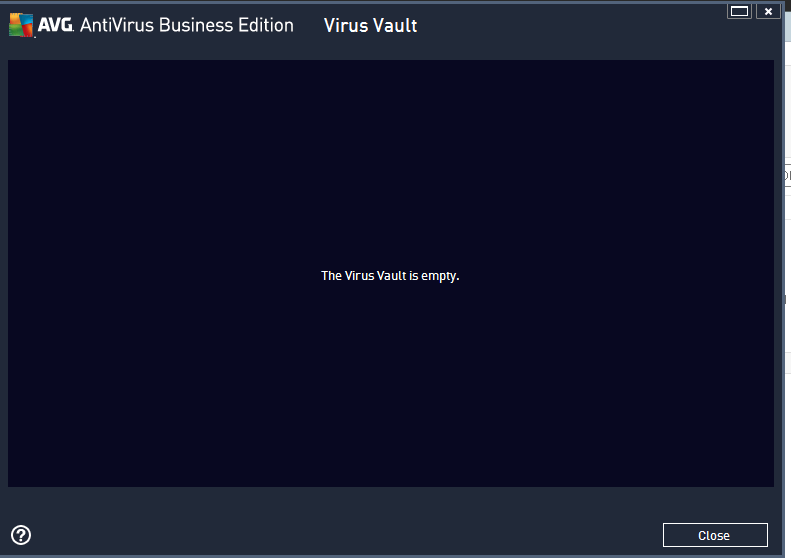
1. If user can network, how does company to mitigate

The company should setup firewalls to stop malicious program or request from coming into the company’s network. In addition, company should install anti-virus software on each individual hosts, which can prevent some malicious software that bypass the firewall.

Reference:

1. killertechtips. (2009, 4 21). How to Update AVG Offline Without Internet Connection? Retrieved 10 28, 2015, from killertechtips.com: http://www.killertechtips.com/2009/04/21/update-avg-offline/

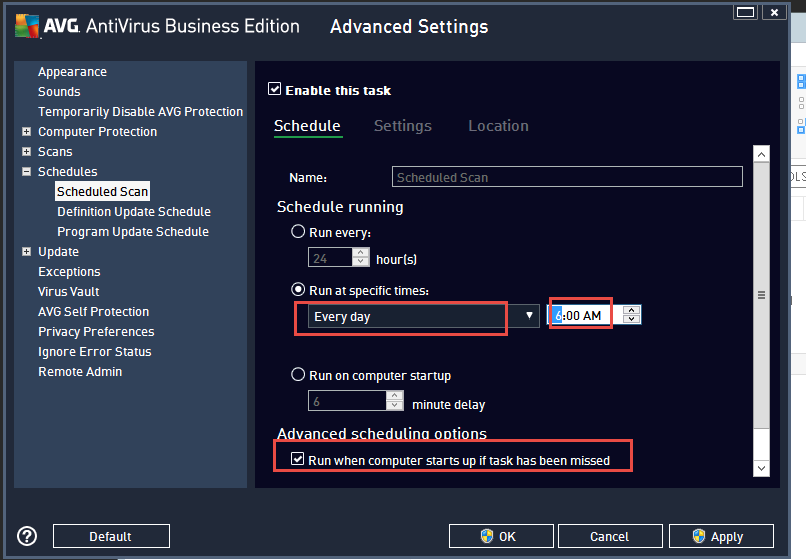
1. Report Screenshot
2. The empty of Virus Vault



Explanation:

In this case, we deleted all the suspicious files within virus vault.

1. The screenshot of AVG schedule



Explanation:

In this case, we set up AVG run as the following schedule.

* AVG runs every day on 6:00 AM
* If the schedule time passed and the schedule haven’t run, then when the computer startup, run the schedule.

1. Other additional supporting text/image content