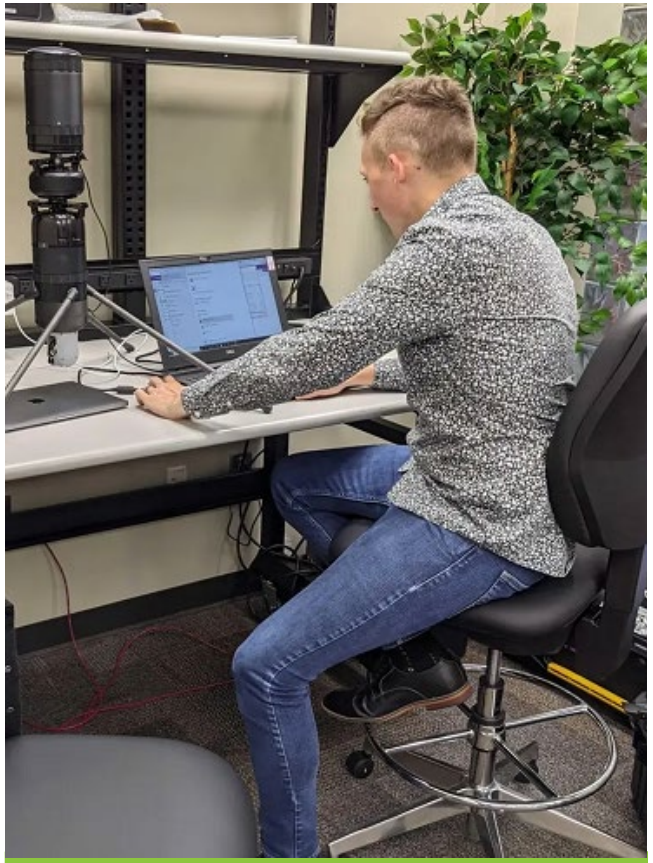
DARK WOLF
SOLUTIONS

Penetration Testing in the Air Force: How the service hacks to move faster

Introduction and Agenda

Hey, I'm Tyler – pentest lead for Dark Wolf and prior 1N4A SSgt. Let's chat about a few things!

- Authorization, Factories and AOs - oh my!
- Where offensive security fits in
- What hacking government systems looks like - yes, with pictures!
- How can it grow from here?



Tyler Fordham

Penetration Testing Team Lead, Dark Wolf Solutions

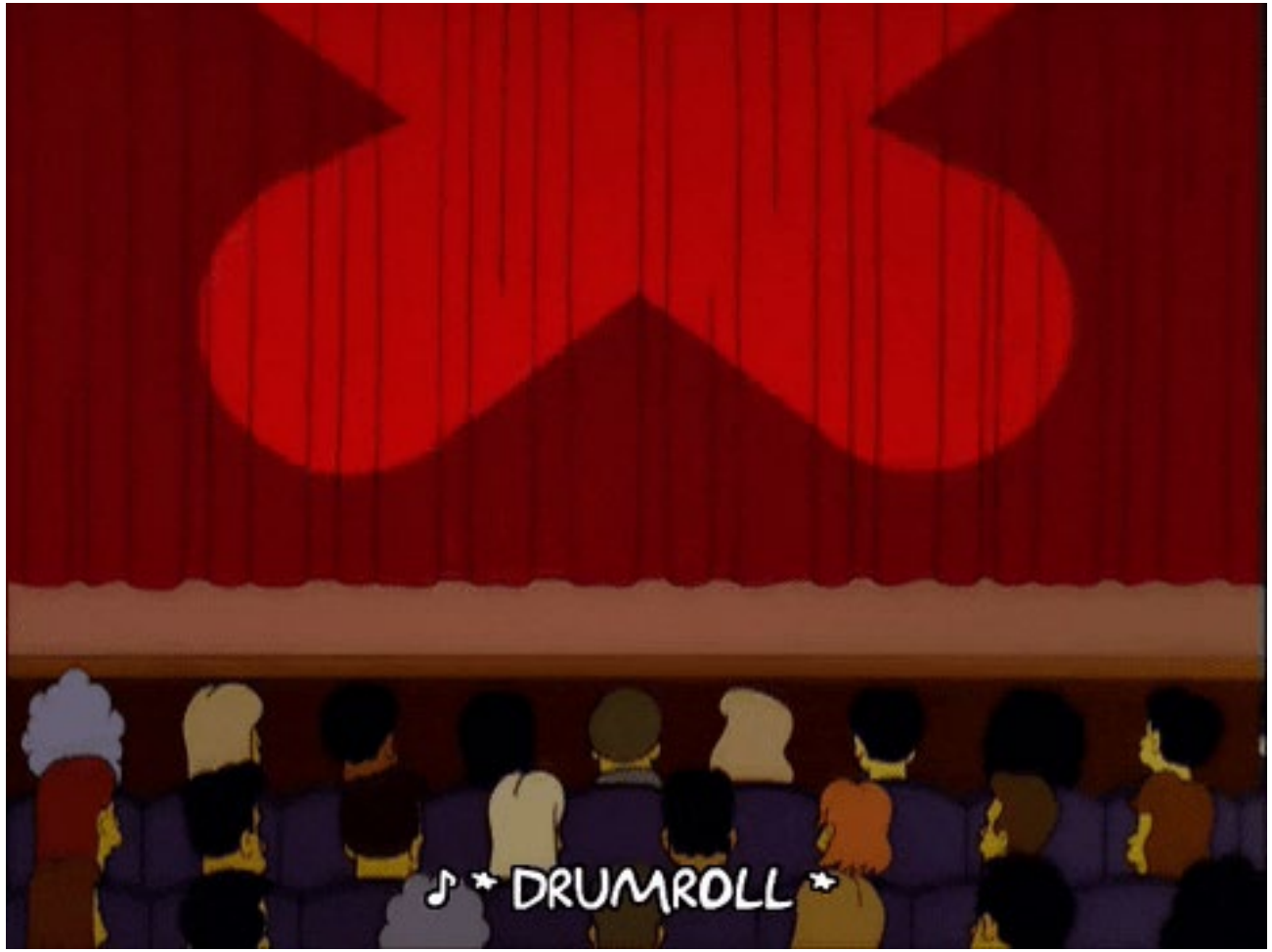
Before I forget: What's pentesting?

DARK WOLF SOLUTIONS

- "An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system."
- Can apply to everything from networks and applications to avionic subsystems and building alarm networks
- At its core, a proactive tool for finding security holes in a system before a bad actor does
- Allows admins, devs and stakeholders alike to find and prioritize security flaws that could damage an organization

But how does this apply to the Air Force?!

SETTING THE STAGE…



Authorization in the DoD: A Brief History For A Long Process

- DIACAP in 2002, then RMF in 2010
- In essence, both standards provide(d) functional cybersecurity controls for assessing a system
- System maturity is defined procedurally by a cadre of assessors with varying levels of technical background
- Primary issues:
  - Speed - an Authority To Operate (ATO) can take years!
  - Lack of consistent technical validation

Software Factories: A New Era

DARK WOLF SOLUTIONS

- Commercial industry has been pushing the DevOps movement since 2008
- Lauren Knausenberger, Chief Transformation Officer at the time, and others take this example and get the political capital to establish Kessel Run
- It's a wild success and the ecosystem explodes nearly overnight
- Over a dozen software factories in USAF alone stood up from 2018 to now

Bringing the AOs Around

- Generally, the prior two slides have inherently involved some conflict with each other
- Many AOs "grew up" with waterfall development, standard authorization and good old DoD "hurry up and wait"
- Trailblazers like Lauren K. and Danny Holtzman broke the mold and helped popularize Fast Track and Continuous ATO
- With precedents set, it's all about getting buy in for faster timelines and technical validation over the traditional model

DARK WOLF SOLUTIONS

Median Audience Member:

"*Okay, but let's talk about penetration testing now!*"

WHERE DOES PENTESTING FIT IN?

DARK WOLF SOLUTIONS

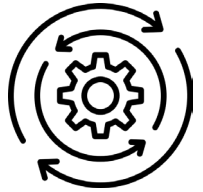
- Factories, authorization and AOs - I promised these were a common thread!
- Penetration testing works as a force multiplier for effectively every software and capability standard used in the USAF
- Alongside the discussed security benefits, the focused security analysis that hackers can provide you <u>actually speeds up</u> the process of getting tools fielded for the warfighter

Traditional ATO

AOs can leverage penetration testing as an additional security check to validate, strengthen and expedite traditional authorization packages.

Fast Track ATO

A penetration test, alongside relevant POA&Ms based on results, can be used in a Fast Track ATO to drastically reduce paperwork and necessary controls.



Continuous ATO

Perpetual penetration testing and/or red teaming as part of a well-oiled DevSecOps pipeline can allow for continuous delivery of authorized software in the Continuous ATO model.

OKAY, BUT HOW IS IT DONE?

- Glad you asked! There are two main models
  - One-off penetration testing: bringing a vendor in to test your capability as a third party and going your separate ways
  - In-house red teams: an organization brings on offensive security specialists full time to test everything in the boundary
- In either model, the amount of information shared changes the type of test drastically; black, grey and white box testing

YEAH, BUT WHO'S DOING THE HACKING?

DARK WOLF SOLUTIONS

- By and large across the service, this is primarily contractors right now
  - Larger entities - often existing vehicles and manpower, niche skill sets are not always around
  - Small firms - often strong talent, not always easy to get to
- In house service teams - 47th, 177th (ANG), 346th, AFRL
  - Generally mirror the more formal DoD assessor model
- Crowdsource model - "Hack the AF" run by Defense Digital Service, leverages platforms like Bugcrowd, HackerOne and Synack

Quantifying the Value

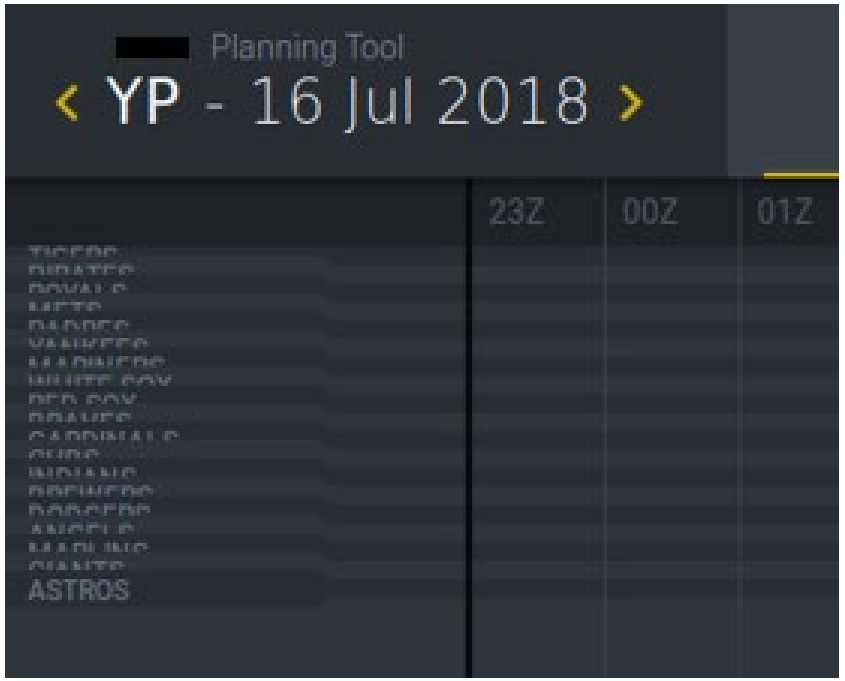
- Commercial regulation has asked for pentesting for a long time - now a common factor of cyber insurance
- Published zero-days, incidence of cyber crime and major vulnerabilities in major vendor products all picking up drastically, particularly in post-COVID era
- Applicable to federal problems; nearly 50% of APTs use off-the-shelf standard commercial pentesting tools
- 80% of all successful database breaches in 2019 came from zero-days
  - Sorry, but ACAS scanning and filled-out SCTMs **won't** find these!

LET'S SEE SOME RESULTS

- So, you've now got all the relevant context. Let's explore what all of this looks like in practice.

2018: HACKING THE DAWN OF FACTORIES

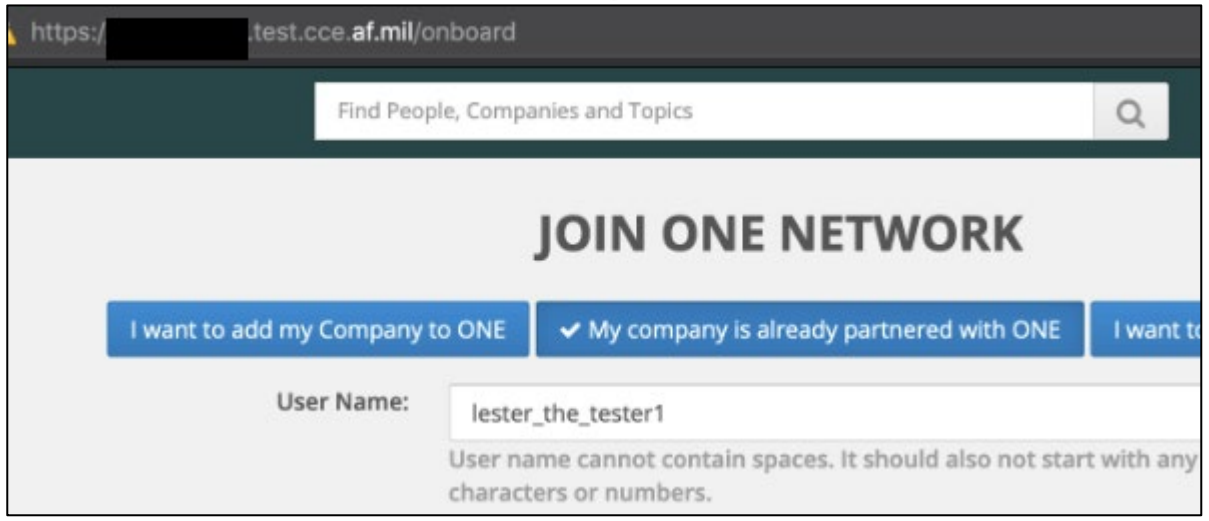
- Initial applications coming out of the new software factory world were some of the first targets of the Air Force's new tool
- In theory, you could validate an ATO with conditions through pentesting, and find things for devs to fix, right?!
- ..in fact, yes. That *is* exactly what happened.
- Early pipelines didn't prevent deserialization and unauthorized backend modification!

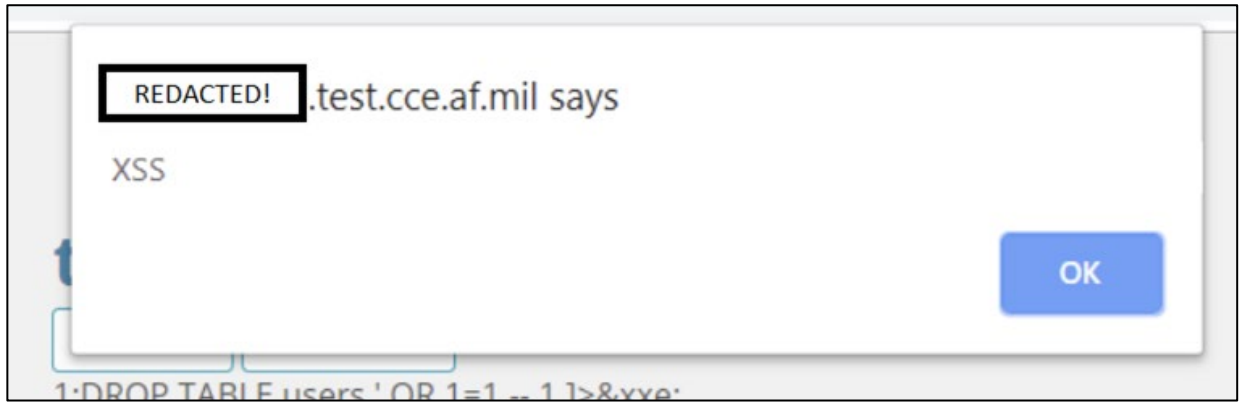


2018 - somehow now an ancient era in terms of DoD software factories.

2019: Squeezing New CloudOne Apps

- Many old applications porting to CloudOne were Fast Track ATO candidates for pentesting
- In general, these were sadly ***full*** of holes
- In one such pictured logistics app, *an entire vulnerable social media platform* was accidentally baked into the application and ready for anyone to find and exploit!
- Web applications being easy targets is a continuing trend to this day





You generally don't want a data-injectable Facebook clone hidden in your COTS logistics software…

2020: DJANGO *SIGH* UNCHAINED

DARK WOLF SOLUTIONS

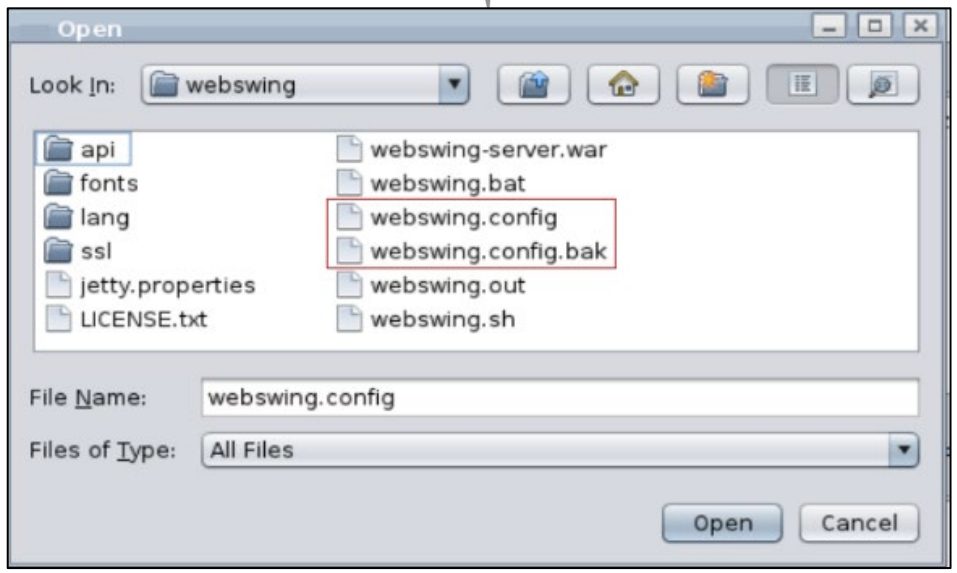
- Major cloud deployment platform was in need of testing in early iterations
- With enough surgical headbashing, the main server eventually spits some confused error codes
- ..however, it's a big problem when those error codes give you credentials for the entire database!
- An example of an issue so big, we didn't test further before reporting

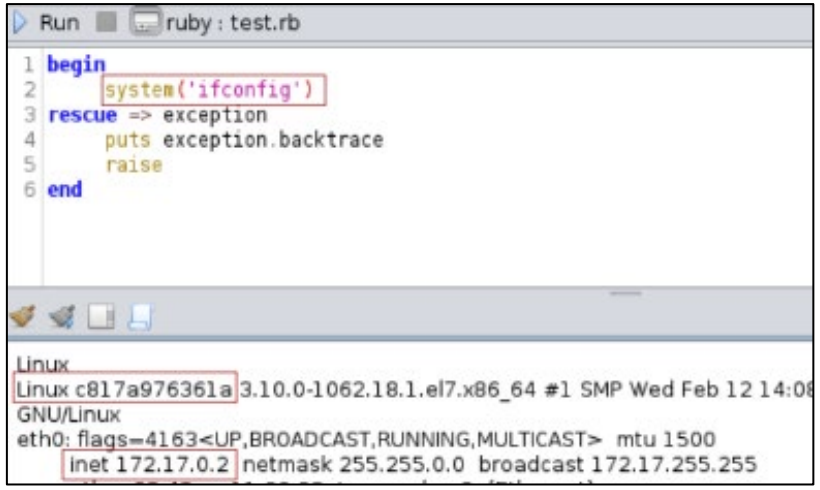
Not the kind of stuff Airman Snuffy should be finding

2021: Dev Tools -> System Admin

DARK WOLF SOLUTIONS

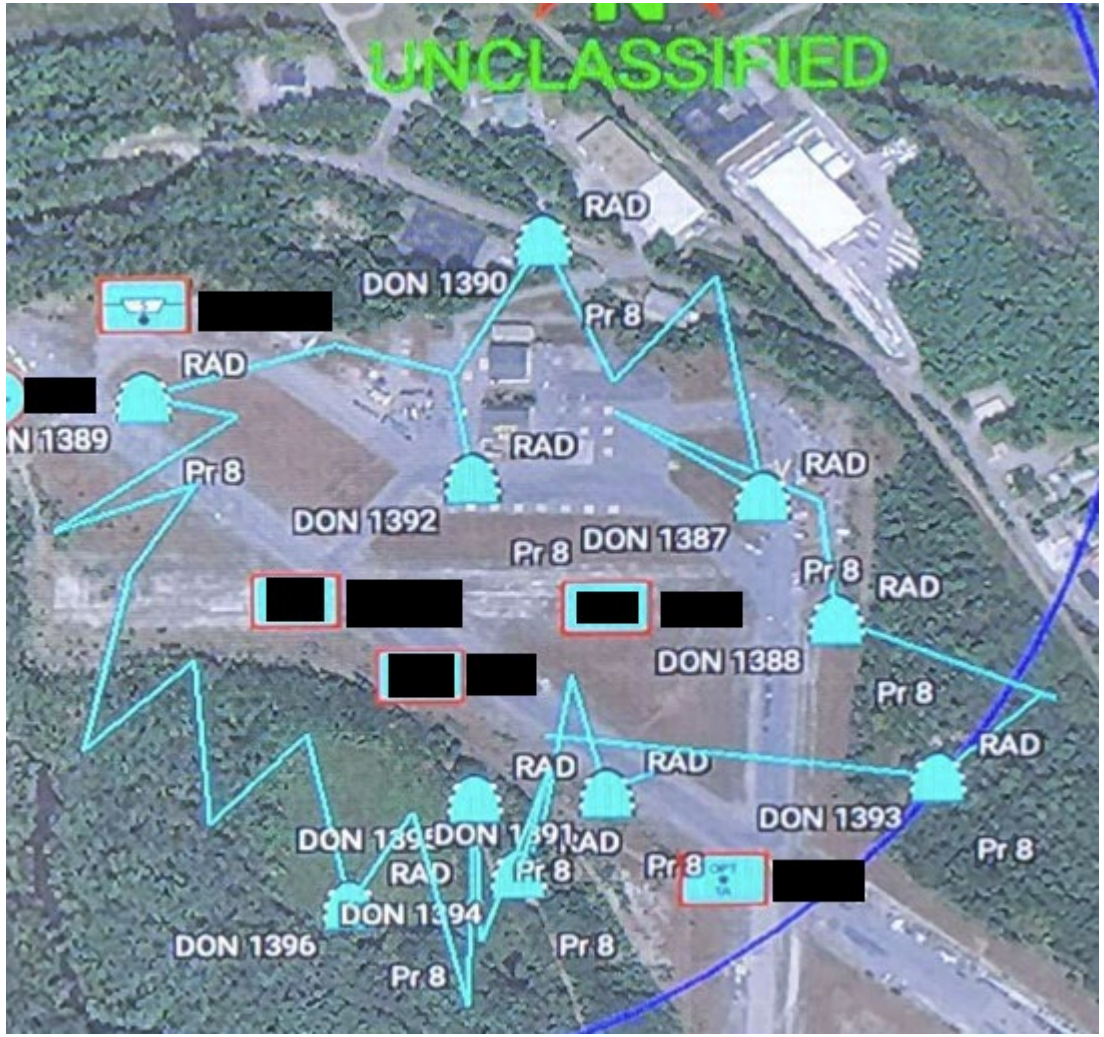
- Software factories deploy a wide range of developer tools into their cloud deployments
- Unfortunately, not all of these are well configured or secured
- By leaving the frontend of this popular code scanner unsecured, testers got in, crafted a custom configuration file, made their own admin user and gained direct code execution on the underlying host





2022: Making sense of sensors

- Organization with an array of sensors, cameras and operations capabilities
- Testers were able to take over the entire operational network with two hours of outdoor hardware access
- Pictured: Creative flight paths to demonstrate newly gained access
- Significant hardware, software and physical security improvements identified

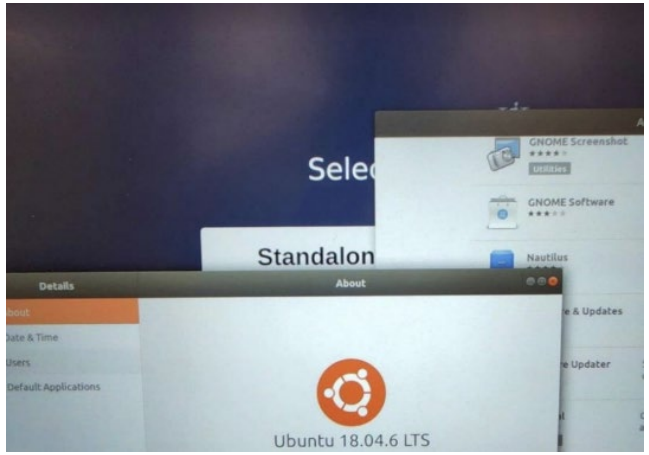


WHEN UAS ARE FUBAR

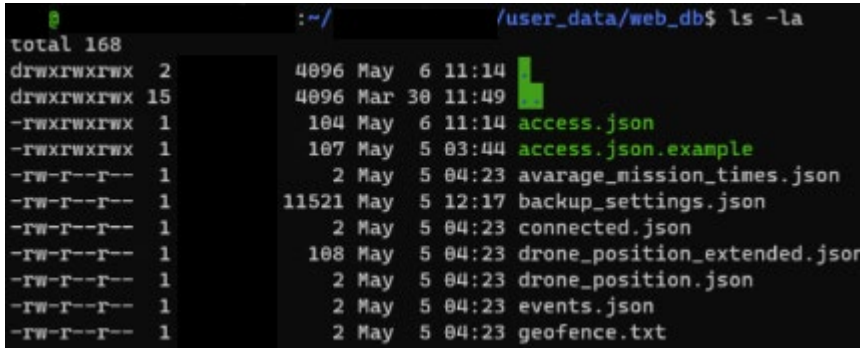
DARK WOLF SOLUTIONS

- The USAF leverages pentesters in the Blue sUAS program to assess commercial drones for DoD use
- Birds, controllers and payloads were sent to our team to test like the enemy would
- In the example below, pentesters went from basic controller access to taking over the vendor's entire online development repository

Note: generic drones pictured!



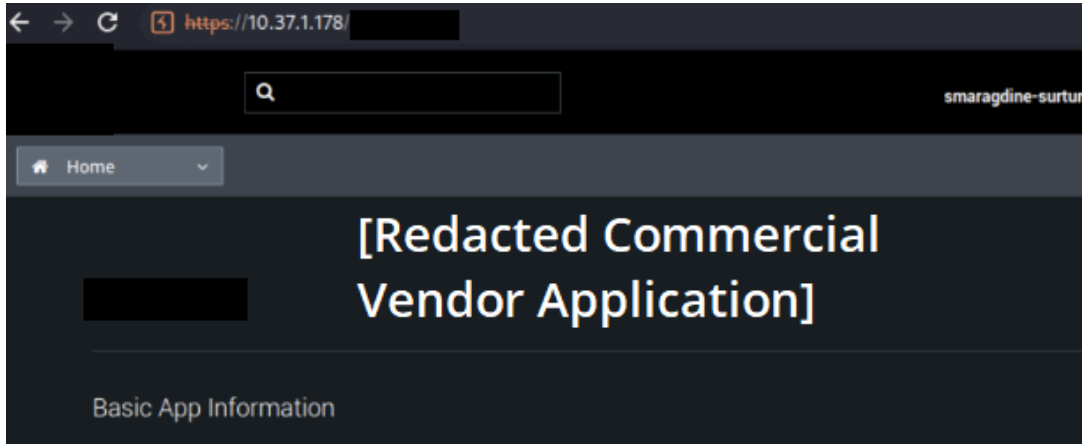
Kiosk fully bypassed



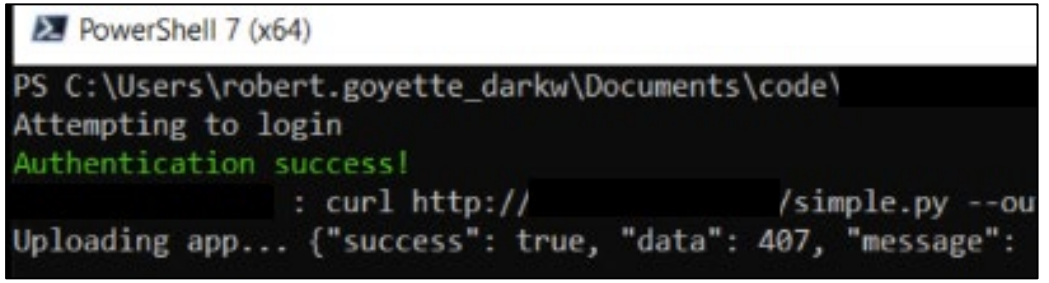
..and there's the entire database

COMMERCIAL APPS ARE AT RISK TOO!

- Many USAF factories and other orgs are bringing in commercial industry tools to supplement or put through their pipeline - these tools must be less risky, right?
- If only; USAF penetration testing regularly reveals unique, CVE-level vulnerabilities in the commercial applications that supplement the enterprise too
- In this example, our team went from a basic user to complete code execution on a well known, commercial vendor web application



Nice commercial app you've got there



It would be a shame if the backend database was hacked

TYING IT ALL TOGETHER

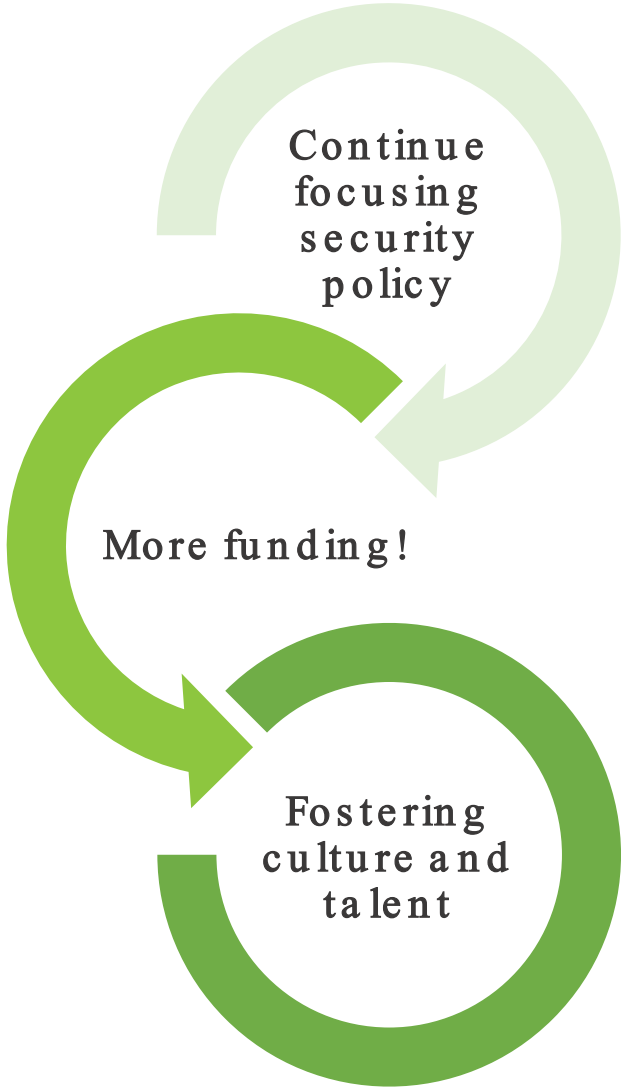
DARK WOLF SOLUTIONS

- In early 2021, we gathered statistics on unclassified penetration tests that our team conducted on a single contract throughout 2020
- Over the course of just 30 tests, across a wide array of system varieties, our team found 168 total reported vulnerabilities
- Applications, hardware, networks, pipelines - each had clear issues an adversary could abuse
- Scary thought: how many AFNet applications and networks that you use daily are vulnerable?

Dark Wolf 2020 Findings Tracker - Overall

Findings by type:	
Network	17
Web App	83
Mobile App	9
Host-based	15
Cloud-based	19
Container Orchestration	10
Policy-based	2
Physical Security	1
UAS	11
Other	1
Findings by Severity:	
High	14
Medium	76
Low	67
Note	11

How do we get to more hacking?



So, this is a capability with a proven value for the service - what can the USAF do to see more?

Baking the explicit need for penetration testing into more policy, plans of actions and milestones and authorizations is where this starts. Testing warfighter supporting IT systems must become the standard!

Policy can only go so far when funding isn't there. From the unit level all the way up to huge DoD contracts, more cybersecurity funding should be earmarked for penetration testing.

Security assessments don't have to be scary, and fostering a culture of pentests being a positive thing is how the USAF can kill that stigma. This brings an added benefit of encouraging more people in the space to learn these skills and be the service's testers of tomorrow!

CLOSING THOUGHTS

DARK WOLF SOLUTIONS

- It's incredibly cool to hack and help fix the same systems that plagued you as an Airman

- This has been a special journey for me coming initially from the blue team and intel worlds

- The government at large needs more people interested in offensive security
  - Penetration testing
  - Reverse engineering
  - Exploit development

- Ideas:
  - Standing up Kessel Run-like organizations focused on offensive cyber to grow talent in the service
  - Perpetual bug bounties on Air Force systems for service members

Questions and Answers

THANK YOU!

DARK WOLF
SOLUTIONS

Special Credit:
My awesome penetration testing team at Dark Wolf Solutions