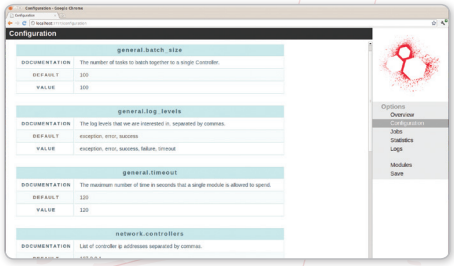
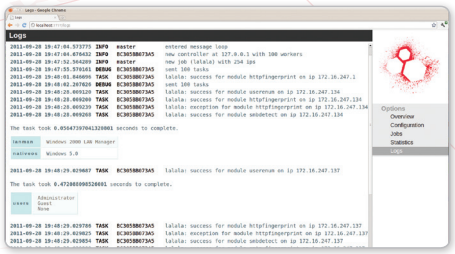
SWARM

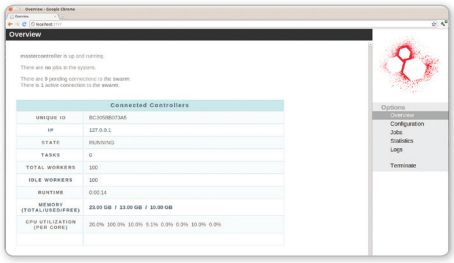
LARGE-SCALE RECONNAISSANCE AND EXPLOITATION

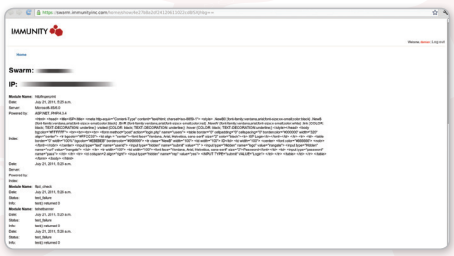
Immunity's SWARM

SPEED + INTELLIGENCE









Overview

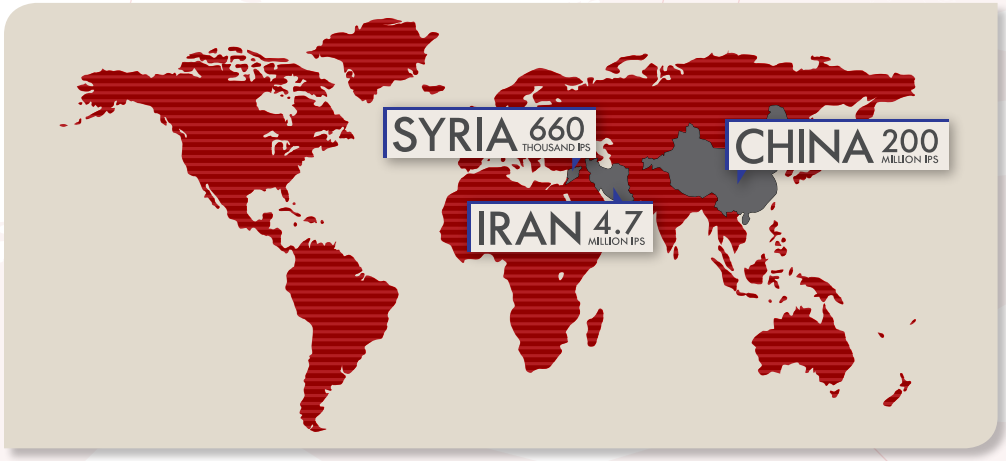
Traditionally penetration testing tools target hosts one at a time. **SWARM** differs in that it can deploy any CANVAS module, exploit or reconnaissance tool against large sections of a cyber range in minutes to hours.

Technology

- The entry-level **SWARM** (installed on a 4U micro-cloud) can scan and actively exploit a million IPs per hour. Because CANVAS uses Python, it is easy to create new modules; **SWARM** allows you to run those modules distributed across virtual machines and targeting IP ranges or specific hosts.
- Each time **SWARM** runs a CANVAS exploit module an actual unique exploitation attempt is made – no replaying of PCAPs! This technique allows you the highest possible assurance that a target is or is not vulnerable. Exploitation attempts can utilize CANVAS's industry-leading covertness features including: RPC fragmentation and SMB encryption.
- Once a target is successfully exploited **SWARM** uses CANVAS trojans that can egress via HTTP, SSL, DNS and standard TCP.
- After a host is exploited you can leverage the CANVAS library of local privilege escalation exploits, many of which are unavailable elsewhere. Likewise, follow on attacks and reconnaissance can target the internal network of a penetrated host and can be started automatically.
- All your results are stored in MongoDB which is designed to be free, extensible and adaptable.

Scalability

- **SWARM** is fast enough to run multiple times a day against even the biggest set of IPs. This allows for massive returns during your testing and modeling.
- **SWARM** is designed to scale! Need quicker results or attacks against larger ranges? Just add additional VMs to the micro-cloud.



SWARM includes a subscription to CANVAS Early Updates – which often has exploits not found elsewhere and which are typically first to market. For example, the exploit for **Samba NDR** heap overflow (CVE-2012-1182, CVSS: 10) is included in **SWARM**, along with exploits for the Microsoft Padding Oracle (CVE-2010-3332, CVSS: 5.0) vulnerability.

Resources: **http://www.darpa.mil/Our_Work/STO/Programs/National_Cyber_Range_(NCR).aspx**

IMMUNITY

Phone (786) 220-0600 | Fax (786) 513-8100 | admin@immunityinc.com | www.immunityinc.com