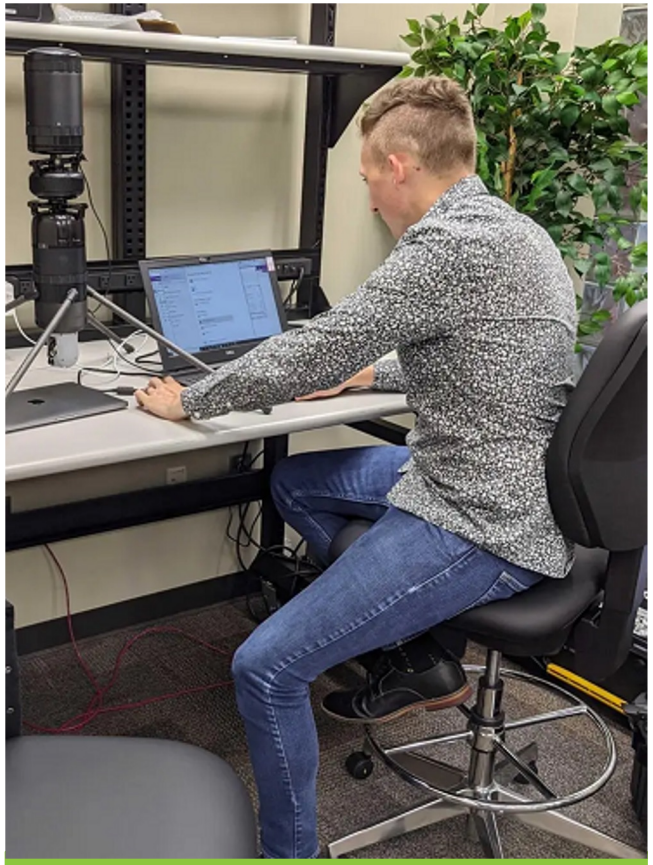
DARK WOLF
SOLUTIONS

Pentesting the Space Force: Modern Targets in the DoD's New Branch

Introduction to the guy talking

- Hey there, I'm Tyler Fordham
- Director at Dark Wolf Solutions
- Built Dark Wolf's pentesting team
- Prior Air Force 1N4A cyber intel analyst
- Have *hopefully* been involved in enough offensive security work to be qualified to be up here talking



Tyler Fordham

Director of Cybersecurity, Dark Wolf Solutions

Goals of the Talk

- Offer insights on testing space-adjacent government systems to both noobs and pros
- Highlight the importance of hacking these systems ourselves before the **bad guys** do
- Demystify targeting USSF cyber - not every system is a complicated satellite; there's a lot of modern infrastructure!
- Show you how talented the people on my team are with some fun examples

DISCLAIMER: This deck contains MY opinions, not necessarily the USSF's!

BUT FIRST, LET'S CATCH UP ON SPACE FORCE

- Popped into existence in 2019, taking over much of what was done by the Air Force's *Space Command*

- Core focuses:
  - Satellite operations
  - Space traffic control
  - Space domain awareness

- In theory, streamlining everything space under one roof will probably improve our efforts in that domain

- Still in its relative infancy with major organizational changes still happening commonly

Pictured: Fictional funny Space Force man

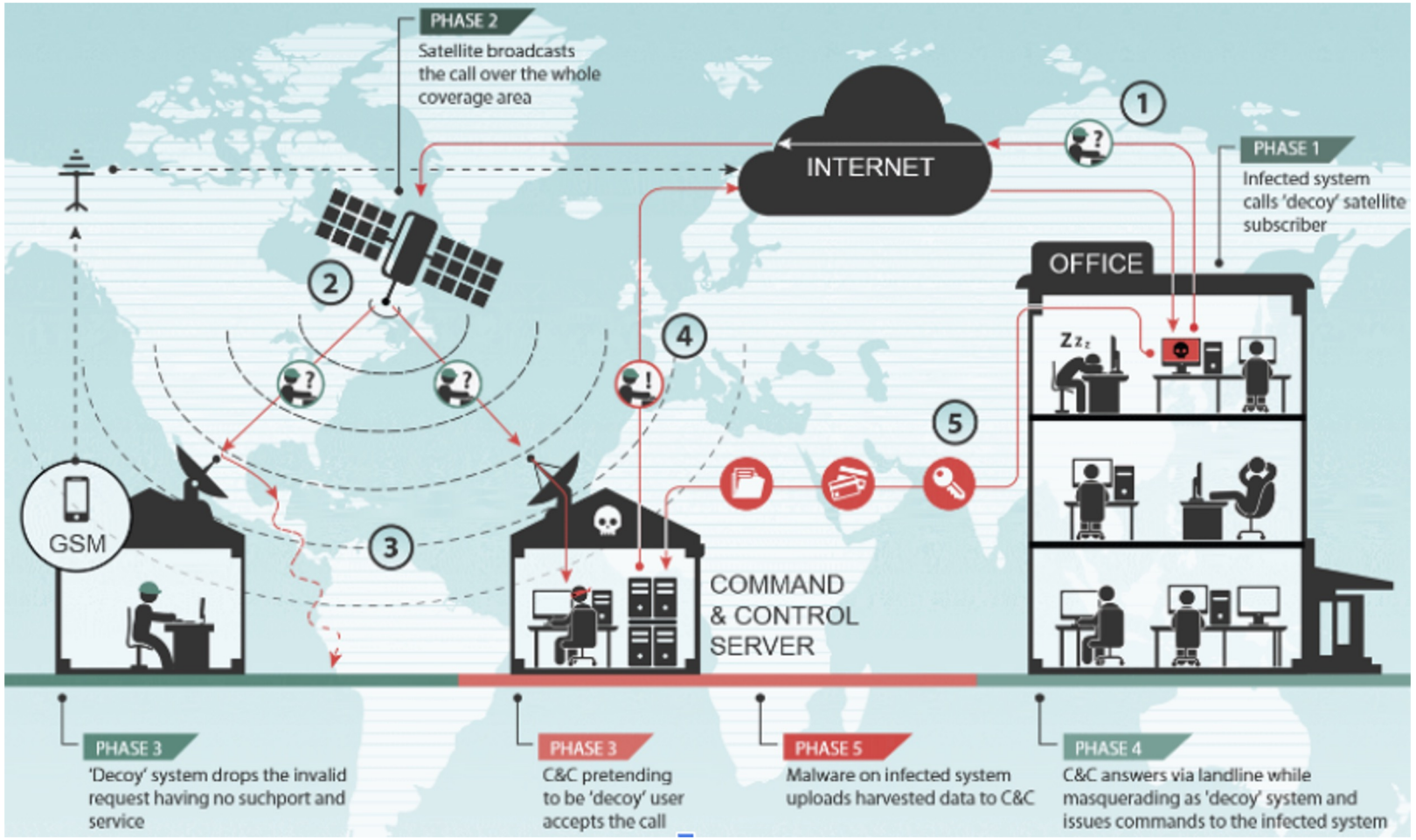
Space Force: Domain Considerations

DARK WOLF SOLUTIONS

- Major current and increasingly future area of geopolitical control for the world's big players
- Weaponization of equipment in orbit and attacks against those represent an increasingly complicated game of space chess
- Denial of space communications can cripple a nation
  - Not the kind of thing you'd want to kick off a war
  - Space Force aims to get a better grip on this problem

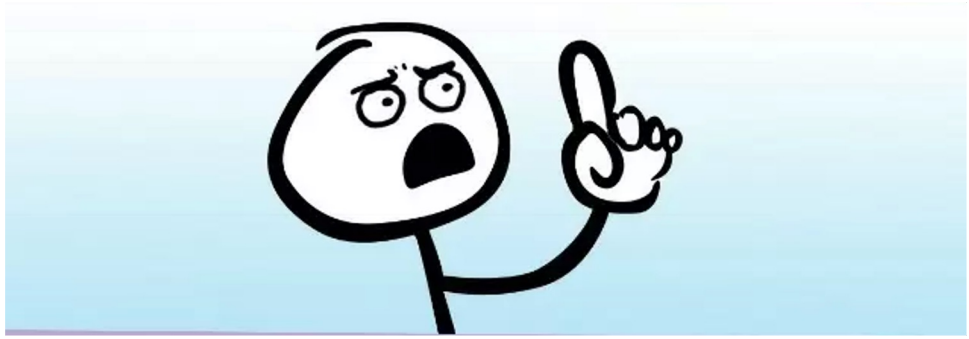
Aforementioned Bad Guys

- Russia and China in particular are major aggressors
- Nonstop targeting of (aero)space biz
  - Commercial, govt., you name it
  - More APTs than can fit on this slide
- Turla Group
  - Campaign pictured here!
- NASA networks hit in SolarWinds attack



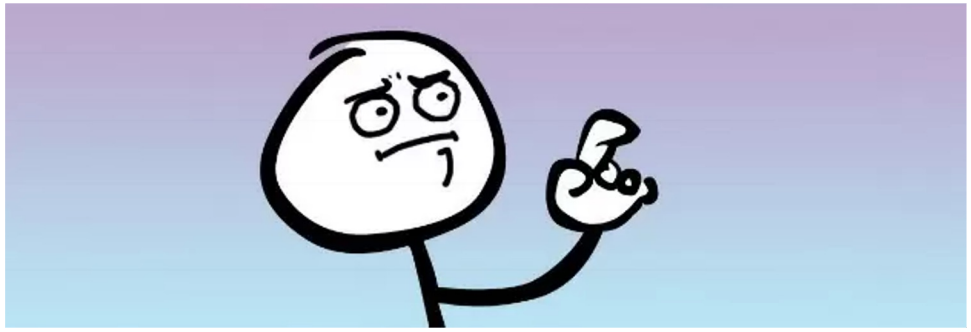
THE ARGUMENT FOR HACKING STUFF FIRST

- Penetration testing, red teaming, vulnerability research… they just work!
  - All of these cybersecurity disciplines give system owners ways to find easy and hard issues alike
- Finding and fixing things before those adversaries safeguards the economy, nation and… maybe world?
- Increasingly a government mandated requirement
  - 2023 White House Cybersecurity Strategy
- Make a note to Google: *USSF Space Enterprise Test Vision*



BUT

It’s not just satellites and cool equipment we need to test!



USSF's support system: Rife with modern tech you know and love

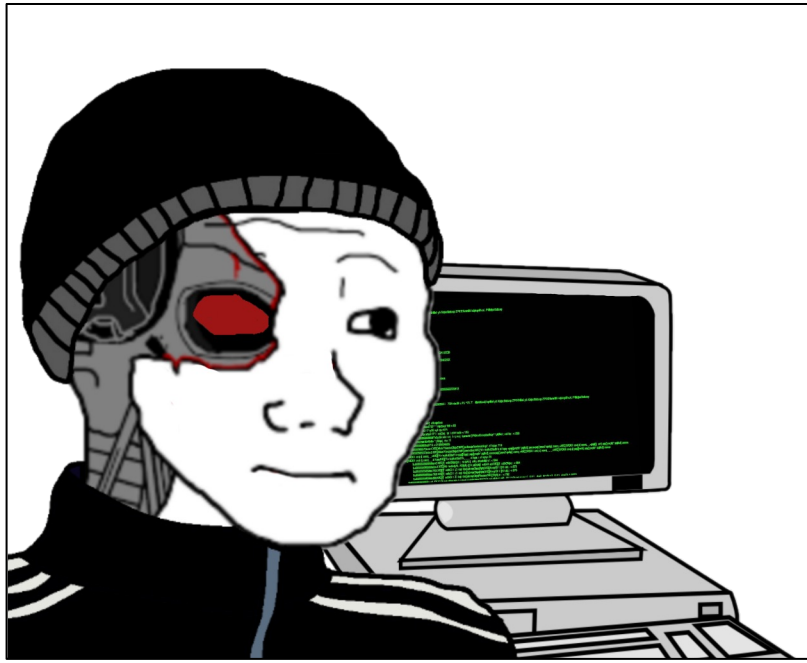
DARK WOLF SOLUTIONS

- Standard hardware, software and infrastructure make up the backbone of orgs that build cool space systems
- Recent USG/DoD trends
  - Move to modern software development; "software factories"
  - Cloud-based architecture for operations and development
- Big focus on upgrading old systems with new tech; mystique of ancient software fading

**gasp* a modern looking dashboard!*

So isn't this just standard pentesting?

- Kind of!
- Make no mistake; there are still a LOT of spicy and complicated space systems
  - See annual Hack-a-Sat CTF!
  - Recent results from DEF CON and more
- However, more "standard" modern systems in space domain opens up the door for your more traditional testing
  - Many young orgs need even simple testing
  - Ignoring modern software supply chain is BAD



DARK WOLF SOLUTIONS

lofi

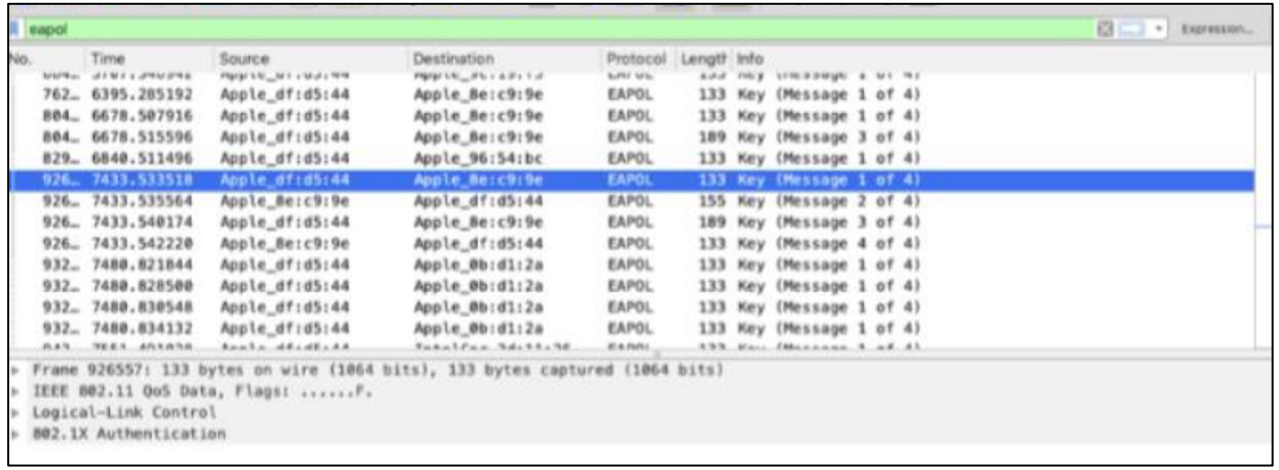
Case Studies

to hack/learn to

Boots on the Ground with the Devs

- Many early players in DoD software development ran in a startup-like fashion
  - A great thing in many ways, to be fair!
  - Young orgs benefit from being shown security pitfalls early

WPA2 you say…?

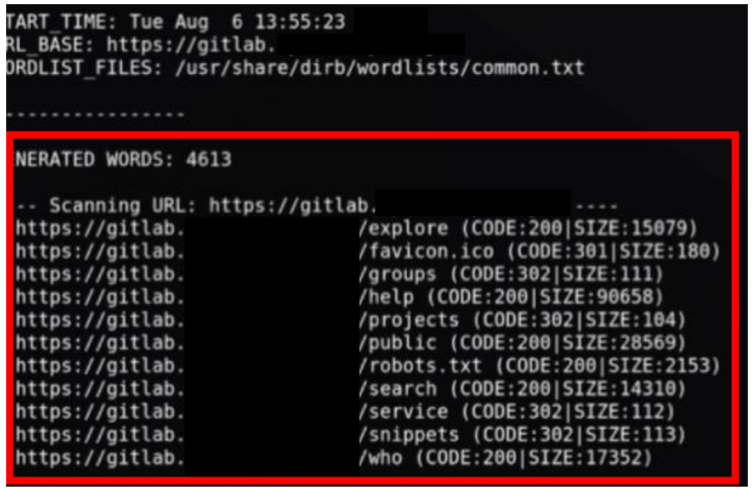


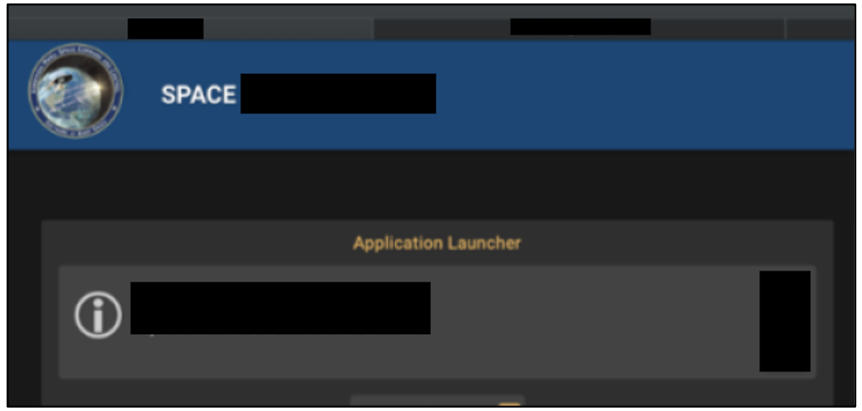
Capturing handshakes; good for conferences, bad for your network

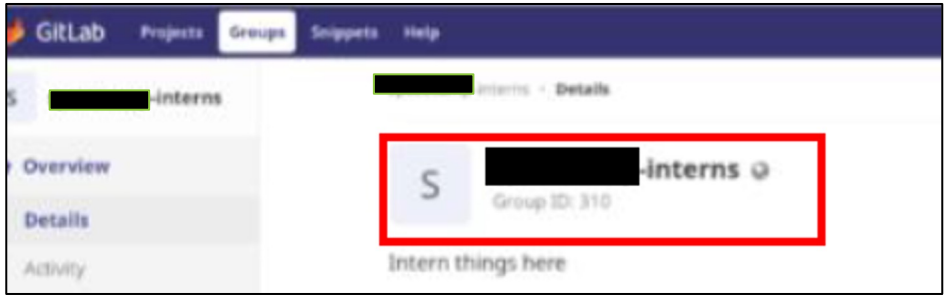
...BUT ENUMERATING BEFORE WE GET THERE

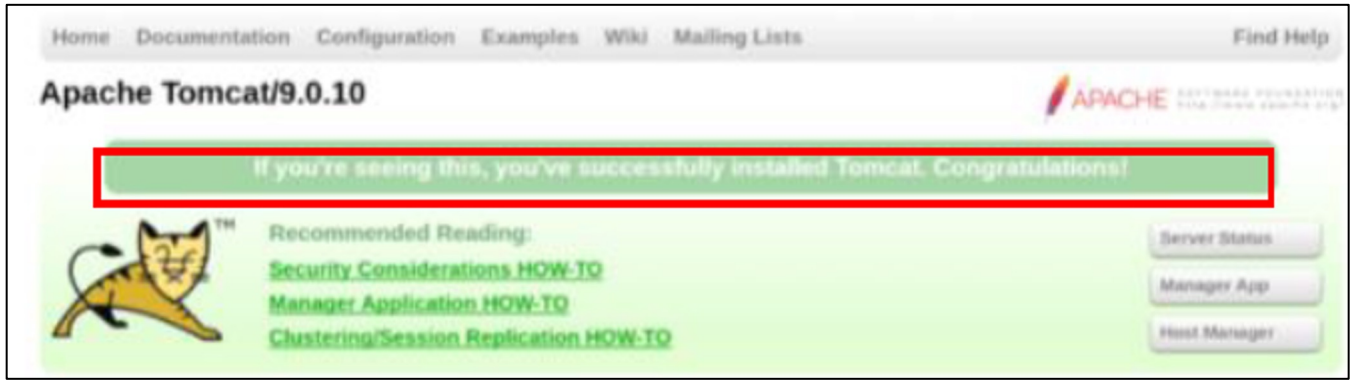
DARK WOLF SOLUTIONS

SHODAN





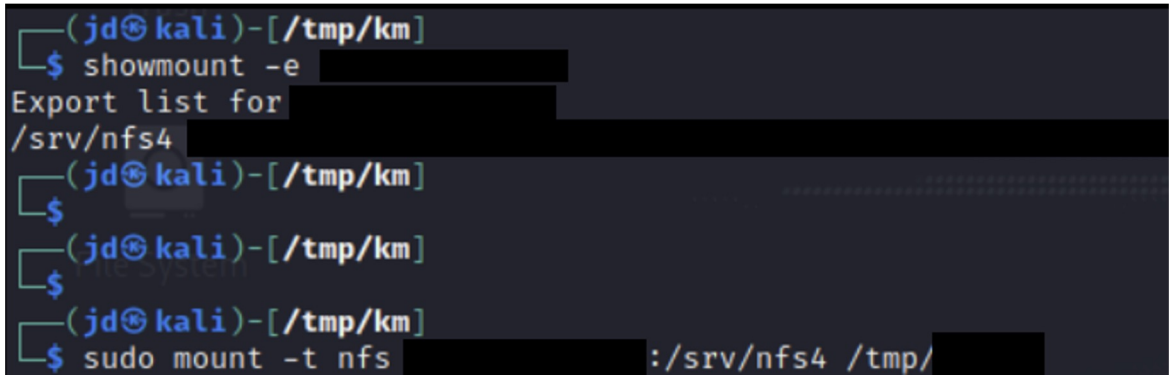




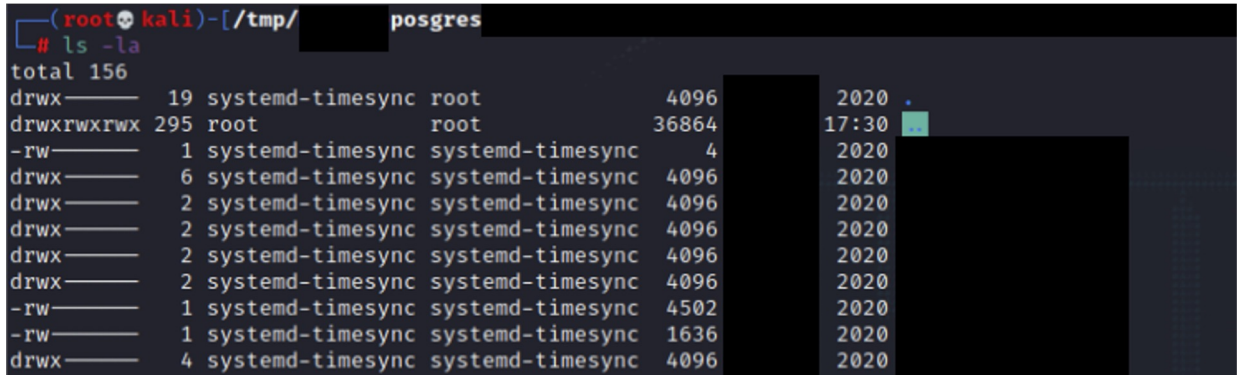
Software is only as secure as its Development Environment(s)

DARK WOLF SOLUTIONS

- Entire organizations dedicated to developing software for the USSF
- Cloud infra and apps are great when locked down well
- Not so much when you let anyone mount your NFS shares



Oh, surely this won't contain any impo-



Welp, core application database files

Dev. Environments – Cloud Woes

- Even in an externally locked down cloud environment, internal security holes can be tantalizing for an insider threat

```
└─$ describe-instance-attribute --attribute userData --instance-id
    | jq -r .UserData.Value | base64 -d | jq .env.    .blobstores[]
{
  "options": {
    "access_key_id": "                    ",
    "bucket_name": "                      ",
    "credentials_source": "static",
    "host":                               ',
    "host_style": false,
    "port": 443,
    "provider": "   ",
    "region": "                           ",
    "s3_region": "                  ',
    "secret_access_key":
    "signature_version":
    "use_ssl": true
  },
  "provider":
}
```

Storing secrets in any general cloud storage is not ideal

- Security Group Opens All Ports to All
- Security Group Opens DNS Port to All
- Security Group Opens MsSQL Port to All
- Security Group Opens MySQL Port to All
- Security Group Opens NFS Port to All

Lock down your security groups!

```
┌──(kali㉿kali)-[~/Downloads]
└─$ aws iam get-account-summary | jq .SummaryMap.AccountAccessKeysPresent
1
```

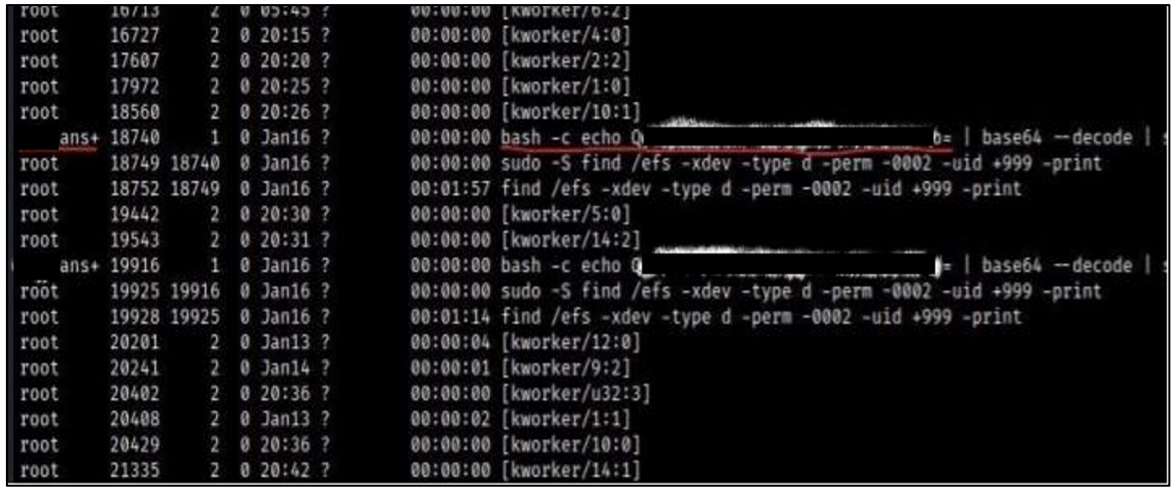
Giving root programmatic accesses - that's a paddlin'

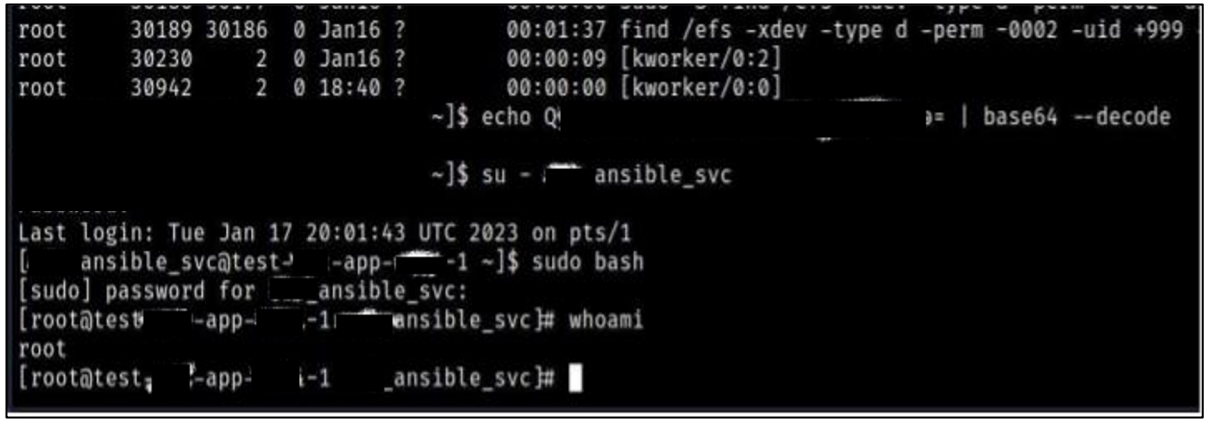
Kubernetes RBAC: Important

```
[redacted][!][ClusterRole]→ c[redacted]-manager Has Admin-Cluster permission!
[redacted][!][ClusterRole]→ [redacted]-manager Has Admin-Cluster permission!
[redacted][!][ClusterRole]→ [redacted]-manager Has Admin-Cluster permission!
```

Service Account: "Here's Root Credentials"

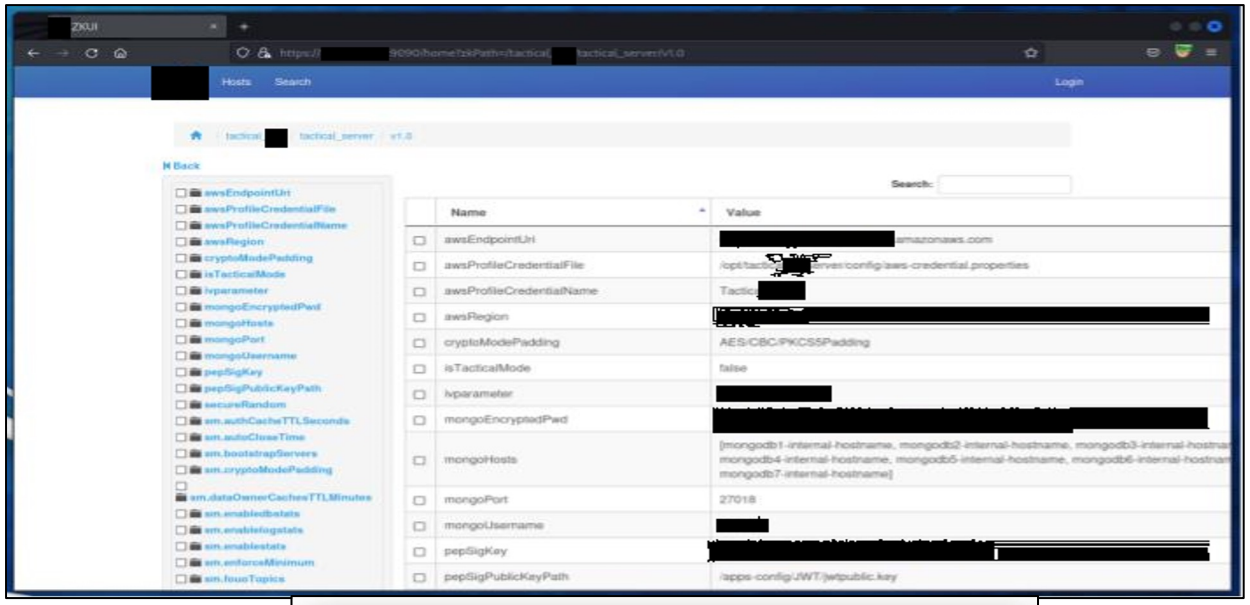
- Large systems deploy a wide range of services into their environments
- Unfortunately, some of these require authentication
- By passing the password of the service account in plain-ish text through a script running as a service, credentials were leaked allowing the elevation to root on the system

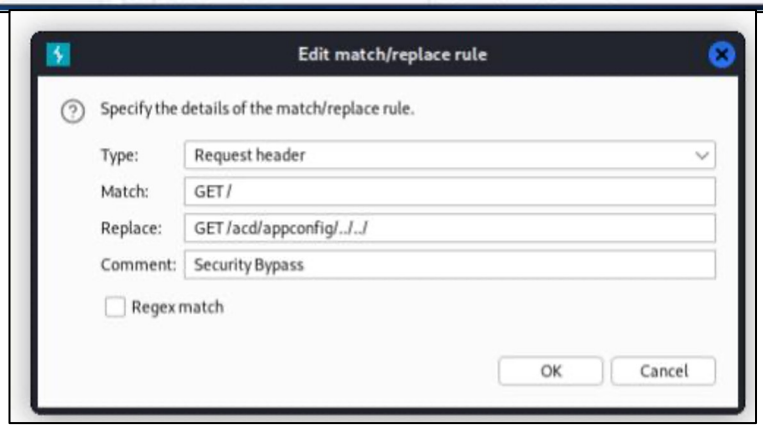




Access Control vs Old Software

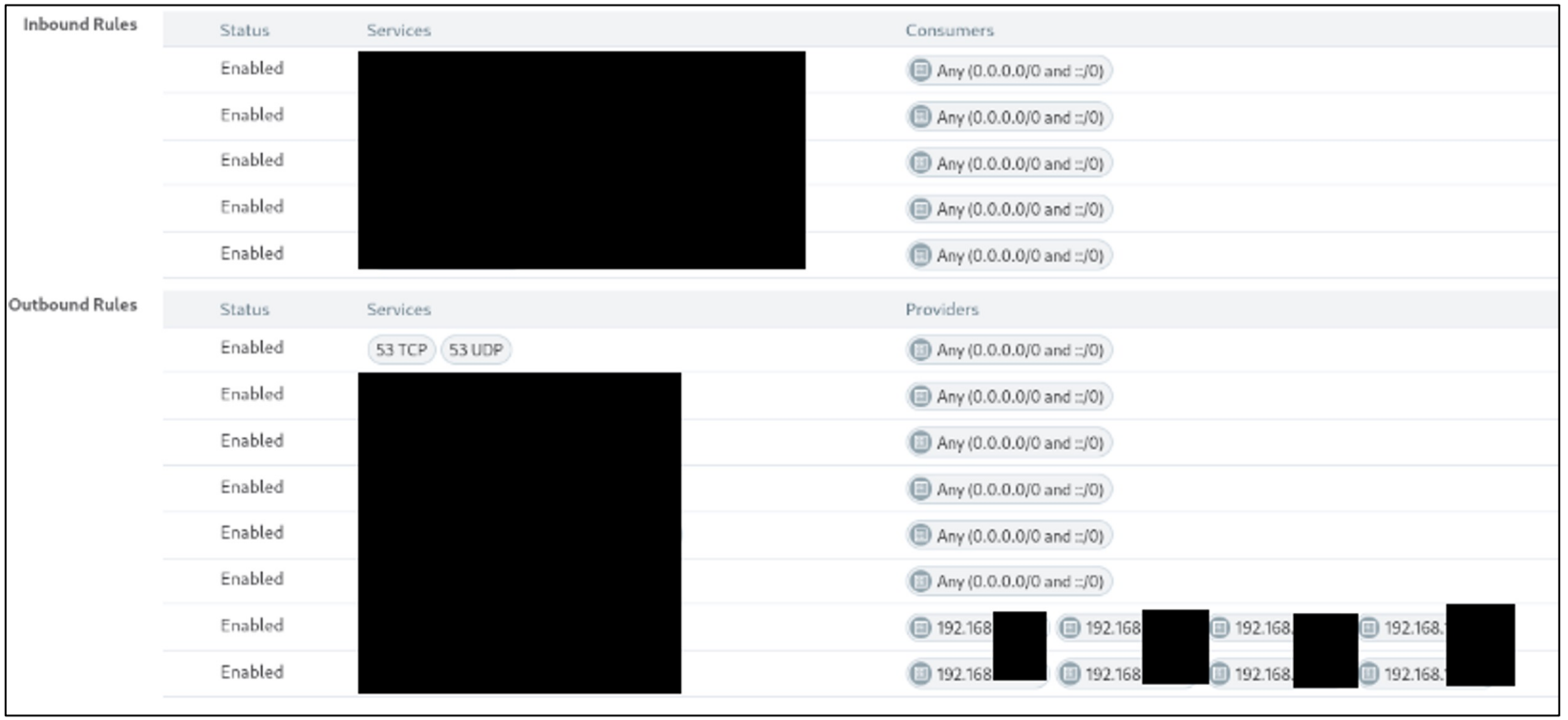
- Many tools exist for managing and interfacing with applications being run in systems where centralized services are used to maintain configuration and authentication
- Some of these apps are outdated and/or occasionally used by developers without the knowledge of the wider team
- Utilizing software in this manner exposes the system to vulnerabilities contained within old/outdated code





Impersonal Boundaries

- DoD and USSF are relying more and more on zero-trust architecture and associated tooling
  - Speaker's note: *This is good*
  - but they better be secure and configured well!
- We helped find gaps here, and…



Inbound and outbound traffic limitations generally shouldn't be "Any"

Impersonal Boundaries, Again

- Even very robust tooling can fail to detect simple bypasses

```
C:\Users\dw_tester3\test>ssh -p 23 redteamuser@
ssh: connect to host 10.60.222.4 port 23: Permission denied

C:\Users\dw_tester3\test>ssh -p 53 redteamuser@
redteamuser@          's password:
Linux redv-kali03 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC
```

```
C:\WINDOWS\system32>dns.exe
*** Node started
[10.60.105.52:50000 Command/? for help]
[10.60.60.55:50001]: APPLICATION TEST
```

…REALLY IMPERSONAL BOUNDARIES

DARK WOLF SOLUTIONS

- but sometimes, your team reverse engineers entire zero trust software packages to deliver one-click remote code execution

Single click on [REDACTED] tool link

Back to Earth – Common Themes

- Modern space support systems and apps in the USSF share many common security issues with their non space counterparts
- Critical/High findings on most tests!
- but even less epic findings can have a huge impact given the domain!
- Simple misconfigs can leave a system just as vulnerable as a major exploit

Future State: USSF and Ethical Hacking

- Increased interest in and willingness to have USSF systems tested per USSF vision and federal mandates
  - Some organizations are already onboard, this trend needs to continue
  - Still viewed as an afterthought or “checkbox” at times; education on the benefits is important
- Software development, and targets, only set to expand
- AI is about to make our lives very interesting, but… I need another slide

The same AI Slide Many Speakers Here Will Have

DARK WOLF SOLUTIONS

- Everything in the industry is set for rapid change. Offense, defense and how we look at critical systems as a whole.

- **DISCLAIMER:**
  This video is all sample and/or fake data other than the public domains.

Closing thoughts

DARK WOLF SOLUTIONS

- Even the most modern parts of the service are at risk from attackers, and those risks aren't always hard to find
- It's very cool to hack and help fix military systems as a veteran
- Anyone can get into this world if they try hard enough. Your personal tasker from me is to get involved in space hacking!
  - PNPT, OSCP, GPEN, CRTO
  - Traditional development and scripting experience
  - …educate yourself on AI and machine learning fast
- Many units, orgs and companies here today, ours included, need more people to come do this work
  - Come grab a card!

Questions and Answers

THANK YOU!

DARK WOLF
SOLUTIONS

Special Credit:
The awesome penetration testing team at Dark Wolf Solutions and our friends at the Space Force!