Hands-on Hacking: Capture-the-Flag

David Raymond, Ph.D.
Director, Virginia Cyber Range
draymond@virginiacyberrange.org

VIRGINIA CYBER RANGE

Agenda

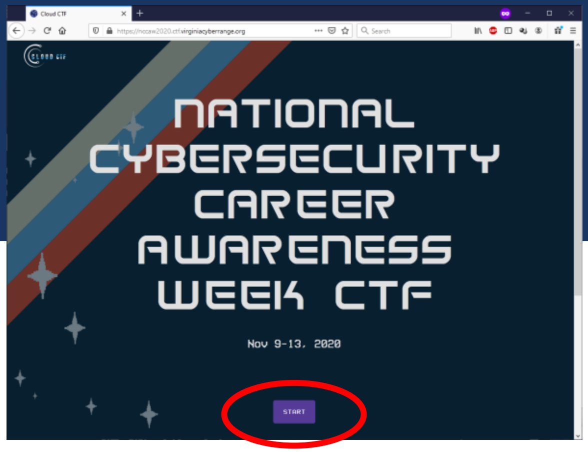
- Introduction and Prep
- Overview of Capture-the-Flag (CTF)
- General CTF challenge-solving tips
- CTF Challenges by type
- Where to find other CTFs to play

Image: https://www.accelevents.com/how-to-build-an-event-agenda/

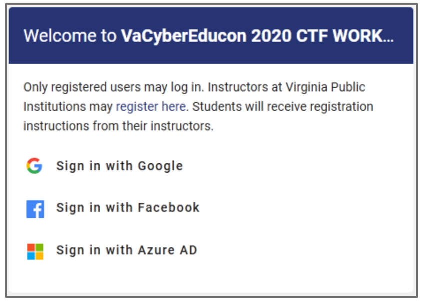
Workshop Notes

- For this workshop and CTF, most challenges will be solvable using just a web browser
- Some of the more advanced CTF challenges will require additional software applications
  - I will mention some software during this workshop; there will always be a freely downloadable option
- Use the chat window to ask questions at any time

- CTF is available at https://nccaw2020.ctf.virginiacyberrange.org/
- Join our CTF Slack Workspace at https://vacr.io/cloudctf-slack
  - Use the **#nccaw2020_ctf** channel



1.



Welcome to VaCyberEducon 2020 CTF WORK...

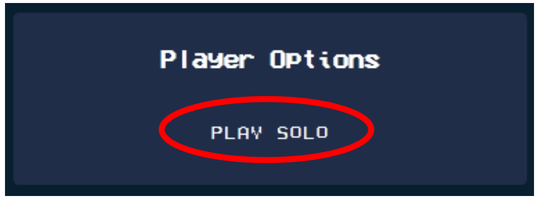
Only registered users may log in. Instructors at Virginia Public Institutions may register here. Students will receive registration instructions from their instructors.

Sign in with Google

Sign in with Facebook

Sign in with Azure AD

2.



3.

VIRGINIA CYBER RANGE

What is *Capture-the-Flag?*

□ Cybersecurity Competition

- Can be individual or team-based
- Sometimes in-person, often remote

□ Various formats

- *Jeopardy-style. Most popular and easiest to create*
- Attack/Defend (Red/Blue)
  - Example: DEFCON CTF

□ Hosted by:

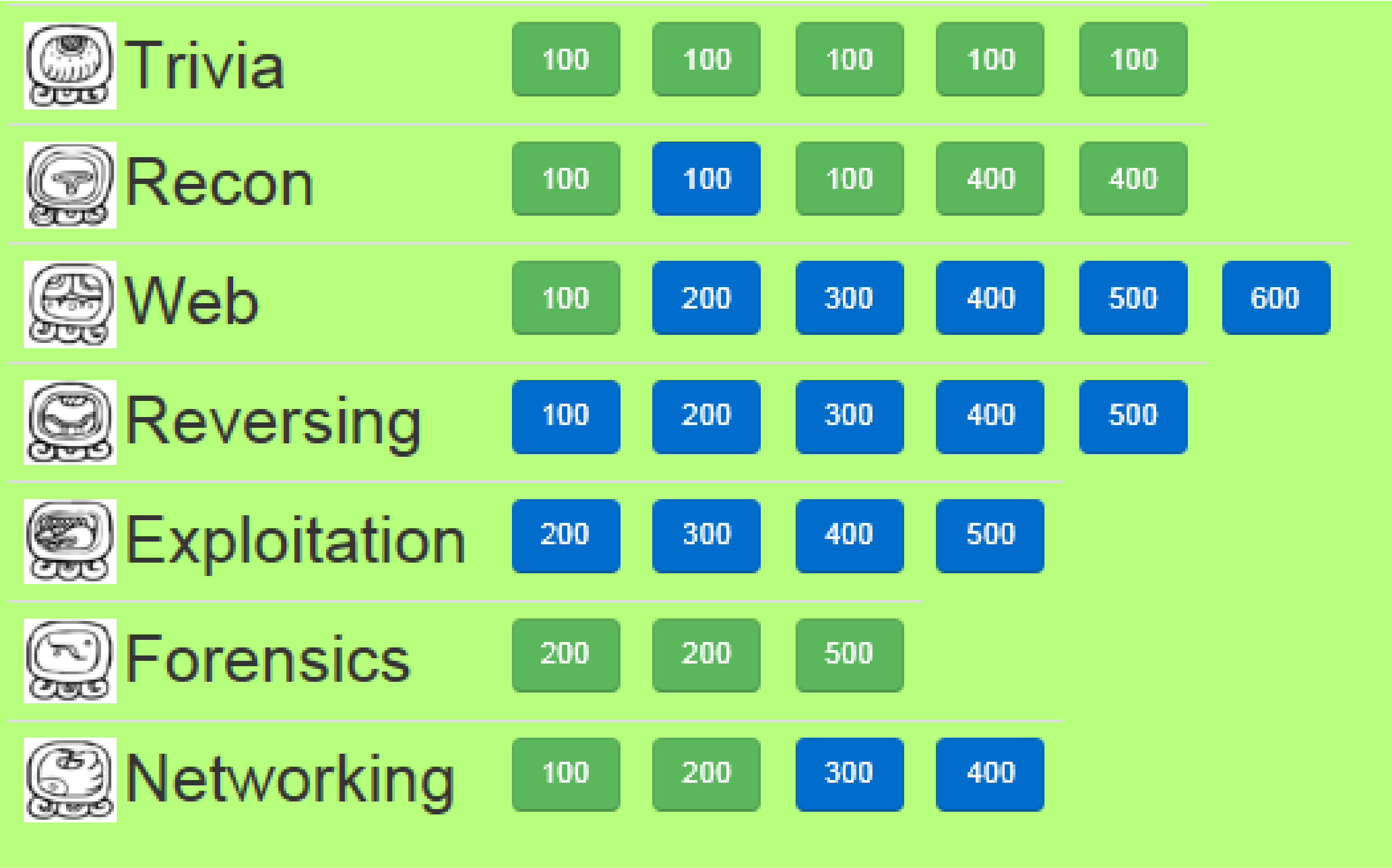
- College CTF teams
- Companies looking for talent
- DoD and other government agencies

Why CTFs?

- Good way to spark interest in cybersecurity topics
  - Very popular among high school and college clubs
- A well-designed CTF . . .
  - Caters to wide range of ability levels
  - Encourages independent learning
  - Exercises real-world skills
- Can be used for . . .
  - Teambuilding events
  - Skills assessment
  - Teaching basic skills and problem-solving

VIRGINIA CYBER RANGE

Example Jeopardy Board (NYU-Poly, 2012)



Trivia	100	100	100	100	100	
Recon	100	100	100	400	400	
Web	100	200	300	400	500	600
Reversing	100	200	300	400	500	
Exploitation	200	300	400	500		
Forensics	200	200	500			
Networking	100	200	300	400		

Common Challenge Types: Overview

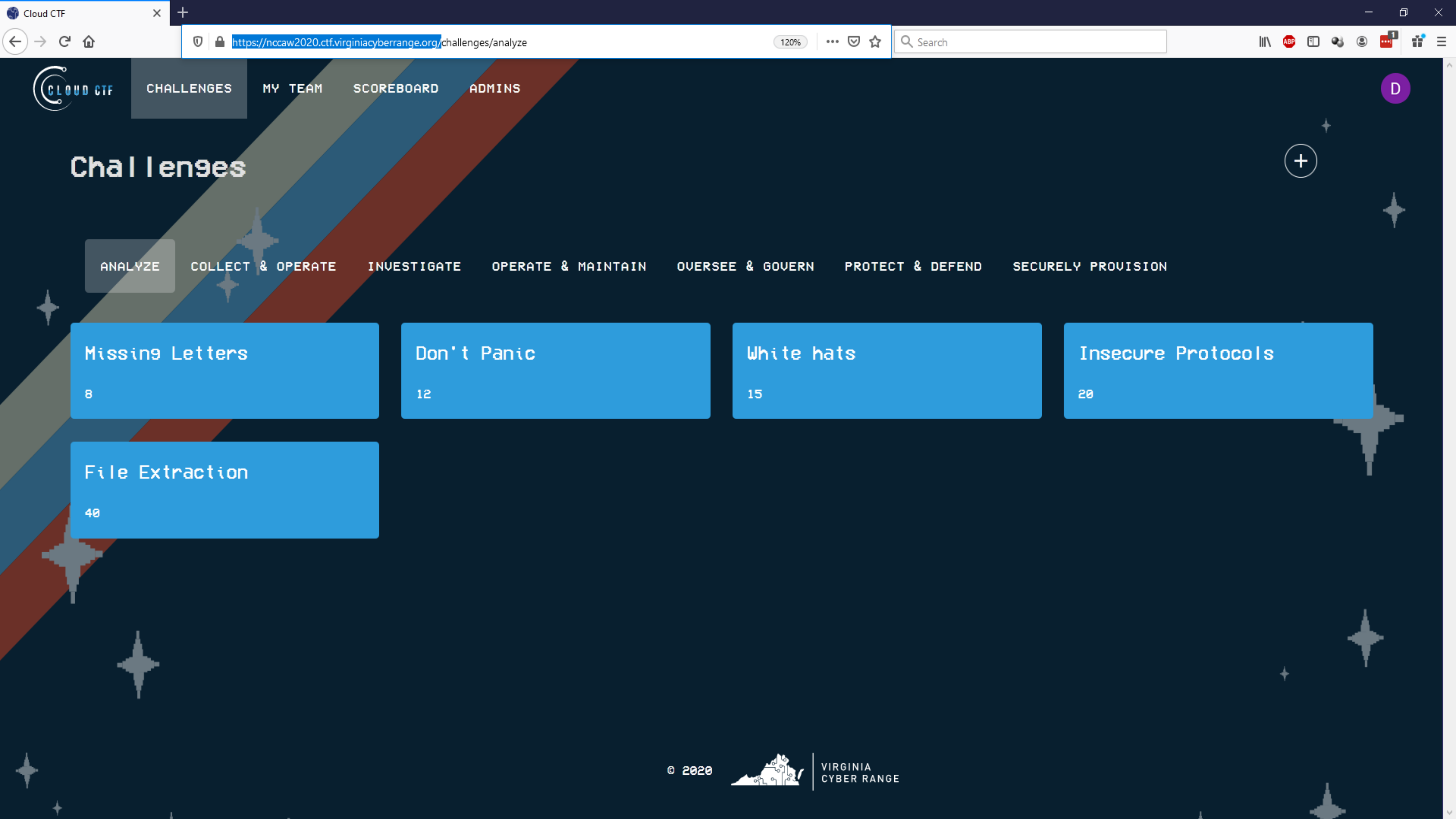
- **General Cyber Knowledge (various category names)**
  - Category name might be targeted to specific topic areas
- **Cryptography**
  - Related to computer encodings, simple ciphers, or modern cryptography algorithms
- **Web**
  - Find flag hidden on a web page or in web traffic; or exploit vulnerable web application
- **Reconnaissance**
  - Follow a trail of hints to find a flag
- **Networking**
  - Find a flag by analyzing captured network traffic
- **Forensics**
  - Find digital artifact in disk or memory image
- **Reverse Engineering** or Binary Exploitation
  - Analyzing an executable program to produce a flag

Challenge Categories for This CTF

NICE Workforce Framework Categories

Securely Provision	**Operate & Maintain**
Oversee & Govern	**Protect & Defend**
Analyze	**Collect & Operate**
Investigate	

- Challenges include
    - Questions related to each career category or associated job roles
    - Technical questions that are related to jobs within the category
- Check back throughout the week for additional challenges!



Challenges

Missing Letters
8

Don't Panic
12

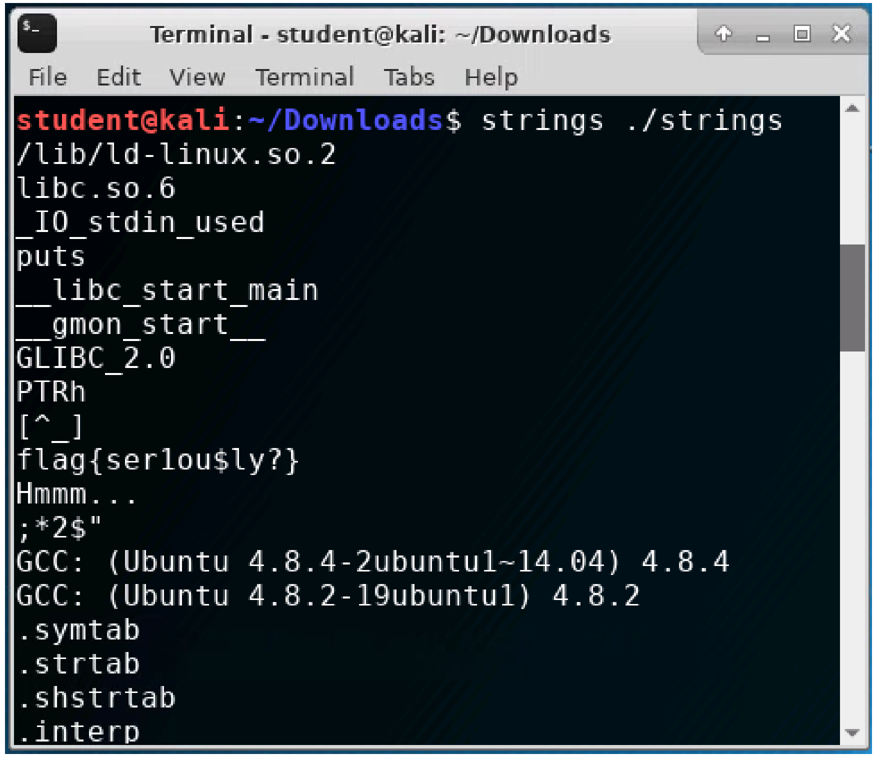
White hats
15

Insecure Protocols
20

File Extraction
40

Approaching Challenges: General Tips

- Point values indicate difficulty level
- Challenge name is almost always a hint
  - Google category along with challenge name
- Read the challenge description carefully
  - Google category along with keywords
- Is there a file? Filename might be a hint
  - The file extension might be misleading – you might have to learn about “magic numbers”
  - Open in Notepad or other text editor
  - Search for ‘strings’ in file
  - Open in hex editor?
- Any names mentioned?
  - Is the name meaningful?
- Your answer has to match exactly (or very closely).
  - May need to try different capitalization, etc

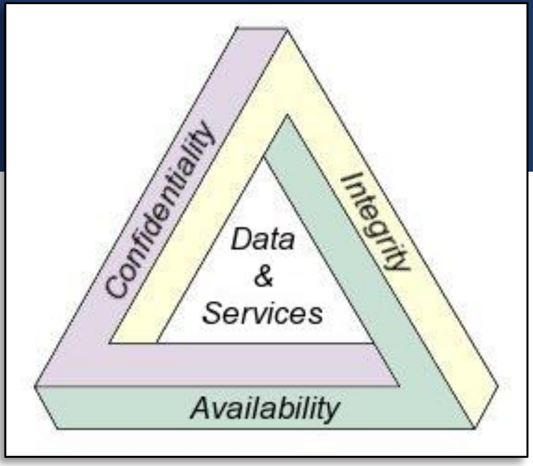


```
student@kali:~/Downloads$ strings ./strings
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
puts
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
flag{ser1ou$ly?}
Hmmm...
;*2$"
GCC: (Ubuntu 4.8.4-2ubuntu1~14.04) 4.8.4
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
.strtab
.shstrtab
.interp
```

Challenge Types: Cyber Knowledge

- Can encompass a variety of different category names
- Basic user awareness
  - Things users should be aware of to protect themselves and their online and other accounts
- Introductory cybersecurity
  - Basic terminology related to cybersecurity
  - Network security devices and software
- Careers
  - Various jobs roles and career paths
- Might even be non-Cybersecurity topics, just to keep things interesting!

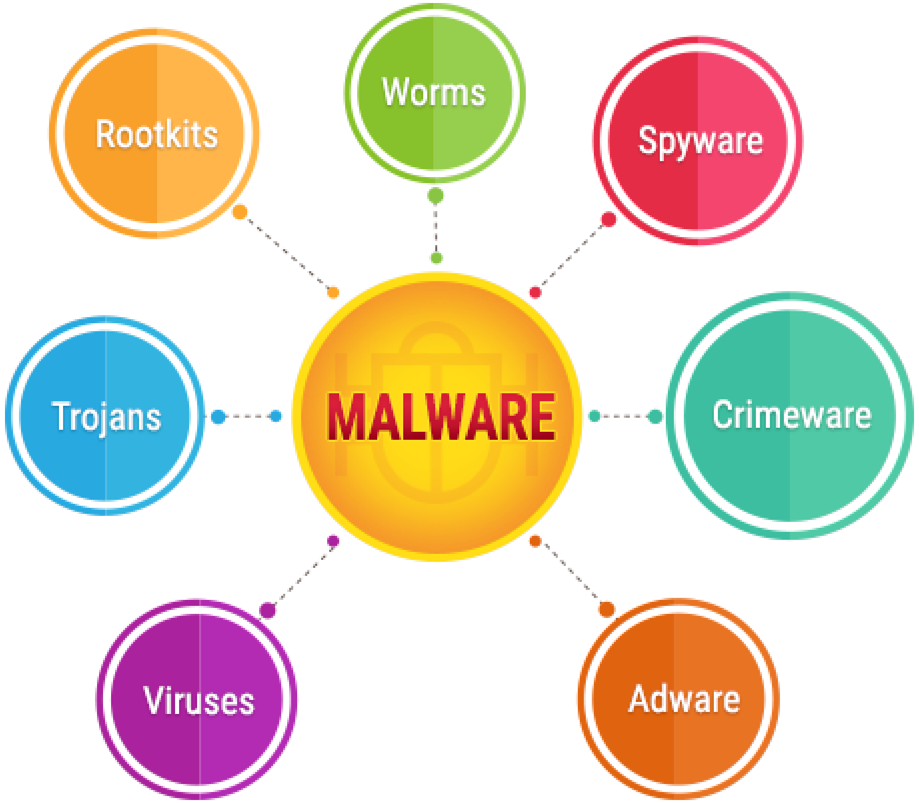
Cyber Principles



- "The CIA Triad"

- Confidentiality
  - Protecting information from disclosure to unauthorized entities
- Integrity
  - Ensuring that information is not altered accidentally or by entities unauthorized to make alterations
- Availability
  - Ensuring information can be used when and where needed

Malware (Malicious Software)



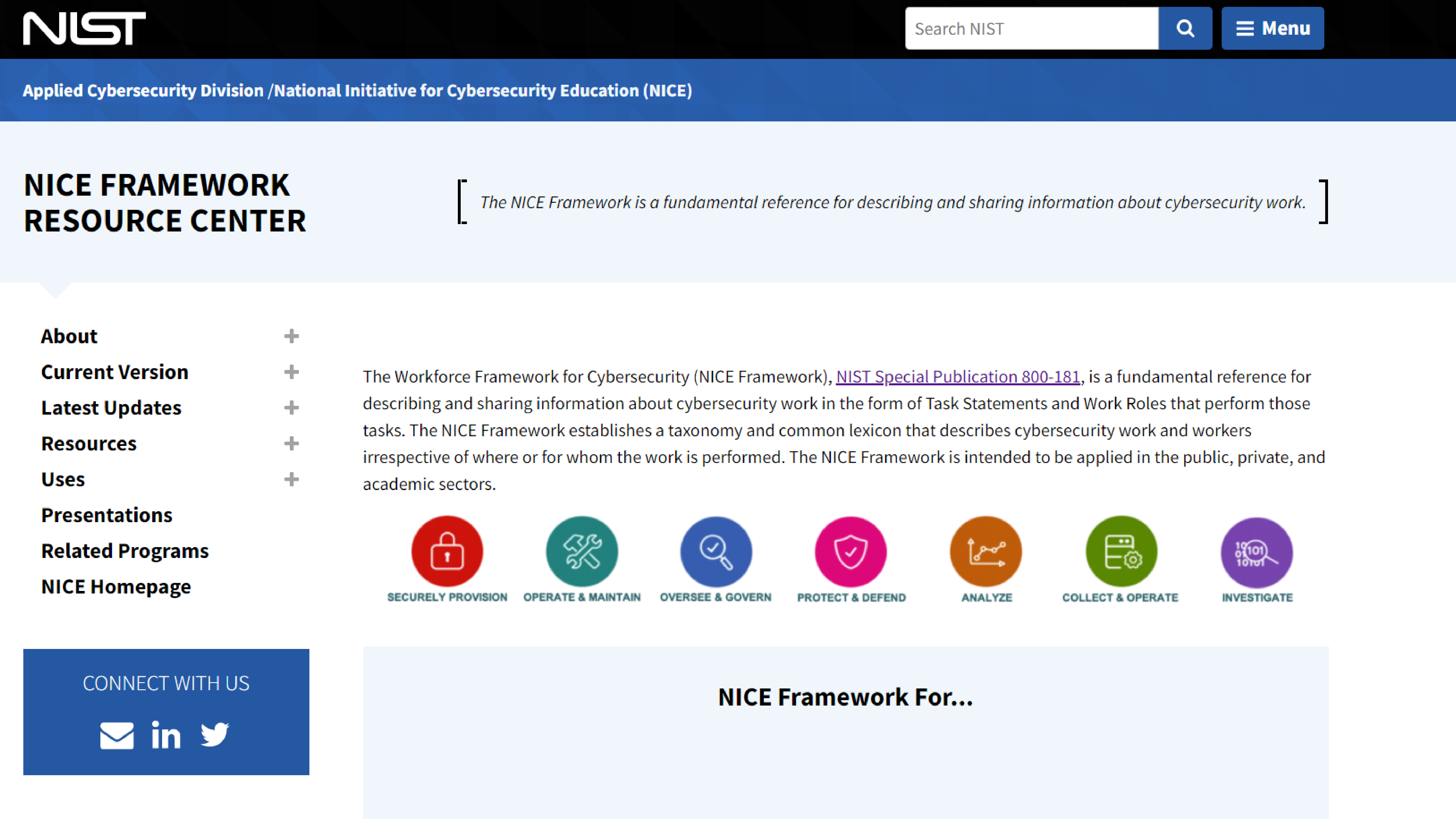
- **Ransomware** –encrypts data and demands a payment for decryption
- **Rootkit** –gains unauthorized privileged (or "root) access and carefully masks its existence from other software
- **Cryptominer** –mines cryptocurrency on behalf of attacker
- **Trojan horse** – disguises itself as a normal program to trick user into running it, then installs malicious payload
- **Botnet** – large networks of infected hosts that function cooperatively on demand
- **Adware** – automatically displays unwanted ads by popping up new windows
- **Spyware** – monitors, or spies, on user activity and reports back to attacker

Image: https://itque.net/wp-content/uploads/2019/05/what-is-malware.png

NICE Workforce Framework

- Includes *Task Statements* and *Work Roles* that help describe cybersecurity work
- Lists *knowledge*, *skills*, and *abilities* related to various cybersecurity jobs
- Details on the framework, including job categories, specialty areas, work roles, and KSA are in *NIST SP 800-181*

- Search on the web for “NICE Workforce Framework”



NIST

Search NIST

Menu

Applied Cybersecurity Division /National Initiative for Cybersecurity Education (NICE)

NICE FRAMEWORK RESOURCE CENTER

The NICE Framework is a fundamental reference for describing and sharing information about cybersecurity work.

- About +
- Current Version +
- Latest Updates +
- Resources +
- Uses +
- Presentations
- Related Programs
- NICE Homepage

CONNECT WITH US

The Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181, is a fundamental reference for describing and sharing information about cybersecurity work in the form of Task Statements and Work Roles that perform those tasks. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

SECURELY PROVISION

OPERATE & MAINTAIN

OVERSEE & GOVERN

PROTECT & DEFEND

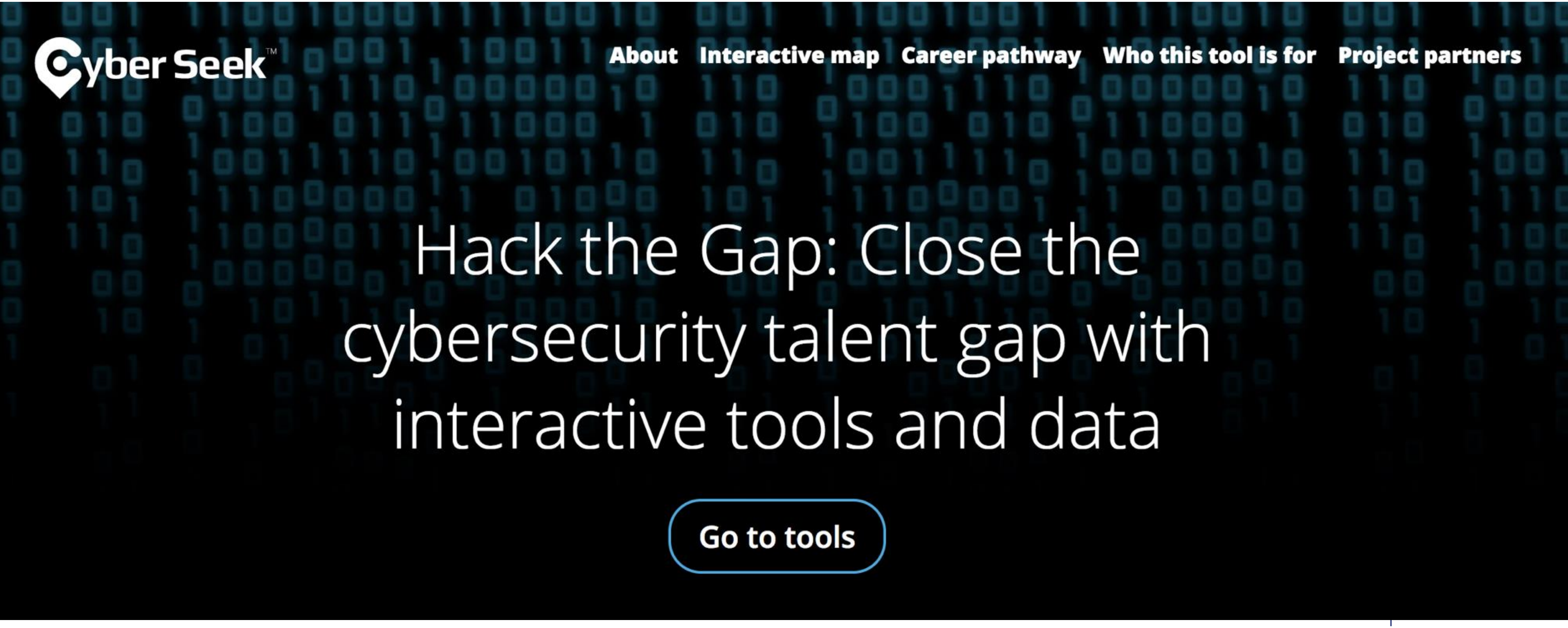
ANALYZE

COLLECT & OPERATE

INVESTIGATE

NICE Framework For...

Cybersecurity Career Pathways (https://www.cyberseek.org/)



Cyber Seek™

About Interactive map Career pathway Who this tool is for Project partners

Hack the Gap: Close the cybersecurity talent gap with interactive tools and data

Go to tools

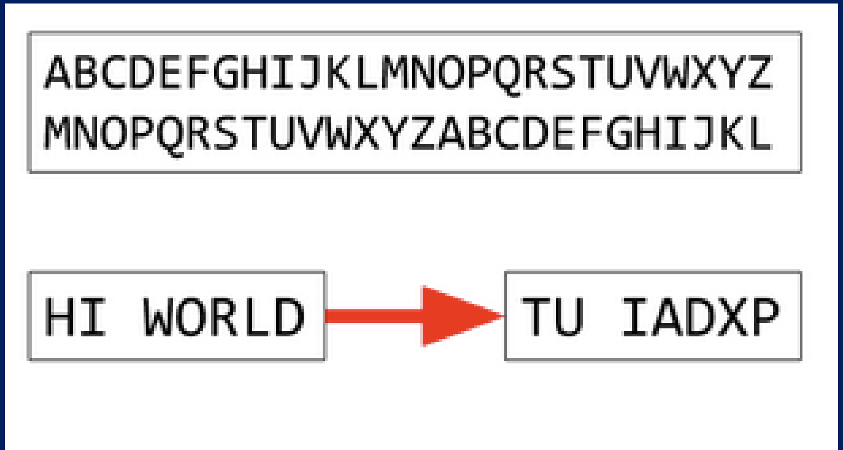
Sample Challenge: Cyber Knowledge

- Challenge: What type of malware encrypts your data and demands a ransom (usually in cryptocurrency) for the decryption key?

- Flag: **Ransomware**

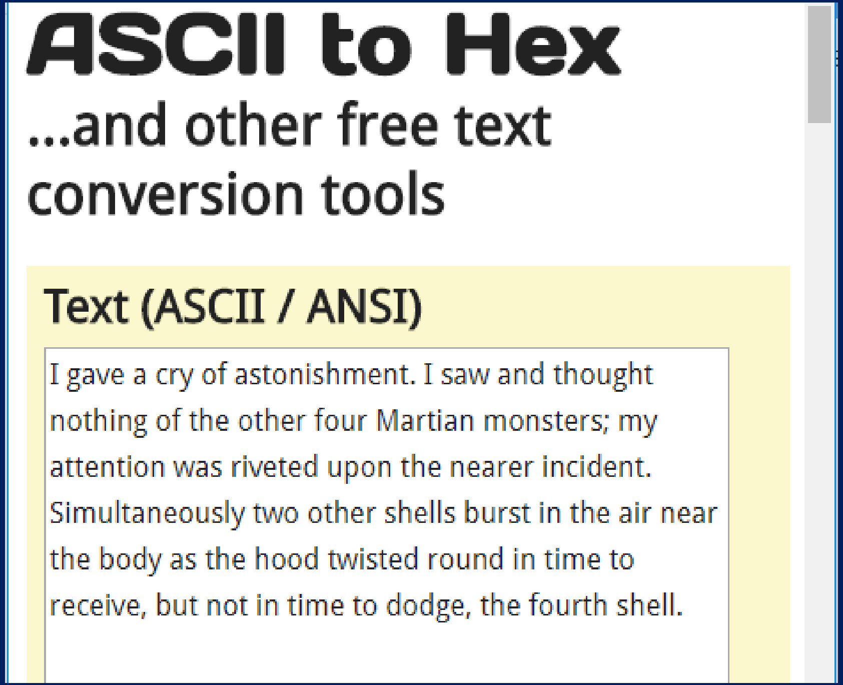
Challenge Types: Cryptography

- Often provided with an encoded message and some hint as to the encoding
- Many challenges are not *encryption*, but *encodings*
  - ASCII (decimal or hex values)
  - BASE64/BASE32
  - UUEncoded
- Simple monoalphabetic ciphers
  - Ceasar/ROT cipher
  - Substitution cipher
  - These can be easily solved w/out key
    - Frequency analysis!



ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNOPQRSTUVWXYZABCDEFGHIJKL

HI WORLD → TU IADXP



ASCII to Hex

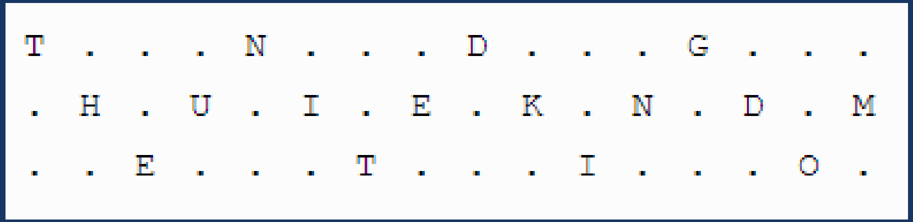
...and other free text conversion tools

Text (ASCII / ANSI)

I gave a cry of astonishment. I saw and thought nothing of the other four Martian monsters; my attention was riveted upon the nearer incident. Simultaneously two other shells burst in the air near the body as the hood twisted round in time to receive, but not in time to dodge, the fourth shell.

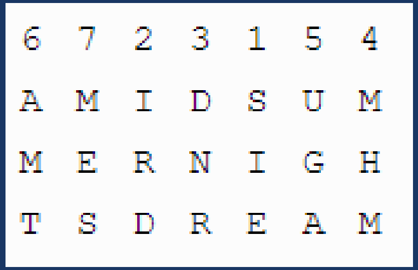
Challenge Types: Cryptography

- Polyalphabetic ciphers
  - Vignere cipher
  - Playfair cipher
  - Beaufort cipher
  - Autokey cipher
- Transposition ciphers
  - Railfence cipher
  - Columnar transposition
  - Route cipher
- For more, see:
  - http://www.crypto-it.net
  - Khan Academy – Intro to Cryptography



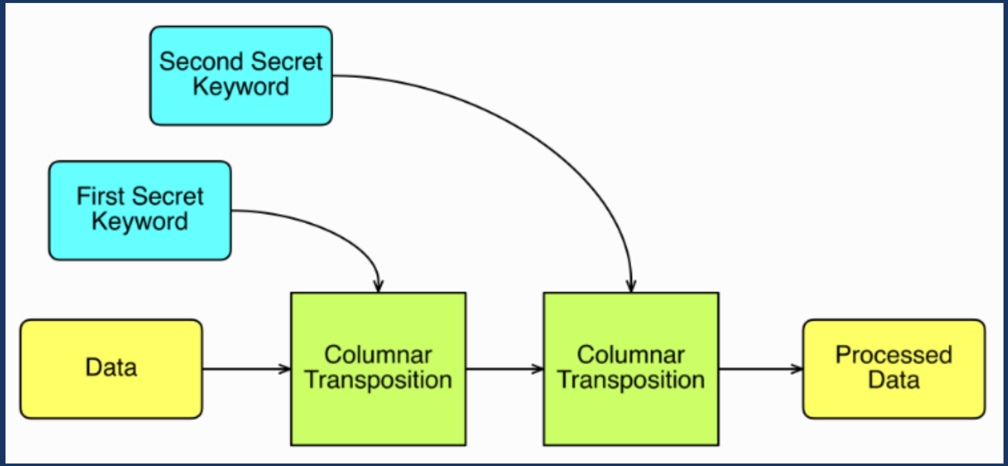
```
T . . . N . . . D . . . G . . .
. H . U . I . E . K . N . D . M
. . E . . . T . . . I . . . O .
```

Railfence Cipher



6	7	2	3	1	5	4
A	M	I	D	S	U	M
M	E	R	N	I	G	H
T	S	D	R	E	A	M

Columnar Transposition



Double Columnar Transposition

Cryptography: Resources

- More information on introductory cryptography
  - Khan Academy: https://www.khanacademy.org/computing/computer-science/cryptography
- Web sites for solving basic cryptographic challenges
  - ASCII to Hex: https://www.asciitohex.com/
  - ROT13.com: https://rot13.com/
  - Boxentriq: https://www.boxentriq.com/code-breaking
  - DCode.fr: https://www.dcode.fr/

Sample Challenge: Cryptography

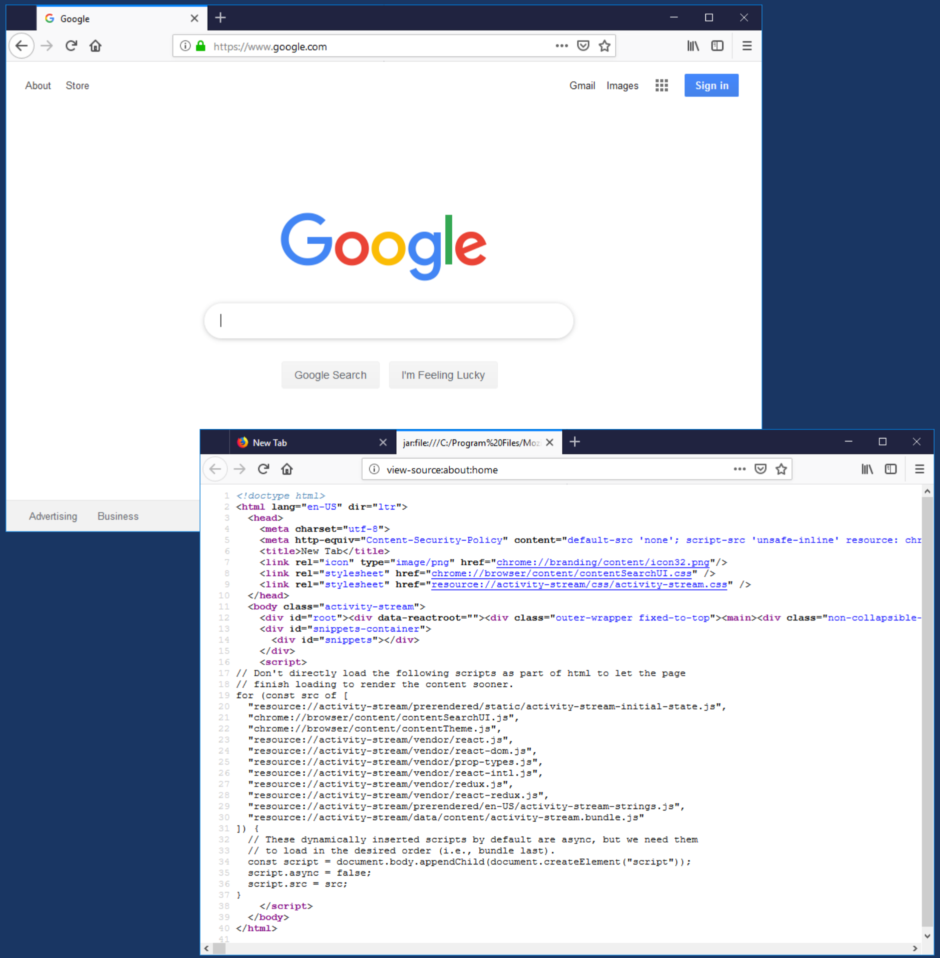
- Challenge: **fvzcyrfuvsgpvcure**

- Hint: Some say that Caesar used this cipher

- Flag: **simpleshiftcipher**

Challenge Types: Web

- Easy challenges rely on basic understanding of HTML and how websites work
- Approaches to solving
  - View Page Source
  - Open ‘Developer Panel’
  - Examine network traffic
  - ‘curl’ the page examine full response
  - Look for robots.txt
  - Directory traversal attack?
  - *What else?*



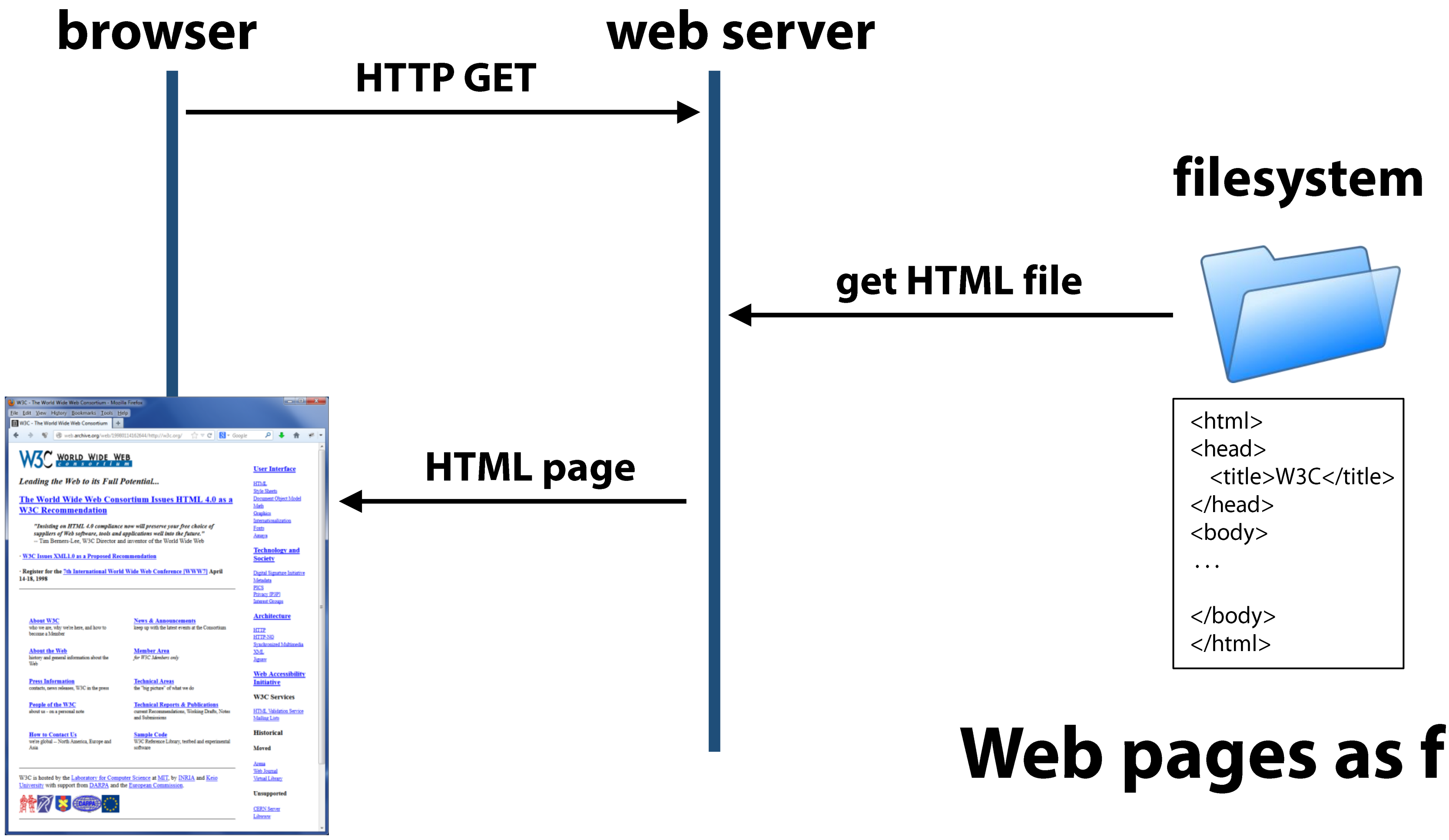
```
<!doctype html>
<html lang="en-US" dir="ltr">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; script-src 'unsafe-inline' resource: chr
    <title>New Tab</title>
    <link rel="icon" type="image/png" href="chrome://branding/content/icon32.png"/>
    <link rel="stylesheet" href="chrome://browser/content/contentSearchUI.css" />
    <link rel="stylesheet" href="resource://activity-stream/css/activity-stream.css" />
  </head>
  <body class="activity-stream">
    <div id="root"><div data-reactroot=""><div class="outer-wrapper fixed-to-top"><main><div class="non-collapsible-
    <div id="snippets-container">
      <div id="snippets"></div>
    </div>
    <script>
// Don't directly load the following scripts as part of html to let the page
// finish loading to render the content sooner.
for (const src of [
  "resource://activity-stream/prerendered/static/activity-stream-initial-state.js",
  "chrome://browser/content/contentSearchUI.js",
  "chrome://browser/content/contentTheme.js",
  "resource://activity-stream/vendor/react.js",
  "resource://activity-stream/vendor/react-dom.js",
  "resource://activity-stream/vendor/prop-types.js",
  "resource://activity-stream/vendor/react-intl.js",
  "resource://activity-stream/vendor/redux.js",
  "resource://activity-stream/vendor/react-redux.js",
  "resource://activity-stream/prerendered/en-US/activity-stream-strings.js",
  "resource://activity-stream/data/content/activity-stream.bundle.js"
]) {
  // These dynamically inserted scripts by default are async, but we need them
  // to load in the desired order (i.e., bundle last).
  const script = document.body.appendChild(document.createElement("script"));
  script.async = false;
  script.src = src;
}
    </script>
  </body>
</html>
```

Inspecting HTML Pages

- HTML is a Markup Language
  - Tags use basic format
    - <opentag>
    - </closetag>
  - Stored on web servers as .html files
  - Simple pages can use just html
  - Most modern pages use javascript or some other scripting language
- You can view a page’s source (html code) in your browser
  - In Chrome, go to 3-dot menu (upper right) and select “**MoreTools→DeveloperTools**”

```
<html>
   <head>
      <title> Page Title Goes Here </title>
   </head>
   <body>
      <!-- this tag starts a comment block
      the following tag ends one -->
      <h1> Large Header </h1>
      <ul>
         <li> Item 1 of list </li>
         <li> Item 2 </li>
      </ul>
      <a href=“https://www.npr.org”> NPR </a>
   </body>
</html>
```

Early WWW Model


browser
web server
HTTP GET
filesystem
get HTML file
HTML page
W3C - The World Wide Web Consortium - Mozilla Firefox
File Edit View History Bookmarks Tools Help
W3C - The World Wide Web Consortium
web.archive.org/web/19980114162644/http://w3c.org/
Google

W3C WORLD WIDE WEB consortium

Leading the Web to its Full Potential...

The World Wide Web Consortium Issues HTML 4.0 as a W3C Recommendation

> ***"Insisting on HTML 4.0 compliance now will preserve your free choice of suppliers of Web software, tools and applications well into the future."***
> -- Tim Berners-Lee, W3C Director and inventor of the World Wide Web

· **W3C Issues XML1.0 as a Proposed Recommendation**

· **Register for the 7th International World Wide Web Conference [WWW7] April 14-18, 1998**

About W3C
who we are, why we're here, and how to become a Member

News & Announcements
keep up with the latest events at the Consortium

About the Web
history and general information about the Web

Member Area
for W3C Members only

Press Information
contacts, news releases, W3C in the press

Technical Areas
the "big picture" of what we do

People of the W3C
about us - on a personal note

Technical Reports & Publications
current Recommendations, Working Drafts, Notes and Submissions

How to Contact Us
we're global -- North America, Europe and Asia

Sample Code
W3C Reference Library, testbed and experimental software

W3C is hosted by the Laboratory for Computer Science at MIT, by INRIA and Keio University with support from DARPA and the European Commission.

User Interface

HTML
Style Sheets
Document Object Model
Math
Graphics
Internationalization
Fonts
Amaya

Technology and Society

Digital Signature Initiative
Metadata
PICS
Privacy [P3P]
Interest Groups

Architecture

HTTP
HTTP-NG
Synchronized Multimedia
XML
Jigsaw

Web Accessibility Initiative

W3C Services

HTML Validation Service
Mailing Lists

Historical

Moved

Arena
Web Journal
Virtual Library

Unsupported

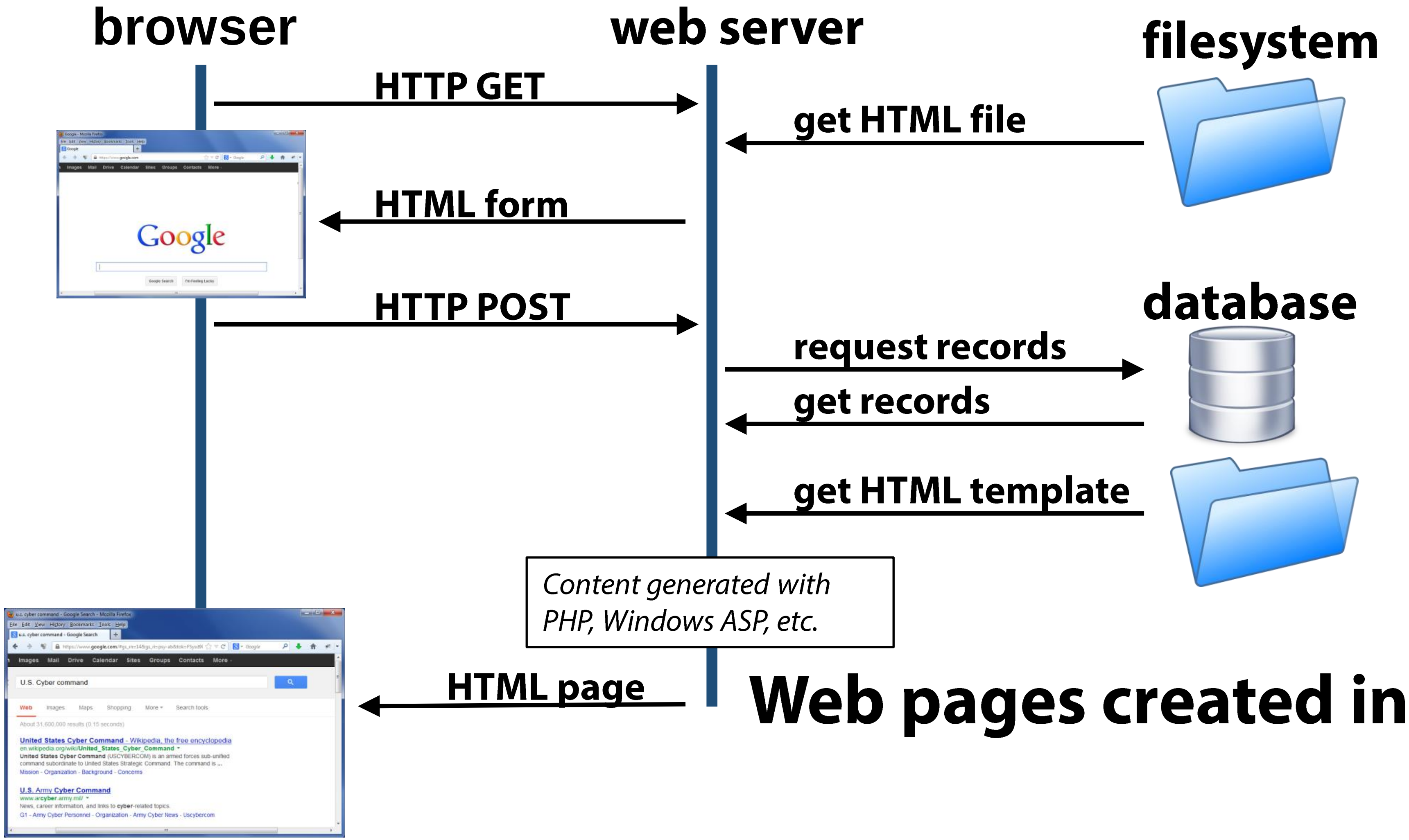
CERN Server
Libwww

```
<html>
<head>
  <title>W3C</title>
</head>
<body>
 . . .

</body>
</html>
```

Web pages as files

Modern WWW Model


browser
web server
filesystem
database
HTTP GET
get HTML file
HTML form
Google
HTTP POST
request records
get records
get HTML template
HTML page
u.s. cyber command - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Images Mail Drive Calendar Sites Groups Contacts More
U.S. Cyber command
Web Images Maps Shopping More Search tools

About 31,600,000 results (0.15 seconds)

United States Cyber Command - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/United_States_Cyber_Command
United States Cyber Command (USCYBERCOM) is an armed forces sub-unified command subordinate to United States Strategic Command. The command is ...
Mission - Organization - Background - Concerns

U.S. Army Cyber Command
www.arcyber.army.mil/
News, career information, and links to cyber-related topics.
G1 - Army Cyber Personnel - Organization - Army Cyber News - Uscybercom

Content generated with PHP, Windows ASP, etc.

Web pages created in real time

VIRGINIA CYBER RANGE

Example Challenge: Web

- Challenge: What is the secret message hidden near the </body> tag at http://www.sekritskwerl.com?

- Hint: View the ‘page source’

- Flag: squiddlydiddly

Challenge Types: Reconnaissance

- These problems focus on general problem-solving
  - Often not much ‘cyber’ experience needed
- Usually require competitors to follow a trail of clues to reach a final flag.
- Useful tools:
  - *Google and other search engines*
  - Internet Wayback Machine (archive.org)
  - Whois lookups? (whois.icann.org)
  - Shodan? (www.shodan.io)

Example Challenge: Reconnaissance

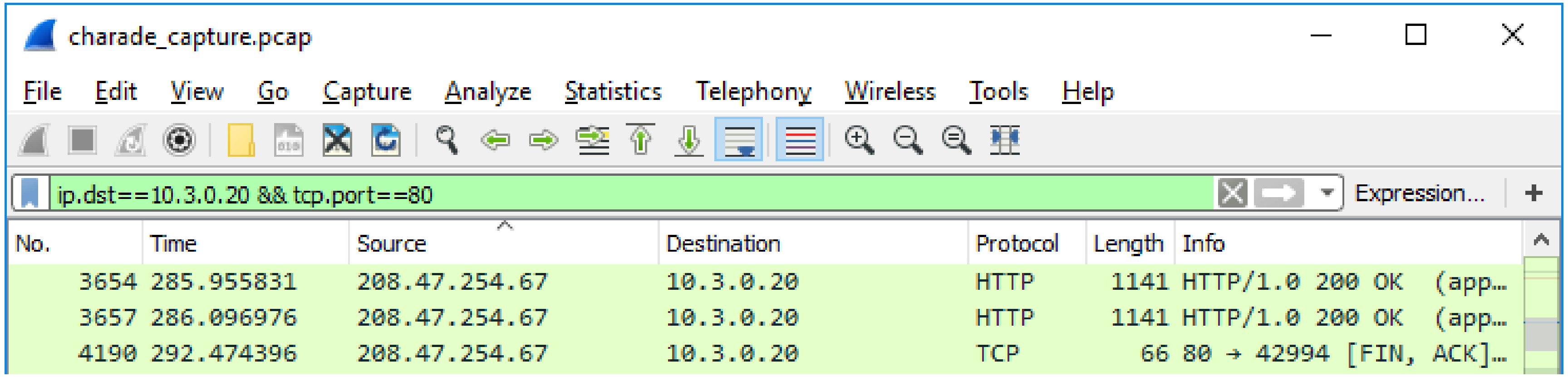
- Challenge: 11,185,272. What's next?

- Flag: 12,837,064

Challenge Types: Networking

- Analyze packet capture to find flag
  - Answer questions related to network traffic
  - “Carve” images and files from packet streams
- Tools
  - Wireshark!
    - Graphical tool for analyzing network traffic
    - Available for Windows, Mac, Linux
    - Download from https://www.wireshark.org/
  - tcpdump/windump
    - Command-line tool for examining network traffic
  - ngrep
    - Search for string sin network packets

Wireshark Display Filters



ip.dst==10.3.0.20 && tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
3654	285.955831	208.47.254.67	10.3.0.20	HTTP	1141	HTTP/1.0 200 OK (app…
3657	286.096976	208.47.254.67	10.3.0.20	HTTP	1141	HTTP/1.0 200 OK (app…
4190	292.474396	208.47.254.67	10.3.0.20	TCP	66	80 → 42994 [FIN, ACK]…

- Enter filters in textbox
  - Use Expression button to get help creating filters
  - Filter box is green for valid filter, red otherwise
- Click Apply to apply filter
- Click Clear to clear filter

VIRGINIA CYBER RANGE

More Wireshark . . .

- **Boolean Expressions in Filters:**
  - The symbol for logical **AND** in TCP filters is **&&** (you can use **and** and **&&** interchangeably)
  - The symbol for logical **OR** is || (you can use **or** and || interchangeably)
  - Use parenthesis to form more specific Boolean expressions
  - Wireshark generally doesn’t care about case except with matching a specific string value.
- Some Examples:

Packets from 192.168.1.1	ip.src==192.168.1.1
Packets to and from port 80	tcp.port==80
From 10.10.3.2 to 10.10.3.40	ip.src==10.10.3.2 && ip.dst==10.10.3.40
To/from 10.10.3.2 on port 443	ip.addr==10.10.3.2 && tcp.port==443

Common Protocols

- HTTP
  - In-the-clear web communications
- FTP/TFTP
  - File transfer without encryption
- Telnet
  - Remote login without encryption
- SMTP (port 25)/POP (port 110)/IMAP (port 143)
  - Email communication protocols

- Protocols to ignore (*unless there is a method provided to break encryption*)
  - HTTPS – encrypted web traffic
  - SSH – encrypted remote login
  - SFTP – secure (encrypted) file transfer
  - SMTP (port 465)/IMAPS (port 993)/POP (port 995) – secure email access

Challenge Types: Forensics

- Given a digital artifact, find some bit of information to answer a challenge question
  - Drive image
  - Partial file system
  - Memory image
  - Packet capture file
- Useful tools:
  - Autopsy – Linux tool for analyzing drive images
  - RegRipper – Linux tool for analyzing Windows registry
  - Volatility – Linux memory forensics tool
  - Rekall – Windows memory forensics tool (FireEye product)
  - Linux search tools
    - Find, grep, etc.

High School Competitions

- picoCTF
  - Annual HS contest by Carnegie Melon’s CyLab and the CMU video game program
- EasyCTF
- HSCTF – “The first CTF by high schoolers, for high schoolers”
- RUSecure CTF
  - Radford University.
  - 3 rounds – preliminary round, qualifying round, in-person finals
- Cyberpatriot
  - Air Force sponsored team-based program

pico CTF

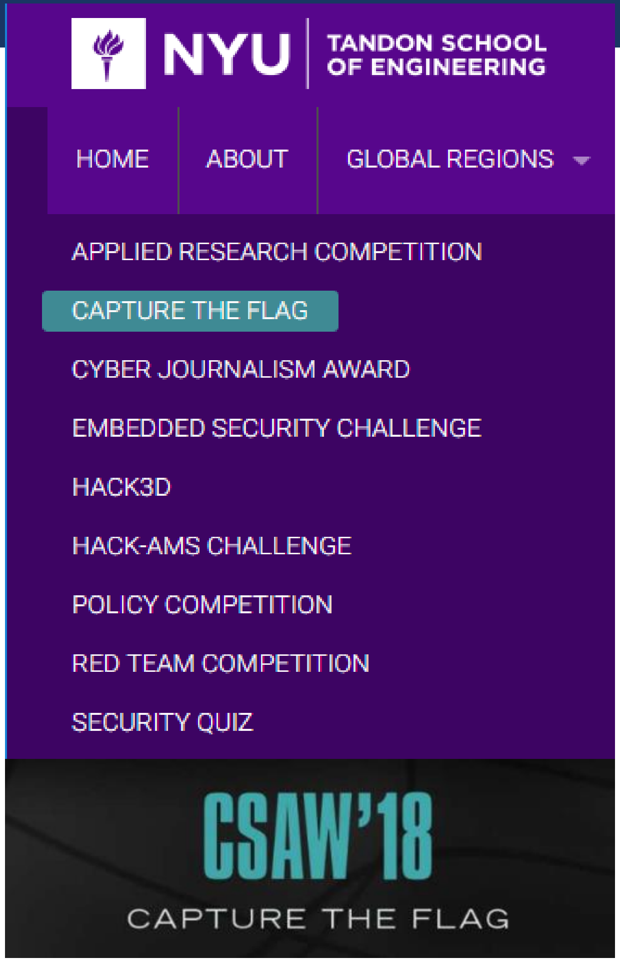
CMU CYBERSECURITY COMPETITION

PICOCTF

092818–101218

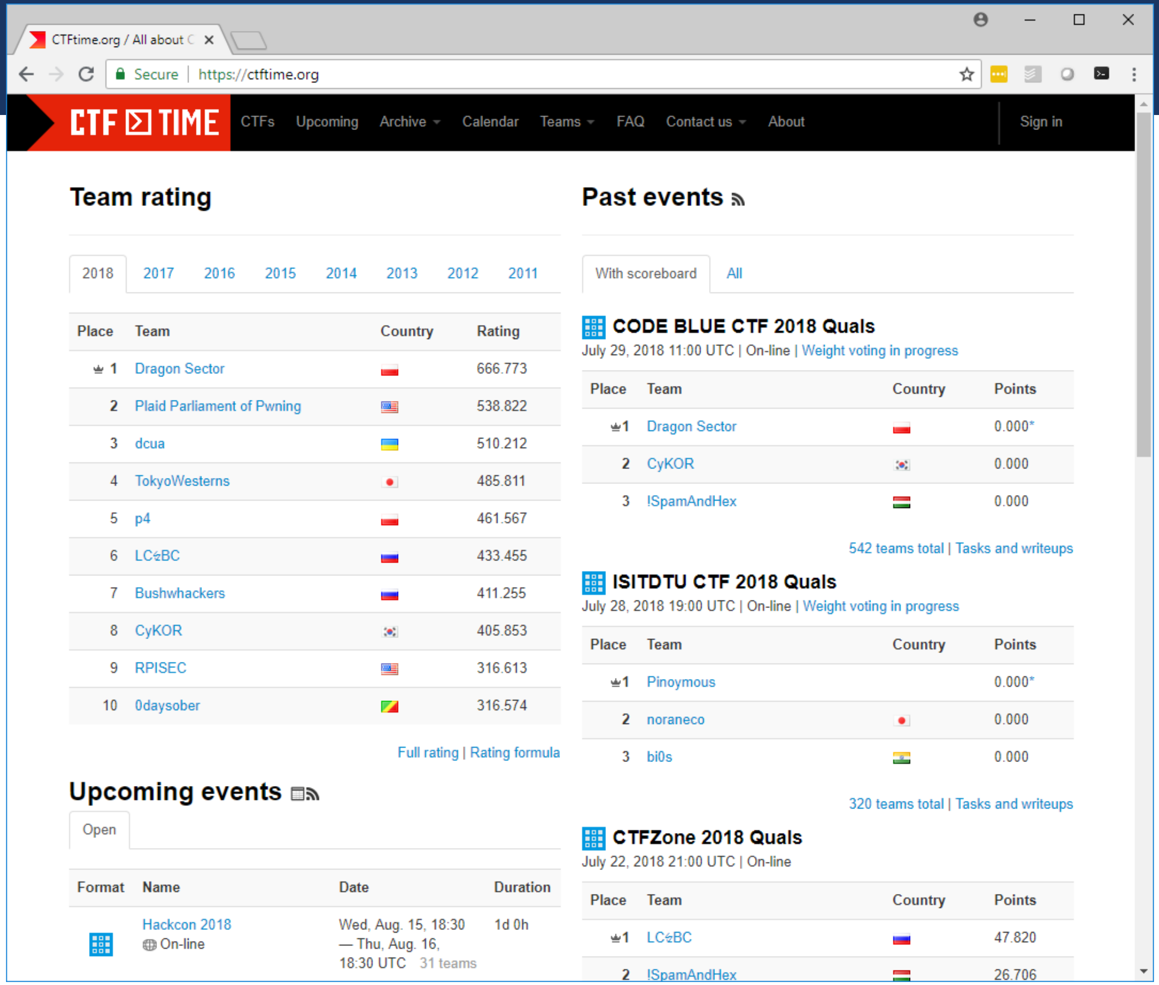
Collegiate/Professional Competitions

- CSAW CTF
  - Annual CTF hosted by NYU-Poly
  - Qualification round followed by in-person final
- Virginia Cyber Fusion CTF
  - Invitation-only event held at VMI for Governor's Cyber Cup
- DEF CON CTF
  - Gold standard of CTFs; held during annual DEF CON conference
- Collegiate Cyber Defense Competition (CCDC)
  - Annual inter-collegiate competition
  - 2018 CCDC champs: University of Virginia!
- LOTS more listed at https://ctftime.org/



https://ctftime.org/

- Central repository of CTF information
  - World-wide leaderboard
  - Calendar of upcoming CTFs
  - CTF archive (going back to 2011)
  - CTF solution write-ups!



Team rating

2018 2017 2016 2015 2014 2013 2012 2011

Place	Team	Country	Rating
♛ 1	Dragon Sector	🇵🇱	666.773
2	Plaid Parliament of Pwning	🇺🇸	538.822
3	dcua	🇺🇦	510.212
4	TokyoWesterns	🇯🇵	485.811
5	p4	🇵🇱	461.567
6	LC↯BC	🇷🇺	433.455
7	Bushwhackers	🇷🇺	411.255
8	CyKOR	🇰🇷	405.853
9	RPISEC	🇺🇸	316.613
10	0daysober	🇨🇬	316.574

Full rating | Rating formula

Upcoming events

Open

Format	Name	Date	Duration
	Hackcon 2018 On-line	Wed, Aug. 15, 18:30 — Thu, Aug. 16, 18:30 UTC 31 teams	1d 0h

Past events

With scoreboard All

CODE BLUE CTF 2018 Quals

July 29, 2018 11:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
♛1	Dragon Sector	🇵🇱	0.000*
2	CyKOR	🇰🇷	0.000
3	!SpamAndHex	🇭🇺	0.000

542 teams total | Tasks and writeups

ISITDTU CTF 2018 Quals

July 28, 2018 19:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points
♛1	Pinoymous		0.000*
2	noraneco	🇯🇵	0.000
3	bi0s	🇮🇳	0.000

320 teams total | Tasks and writeups

CTFZone 2018 Quals

July 22, 2018 21:00 UTC | On-line

Place	Team	Country	Points
♛1	LC↯BC	🇷🇺	47.820
2	!SpamAndHex	🇭🇺	26.706

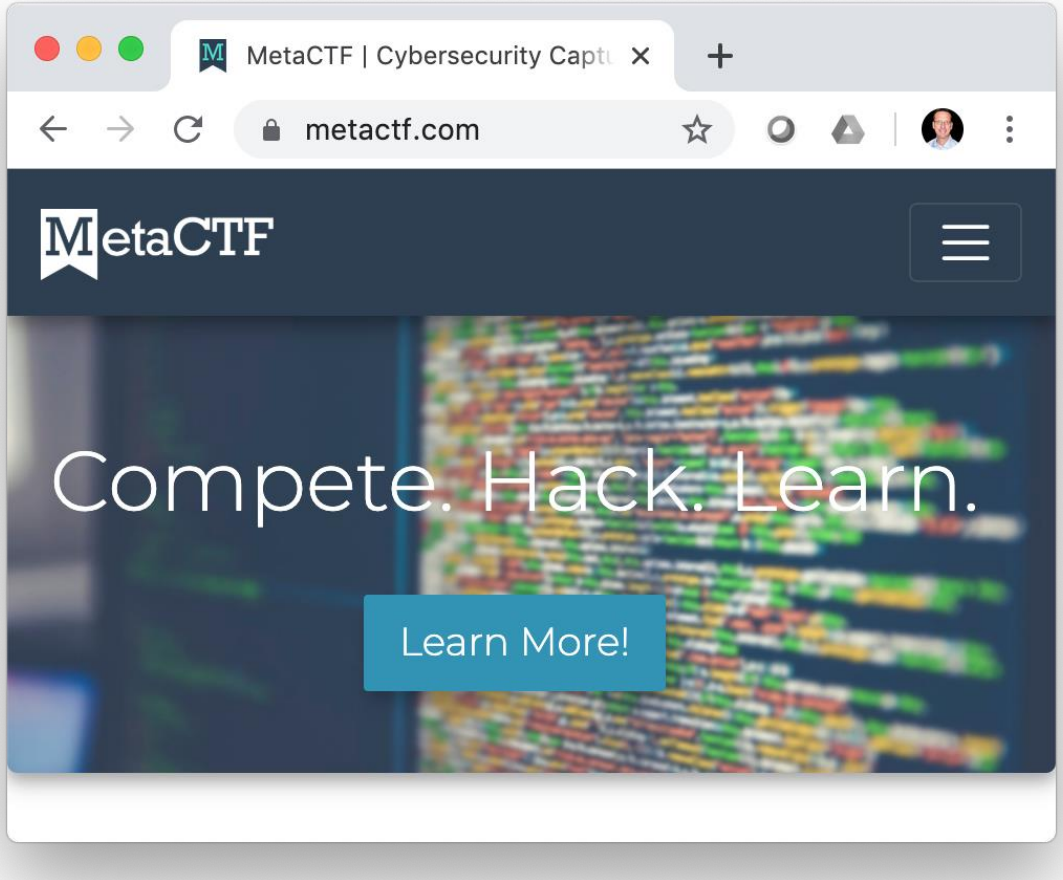
VIRGINIA CYBER RANGE

Host your own! – Free CTF frameworks

- CTFd
  - The CTF you use today is based on this
  - Purely Jeopardy-style
  - Downloadable from GitHub

- Facebook CTF (fbctf)
  - Downloadable from GitHub
  - Install as Docker container
  - Three “levels”
    - Quiz levels – trivia questions
    - Flag levels – Jeopardy-style challenges
    - Base levels – ‘King of the Hill’

Host your own! – CTF as a Service



MetaCTF | Cybersecurity Captu

metactf.com

- CTFd
  - https://ctfd.io
  - Hosted CTF platforms
  - Tiered pricing starting at $50/month
- MetaCTF
  - https://metactf.com
  - Hosted CTF competitions
  - Workshops and Hands-on labs
- U.S. Cyber Range: CloudCTF
  - https://cloudctf.com
  - Hosted CTF platforms and competitions
  - Coming soon!

VIRGINIA CYBER RANGE

Questions?

VIRGINIA CYBER RANGE

Making Virginia a
national resource for
cybersecurity education.

CONNECT WITH US

@VaCyberRange

virginiacyberrange.org