

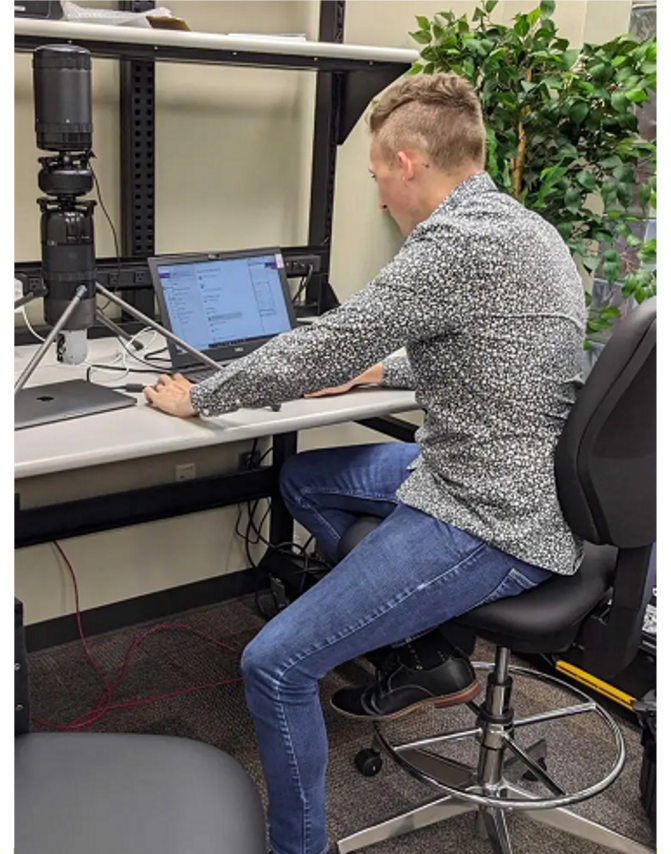


DARK WOLF SOLUTIONS

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

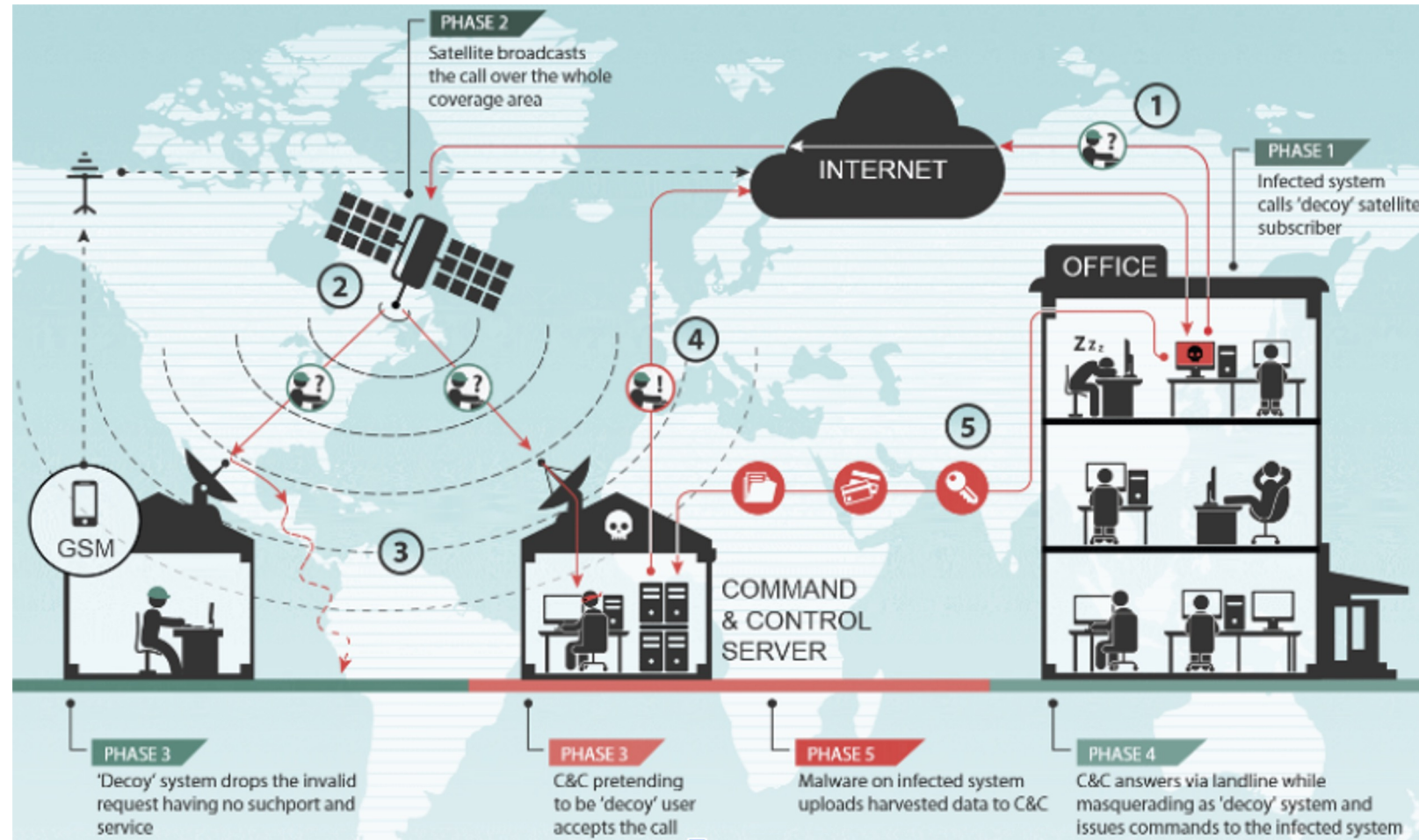


- Major current and increasingly future area of geopolitical control for the world's big players
- Weaponization of equipment in orbit and attacks against those represent an increasingly complicated game of space chess
- Denial of space communications can cripple a nation
 - Not the kind of thing you'd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

AFOREMENTIONED **BAD GUYS**



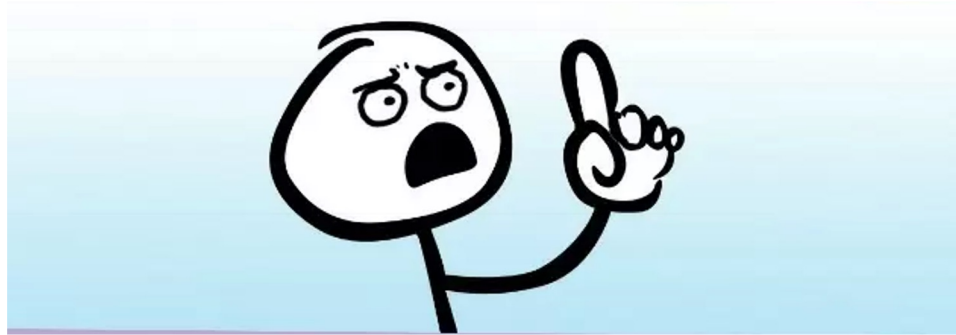
- Russia and China in particular are major aggressors
- Nonstop targeting of (aero)space biz
 - Commercial, govt., you name it
 - More APTs than can fit on this slide
- Turla Group
 - Campaign pictured here!
- NASA networks hit in SolarWinds attack



THE ARGUMENT FOR HACKING STUFF FIRST

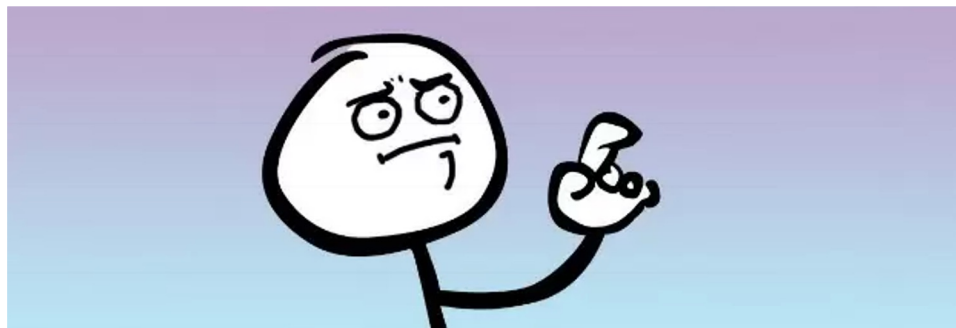


- Penetration testing, red teaming, vulnerability research... they just work!
 - All of these cybersecurity disciplines give system owners ways to find easy and hard issues alike
- Finding and fixing things before those adversaries safeguards the economy, nation and... maybe world?
- Increasingly a government 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



- 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?

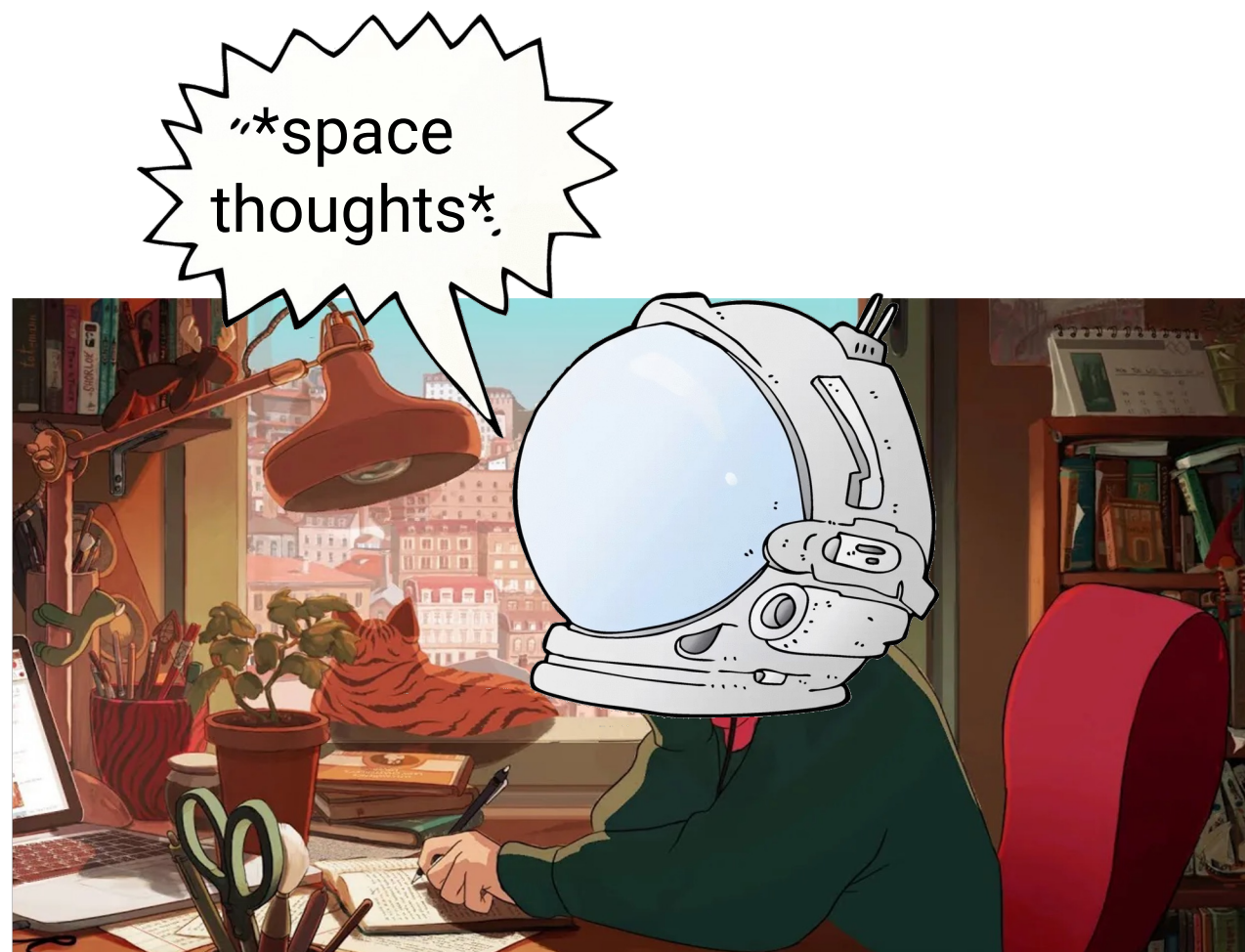
- Kind of!
- Make no mistake; there are still a LOT of spicy and complicated space systems
 - See annual Hack-a-Sat CTF!
 - Recent results from DEF CON and more
- However, more “standard” modern systems in space domain opens up the door for your more traditional testing
 - Many young orgs need even simple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



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



No.	Time	Source	Destination	Protocol	Length	Info
762...	6395.285192	Apple_dfd5:44	Apple_8e:c9:9e	EAPOL	133	Key (Message 1 of 4)
804...	6678.507916	Apple_dfd5:44	Apple_8e:c9:9e	EAPOL	133	Key (Message 1 of 4)
804...	6678.515596	Apple_dfd5:44	Apple_8e:c9:9e	EAPOL	189	Key (Message 3 of 4)
829...	6840.531496	Apple_dfd5:44	Apple_96:54:bc	EAPOL	133	Key (Message 1 of 4)
926...	7433.533518	Apple_dfd5:44	Apple_8e:c9:9e	EAPOL	133	Key (Message 1 of 4)
926...	7433.535564	Apple_8e:c9:9e	Apple_dfd5:44	EAPOL	155	Key (Message 2 of 4)
926...	7433.540174	Apple_dfd5:44	Apple_8e:c9:9e	EAPOL	189	Key (Message 3 of 4)
926...	7433.542220	Apple_8e:c9:9e	Apple_dfd5:44	EAPOL	133	Key (Message 4 of 4)
932...	7480.821844	Apple_dfd5:44	Apple_0b:d1:2a	EAPOL	133	Key (Message 1 of 4)
932...	7480.828500	Apple_dfd5:44	Apple_0b:d1:2a	EAPOL	133	Key (Message 1 of 4)
932...	7480.830548	Apple_dfd5:44	Apple_0b:d1:2a	EAPOL	133	Key (Message 1 of 4)
932...	7480.834132	Apple_dfd5:44	Apple_0b:d1:2a	EAPOL	133	Key (Message 1 of 4)

Capturing handshakes; good for conferences, bad for your network

WPA2 you say...?

Proprietary & Confidential |

...BUT ENUMERATING BEFORE WE GET THERE

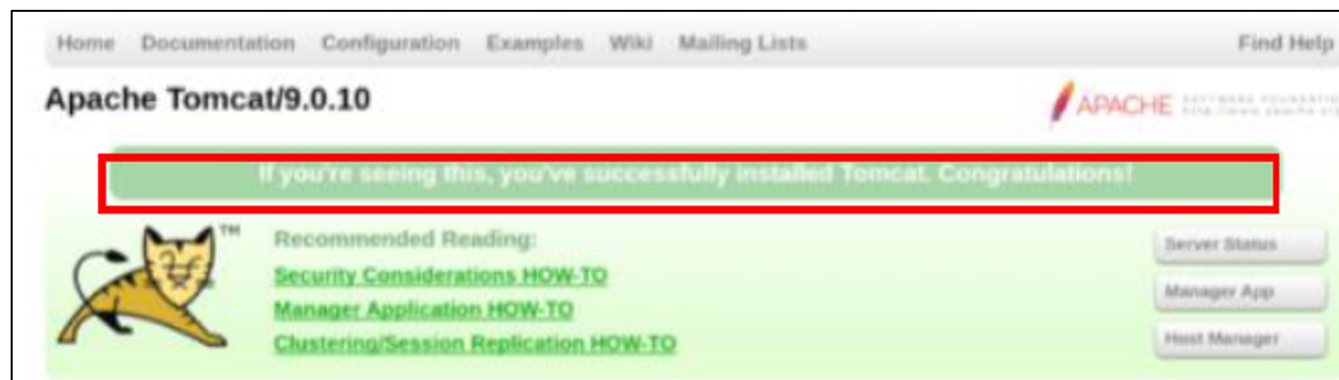
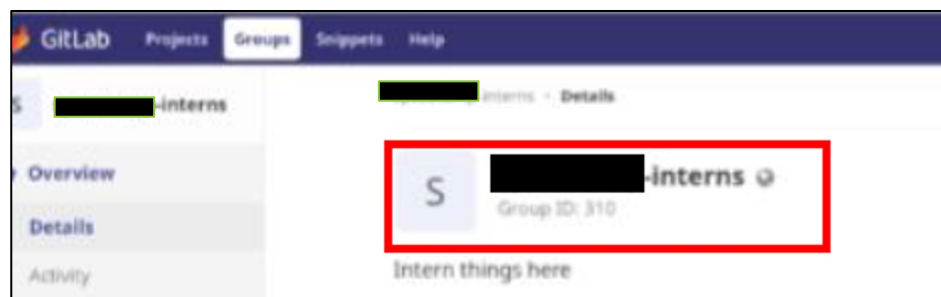
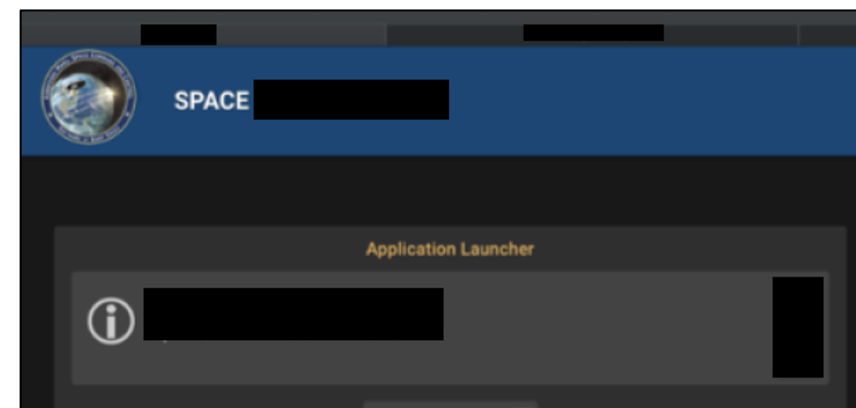


```
START TIME: Tue Aug 6 13:55:23
URL_BASE: https://gitlab.
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4613

-- Scanning URL: https://gitlab.
https://gitlab. /explore (CODE:200|SIZE:15079)
https://gitlab. /favicon.ico (CODE:301|SIZE:180)
https://gitlab. /groups (CODE:302|SIZE:111)
https://gitlab. /help (CODE:200|SIZE:90658)
https://gitlab. /projects (CODE:302|SIZE:104)
https://gitlab. /public (CODE:200|SIZE:28569)
https://gitlab. /robots.txt (CODE:200|SIZE:2153)
https://gitlab. /search (CODE:200|SIZE:14310)
https://gitlab. /service (CODE:302|SIZE:112)
https://gitlab. /snippets (CODE:302|SIZE:113)
https://gitlab. /who (CODE:200|SIZE:17352)
```



SOFTWARE IS ONLY AS SECURE AS ITS DEVELOPMENT ENVIRONMENT(S)



- 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

```
(jd@kali)-[/tmp/km]
$ showmount -e
Export list for
/srv/nfs4
(jd@kali)-[/tmp/km]
$
(jd@kali)-[/tmp/km]
$
(jd@kali)-[/tmp/km]
$ sudo mount -t nfs :/srv/nfs4 /tmp/
```

Oh, surely this won't contain any impo-



```
(root@kali)-[/tmp/ postgres]
# ls -la
total 156
drwx----- 19 systemd-timesync root 4096 2020 .
drwxrwxrwx 295 root root 36864 2020 ..
-rw----- 1 systemd-timesync systemd-timesync 4 2020
drwx----- 6 systemd-timesync systemd-timesync 4096 2020
drwx----- 2 systemd-timesync systemd-timesync 4096 2020
drwx----- 2 systemd-timesync systemd-timesync 4096 2020
drwx----- 2 systemd-timesync systemd-timesync 4096 2020
drwx----- 2 systemd-timesync systemd-timesync 4096 2020
-rw----- 1 systemd-timesync systemd-timesync 4502 2020
-rw----- 1 systemd-timesync systemd-timesync 1636 2020
drwx----- 4 systemd-timesync systemd-timesync 4096 2020
```

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

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

Lock down your security groups!

Giving root programmatic accesses – that's a paddlin'

Kubernetes RBAC: Important

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

```
root 16713 2 0 05:45 ? 00:00:00 [kworker/0:2]
root 16727 2 0 20:15 ? 00:00:00 [kworker/4:0]
root 17607 2 0 20:20 ? 00:00:00 [kworker/2:2]
root 17972 2 0 20:25 ? 00:00:00 [kworker/1:0]
root 18560 2 0 20:26 ? 00:00:00 [kworker/10:1]
ans+ 18740 1 0 Jan16 ? 00:00:00 bash -c echo Q b= | base64 --decode |
root 18749 18740 0 Jan16 ? 00:00:00 sudo -S find /efs -xdev -type d -perm -0002 -uid +999 -print
root 18752 18749 0 Jan16 ? 00:01:57 find /efs -xdev -type d -perm -0002 -uid +999 -print
root 19442 2 0 20:30 ? 00:00:00 [kworker/5:0]
root 19543 2 0 20:31 ? 00:00:00 [kworker/14:2]
ans+ 19916 1 0 Jan16 ? 00:00:00 bash -c echo Q f= | base64 --decode |
root 19925 19916 0 Jan16 ? 00:00:00 sudo -S find /efs -xdev -type d -perm -0002 -uid +999 -print
root 19928 19925 0 Jan16 ? 00:01:14 find /efs -xdev -type d -perm -0002 -uid +999 -print
root 20201 2 0 Jan13 ? 00:00:04 [kworker/12:0]
root 20241 2 0 Jan14 ? 00:00:01 [kworker/9:2]
root 20402 2 0 20:36 ? 00:00:00 [kworker/u32:3]
root 20408 2 0 Jan13 ? 00:00:02 [kworker/1:1]
root 20429 2 0 20:36 ? 00:00:00 [kworker/10:0]
root 21335 2 0 20:42 ? 00:00:00 [kworker/14:1]
```

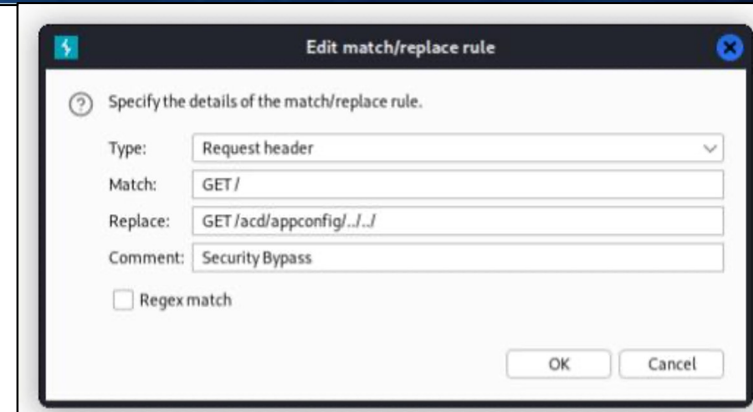
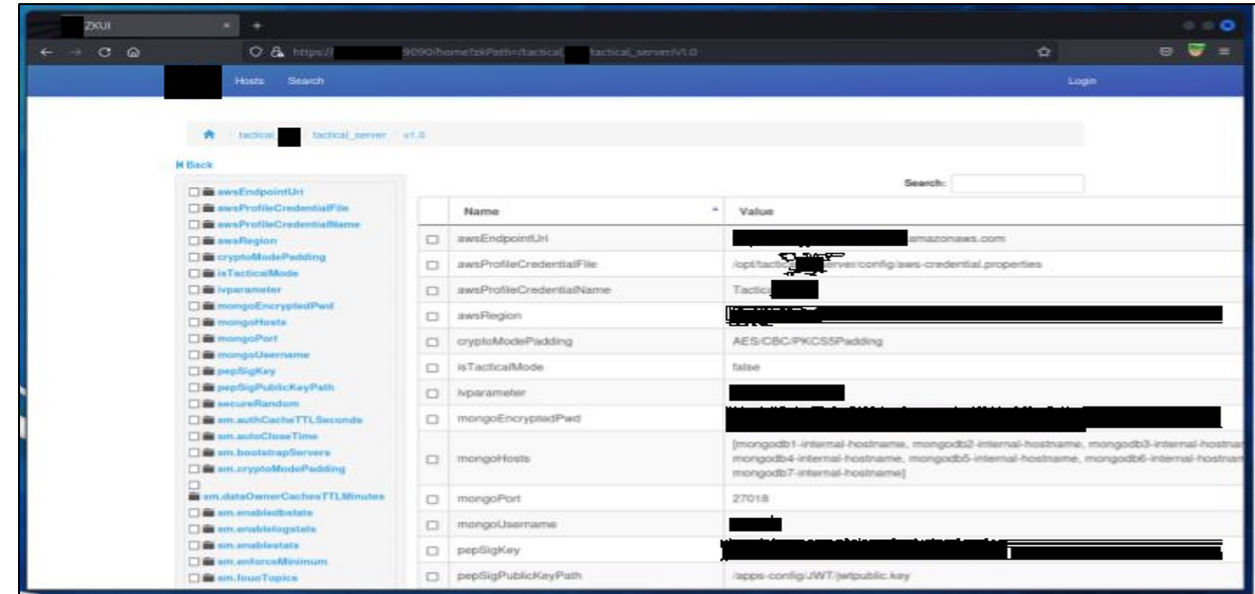
```
root 30189 30186 0 Jan16 ? 00:01:37 find /efs -xdev -type d -perm -0002 -uid +999
root 30230 2 0 Jan16 ? 00:00:09 [kworker/0:2]
root 30942 2 0 18:40 ? 00:00:00 [kworker/0:0]
~]$ echo Q f= | base64 --decode
~]$ su - ansible_svc

Last login: Tue Jan 17 20:01:43 UTC 2023 on pts/1
[ ansible_svc@test ~] -app- -1 ~]$ sudo bash
[sudo] password for ansible_svc:
[root@test ~] -app- -1 ansible_svc# whoami
root
[root@test ~] -app- -1 ansible_svc#
```

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 Rules	Status	Services	Consumers			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
Outbound Rules	Status	Services	Providers			
	Enabled	53 TCP 53 UDP	Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		Any (0.0.0.0/0 and ::/0)			
	Enabled		192.168. 192.168. 192.168. 192.168.			
Enabled	192.168. 192.168. 192.168. 192.168.					

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
```

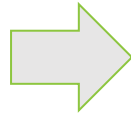


...REALLY IMPERSONAL BOUNDARIES



- 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



- 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

- 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, CRT0
 - 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!



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