COMP6843 – WEEK 1

Attack Surface Discovery

- Finding hosts vs content / issues
- Your risk vs their risk
- Logic vs automation

DNSDUMPSTER, CERTIFICATES

DNS Name	reference.dex.unsw.edu.au
DNS Name	*.reference.dex.unsw.edu.au
DNS Name	sandbox.dex.unsw.edu.au
DNS Name	*.sandbox.dex.unsw.edu.au
DNS Name	assets.unsw.edu.au
DNS Name	*.assets.unsw.edu.au
DNS N	
DNS N	
DNS N	
DNS N	
DNS N	
DNS N	
DNS N	
DNS N	

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
3695246382	2020-11-25	2015-04-27	2018-04-27	medicine.unsw.edu.au	certmaster@unsw.edu.au medicine.unsw.edu.au www.medicine.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2386861098	2020-01-29	2008-02-25	2009-03-21	mail.cofa.unsw.edu.au	mail.cofa.unsw.edu.au	C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
2386775162	2020-01-29	2008-02-18	2009-03-20	secure.cofa.unsw.edu.au	secure.cofa.unsw.edu.au	C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
2386681439	2020-01-29	2007-01-24	2008-02-24	secure.cofa.unsw.edu.au	secure.cofa.unsw.edu.au	C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
2386508418	2020-01-28	2007-01-23	2008-02-23	mail.cofa.unsw.edu.au	mail.cofa.unsw.edu.au	C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
2382764501	2020-01-27	2016-06-06	2019-06-06	grouper-dev.teaching.unsw.edu.au	grouper-dev.teaching.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382694578	2020-01-27	2016-10-13	2019-10-13	changepoint.unsw.edu.au	changepoint.unsw.edu.au www.changepoint.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382693827	2020-01-27	2015-09-03	2018-09-03	infplrec01.ad.unsw.edu.au	a.pitt@unsw.edu.au infplrec01.ad.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382557635	2020-01-27	2016-03-15	2019-03-15	www.works.it.unsw.edu.au	www.works.it.unsw.edu.au www.works.preprod.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382542271	2020-01-27	2016-01-11	2019-01-11	confluence.unsw.edu.au	certmaster@unsw.edu.au confluence.it.unsw.edu.au confluence.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382411789	2020-01-27	2015-02-22	2018-02-22	ddi-member4.net.unsw.edu.au	cu-coregroup@unsw.edu.au ddi-member4.net.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382283704	2020-01-27	2015-05-01	2018-05-01	jira.it.unsw.edu.au	certmaster@unsw.edu.au jira.it.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2
2382278868	2020-01-27	2015-06-15	2018-06-15	cisco.uc.unsw.edu.au	certmaster@unsw.edu.au cisco.uc.unsw.edu.au imp00.uc.unsw.edu.au	C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2

DNS RECON: BRUTE FORCING (FASTER)

```
evelynn.unsw.edu.au
b.unsw.edu.au
europewest.unsw.edu.au
march.unsw.edu.au
oceania.unsw.edu.au
7.unsw.edu.au
web1.unsw.edu.au
ghcpi.unsw.edu.au
skins.unsw.edu.au
kr.unsw.edu.au
api.unsw.edu.au
apollo.unsw.edu.au
pantheon.unsw.edu.au
2018.unsw.edu.au
ssl.unsw.edu.au
pc.unsw.edu.au
sept.unsw.edu.au
pass.unsw.edu.au
swagger.unsw.edu.au
s3.unsw.edu.au
2016.unsw.edu.au
nautilus.unsw.edu.au
backend.unsw.edu.au
```

- altdns + zdns / masscan
- double check results
- benchmark your tools
- note: provider blocking, target blocking (round robin dns?)
- note: rate limiting

```
ubuntu@ip-172-31-19-173:~$ dirb https://www.unsw.edu.au

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb 14 00:23:02 2024
URL_BASE: https://www.unsw.edu.au/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.unsw.edu.au/ ----
^C> Testing: https://www.unsw.edu.au/.hta
```

WHOIS / IP ADDRESSES

```
# whois.apnic.net

% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '129.94.0.0 - 129.94.255.255'

% Abuse contact for '129.94.0.0 - 129.94.255.255' is 'hostmaster@unsw.edu.au'

inetnum:        129.94.0.0 - 129.94.255.255
netname:        UNSW
descr:          University of New South Wales
country:        AU
```

- nslookup www.cse.unsw.edu.au
- whois [result]
- (vs whois www.cse.unsw.edu.au)
- (cloud infrastructure nowdays)

MOBILE APPS (ANDROID)

- tl;dr:
  - pull it off a test phone
  - unzip blah.apk
  - (apktool d blah.apk)
  - dex2jar (or d2j-dex2jar)
  - jd-gui (or whatever) classes-dex2jar.jar
- Look for URL’s and hosts
- Look for white-labelled software
- Native vs code

WEB RECON: HISTORICAL SNAPSHOTS

INTERNET ARCHIVE
WaybackMachine

Wayback Machine APIs

The Internet Archive Wayback Machine supports a number of different APIs to make it easier for developers to retrieve information about Wayback capture data.

The following is a listing of currently supported APIs. This page is subject to change frequently, please check back for the latest info.

Updated on September, 24, 2013

Wayback Availability JSON API

This simple API for Wayback is a test to see if a given url is archived and currenlty accessible in the Wayback Machine. This API is useful for providing a 404 or other error handler which checks Wayback to see if it has an archived copy ready to display. The API can be used as follows:

`http://archive.org/wayback/available?url=example.com`
which might return:

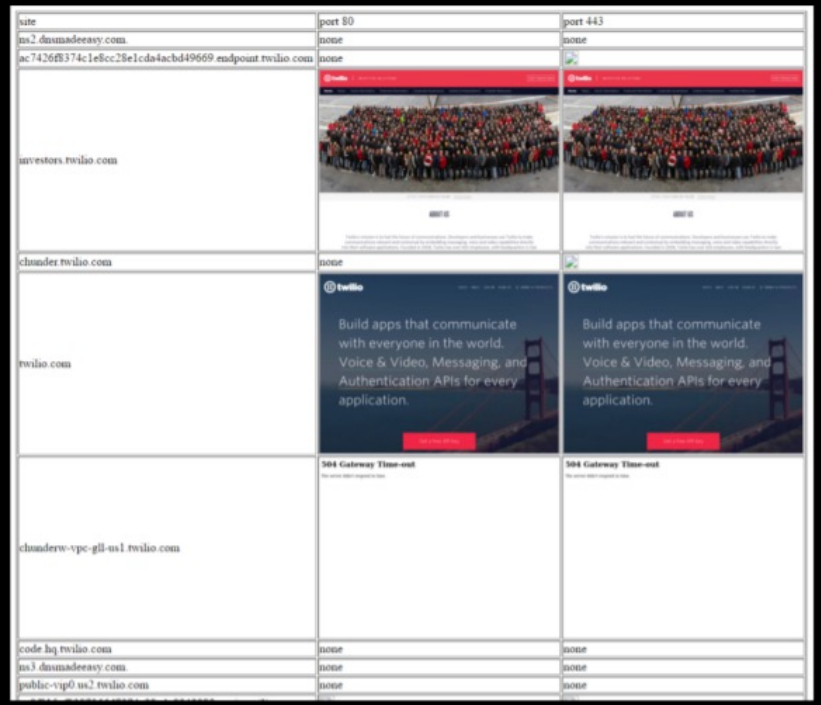

```
{
    "archived_snapshots": {
        "closest": {
            "available": true,
            "url": "http://web.archive.org/web/20130919044612/http://example.com/",
            "timestamp": "20130919044612",
            "status": "200"
```

YE OLDE WEB SECURITY

and the increasing excellence of software

VISUAL INSPECTION

WRITE YOUR OWN TOOLS.



This is now broken (PhantomJS / OpenSSL, replace with selenium?)

Write your own:

- Better cookie support
- Automated clicking stuff?
- Different user agents
- Referer control / Page flow control
- Passive fingerprinting (“this looks like a soft 404”)
- Integration with burpsuite (?)

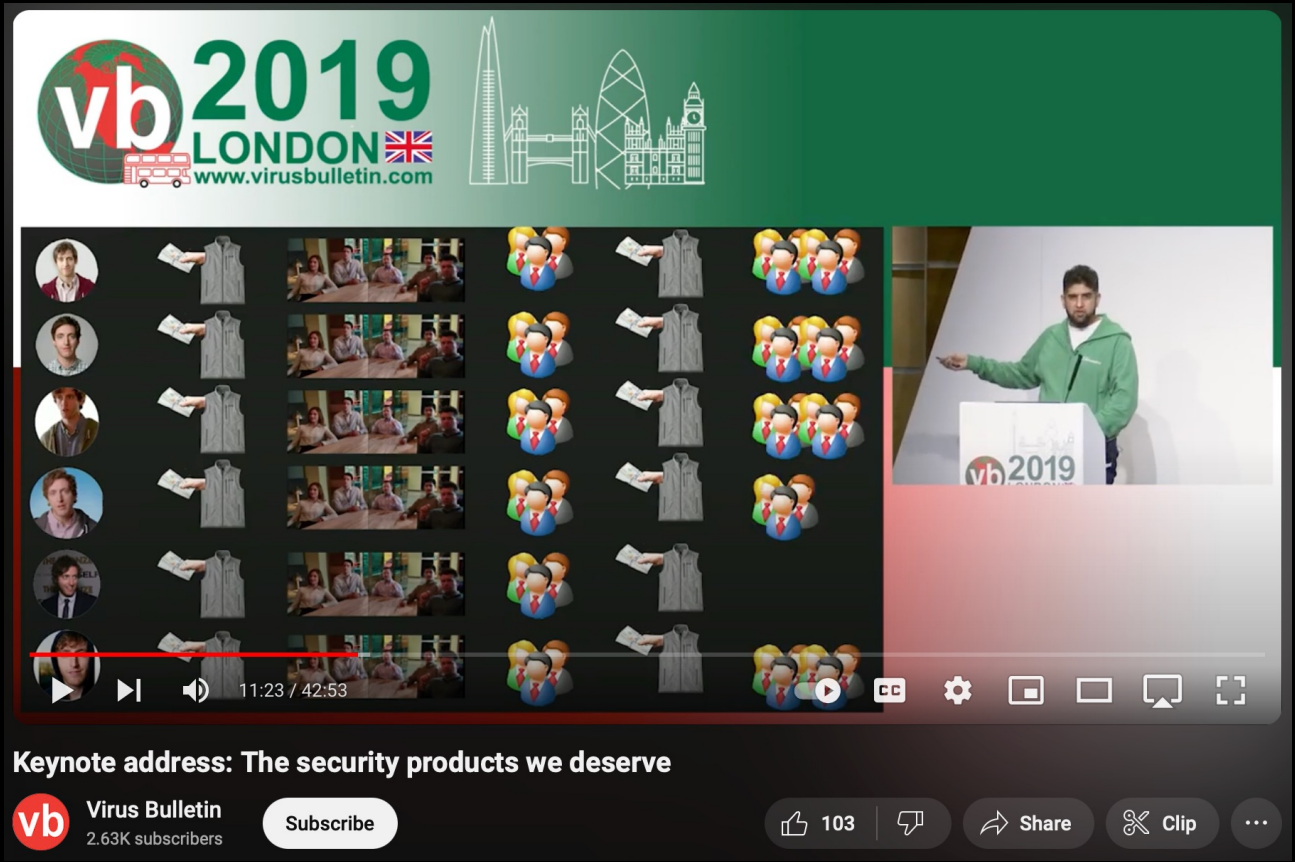
snapple.py, but write your own.

AUTOMATED INTERACTION

burp scanner, burp intruder

GREP AND YOU

don’t get blocked because you did alert(1)



https://www.youtube.com/watch?v=GHuQC1qLnJ4

TRIAL SOFTWARE

Selected AMI: (ami-02eec49345a878486) (Quickstart AMIs)

trial

Quickstart AMIs (0) Commonly used AMIs | **My AMIs (0)** Created by me | **AWS Marketplace AMIs (231)** AWS & trusted third-party AMIs | **Community AMIs (13)** Published by anyone

Refine results

Categories

- Infrastructure Software (199)
- DevOps (111)
- Business Applications (29)
- Machine Learning (26)
- Industries (7)
- IoT (4)

Publisher

- NGINX, Inc. (60)
- F5, Inc. (22)
- Apps4rent LLC (14)
- Cisco Systems, Inc. (11)
- SIOS Technology Corp.

trial (231 results) showing 1 - 50

1 ...

Sort By: Relevance

Dataiku Trial (Sandbox) Select

By Dataiku | Launch an instance

★★★★★1 AWS review | 36 external reviews

This version of Dataiku allows you to deploy a fully functional single DSS node in your AWS environment to be used for prototyping, testing and understanding the full extent of Dataiku capabilities. With Dataiku visual, end-to-end collaborative AI platform: - Data Scientists spend more time on hig...

N2WS Backup & Recovery for AWS Free Trial/BYOL Select

By N2W Software | Ver 4.2.2

★★★★★25 AWS reviews | 14 external reviews

EMBEDDED WEB / HTTP vs HTTPS

ALSO: SSL AND LOW RISK VULNERABILITIES

Internet

The Internet Channel for the Wii does not feature the ability to download files by any normal means. By run
exploit code.

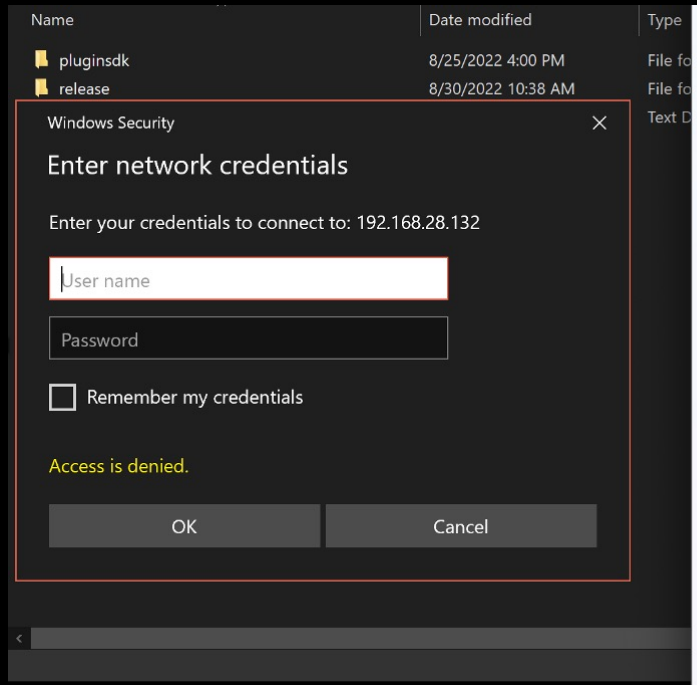
The EULA for WiiConnect24 and Wii Shop downloads HTML from Nintendo's official servers over HTTP; by

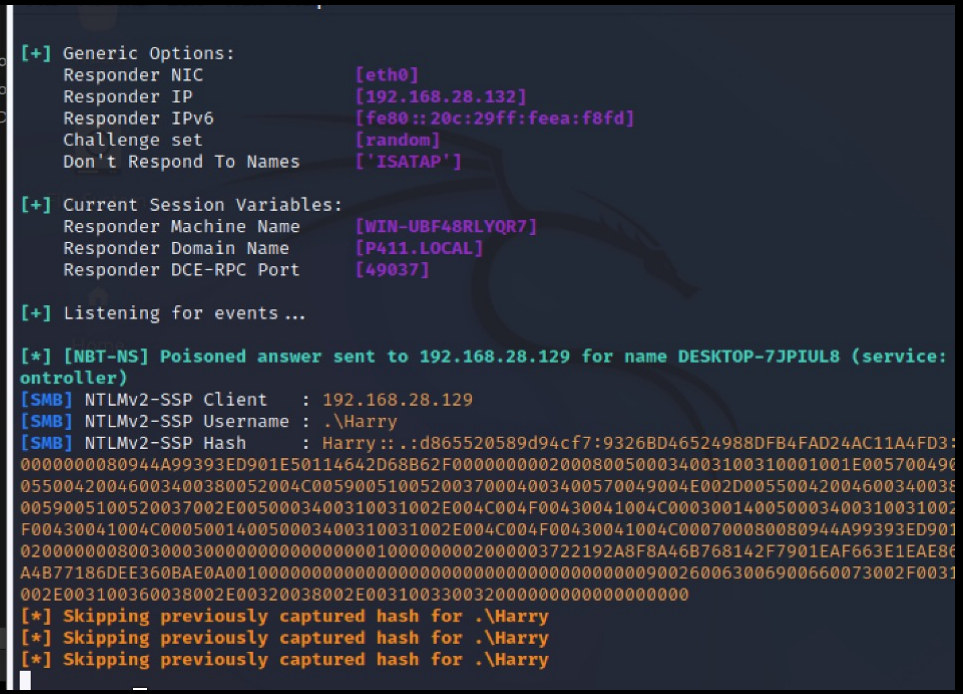
Exploits

- FlashHax
- Str2hax

- HTTPS provides Trust (verify the endpoint) and Encryption. One or both could be done incorrectly.
- Ethics of restricting users

WINDOWS TRICKERY





WINDOWS PROXY AUTO-DISCOVERY (WPAD)

```
# Uncomment this to enable the integrated DHCP server, you need
# to supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
# dhcp-range=192.168.55.50,192.168.55.60,255.255.255.0,1h
dhcp-range=10.10.10.50,10.10.10.60,255.255.255.0,1h
dhcp-option=252,http://10.10.10.1:8080/lol.pac
```

For fun:

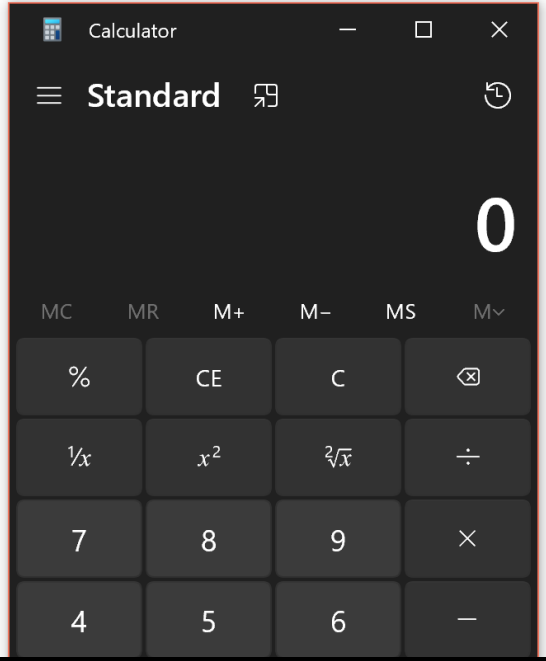
- Look up CVE-2018-1111 (cmd exec in dhcp option)
- Test your other network devices (how?)
- The Post Bash Bunny Era

MSHTA

- Run web applications locally, with some additional scripting support.
- Used by kiosks, malware and occasionally legitimate applications.
- Migrate out of “web world” via PowerShell
- CTRL-P to print

```
Sub RunProgram
        Set objShell = CreateObject("WScript.Shell")
        objShell.Run("calc.exe")
End Sub
```

hi



PROTOCOL HANDLERS

- Inconsistent browser support (incl. embedded)
- Potentially insecure application-side behaviour (esp kiosks)
- User-modifiable (plugins)
- CVE-2022-30190 (ms-msdt bug)
- CVE-2021-40444 (mshtml bug)

macOS Ventura 13.2

TL;DR:

- I’m terrible at pentesting don’t listen to me. Listen to these guys instead:
  - Live Recon and Automation on Shopify's Bug Bounty Program with @TomNomNomDotCom (https://www.youtube.com/watch?v=SYExiynPEKM)
  - The Bug Hunter's Methodology - Application Analysis | Jason Haddix (https://www.youtube.com/watch?v=FqnSAa2KmBI)
  - https://www.hackerone.com/ethical-hacker/how-recon-and-content-discovery
  - Google.

- Understand technology better than the people who made it.

THANKS FOR LISTENING TO ME YELL AT CLOUDS!

questions?