**Recon-Tool - Ash Nazg**

Recon-Tool - Basic goal is to create a Penetratoin testing / Recon Framework so that the vulnerability scanning on a target is better and more effiecent. Also I'm tired of running the same commands over and over again.

Depending on code complexity this project may get ported to python. At this point the game plan is to make a list of tools and see what works and go from there.

**Order of Ops**: **Passive Recon 🡪 Site Mapping 🡪 Active Recon 🡪 Manual Resources 🡪 Exploitation**

**Profile**

Domain: Example.com

IP Address: 192.168.11.1 (NSLookup Info)

Operating System: Windows / Linux

Server Host Software: IIS / Apache / Tomcat

Server Software: IBM WebSphere, Adobe, ASP, etc (nmap -sV hostname?)

Port List:

Website Map (crawler):

Wayback Enum:

**Passive Recon**

Whois

NSlookup

Wayback Enum

TheHarvester

Google Dorking

**Precondition**

Website (ie google.com) says HTTP/1.1 200 OK

**Site Mapping**

msfcrawler

maltego

skipfish

**Active Recon**

Nikto

nmap (http-enum, etc)

Robots.txt

dirb

Need a way to identify the Web Server Software (ie Adobe, iis, oracle, etc): Wappalyzer

**Manual Resources**

ViewDNS.info (website)

Pipl (website)

Netcraft (website)

Sn1per (all-in-one)

Google Analytics ID (Just to find what other sites are using the same ID)

WAppalyzer

pentest-tools.com (website)

**Exploitation**

sploitus.com (based on webservice)

Burpsuite