ISCX
Information Security
Centre *of* Excellence

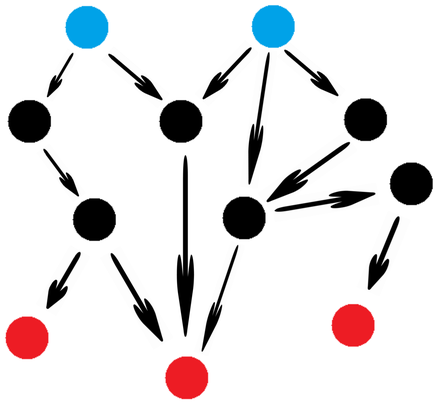
Graph-Based Risk Assessment of Network Assets: An Application to Botnet Mitigation

Amir Pourafshar, Hadi Shiravi, and Ali A. Ghorbani

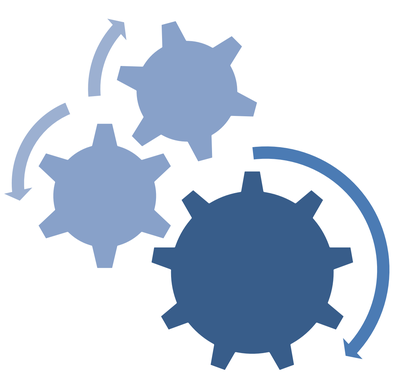
Botnets, defined as a network of infected machines, have become the predominant factor behind malicious attacks such as DDoS, spam, and click fraud. Reflecting the relationship between network assets and their importance to an enterprise, understanding the most critical threats, and selecting the most effective countermeasures can provide continuous visibility into the effectiveness of maintaining protection of critical assets. By accurately measuring risk for enterprise networks, attack graphs allow administrators to identify components of their networks that possess higher security risks. We combine the measurements of individual vulnerabilities obtained from attack graphs into a probabilistic security metric that can be used to assess host risks, accelerate mitigation processes, and protect vital assets.

Network Topology

Vulnerability Scan Report



Attack Graph Generation



Host Ranking Algorithm

Step 1.

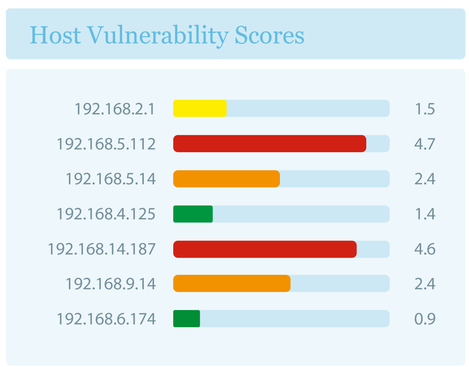
1) Extract vulnerabilities for each host.
2) Define network topology.

Nessus is the most predominant vulnerability scanner available, capable of generating vulnerability analysis reports. OVAL is the Open Vulnerability and Assessment Language which accompanied by the OVAL interpreter serves as the base engine of many vulnerability scanners.

Step 2. Automated analysis of network configuration and host vulnerabilities provides an attack graph showing all possible paths to critical assets.

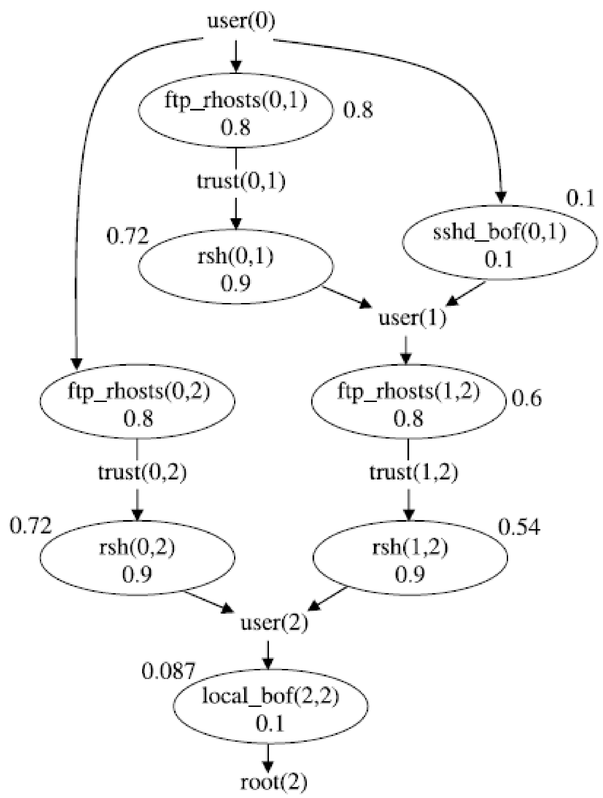
Step 3. The host ranking algorithm receives an attack graph G with individual scores assigned to all vertices as input. Then outputs is a set of cumulative scores for all vertices of G.

Step 4. Finally, scores are assigned to hosts. Hosts are ranked and sorted based on their vulnerability scores. The network administrator is now able to easily identify critical hosts and mitigate potential threats.



Network Host Vulnerability Score

Host Ranking Algorithm:



Attack graph: Models how multiple vulnerabilities may be combined for advancing an intrusion.

Condition: Represents the system state ***Exploit:*** Transition between system states

Individual Score (Inside oval): The probability whether an attacker has the skills and resources to execute an *exploit*, and whether he/she will choose to do so.

Cumulative Score (Outside oval): The likelihood, or the fraction of, attackers who will successfully exploit an event or satisfy a condition in a given network.