“Our ability to know is a function of our tools for knowing” -Carmen Medina

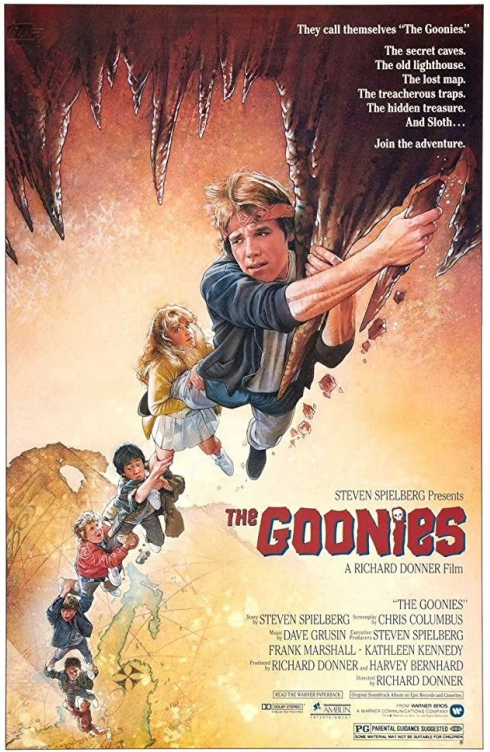
Hackers Teaching Hackers - 2022
Casey Smith
@subTee

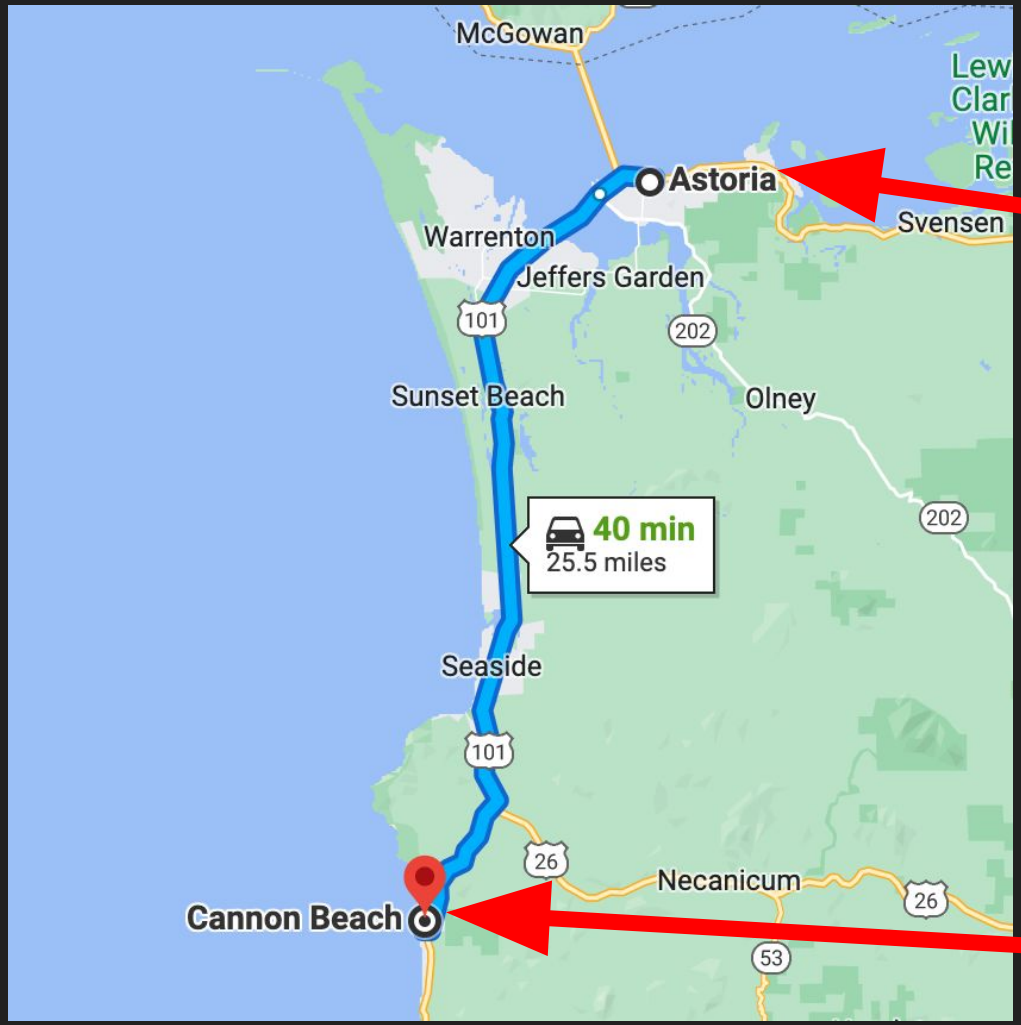
3 Big Ideas

1. Hackers get their edge knowing how things work behind the scenes
2. Defense and Offense taking the same perspectives (Tools)
3. Combining Things and Learning From Other Domains

Examples / Case Studies / References

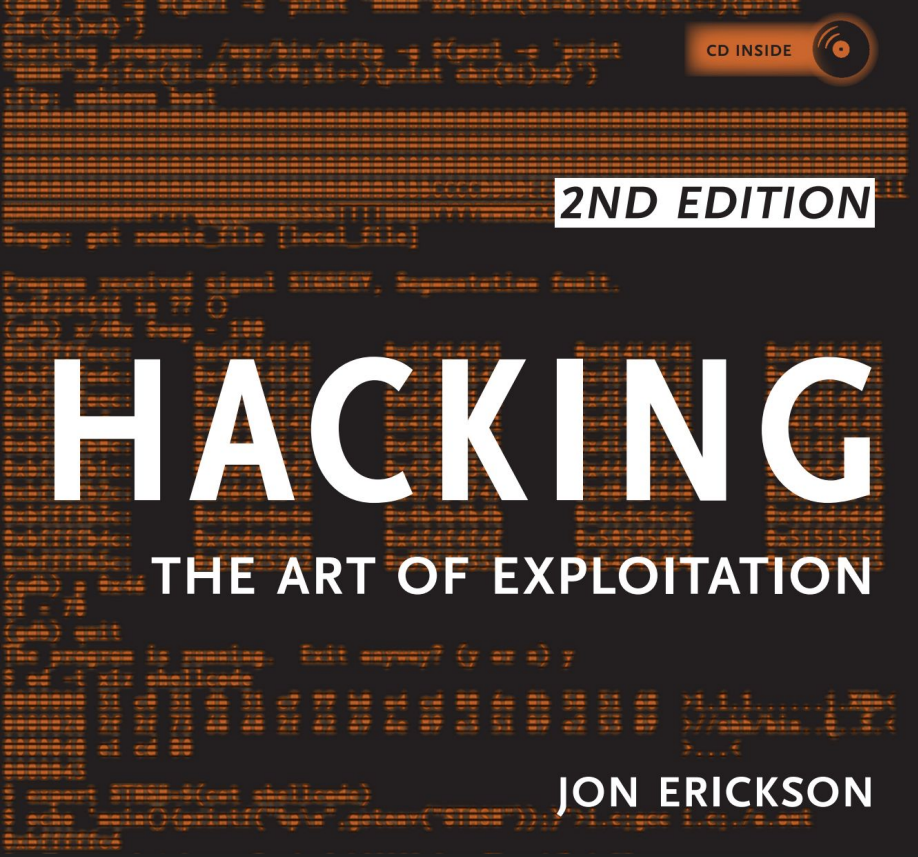

COUNTY JAIL


They call themselves "The Goonies."
The secret caves.
The old lighthouse.
The lost map.
The treacherous traps.
The hidden treasure.
And Sloth...
Join the adventure.
STEVEN SPIELBERG Presents
THE GOONIES
A RICHARD DONNER Film
"THE GOONIES"
Story by STEVEN SPIELBERG Screenplay by CHRIS COLUMBUS
Music by DAVE GRUSIN Executive Producers STEVEN SPIELBERG
FRANK MARSHALL - KATHLEEN KENNEDY
Produced by RICHARD DONNER and HARVEY BERNHARD
Directed by RICHARD DONNER
READ THE WARNER PAPERBACK
Original Soundtrack Album on Epic Records and Cassettes
DOLBY STEREO
AMBLIN ENTERTAINMENT
FROM WARNER BROS.
A WARNER COMMUNICATIONS COMPANY
PG PARENTAL GUIDANCE SUGGESTED
SOME MATERIAL MAY NOT BE SUITABLE FOR CHILDREN



Opening Car Chase Scene

4wd Race Cannon Beach



"Hackers get their edge from knowing how all the pieces interact within this bigger picture."

Hackers Gain Advantage By Their Tools

“Our Ability To Know, Is a Function of our Tools for knowing”

The world we understand today, is largely the results of TOOLS and Observation.

See :

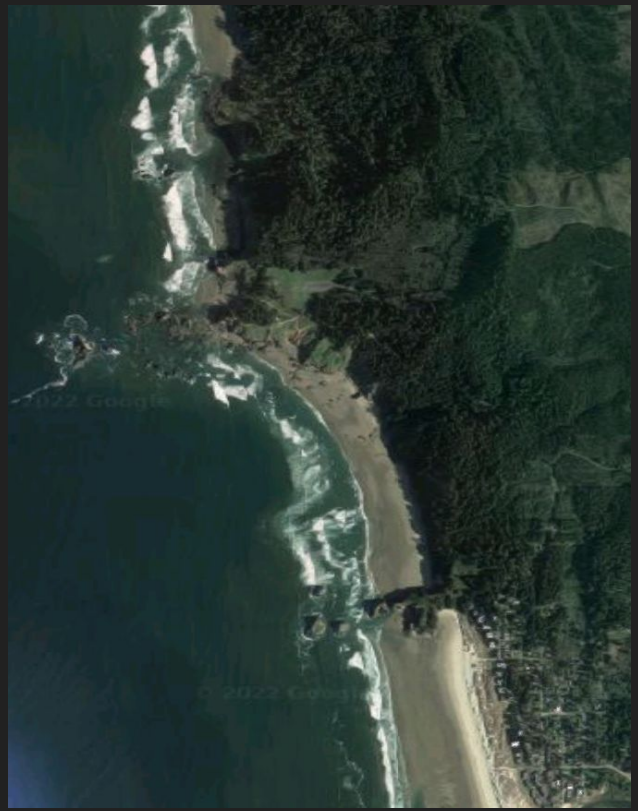
https://www.thecipherbrief.com/thinking-in-the-time-of-coronavirus-part-two

1. Individuals, Even Trained Scientists, Are REALLY Bad At Drawing Appropriate Conclusions From Available Evidence.
2. Our Ability To Know Is A Function Of Our Tools For Knowing.
3. The Streetlight Effect.

Maps as a Tool - Abstraction of Terrain

What can you tell me about this area?

How about now?

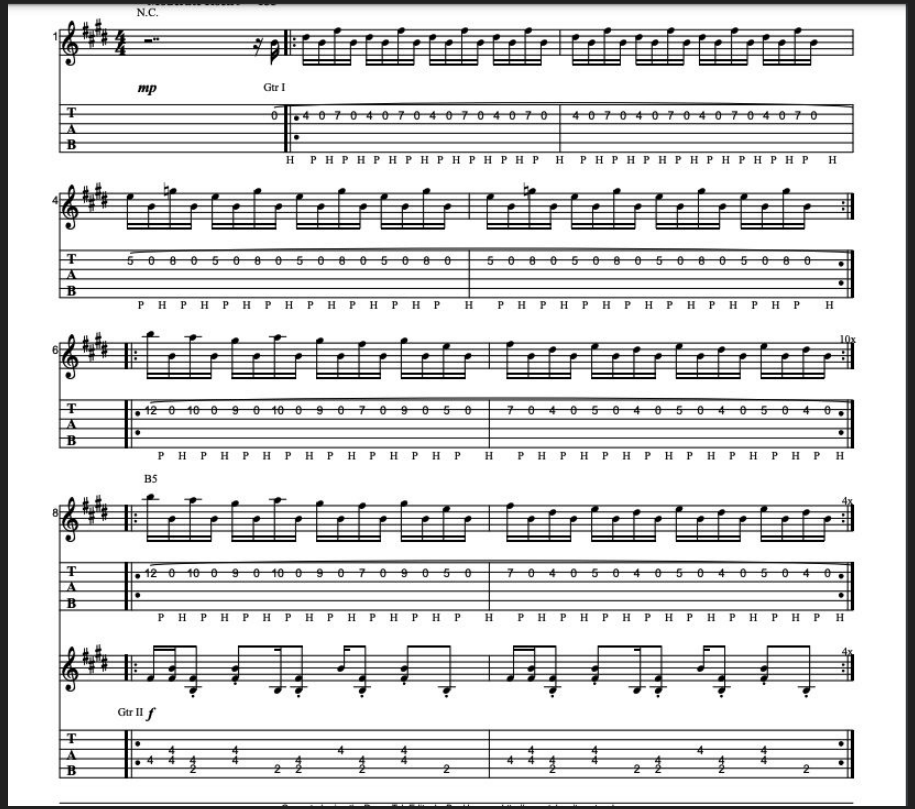


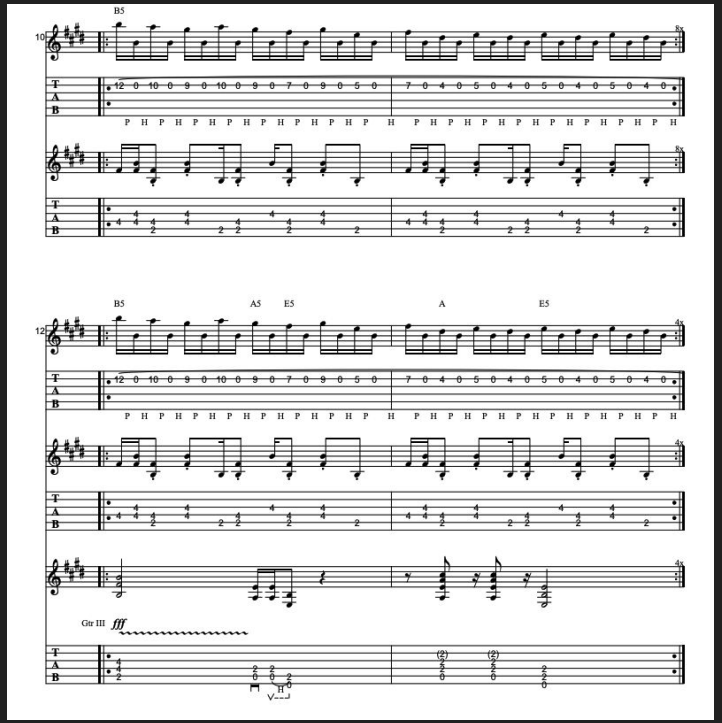
Ecola State Park, Oregon - Fratelli’s Hideout

The Map Is Not The Territory

Context Is Key =)

The Sheet Music is Not The Song





ThunderStruck

The sound of getting hacked is apparently Thunderstruck by AC/DC

By Dieter Bohn | @backlon | Aug 25, 2015, 3:02pm EDT

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

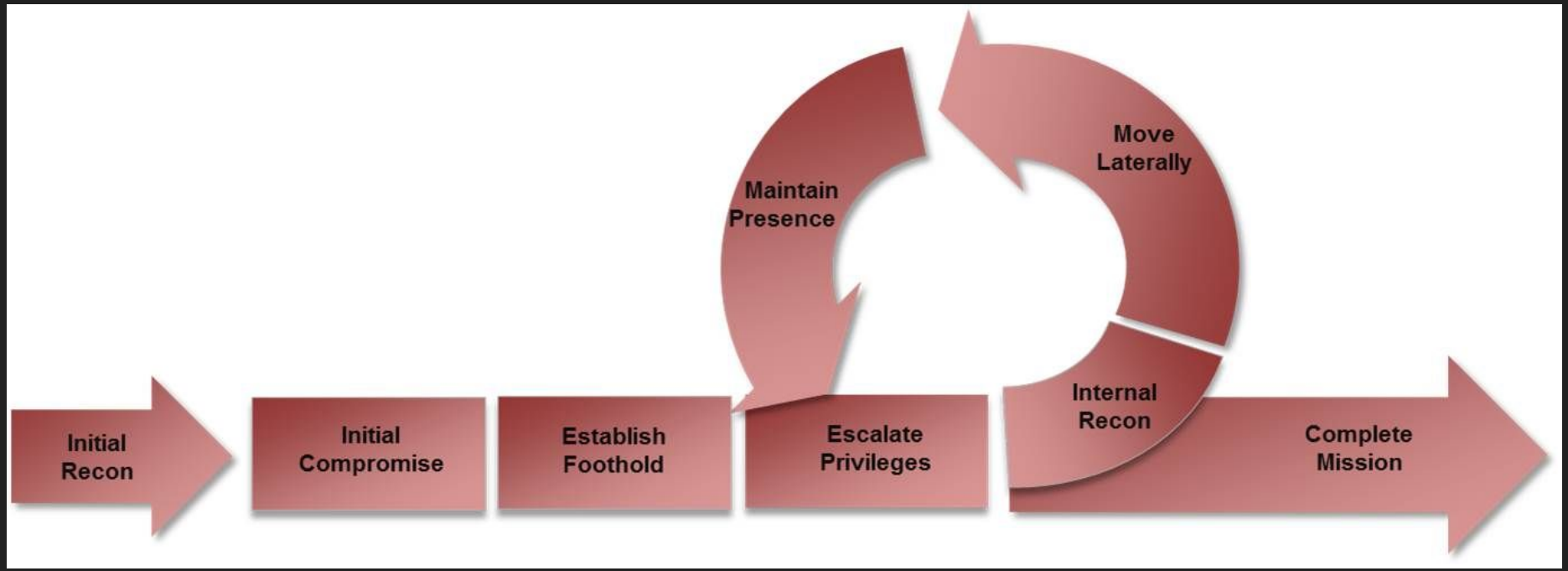
SHARE

Karl Walter/Getty Images

The Threat Report Is Not The Attack

“Thank you for that fine forensic analysis Mr. Bodine.”

“Of course, the experience was… somewhat different.”


Initial Recon
Initial Compromise
Establish Foothold
Escalate Privileges
Maintain Presence
Move Laterally
Internal Recon
Complete Mission

It is never that clean, never that easy

https://twitter.com/networkattack/status/888006186737553408?s=20&t=mga4Fb7TQfkw_RCqhl5H4w

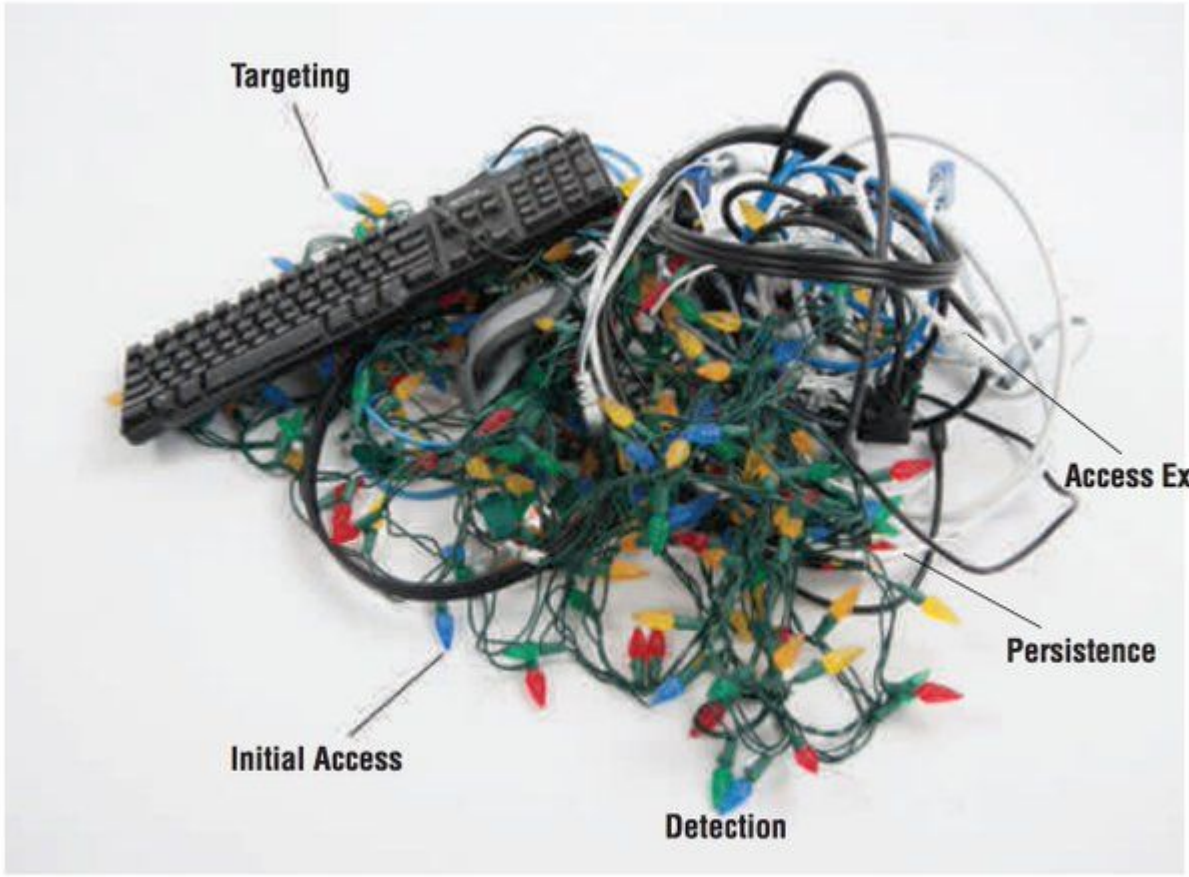


Figure 2.2: Real operational life cycle

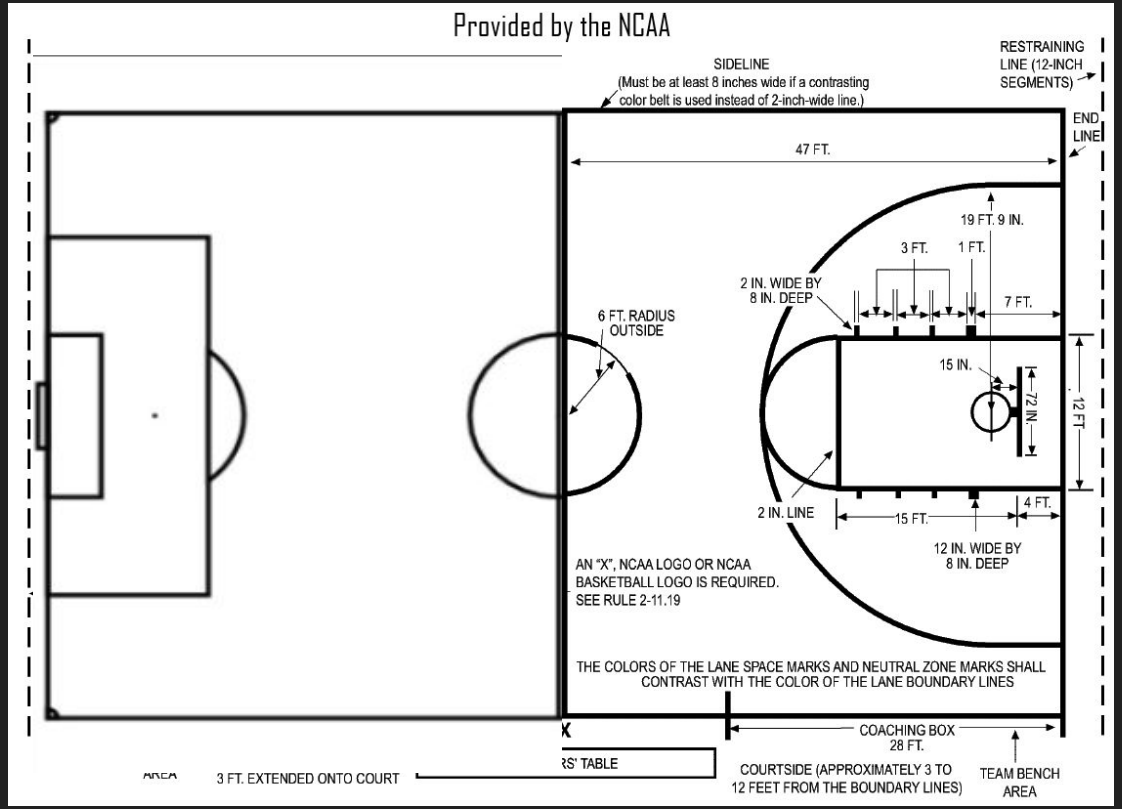
Tools Help Us More Accurately Understand Reality

Hypothesis:

Defense and Offense Need Same View

CyberBall - Defender's Can Take an Attacker View

Defender Map and Rules



Attacker Map and Rules

What Do Analysts See? What Tools Do They Use?

Before

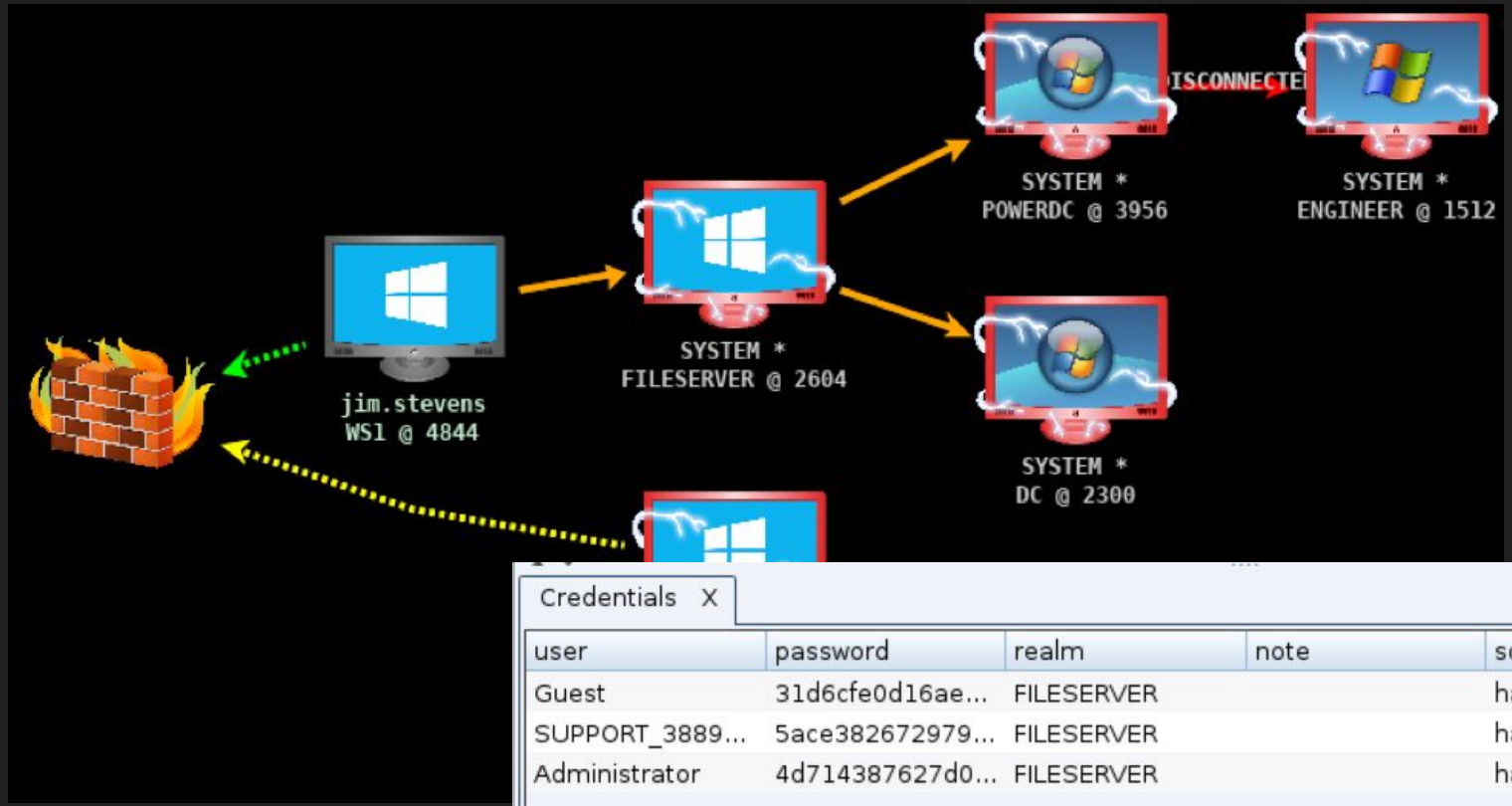
During

After

Can we replay? Pause, Rewind , Train ?

As a defender, I want the same TOOLS as an attacker!

Cobalt Strike Beacon - Lateral Mvmt View



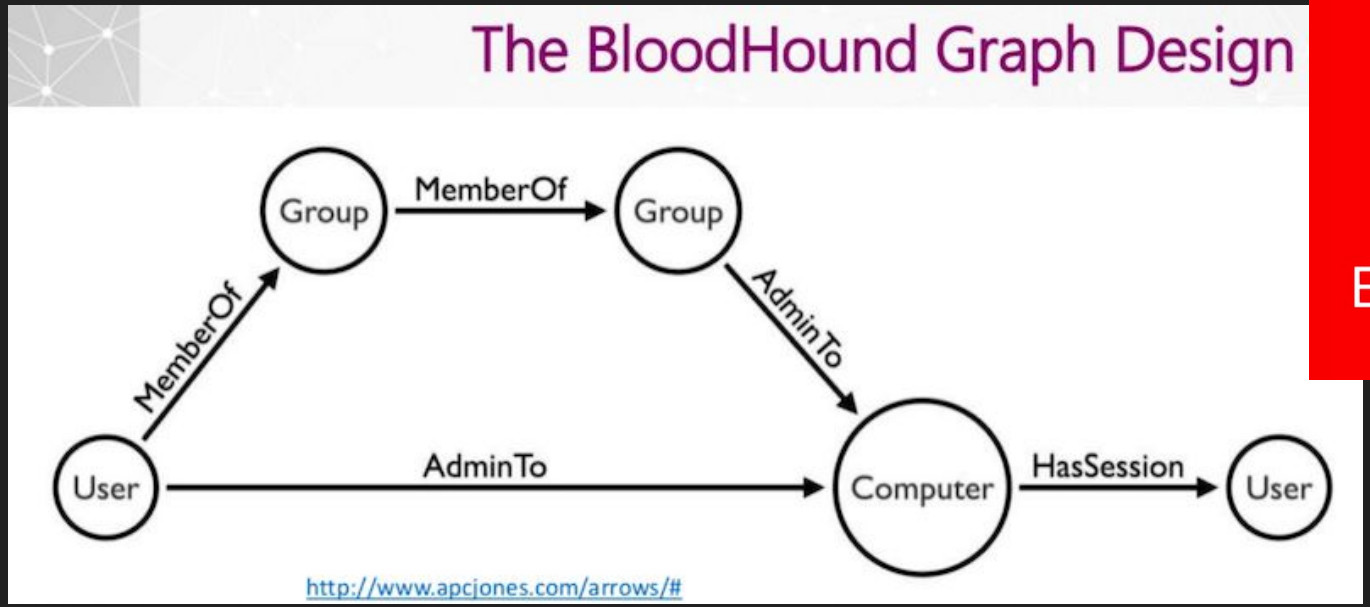
Credentials X

user	password	realm	note	source	host
Guest	31d6cfe0d16ae...	FILESERVER		hashdump	10.10.10.4
SUPPORT_3889...	5ace382672979...	FILESERVER		hashdump	10.10.10.4
Administrator	4d714387627d0...	FILESERVER		hashdump	10.10.10.4

Add | Edit | Copy | Remove | Help

How we think & Visualize Attacks and Incident Response

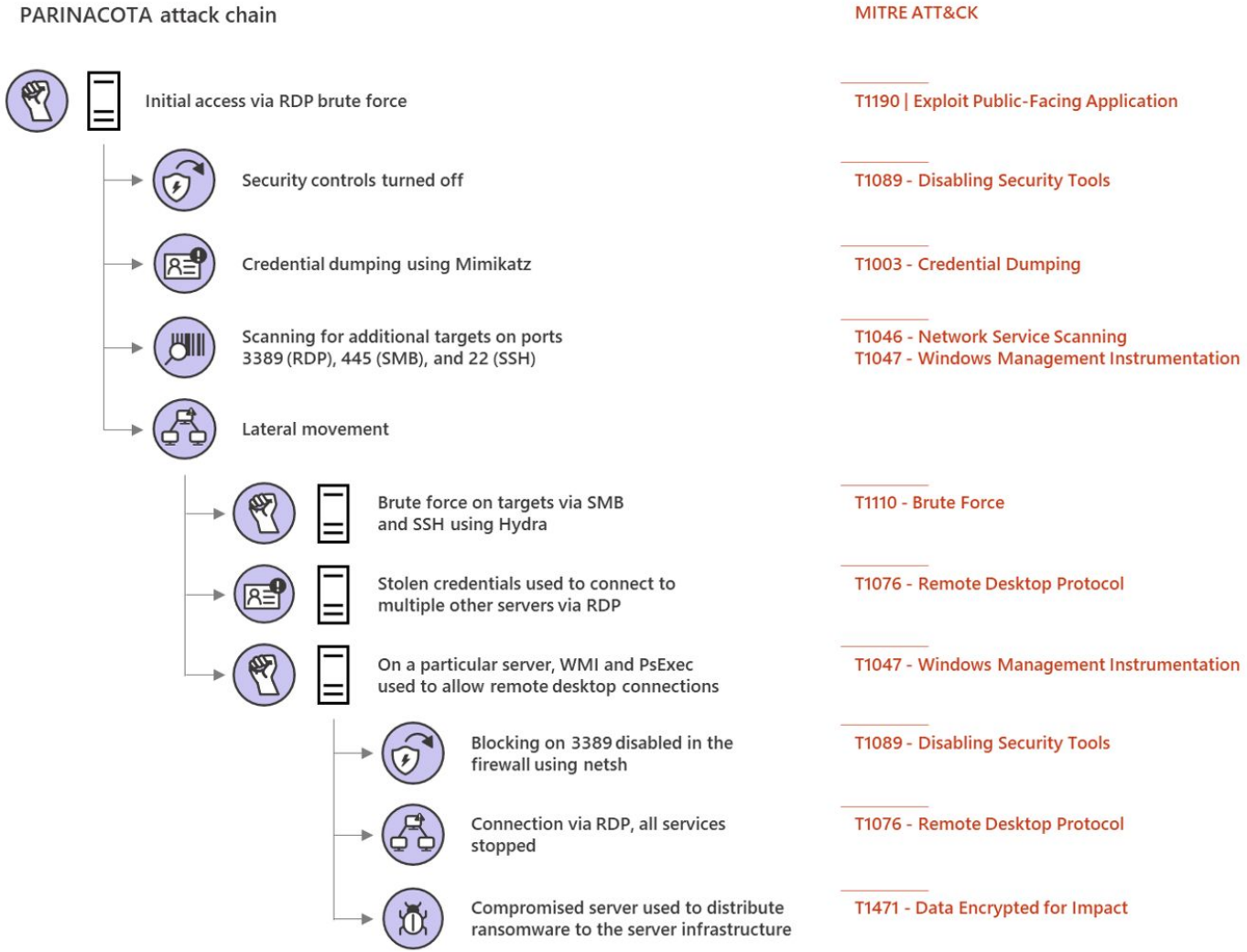
How do we model these?

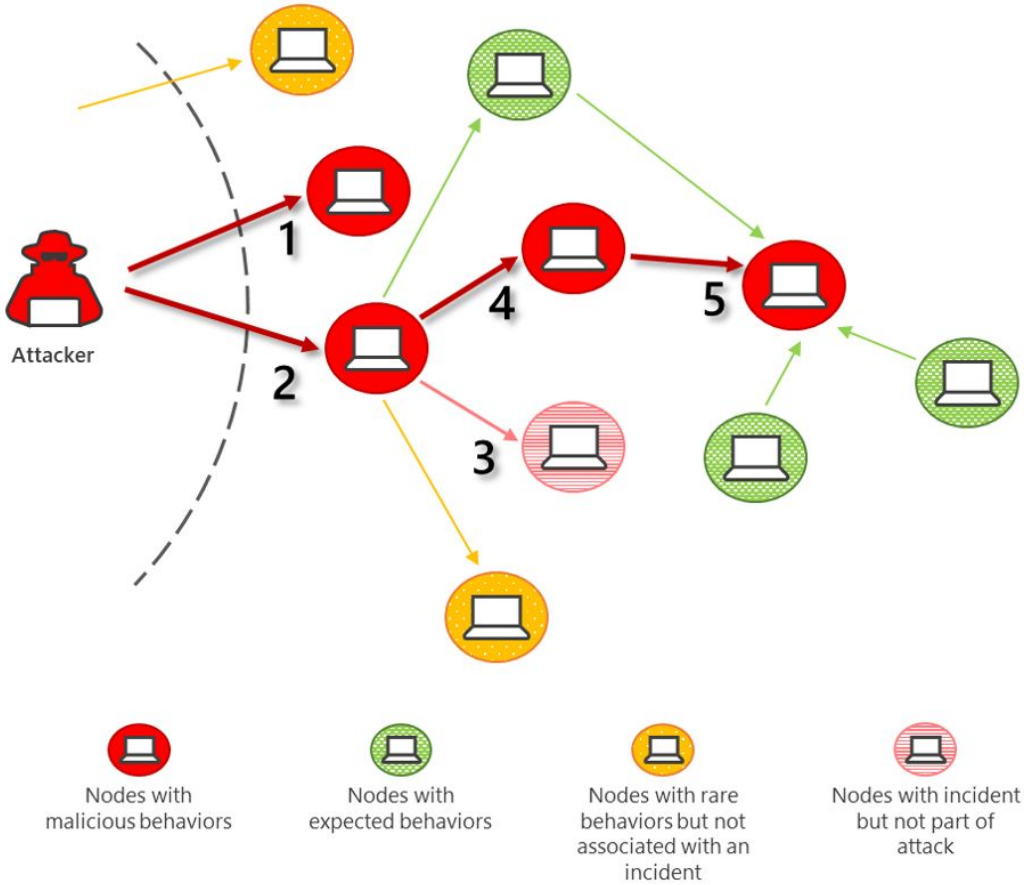


BLOODHOUND

https://neo4j.com/blog/bloodhound-how-graphs-changed-the-way-hackers-attack/


Red Team's BloodHound Map
Blue Team's BloodHound Map
Corporate needs you to find the difference between this picture and this picture
They're the same picture


PARINACOTA attack chain
MITRE ATT&CK
Initial access via RDP brute force
T1190 | Exploit Public-Facing Application
Security controls turned off
T1089 - Disabling Security Tools
Credential dumping using Mimikatz
T1003 - Credential Dumping
Scanning for additional targets on ports 3389 (RDP), 445 (SMB), and 22 (SSH)
T1046 - Network Service Scanning
T1047 - Windows Management Instrumentation
Lateral movement
Brute force on targets via SMB and SSH using Hydra
T1110 - Brute Force
Stolen credentials used to connect to multiple other servers via RDP
T1076 - Remote Desktop Protocol
On a particular server, WMI and PsExec used to allow remote desktop connections
T1047 - Windows Management Instrumentation
Blocking on 3389 disabled in the firewall using netsh
T1089 - Disabling Security Tools
Connection via RDP, all services stopped
T1076 - Remote Desktop Protocol
Compromised server used to distribute ransomware to the server infrastructure
T1471 - Data Encrypted for Impact



https://www.microsoft.com/security/blog/2020/06/10/the-science-behind-microsoft-threat-protection-attack-modeling-for-finding-and-stopping-evasive-ransomware/

What kind of tools/visualizations do we have?

What kind of tools are helpful?

What kinds of tools do other industries have?

What Kind of tools do we lack?

What if we could model / see across TIME

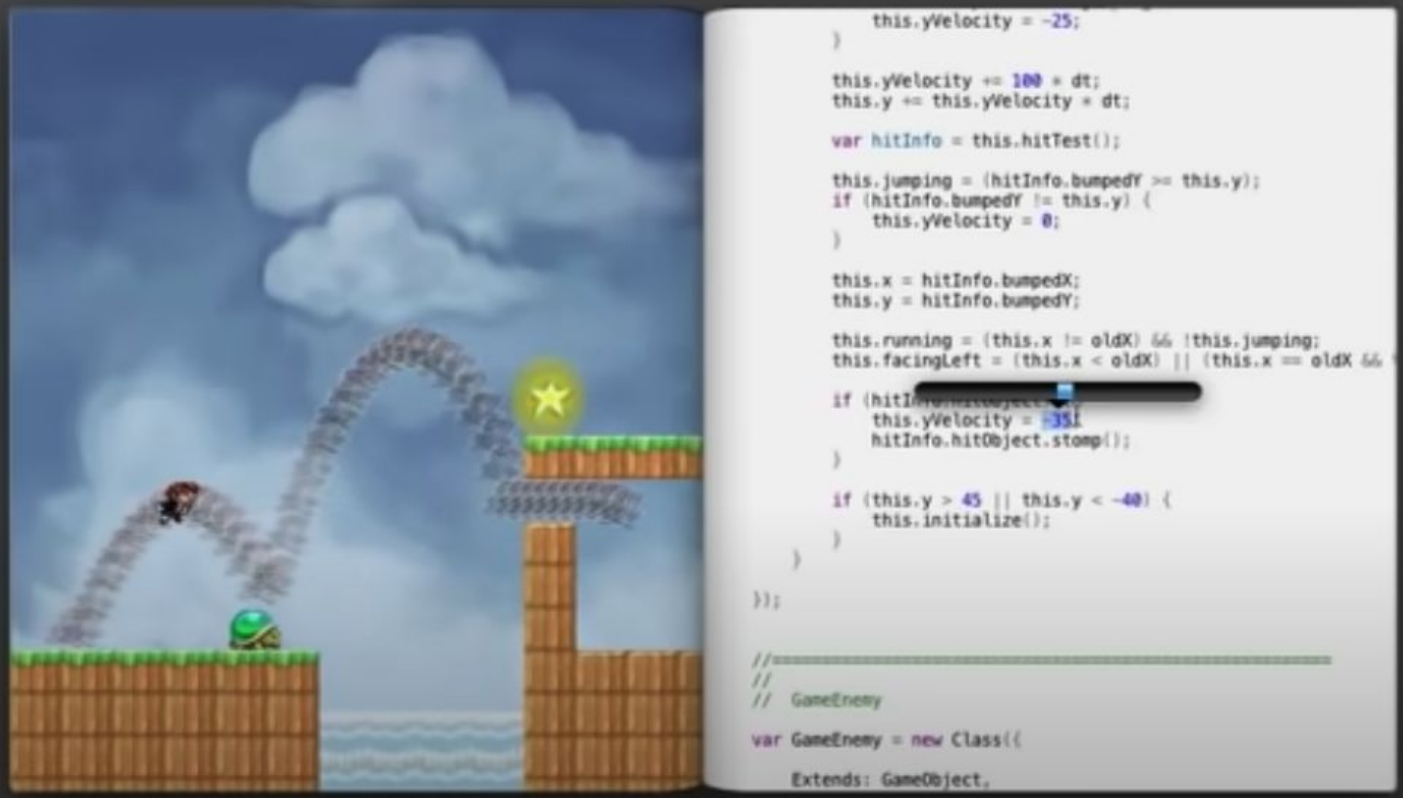
See drift

Anticipate area of new service deployments and features

Look back at the state when the incident occured?

Time Travel - Images Over Time Weather

Time Travel Debugging



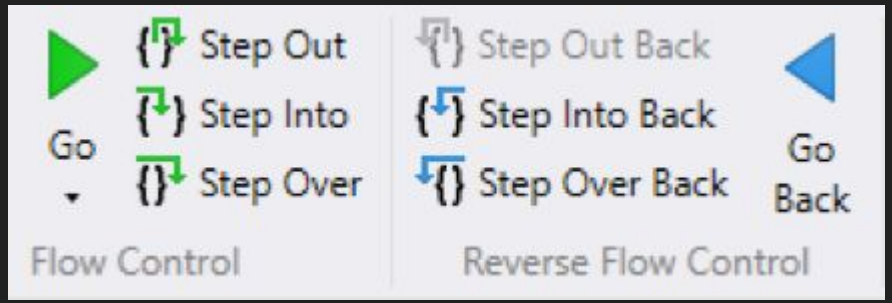
Bret Victor - Inventing on Principle

Windbg - Ghidra - Ida

Developer ⇔ Reverse Engineer

Exploit & Developers

Same View



← **Tweet**

Rob Napier
@cocoaphony

Periodic Reminder: When debugging, you must first accept that something you believe is true is not true. If everything you believed about this system were true, it would work. It doesn't, so you're wrong about something.

This is a surprisingly common stumbling block for devs.

8:10 AM · Feb 3, 2020 · Twitter Web App

RWX Detection

Detecting In-Memory Attacks: these are type ‘Private’ and do not map to a file on disk. They are therefore referred to as unbacked executable sections or floating code.

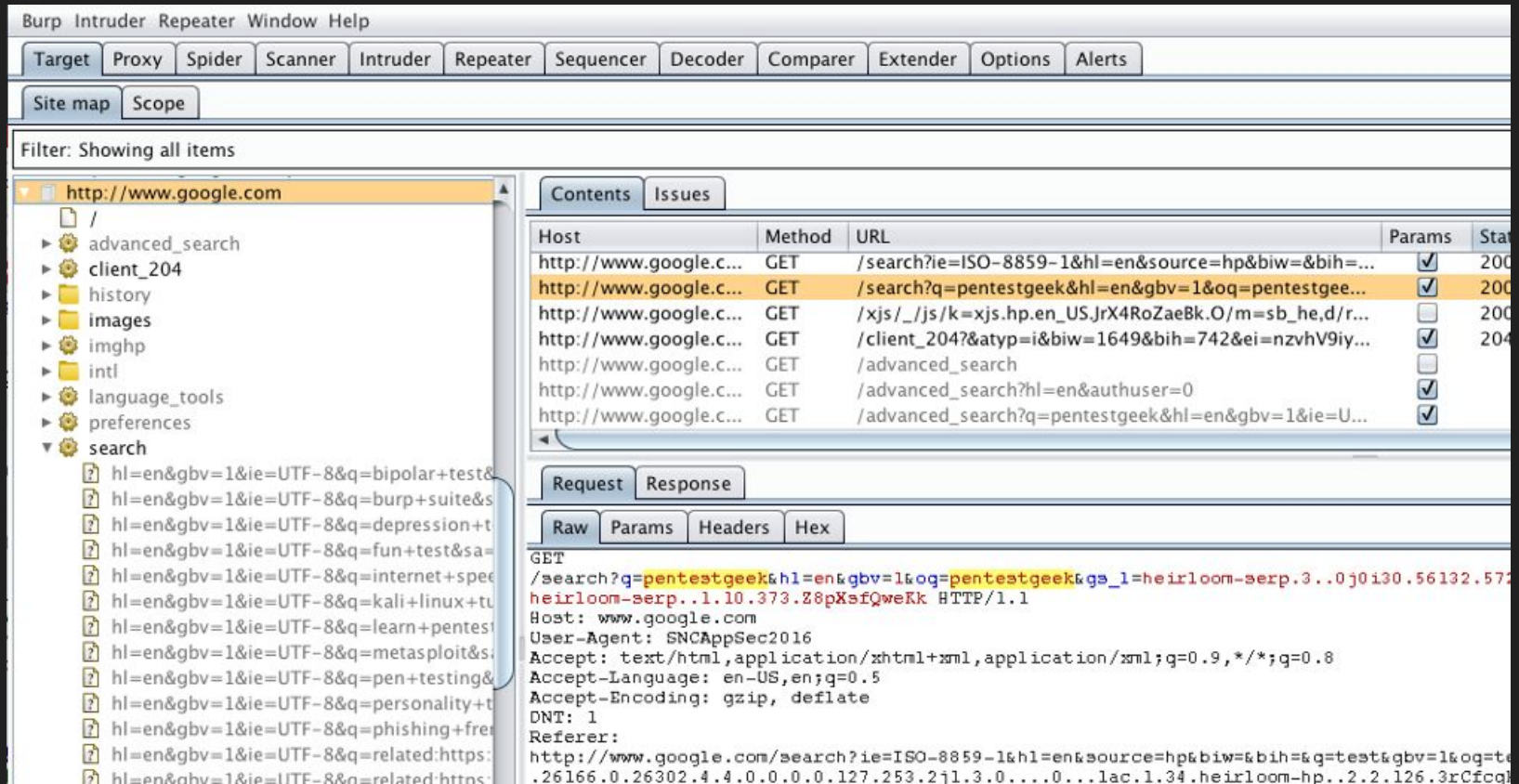
Can we find any RWX memory on disk backed by image?
Yes Yes we can

Image: Commit	7,016 kB	RX	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\9d4a21...
Image: Commit	7,384 kB	RX	C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\4ad732c...
Image: Commit	3,284 kB	RX	C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Baa2ca56b...
Image: Commit	8 kB	RWX	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll

https://www.elastic.co/security-labs/hunting-memory

The tools we use helps us make predictive and analytical and strategic decisions

Burp Suite - Web Application Testing

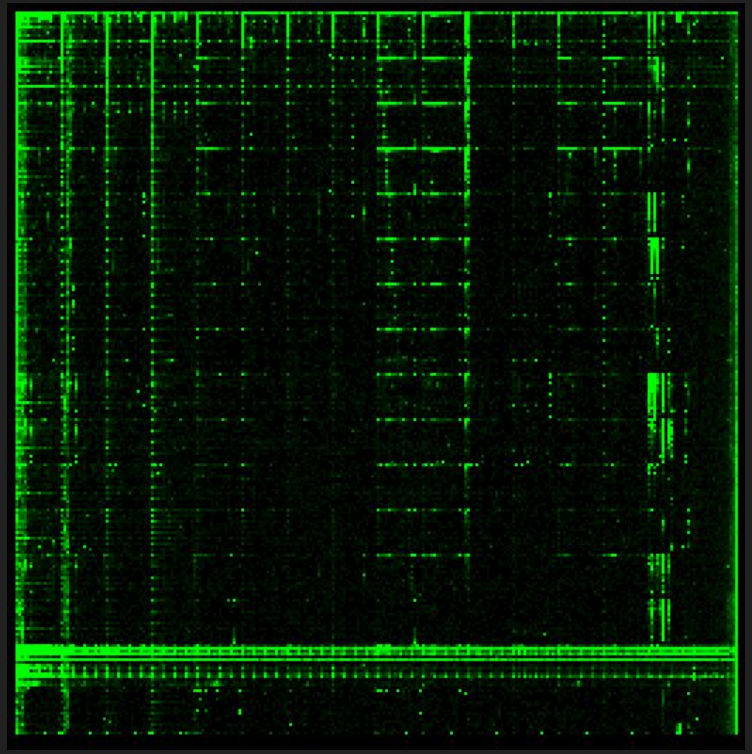


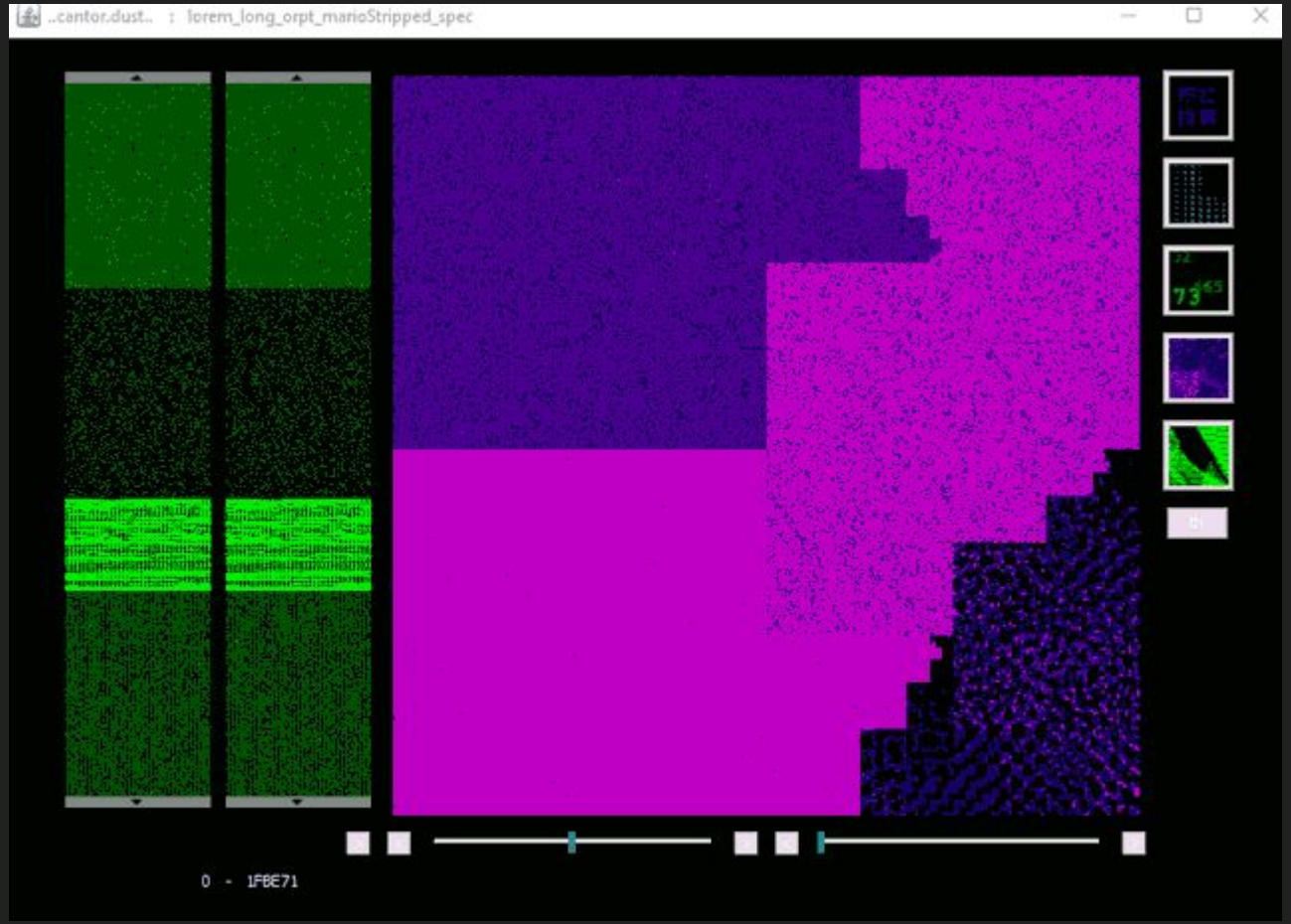
All 500 code errors
All unexpected outbound requests initiated inside

METHOD	RESPONSE	COUNT
GET	500	5000
GET	200	450

Cantor Dust - Binary Visualizations

https://inside.battelle.org/blog-details/battelle-publishes-open-source-binary-visualization-tool




..cantor.dust.. : lorem_long_orpt_marioStripped_spec
0 - 1FBE71

Think about what the defender SEES

What Might An Astronomer Teach us about Cyber Security?

Think about that for a moment, before you answer :) ?

Carmen Medina - Diversity of Thought - The Key to Innovation | Øredev 2019

from Øredev Conference

Cecilia Payne-Gaposchkin

Diverse thinking outperforms even the smartest expert

6-8 NOV 2019
Carmen Medina
Diversity of Thought - The Key to Innovation

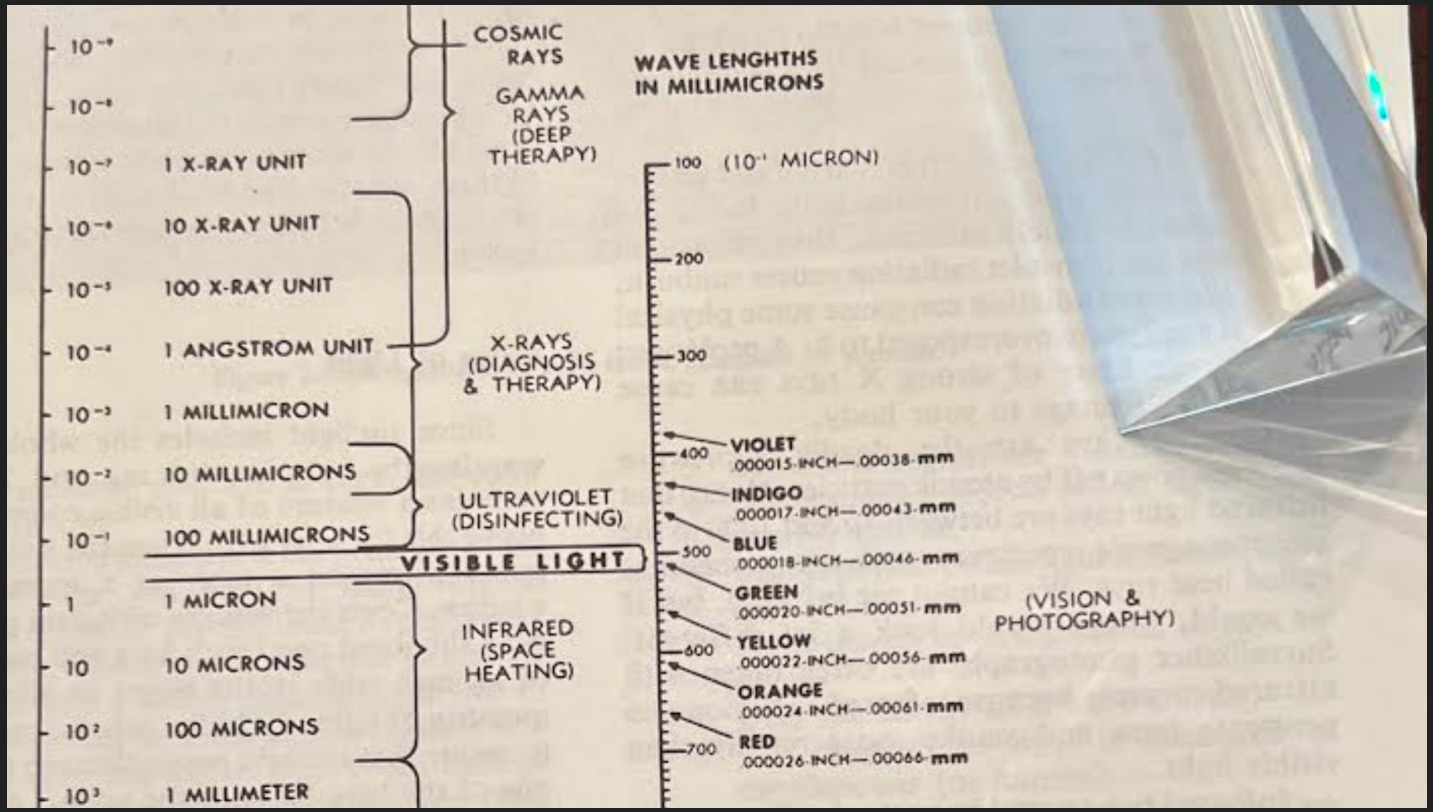
Scandinavian Developer Conference
Malmö,Sweden
oredev.org

Hackers Challenge Authority and Seek Reality

Like any great scientist

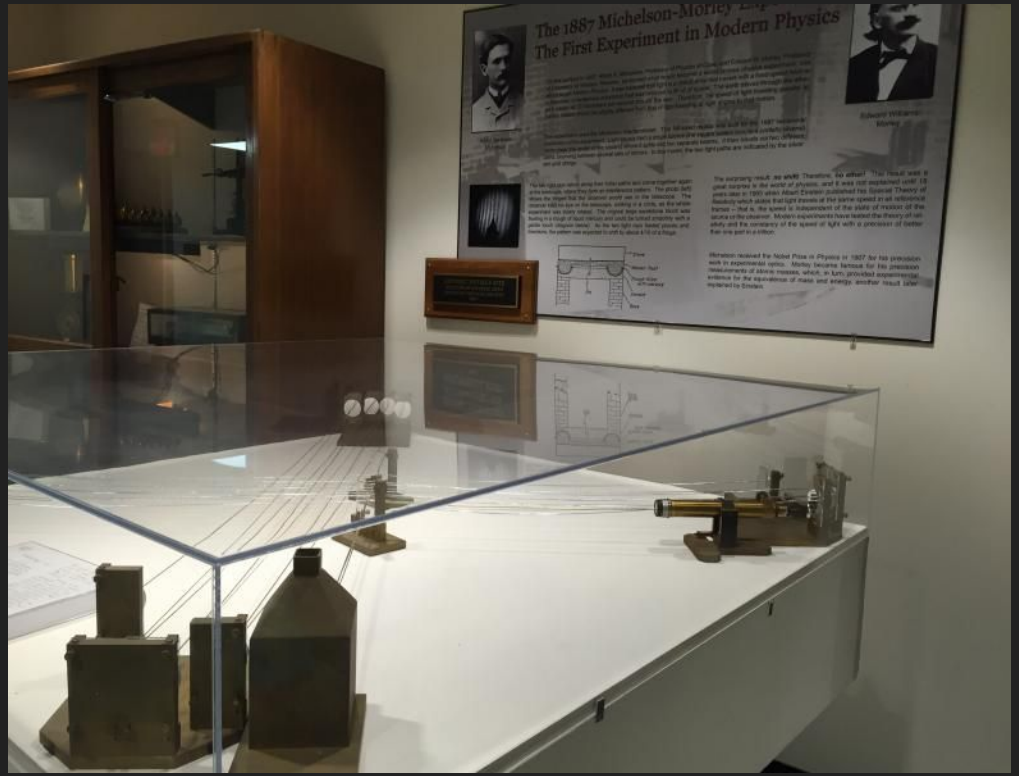
Driven by curiosity of how things really work, and to dispel myths.

Let there be light - Michelson & Morley



https://www.youtube.com/watch?v=7qJoRNseyLQ

People ignored / dismissed the evidence



Combine 2 or More Different Ideas

Telescopes and Photography

Couple Cyber with ???? Cooking, Recipes, Drones, Zillow,

I don’t know :)

What takes time today?

What is Expensive Today?

Tedious?

Reduce that .

Applied To Cyber - Example

Problem - Malicious Domain Detected in Log?

Find:

1. Which Host Performed the lookup (DNS from domain controller, host or proxy?)
2. Which process on the host performed the lookup? (Browser, svchost? User-agent spoofed?)
3. Which OTHER hosts and processes performed the same lookup
4. Repeat

What do you need to answer that?

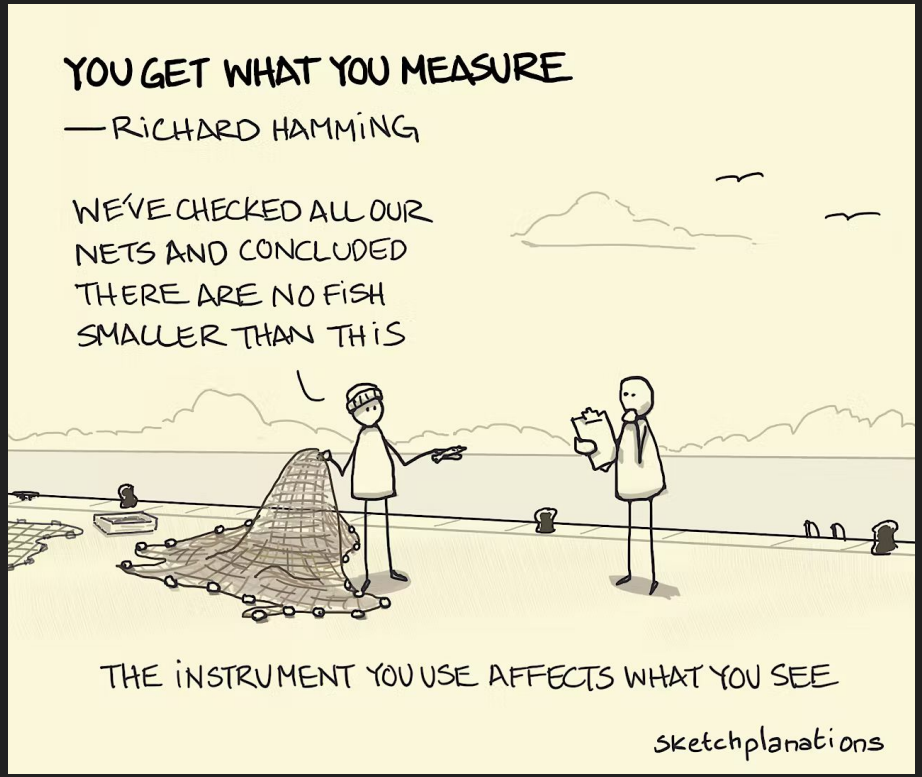
The speed with which you ask and answer questions may affect outcomes

Asking and answering faster than an adversary might be a goal.

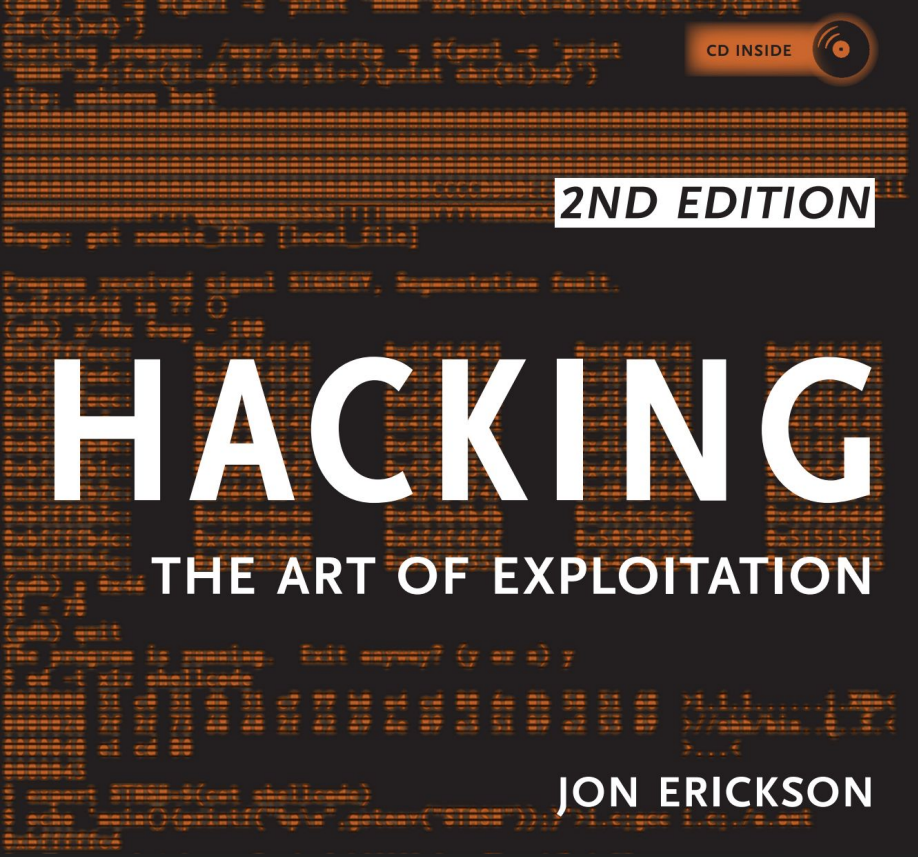
Closing Thoughts

Our Tools, Our Maps, Our Models Matter

“How do you know that? How could anyone know that?



The Instrument You Use Affects What You See”
- Richard Hamming



This gives hackers their edge, allowing them to solve problems in ways unimaginable for those confined to conventional thinking and methodologies

“Our Ability to know is a function of our tools for knowing” - Carmen Medina

3 Big Ideas

1. Hackers get their edge knowing how things work behind the scenes
2. Defense and Offense taking the same perspectives (Tools)
3. Combining Things and Learning From Other Domains

Examples / Case Studies / References

Go Build :) Have fun! Thank you