Intro to Penetration Testing: RECON

October 4th 2017
Brown Bag Talks

11:00 PM on Friday, ECSS 4.619

Come and join us for security discussions during lunch
Phases of Penetration Testing

1. Reconnaissance - gathering all information on the target, this data will be used when password guessing or scanning for vulnerabilities
2. Enumeration - scanning the target for all servers/apps, seeing open ports and running services that could be used for exploitations
3. Exploitation - the best part, getting into the system. Using the knowledge of recon and enum to exploit and password guess into the target
4. Persistence - leaving a backdoor or path to get access to the system/service later in case the system admin patches or you need quicker accessibility.
5. Clean up - removing any trace you gained access and left persistence, Replacing logs, deleting dropped files, etc.
What is the Point of Recon?

1. Making enumeration easier
2. Understanding your target
3. Finding things that scanning can not find
4. Making password guessing easier
OSINT- Open Source Intelligence

- [https://osintframework.com](https://osintframework.com) - A list of all open source intelligence gathering tools that can be used on a target depending on what the target is.
- **Looking up the target on search engines**
  - Find any information that may help you password guess, understand how the target sets things up
  - **Internal System Information**
- **Searching the domain for information**
  - Whois record, DNS record, Reputation, Server Location, Certificates
  - Scraping the domain for all email address, and names
  - Documents, Videos, Images
  - Social Media Accounts
  - Leaked Passwords
- **Public Records**
  - History of the target
  - Locations, Services, Interactions
  - Venders they have used
Tools of the Trade

1. Every search engine ever
2. Google Dorks - ex: site:domain.com - searching google with context
4. theHarvester - Finding Emails, DNS, Subdomains, by mass searching different locations
   a. API's not required but preferred
5. Recon-ng - Like metasploit for recon, searches every api you give it in a nice format
   a. API's required
6. AQUATONE - Similar to previous two but more of a brute force approach
Google Dorks

- `inurl:"Port" and intext:"Login Portal Title"` - find login portals and unique applications
- `Site:domain.com and ext:.key` - finds all extensions in domain that end with .key
- `inurl:login/admin/` - find admin portals
  - `inurl:login/admin/ -https` - for only https
  - `Put site:domain.com in front to only search for ones with specific domain`
- `site:pastebin.com intext:"*@*.com:*"` - searches pastebin for mailist and password lists
- "-----BEGIN RSA PRIVATE KEY-----" ext:ke… -finds private keys online
  - `Partner with site:domain.com to search domain`
Shodan.io

- Search for a domain - Boom information
- Find Services and Servers that are running, with all public information you want
- Good for determining where and what they are running so you can prepare for that during enumeration, exploitation, persistence, and clean up.
theHarvester

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google, bing, bingapi, pps, linkedin, google-profiles, people23, jigsaw, all)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-e: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with (bing goes from 50 to 50 results,
-h: use SHODAN database to query discovered hosts

go google

Examples:/theharvester.py -d microsoft.com -l 500 -b google
/theharvester.py -d microsoft.com -b pps
/theharvester.py -d microsoft.com -l 200 -b linkedin

[0] Hosts found in search engines:

23.30.3.111:www.nasa.gov
54.109.106.225:www.gsfc.nasa.gov
198.122.121.196:jsc.nasa.gov
128.187.173.182:summerthoday.nasa.gov
128.183.194.178:gsfc.nasa.gov
23.182.49:science.nasa.gov
109.154.142.53:aviso.gsfc.nasa.gov
128.187.183.247:earthobservatory.nasa.gov
129.164.719.22:go.nasa.gov
65.58.184.18:go.nasa.gov
23.62.3.18:spaceflight.nasa.gov
128.183.186.93:aba.gsfc.nasa.gov
109.164.719.2:theserver.gsfc.nasa.gov

[1] Hosts found in search engines:

0.0.0.0

Reminder About Recon

You can never have too much information when you are first starting! Overtime you will find out what is useful and what is not.

1. DNS
2. WHOIS
3. Emails
4. Certificates
5. Passwords/Keys
6. Services
7. Servers
8. Login Portals

Just a few of the many things to look for when doing recon
Questions?