**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.

**LEGAL DISCLAIMER:**

Usage of Recon-Tool / Ash Nazg for attacking targets without prior mutal consent is illegal. It is the end user's responsibility to obey all applicable local, state, and federal laws. Deveopers assume no liability and are no responsible for any misue or damage caused by this program.

**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 (WhatWeb)

Port List:

Target Website Map (crawler):

**Precondition**

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

**Passive Recon**

Whois

NSlookup

Wayback Enum

Google Dorking: Recon-ng (recon/domains-hosts/google\_site\_web)

**Site Mapping**

msfcrawler

maltego

skipfish

**Active Recon**

Nikto

nmap (http-enum, etc)

Robots.txt: Recon-ng (discovery/info\_disclosure/interesting\_files)

* Run on 443 / HTTPS
* Run on 80 / HTTP

Dirb (brute force tool)

Whatweb (ID Server Software)

**Manual Resources**

ViewDNS.info (website)

Netcraft (website) – Use Recon-NG

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

**Social Engineering**

TheHarvester

Pipl (website)

Social Engineering Toolkit (SET)