CPEN 442, Fall 2015 KEYs

Quiz #4

Your Family name: _____

Your Given name: _____

Your student ID: _____

Your CPEN 442 alias: _____

_____

#	Points	Out of
1		4
2		4
3		6
4		2
5		3
6		5
TOTAL		24

Notes:

- Make sure your handwriting is legible. If the teaching staff does not understand what your wrote, they mark your answer as if the unreadable text is missing.

- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

- As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.

- Don't panic if you feel like you are severely short on time. Everybody is. ☺

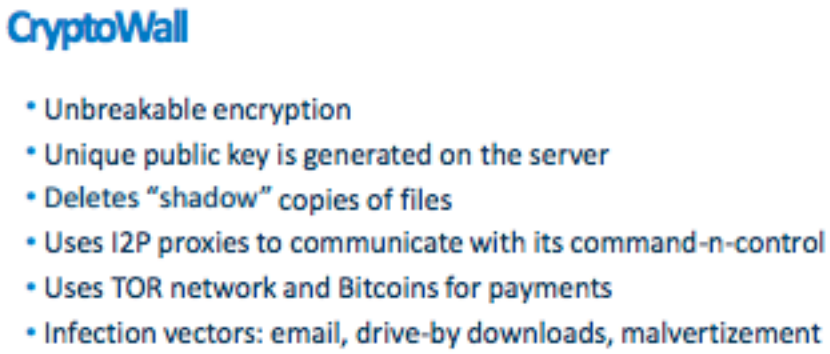
1. **(4 points) Explain what DGA acronym (in the context of Botnets) stands for and how DGA works and what it's used for.**

DGA is Domain Generation Algorithm
The algorithm allows selecting a domain name from a specific set of pre-registered domain names, so that the defender has no direct visibility which one is going to be used.

2. **(4 points) Why would a piece of malware use encryption/decryption and compression?**

To delay malware analyst.
Ransom.

3. **(6 points) List the 6 design features of CryptoWall.**



Mentioning user-friendly interface gives a point.

4. **(2 points) What's one most important thing any end-user can do to protect their personal computer from those zero-day exploits that are produced by reverse engineering security updates released by software vendors?**

Keep up with security updates, i.e., apply updates right away.

5. **(3 points) What is an APT and how is it different from the threat of an opportunistic attack?**

Advance Persistent Threat
APT is a targeted attack, while opportunistic is not.

6. (5 points) What are Botnets used for (five use-cases)?

Botnets use

1. Email spam
   - "Grum" ~ 200,000 PCs
   - "Rustock" ~ 815,000 PCs
2. Web spam
3. DDoS
4. "Installs"
5. Information stealers