Assignment 6

Abbas Khan , Mariia Rybalka , Linara Adilova

June 27, 2016

Task 6.1 (theoretical): Fast-Flux, Double-Flux

Task 6.2 (theoretical): Buzzword Bingo

Used material - [?].

Task 6.3 (theoretical): Firewalls

Task 6.4 (theoretical) TOR

Task 6.5 (practical): Simple Buffer Overflow

Task 6.6 (bonus) Multiple Choice

Q1: What ISO/OSI layers does a packet filter usually inspect? - 1) Layer 1 and 2
Q2: What method can NOT be used during a TLS connection establishment (to an HTTPS webserver)? - 3) RADIUS
Q3: Which key(s) belong into an X.509 certificate? - 2) The public key
Q4: Consider you want to connect to a LAN that has 802.1X-controlled ports. What traffic is allowed to pass before a successful authentication? - 1) EAPoL

Task 6.7 (bonus) Citing Correctly

"Centralized botnets are easy targets for takedown efforts by computer security researchers and law enforcement." [1] However, there are also peer-to-peer botnets.
...
The authors propose a graph model to capture the vulnerabilities of P2P botnets and apply it several malware families in order to asses their resilience against different attacks [1]. ...

References

[1] SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets *Plohmann et al.* Fraunhofer FKIE, Bonn, Germany, daniel.plohmann@fkie.fraunhofer.de