For Further Information Visit:

WWW.HACKERONE.COM | WWW.HACKER101.COM

ADDITIONAL NOTES SECTION:

Digital Dumpster Diving

GITHUB RECON EXAMPLES

- “company.com” “dev”
- “dev.company.com”
- “company.com” API_key
- “company.com” password
- “api.company.com” authorization

Tools

- gitrob
- git-all-secrets
- truffleHog
- git-secrets
- repo-supervisor
- Do it manually?

JAVASCRIPT FILE EXAMPLES

Process

Look for:

- (hidden) endpoints
- Leaked cloud instances and their secret_keys
- ...and definitely more bugs

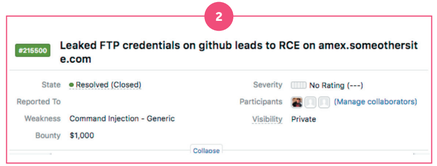
DIGITAL DUMPSTER DIVING EXAMPLES

1

- Looked up the “umbrella” company name
- Combine “umbrella_company” + asset_name + “password”, and found below code:

  “server”: {
  “host”: “dedXXXX.PATTERN.PROVIDER.com”,
  “port”: 21,
  “user”: “some_username”,
  “password”: “definitely_ftp_passwords”
  }
- Got access to umbrella_company’s FTP server → $10,000 Bounty

2



NOTES SECTION:

hackerone

Recon Cheat Sheet

A Reference Guide for Our Newest Hackers

hackerone

Reconnaissance Quick Reference Guide

Asset Discovery

BRUTE FORCE

Brute force domain → Find different environments (.dev, .corp, .stage, uat, etc.) → Brute force again

- Different permutations, Different environment, e.g. dashboard.dev.site.com vs dashboard-dev.site.com
- Google Dork: site.com +inurl:dev -cdn

Tools

- sublist3r
- enumall
- massdns
- altdns
- brutesubs
- dns-parallel-prober
- dnscan
- knockpy
- tko-subs
- HostileSubBruteforce

CERTIFICATE TRANSPARENCY TOOLS

Censys

Look for SSL certificates: Example: 443.https. tls.certificate. parsed. extensions.subject_alt_name. dns_names:snapchat.com

Shodan

Search by hostname. Filter for: Ports: 8443, 8080, etc | Title: "Dashboard [Jenkins]" | Product:Tomcat Hostname: somecorp.com | Org: evilcorp | ssl: Google

Certspotter

Great API | Easy to automate | Make a bash alias → Automate → Win

Crt.sh

Great API and web interface | Allows using a wild card | You may get different results from differents sources

CERTIFICATE TRANSPARENCY EXAMPLES

Vulnerabilities found with Shodan

Search Query: hostname:host.com port:15672

#100828 Access to RabbitMQ on stageREDACTED.REDACTED.com:15672

Search Query: hostname:host.com title:Dashboard [Jenkins]

#320836 jenkins-REDACTED.REDACTED.REDACTED.com publicly facing without authentication leaks AWS_Secret_key + Build info

Vulnerabilities found with Censys

AUGUST 22, 2017

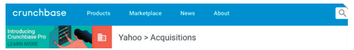
"Secure your jenkins instance or hackers will force you to! (Snapchat's $5,000 vulnerability)"

NOTES SECTION:

OSINT

ACQUISITIONS

- Big programs (Facebook, Google, Verizon Media, etc.)
- Acquired assets usually in scope after 6 months



WHOIS

- ARIN (Canada, United States, some Caribbean nations) | RIPE NCC (Europe, Russia, Middle East, Central Asia) | APNIC (Asia-Pacific region) | LACNIC (Latin America, some Caribbean nations) | AFRINIC (Africa)
- Search Yahoo, or any other large program. Shodan helps here, too

Network Resources	
LVLT-YAHOO-1-8-3-34 (NET-8-3-34-0-1)	8.3.34.0 - 8.3.35.255
NET-216-34-77-0 (NET-216-34-77-0-1)	216.34.77.0 - 216.34.77.127
COLOC-1-YAHOO-1-8-8-178 (NET-8-8-178-0-1)	8.8.178.0 - 8.8.178.255
SAVV-64-209-232-0-0-1 (NET-64-209-232-0-1)	64.209.232.0 - 64.209.232.255
SAVV-S235114-9 (NET-64-39-38-208-1)	64.39.38.208 - 64.39.38.223

Content Discovery

CONTENT DISCOVERY PROCESS

Port scan → Screenshot open ports (default: 80, 443) → Look for interesting • Files • Directories → Always keep an archive of your report

Tools

- dirbuster
- gograbber
- gobuster
- dirsearch

CONTENT DISCOVERY EXAMPLES

1

- You see an open port on 8443
- Directory brute force
- /admin/ returns 403
- You brute force for more files/dirs on /admin/
- /admin/users.php returns 200
- Repeat on other domains, ports, folders, etc.

2

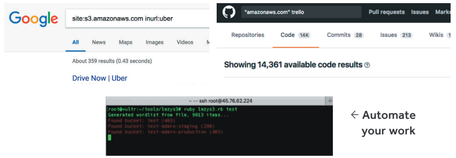
- Nmap common ports (3868,3366,8443,8080,9443, 9091,3000,8000,5900,8081,6000,10000,8181,3306, 5000,4000,8888,5432,15672,9999,161,4044,7077, 4040,9000,8089,443,7447,7080,8880,8983,5673,7443)
- Take screenshots (webscreenshot.py)
- Directory/File brute force
- Robots.txt sometimes does this for you ¯_(ツ)_/¯

NOTES SECTION:

Vendor Services

AWS RECON PROCESS

- Look for S3 buckets on Google (site:s3.amazonaws.com + inurl:company_name) | AWS instances (site:amazonaws.com -s3)
- Repeat on Github!

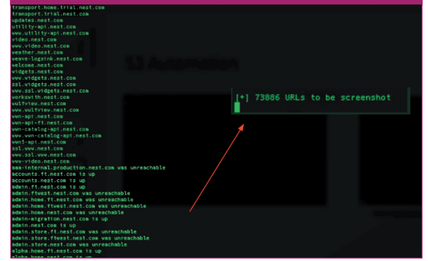


← Automate your work

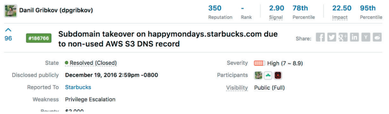
Create aliases to cut down your work

```
certspotter() {
 curl -s https: //certspotter.com/api/v0/certs\?domain\=$1 | jq '.
 [].dns_names[]' | sed 's/\"//g' | sed 's/\*\.//g' | sort -u | grep $1 >
 ~/$1/$1.txt
}
dirbruteforce() {
 cd / tools / dirsearch
 cat~/$1/$1.txt |
  while read line;
 do python3 dirsearch.py - e. - u" https: //$line"; done
}
screenshot() {
 python~/tools/webscreenshot / webscreenshot.py - o. / $1 / screenshots /
 -i~/$1/$1.txt--timeout = 10 - m
}
recon() {
 certspotter $1
 dirbruteforce $1
 screenshot $1
}
```

Automate the tasks you perform for each target



AWS RECON EXAMPLES



NOTES SECTION: