

Hunter / Gather

Finding that low hanging fruit.



Sean Arries
Security Engineer
Terremark Worldwide

About Me..

- Member of the Terremark's Threat Intelligence Team, a division of the Secure Information Services group. The Team provides clients around the world with rapid incident response, memory forensics, malware reversing and other critical security services including evaluating security posture through vulnerability assessments and penetration testing. The team is also tasked with staying up to date with the latest threats in the Information Security world. (we have a good time)
- personally.. I like web stuff.... Python.. And riding my motorcycles..



What this is...

- It is a methodology to owning your target the lazy way, instead of the Chinese way..
- Basic and used by APTs everywhere.. From their parents basement owning your network and stealing your Certs!
- Having a strong methodology is just as important as having the exploits..
- What is the point in having exploits from an attackers point of view if you can't use the exploits to your full benefit in penetrating your targets?

Why we need to know this....

- Most organizations today use some form of 'known' web application. Whether its an open source or closed source application.
- These applications are the gate keepers to the internal network.
- Understanding how to find vulnerable web applications has a couple side effects.
 - Discovering a detailed inventory of what an organization has exposed to the internet
 - Aids in creating a comprehensive web application planning and assessment methodology

How do we raise the attack surface?

- www.targethost.com
- Small attack surface.. Single host.. Attacker may not find a way on, at first look.
- Raising the attack surface with a simple methodology..
 - 1. Finding sub domains.
 - 2. Finding net blocks.
 - 3. Finding web servers.
 - 4. Finding vhost domains on target IP
 - 5. Finger print web applications on target domain / vhost.

Attack surface to Attack success?

- With company (X) having (XX) net blocks, there could be (XXX) amount of domains per-IP with (XXXX) web applications per-domain per-IP.
- If target is a small time web site hosted on shared hosting we only have to fingerprint applications on domains for one IP.. How many out dated WordPress blogs can we find in 200 Domain names?
- What if the target is slightly larger?
 - Then company (X) probably has a few net blocks at least.. Probably old Jboss.. Old Blogs.. Or some phpMyAdmin somewhere or SOMETHING.. How many old PHP blogs can we find on 200 IP's?
- Lazy people make it possible for lazy people to own them.
 - Don't update or patch or keep up with your applications? You will get owned..

Applying these tactics..

- Since we are talking about penetration and offensive security here.. What better than an example to show how to theoretically have “non-consensual ways” with a porn site :D
- Target: xhamster.com – russian owned porn network.
 - Note: We will just recon the network in a few examples, since we don't want to cause any harm.
 - And of course we didn't go any farther than mapping out what's what.. :>
- Now lets get on with it..

Finding Subdomains..

- Google Dorks - site: | inurl: | filetype: | intext: | intitle:

The screenshot shows a Google search interface. The search bar contains the query: `site:xhamster.com -new -stories -channels`. The search results are displayed on the right side of the page. The first result is titled "Tranny Tube - Tranny Porn -" and includes tags such as "ass", "cock", "fingering", "fucked", "fucking", "hardcore", "horny", "moaning", "sex", "shemale", "titties", "tranny", and "transsexual ...". Below the title, there is a link to `download.xhamster.com/` marked as "Cached".

The second result is a "[FLASH] LOADING" message, indicating a file format of "Shockwave Flash". Below this, there is a link to `static.xhamster.com/xplayer14.swf` marked as "Similar".

The third result is another "[FLASH] LOADING" message, also indicating a "Shockwave Flash" file format. Below this, there is a link to `static.xhamster.com/xplayer17.swf`.

The fourth result is titled "King-901's Profile" and includes the text: "We're: Couple. Seeking: Woman. Country: United Kingdom. About Us: My profile has recently changed... I have now changed my personal information to a Couple! ...". Below this, there is a link to `xhamster.com/user/king-901` marked as "Cached".

The fifth result is titled "Sexy-berlin's Profile" and includes the text: "Found a technical problem? Please report it to make xHamster better! Sign Up | Login. Video, Pictures, Stories, Blogs, DVDs ...". Below this, there is a link to `xhamster.com/user/sexy-berlin` marked as "Cached".

On the left side of the page, there is a navigation menu with options: "Everything", "Images", "Videos", "News", "Shopping", and "More". A red arrow points from the "Videos" option to the search results. Below the navigation menu, there is a location setting for "Miami, FL" with a "Change location" link. A red arrow points from the "Change location" link to the search results. At the bottom left, there is a "Show search tools" link.

Finding Sub domains cont...

- Brute force sub domains.
 - Not very hard to write a few lines to brute force .domain.ext
 - Or, if you're lame.. Or have budget and no in house people.
 - Acunetix – Webinspect – dnsmap – knock

```
[+] Bruting: xhamster.com
[+] Threads: 20

[+] Words Loaded: 1906
=> Domains: 11 | Finished/Total: 1906/1906 | Complete 100%

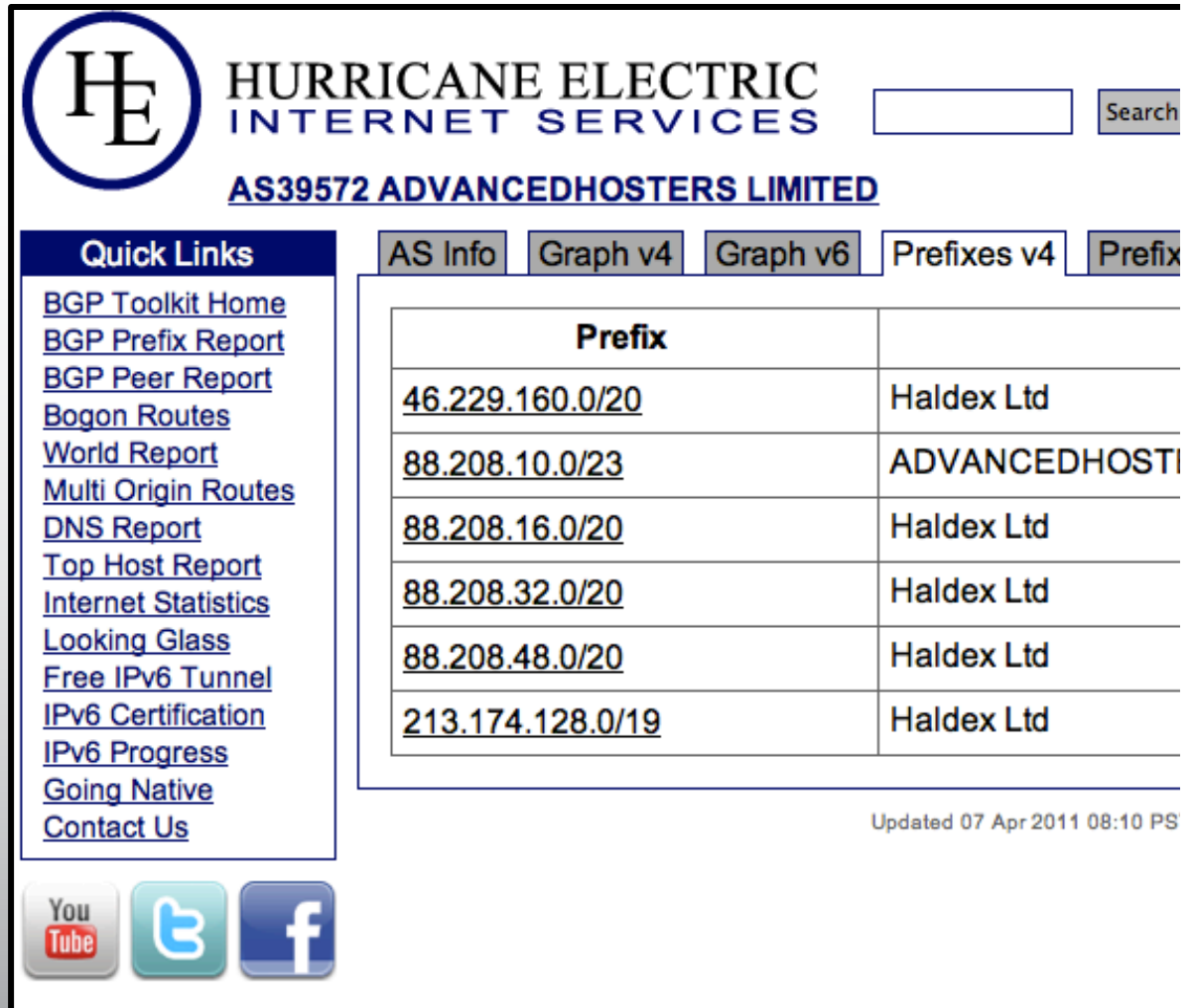
[+] Sub-Domains Found

88.208.23.103 : ads.xhamster.com
88.208.17.30 : download.xhamster.com
88.208.24.43 : mobile.xhamster.com
88.208.24.43 : ns1.xhamster.com
88.208.24.45 : ns2.xhamster.com
88.208.16.86 : partners.xhamster.com
88.208.24.43 : secure.xhamster.com
88.208.12.1  : st.xhamster.com
88.208.24.44 : static.xhamster.com
88.208.24.5  : upload.xhamster.com
88.208.24.44 : www.xhamster.com

[+] done
```

Finding NetBlocks..

- Good old ./whois
- If you like a web app
 - www.ripe.net
 - www.arin.net
 - bgp.he.net
- Now we know what other net block's relate to our target network..



HE HURRICANE ELECTRIC
INTERNET SERVICES

AS39572 ADVANCEDHOSTERS LIMITED

Quick Links

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefix

Prefix	
46.229.160.0/20	Haldex Ltd
88.208.10.0/23	ADVANCEDHOSTI
88.208.16.0/20	Haldex Ltd
88.208.32.0/20	Haldex Ltd
88.208.48.0/20	Haldex Ltd
213.174.128.0/19	Haldex Ltd

Updated 07 Apr 2011 08:10 PS

YouTube | Twitter | Facebook

Finding Web Servers..

- NMAP
 - Works fine for me..
- Acunetix
 - Has a built in web server finder
- WebInspect
 - Has a built in web server finder
- In this case if you want to reinvent the wheel and write your own, your call.



Finding.. More web servers!

- Useful nmap command to find common web servers on a target range:
 - `nmap --open -p80,443 -PN -n 88.208.16.0/20 \`
`| grep 'Nmap scan' \`
`| awk '{print $5}' > xham_ip.txt`

```
88.208.16.25  
88.208.16.27  
88.208.16.28  
88.208.16.32  
88.208.16.35  
88.208.16.39  
88.208.16.48  
88.208.16.49  
88.208.16.51  
88.208.16.55  
88.208.16.59  
88.208.16.64  
88.208.16.68
```

Find Virtual Hosted Domains..

- Currently, there are no commercial applications doing this. (doing it well.. anyways)
- There are a bunch of websites that do this.
 - <http://www.yougetsignal.com/tools/web-sites-on-web-server/>
 - <http://ip2web.web-max.ca/>
 - <http://bing.com> -- IP:74.125.45.17
- Microsoft's Bing is the way to go.
 - Bing has a API for interface
 - <http://www.bing.com/developers> ←signup for your api key
 - <http://pastebin.com/mYdLv1R> - pastebin to my ip2vhost.py script



All we care about..

- `http://api.bing.net/xml.aspx?Appid='+bing_api_key
+'&query=IP:'+hostIP
+'&sources=web&web.count=50&Adult=Off&web.offset='+str(index)`
- Now are data is returned in nice easy to parse xml.. Pick a library of your choice and do it..
- (you will need to sort and uniq the domains returned)

ip2vhost.py -- http://pastebin.com/mYdLv1R

```
[+] finding vhosts for 419 IP's  
{*} please wait...  
[+] 1254 found!
```

```
1-udar.ru  
10keuro.com  
123youngporn.com  
18sextube.com  
1c-kb.ru  
1sextube.com  
247nylon.com  
24fetish.com  
2crazydaughters.com  
3d-bdsm.adultcomicsdreams.com  
3d-cartoons.adultcomicsdreams.com  
3d-monsters.adultcomicsdreams.com  
3d-porn.adultcomicsdreams.com  
3d-shemale-comics.adultcomicsdreams.com  
3d-shemale.adultcomicsdreams.com  
3dcartoonsworld.com  
3drapeporn.com  
3xgays.com  
55-job.ru
```

Web Application Enumeration..

- WhatWeb by Andrew Horton
 - Developed in Ruby
 - Detects over 900 different web applications
 - Very active development
 - First “public” tool of its type
 - Carries out detection via simple regex detection
 - Does version detection of known applications
 - Has the function to crawl a site for other web applications
 - Can load a list of urls 😊
- Very light impact. Nothing more than a request to the index page, is required to determine most web applications
- <http://www.morningstarsecurity.com/research/whatweb>

```
x@demonico:~/pen/apps/WhatWeb$ ./whatweb -i xham2.txt --color=never -t 20
http://bdsm-worlds.com [200] Title[Bdsm worlds], HTTPServer[nginx/0.7.62], MD5[80d967259a60390ec:
b54e5eead56b4a5f2166939410db9af], Tag-Hash[bdd80f890ad008a533f10faab0bf8957], Footer-Hash[044cb7f
http://babesportfolio.com [200] Title[Babbes Portfolio], HTTPServer[nginx/0.7.62], MD5[aef4a2dd5:
r-Hash[64e47007af50911a5c3e1e88ff5c8ea1], Tag-Hash[174b13c9af753991a3448e5f482d92d8], Footer-Hash
1da]
http://beachtgp.net [200] Title[beachTGP], HTTPServer[nginx/0.5.38], Be901a68e9a4b8fbbf
f5799eb484724f59f49b39925], Tag-Hash[fab5e0d84d3db208a1c2b10934f11013], Footer-Hash[4cb011668fce:
http://backstreetporn.com [200] Title[Back Street Porn - free amateur porn movies!], Google-Anal:
[Apache/1.3.39 (Unix) PHP/4.4.7], Header-Hash[0035f69227aedda468a94c760697ef1b], MD5[8f2d9905aed:
h[ec46050148c44a2f56312b3843ab3d8d], Footer-Hash[348f358bdb488d5ed842a9247e2aac05]
http://bbwbuff.com [200] Cookies[tm_key,tm_reldomain,tm_visit], Title[BBW Buff - We want to shar
h you, dear surfer.], HTTPServer[Apache/1.3.39 (Unix) PHP/5.2.4], X-Powered-By[PHP/5.2.4], Heade
71554786], Tag-Hash[257070e269b33b7ac771b29690d477d3], Footer-Hash[668bd7bda3d22525d85d7e10baae0:
26f175295af]
http://bareback-porn.com [200] Title[Bareback porn at bareback-porn.com], HTTPServer[nginx/0.7.6:
20dcac81c], Header-Hash[689b8e47c463cab22016972ca04d591e], Tag-Hash[59977675bd092152f3d546c47b84:
d120d7fab8c230d53f94]
http://bareback-porno.com [200] Title[Bareback porno at bareback-porno.com], HTTPServer[nginx/0.:
fb76ef350a95], Header-Hash[e13875408f15bddf6a1d1548b76044bd], Tag-Hash[e813ad8a16e26d78762e1ee6f:
d0001b57734078f75a0e402]
http://beautyandthesenior.org [200] All-in-one-SEO-Pack, X-Powered-By[PHP/5.2.6], Google-Analyti
ache/1.3.41 (Unix) PHP/5.2.6], WordPress, ders[x-pingback], Title[Beauty and the seni
esenior.org/wp-content/themes/TheShorthandOfMotion/style.css], MetaGenerator[WordPress abc], Tag
e2caee13], MD5[39fbda5910e2e6df115213c45be8e2e9], Header-Hash[0beb435e63017ae745cf98192a5ea282],
e08168a57ef4d6]
http://badsoccermom.com [200] Cookies[tm_key,tm_reldomain,tm_visit], Title[Bad Soccer Mom. Explo.
], HTTPServer[Apache/1.3.37 (Unix) PHP/5.2.3], X-Powered-By[PHP/5.2.3], Header-Hash[5bc2ac80dedc:
[c81172263c271f6414a1452ad465359a], Footer-Hash[665b45d09f31506b21a5b1873dfafd34], MD5[8ff7d8cb3:
http://bbwgalleries.in [200] Cookies[tm_key,tm_reldomain,tm_visit], Title[BBW Galleries - big be
ies galleries post], HTTPServer[Apache/1.3.39 (Unix) PHP/5.2.4], X-Powered-By[PHP/5.2.4], Header-
aa84e5f], Tag-Hash[8a850a7e8cdf0ddd6b72f60f3f09d7ad], Footer-Hash[8db0a5aaa54da2ee05ff8f7bddac26:
0e1d454f93]
```

VULNERABILITY INFORMATION

- Now that we know what's out there, it's time to find some vulnerabilities for those web applications
- <http://cve.mitre.org/>
- <http://www.exploit-db.com/>
- <http://osvdb.org/>
- My favorite... Audit the application and find new oday for yourself.





Being able to do this all “automattic”.. In a clean way.. Would be beneficial to any offensive attack that is straight to the point.. Which is getting that low hanging fruit on a owned IP space and owning the target from there.

Demo.. Sort of. You get the idea.

```
AIDS
-----
detection

[+] nmap ver: 5.0

aids-192M> threads 50
[+]Threads: 50
aids-192M> range 88.208.16.0/20
[+] Target Range: 88.208.16.0/20
aids-192M> scan

[~] THREADS: 50
[~] PATHS: 30

[+] Starting search for webservers in 88.208.16.0/20
[+] nmap -oX - -p 80,443 -sT -PN -n 88.208.16.0/20
[+] Web Servers Found: 384

[+] Starting domain enumeration on 384 IP'S

=> Domains: 1502 | Finished/Total 384/384 | Active Threads: 0 | Complete 100%

[+] Looking for known apps on 1502 domains!

=> w00ts: 5 | Found: 90 | Finished/Total 1495/1502 | Threads: 7 | Complete 99%^C
[>] http://www.forum.zagruzi.com/ IP.Board Found!
    VER: UnKnown
    PHP: PHP/5.2.10
    SERVER: Apache/1.3.41 (Unix) PHP/5.2.10
    IP: 88.208.16.191

[>] http://88.208.19.146/ Wordpress Found!
    VER: 2.7
    REG: ENABLED <-- w00t exploits/wp284.py
    PHP: PHP/5.2.6
    SERVER: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8e mod_ruby/1.2.6 Ruby/1.8.6(2007-09-24) mod_scgi/1.12 PHP/5.2.6
    IP: 88.208.19.146
```


Possibilities for this framework

- Define web app oday or public bugs and have the framework hunt out these sites for you.
- Add functionality to the detection modules that find out variables about known web applications found.. Such as exploit specific variables.. (registration on or off)
- Add randomization into the scanning.. User-agent randomization, path bruteforcing for know applications.. i.e /blog/, /forum/. Include subdomain bruteforcing also.
- Exploitation / Post Exploitation via web apps.. Or the interpreter :>

Questions?

If none.
Go hack something...

