Muhammad Izham Bin Norhamadi
B032020039

Lab 8

Question 1 – Using behavior-based monitoring tools

a) What is behavior-based security?

Behavior-based security is a proactive approach to security in which all relevant activity is monitored so that deviations from normal behavior patterns can be identified and dealt with quickly. This type of security works a little different than the traditional signature based security where the monitored data streams are compared with baseline normal behavior to look for anomalies.

b) Explain 3 benefits of behavior-based security.

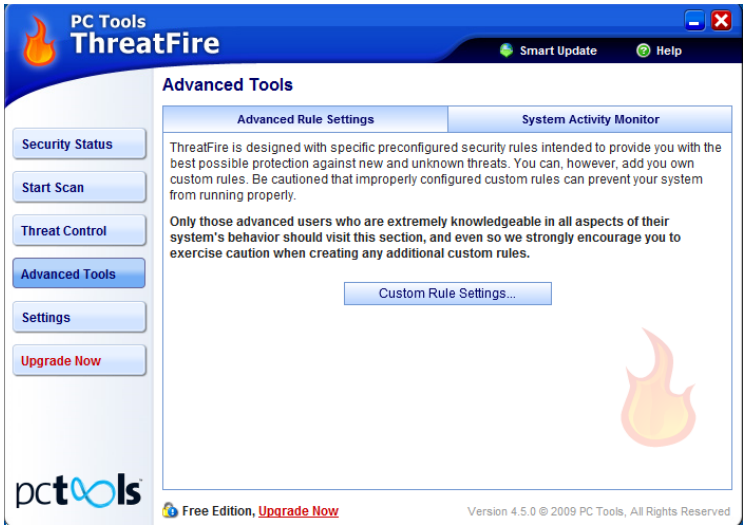
- Behavior-based security is best for zero-day exploits where the latest threat has not made into the list of known threat signatures
- Most behavior-based security programs comes with set of policies on what behaviors are allowed, administrators can customize these policies aswell
- Applies machine learning algorithms that boosts security analysis on what comprises of normal behavior

c) Explain 4 features of ThreatFire.

- Realtime Spyware and virus protection to detect malicious activities on system

- Rootkit Scan for any hidden rootkits/backdoor

- Threat Control Center to display scan results and quarantined programs



- Custom advanced security rules and activity monitor

Question 2 – Using Internet content filter

a) What is internet content filter?

Internet content filter is the practice or use of program to block or exclude access to web content that may be deemed offensive, inappropiate, or dangerous.

b) Why is internet content filter is important?

Internet contenting filtering will prevent user access to harmful, malicious and unsafe websites and contents and is suitable to protect workplace with stringent internet access policies.

c) Explain 5 features of Kurupika Web Filter.

- Web filter – Protects user from unsafe and harmful websites
- Allow and Block Websites – Provide user settings to allow or block particular websites
- Time Controls – Monitor user's time and set usage limit for any time consuming websites
- Application Filter – Blocks harmful applications from running on the system
- Capture Screen – Provides a screenshot tool to capture any running software.

Question 3 – Secure wireless network

Two security methods/settings to secure wireless network

- Enable network encryption to secure the network, the most recent and effective encryption is WPA2
- Install and active a good firewall solution for connected devices such as PCs and routers, firewall helps filters the network traffics from malicious attacks.