whois Jeff Foley

- Founder & Project Lead for OWASP Amass
- Purple Team Manager at National Grid
- https://twitter.com/jeff_foley
- https://github.com/caffix
whois Anthony Rhodes

- Contributor to the OWASP Amass Project
- Senior Purple Team Member at National Grid
- https://twitter.com/fork_while_fork
- https://github.com/fork-while-fork
Agenda

• Internet Exposure
• The Amass Project
• Demonstrations
Internet Exposure

• Many organizations do not know what their infrastructure looks like on the Internet

• And consequently, do not understand what their networks look like to an adversary

• Assets only receive protection when identified and properly managed
  
  – This has become harder to perform due to enterprise networks becoming more fragmented; e.g. cloud solutions.
Internet Exposure - Methods

• Open Source Intelligence (OSINT) methods can discover much of an organization’s external network infrastructure using:
  – DNS enumeration
  – TLS certificate transparency
  – Web scraping and archives
  – Passive scanning services with APIs
  – Whois and Reverse Whois
  – Registered autonomous system numbers (ASNs)

• Adversaries use these techniques to map networks on the Internet.
Internet Exposure - Visualization

- Red – Domain Name
- Green – Subdomain
- Yellow – PTR Record
- Purple – Mail Record
- Turquoise – Name Server
- Orange – IP Address
- Pink – Netblock
- Blue – AS Number
Internet Exposure Cont.

• Once an adversary has mapped a network, additional reconnaissance can be performed:
  – Visual inspection of websites; e.g. Aquatone
  – Discovery of web directories/files; e.g. Gobuster
  – Application layer scanning; e.g. ZGrab
  – Port scanning; e.g. Nmap

• Blue teams need to understand their exposure on the Internet better than adversaries do.
Internet Exposure – Use Cases

- Most organizations have more public exposure than they realize, and are starting to use OSINT and scanning techniques

- **Adobe** recently released the **Marinus** open source project that assists organizations in creating maps of their networks
  - Adobe Marinus utilizes the OWASP Amass project

- **Shodan Monitor** was recently announced that provides customers the ability to track devices exposed on the Internet

- These approaches allow security teams to understand exposure when **asset management is just not enough**.
The Amass Project

- In-depth DNS enumeration and network mapping
- Automates the various OSINT techniques
- Supports the visualization of findings
- Tracks changes to an organization’s exposure.

High Level Architecture

- Data Source → Alt Names → DNS Queries → Graph DB → Output
- Data Source → Brute Forcing → DNS Queries

Resolved Names
The Amass Project – Use Cases

• Various **blue teams** benefit from quickly discovering changes in their organization’s attack surface

• **Red teams** and **penetration testers** identify missing scope at the beginning of engagements

• **Bug bounty hunters** save time automating these techniques and finding new targets within scope

• **OSINT investigators** and **intelligence analysts** utilize Amass to hunt down threats on the Internet.
The Amass Project – Large Graph
The Amass Project – Maltego

NOT FOR COMMERCIAL USE
The Amass Project - FAQ

• Can Amass handle DNS wildcards?
  – Yes. DNS wildcard detection is performed automatically.

• Does Amass support limiting the rate of DNS queries?
  – Yes. The ‘-max-dns-queries’ flag controls the number of simultaneous queries.

• Can Amass perform DNS name alterations?
  – Yes. Various types of permutations are attempted.
The Amass Project - Alterations

• Number Flipping
  – test1.owasp.org -> test2.owasp.org ... test99.owasp.org

• Add suffixes and prefixes
  – test.owasp.org -> test-prod.owasp.org
  – test.owasp.org -> new-test.owasp.org

• Swapping of suffixes and prefixes
  – test-prod.owasp.org -> test-dev.owasp.org

• Fuzzy Label Searches
  – us.owasp.org -> uk.owasp.org

• Predictive name guessing using Markov models.
The Amass Project – Get it!

• Official project page: https://www.owasp.org/index.php/OWASP_Amass_Project

• Project repository: https://github.com/OWASP/Amass

• The Snapcraft package: https://snapcraft.io/amass

• The Homebrew package:

  $ brew tap caffix/amass
  $ brew install amass
Demonstration – netdomains

```
$ ./amass.netdomains -org "Utica College"
26808. US. ARIN, UTICA-COLLEGE - Utica College, US
$ ./amass.netdomains -asn 26808
utica.edu
uixio2.com
donotclickthislink.info
e-mailpixie.com
ucphishing.com
gophishme.com
uticocollege.com
$ ./amass.netdomains -asn 26808 -whois
utica.edu
blagolf.com
aaronsonmicrobiology.com
auuticocollege.org
aptalbany.com
bleedingsports.com
brlanagreco.com
cimip.com
cimip.net
cimip.org
ctctf.com
donotclickthislink.info
drhaasbeek.com
emailpixie.com
engageutica.com
fearofmissingoutmedia.us
guradosgrassandsnow.com
hireugrads.com
 historichomeassociates.com
three.org
lij-ciif.org
ljde.net
jcem.org
jefipyoga.com
lavandexpress.com
lenoxlandtrust.org
```
Demonstration – netdomains

$ dig +short utica.edu
22.237.4.113
$ whois 22.237.4.113

# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#
# start

NetRange: 72.237.4.0 - 72.237.4.255
CIDR: 72.237.4.0/24
NetName: TELECOE-SYRC-UTICOL6
NetHandle: NET-72-237-4-0-1
Parent: LVLT-ORG-72-236 (NET-72-236-0-0-1)
NetType: Reassigned
OriginAS: Customer: UTICA COLLEGE (CO1574555)
RegDate: 2007-02-20
Updated: 2007-02-20
Ref: https://rdap.arin.net/registry/ip/72.237.4.0

$ ./amass.netdomains -cidr 72.237.4.0/24
utica.edu
dotcom2.com
cpamphishing.com
eallpixie.com
uticocollege.com
cpamphishme.com
cdotclickthislink.info
$
Demonstration – Passive

```bash
$ ./anass -passive -d owasp.org
new-wiki.owasp.org
owasp.org
owasp4.owasp.org
austin.owasp.org
cheesemonkey.owasp.org
phpsec.owasp.org
name-virt-host.owasp.org
haroldtest.owasp.org
contact.owasp.org
www.lists.owasp.org
kerala.owasp.org
my.owasp.org
discourse.owasp.org
www.ocms.owasp.org
lists.owasp.org
owaspsforce.owasp.org
groups.owasp.org
gapos.owasp.org
si.owasp.org
www.owasp.org
docs.owasp.org
mail.owasp.org
temocali.owasp.org
ocms.owasp.org
update-wiki.owasp.org
talk.owasp.org
dsandbox.owasp.org
es.owasp.org
calendar.owasp.org
admin.owasp.org
forum.owasp.org
```
```ini
[domains]
domain = owasp.org
```
```ini
output_directory = amass_output
maximum_dns_queries = 10000
mode = active
port = 443

[bruteforce]
enabled = true
recursive = true
minimum_for_recursive = 0
wordlist_file = subdomains-top1mil-5000.txt
wordlist_file = namelist.txt

[alterations]
enabled = true
min_for_word_flip = 0
wordlist_file = alterations.txt
add_words = true
add_numbers = true
flip_words = true
flip_numbers = true
edit_distance = 1
```
Demonstration – amass

```bash
$ ./amass -config amass_config.ini -src -ipv4
{Crtsk}
  lists.owasp.org 178.126.177.22
{Crtsk}
  name-virt-host.owasp.org 159.203.183.216
{BufferOver}
  ccm.owasp.org 159.203.183.216
{BufferOver}
  new4ik.owasp.org 154.150.219.202
{Brute Forcing}
  origin-www.owasp.org 192.237.166.82
{BufferOver}
  www.owasp.org 104.130.219.202
{Brute Forcing}
  contact.owasp.org 198.101.154.205
{BufferOver}
  kerala.owasp.org 151.101.1.195,151.101.55.195
{Crtsk}
  austin.owasp.org 159.203.183.216
{Forward DNS}
  owasp.org 104.130.219.202
{BufferOver}
  owasp4.owasp.org 198.101.154.205
{BufferOver}
  update-iki.owasp.org 22.253.174.254
{BufferOver}
  owaspforce.owasp.org 172.217.10.243
{Brute Forcing}
  my.owasp.org 208.82.15.69
{Brute Forcing}
  calendar.owasp.org 172.217.10.243
{Brute Forcing}
  s1.owasp.org 172.217.10.243
{Brute Forcing}
  groups.owasp.org 172.217.10.243
{Brute Forcing}
  google.owasp.org 172.217.10.243
{Brute Forcing}
  mail.owasp.org 172.217.10.243
{Brute Forcing}
  docs.owasp.org 172.217.10.243
{Brute Forcing}
  mod.owasp.org 172.217.10.243
Average DNS queries performed: 3843/sec, DNS names remaining: 180
Average DNS queries performed: 23/sec, DNS names remaining: 182
Average DNS queries performed: 14/sec, DNS names remaining: 98

OWASP Amass v2.9.18  https://github.com/OWASP/Amass

21 names discovered - cert: 9, api: ?, brute: 10, dns: 1

ASN: 14061 - DIGITALOCEAN-ASH - DigitalOcean, LLC, US
  178.129.176.0/20  1 Subdomain Name(s)
  159.203.176.0/20  3 Subdomain Name(s)
ASN: 19994 - RACKSPACE - Rackspace Hosting, US
  23.253.160.0/19  1 Subdomain Name(s)
  104.150.192.0/19  3 Subdomain Name(s)
  192.207.128.0/10  1 Subdomain Name(s)
  198.191.128.0/16  2 Subdomain Name(s)
ASN: 54113 - FASTLY - Fastly, US
  151.101.0.0/22  1 Subdomain Name(s)
  151.101.64.0/22  1 Subdomain Name(s)
ASN: 51589 - GOOGLE - Google LLC, US
  172.217.10.0/24  8 Subdomain Name(s)
ASN: 13335 - NING - Ning Interactive, Inc., US
  208.82.16.0/24  1 Subdomain Name(s)
```

OWASP Open Web Application Security Project
Demonstration – tracker

$ ./amass.tracker -d owasp.org

Between 03/22 09:35:41 2019 EDT -> 03/22 09:36:57 2019 EDT
and 05/07 10:10:10 2019 EDT -> 05/07 10:13:12 2019 EDT

Moved: gapps.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: docs.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: groups.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: mail.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: sl.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: calendar.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Moved: owaspforce.owasp.org
    from 173.194.222.121,2507:f8b0:4006:810::2013
    to   172.217.10.243,2607:f8b0:4000:808::2013
Removed: discourse.owasp.org 216.218.240.87,2001:470:1::669::87
Found: mod.owasp.org 172.217.10.243,2607:f8b0:4000:808::2013
$
Demonstration – Visualizations

```
$.amass.viz -d3 -i data_output.json
```

![Visualization Diagram]
Conclusion

• **Assets** only receive protection when **identified** and properly managed

• **Blue teams** benefit from quickly **discovering changes** in their organization’s attack surface

• **OWASP Amass** performs in-depth DNS enumeration and network mapping by **utilizing** the methods in a **cyclic** manner.
Thank you!

Questions?