Multiplayer Metasploit

Tag-Team Pen Testing and Reporting

Ryan Linn

Defcon 18

Outline

- Description of Problem
- Discussion of current solutions
- Overview of XMLRPC database integration
- Discussion of types of objects
- Demos

What's the problem?

- Pen testing/security audit teams need to share information
- How do you plan further action?
- What about deltas from previous tests?
- No easy way to automate reporting

Analysis of current solutions

- Dradis - best alternative, imports data great, but hard to further actions, no integration with other tools
- Leo - geared toward one person and logging/reporting only
- Wiki - multi-user but arbitrary organization, hard to convert to further action or reporting

OVERVIEW OF SOLUTION

- Metasploit is readily available
- Extend XMLRPC to facilitate DB transactions
- XMLRPC extension allows central logging
- All information is actionable
- Data can be added real time

Types of Objects

- workspaces - separate spaces for data
- hosts
- services
- vulns
- notes - general purpose data storage
- events - log of commands executed
- loots - phat loots lives here
- clients - web clients
- users - users + credentials

Workspaces

- Values:
  - name
  - created_at
  - updated_at
  - boundary
  - description

Hosts

- created_at
- updated_at
- address
- address6
- mac
- comm
- name
- state
- os_name
- os_flavor
- os_sp
- os_lang
- arch
- purpose
- info
- comments

Services

- host
- port
- proto
- state
- name
- info

Vulns

- host
- service
- name
- info

Notes

- ntype
- service
- host
- critical
- seen
- data

Events

- host
- name
- seen
- critical
- username
- info

LOOTS

- host
- service
- ltype
- path
- data
- content_type
- name
- info

Clients

- host
- ua_string
- ua_name
- ua_ver

Users

- username
- crypted_password
- password_salt
- persistance_token
- fullname
- email
- phone
- company
- prefs

Demos

- Service Startup
- Launching Nmap with Nsploit
- Storing BeEF data in Metasploit
- External report generation
- Diffing workspaces

Thanks

- Defcon staff and attendees for a great conference
- Heather Pilkington, Scott Hilbert, Jonathan Cran, HD Moore, Egypt, anyone else I've forgotten
- Fyodor, Wade Alcorn for Nmap and BeEF

Contact Information

- IRC: sussurro
- Twitter: @sussurro
- Blog: blog.happypacket.net

Questions?