All Access: A photographer’s perspective on Red Teaming

by Mansoor Ahmad

- Photographer-turned-pen tester
- 5 years as a press photographer, 2 seasons as team photographer
- Big fan of social engineering and Burp Suite

EVERLAST
Dynasty
CS

13 48
10
3
MINNESOTA STATE
84
24
TEXANS

CCHA
21

BAUER
BAUER
BAUER

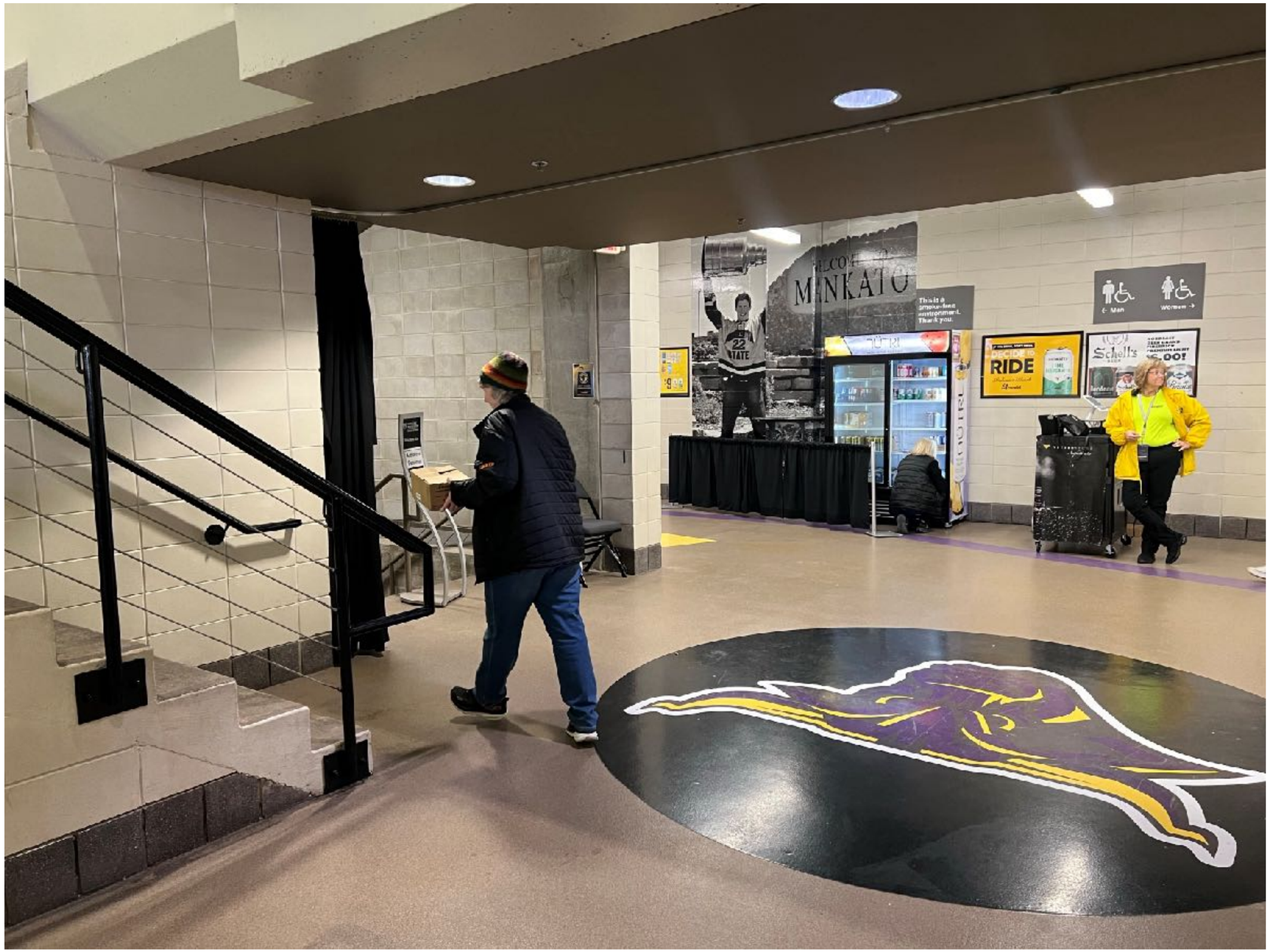
MINNEAPOLIS
POLICE

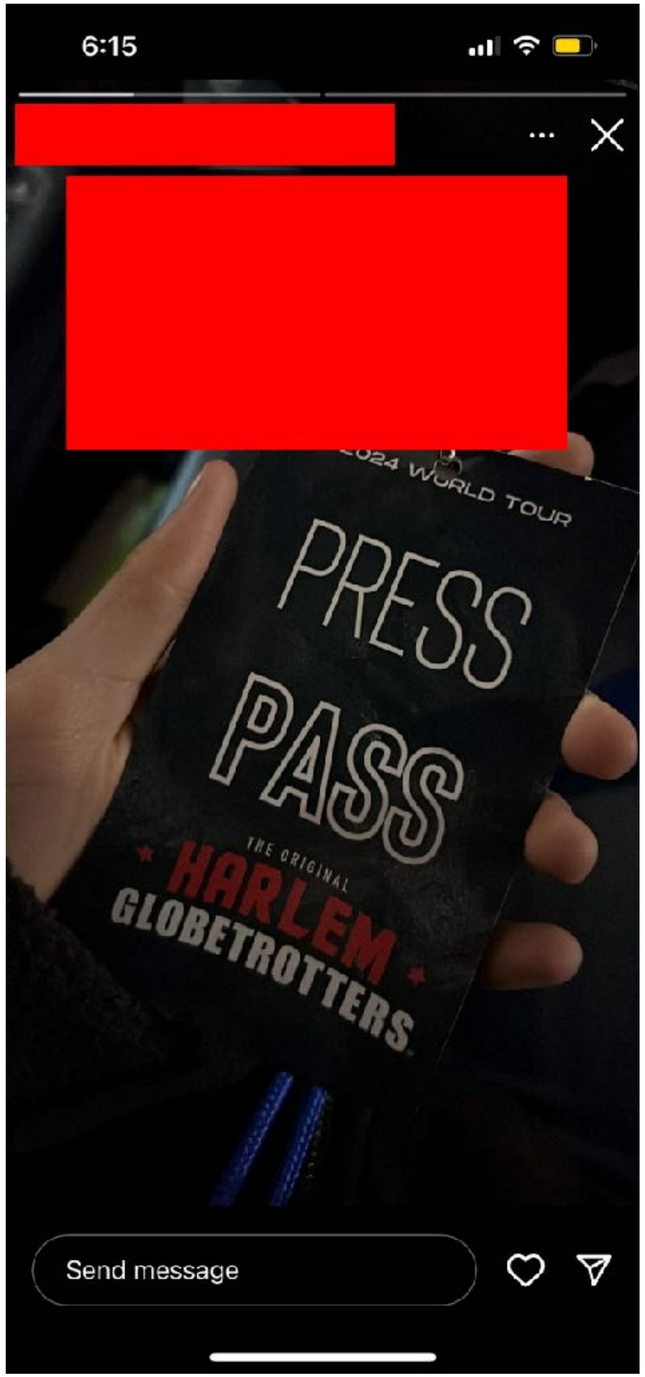
The short and sweet

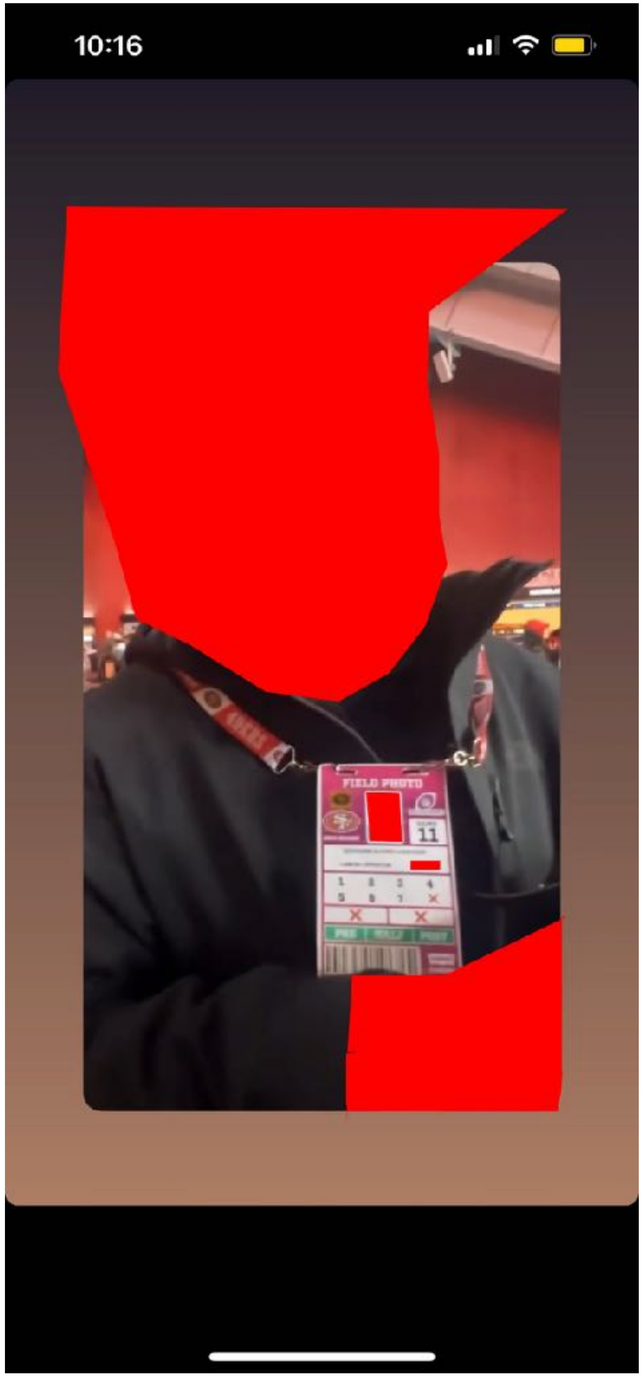
- The WHO: Media, ops staff and security folks (and bad guys)
- The WHAT: Abusing the First Amendment to get physical, network and device-level access
- The WHERE: Your favorite sporting or music venue
- The WHY: Get lucky, and you can get secrets about your favorite team or drama about your favorite band

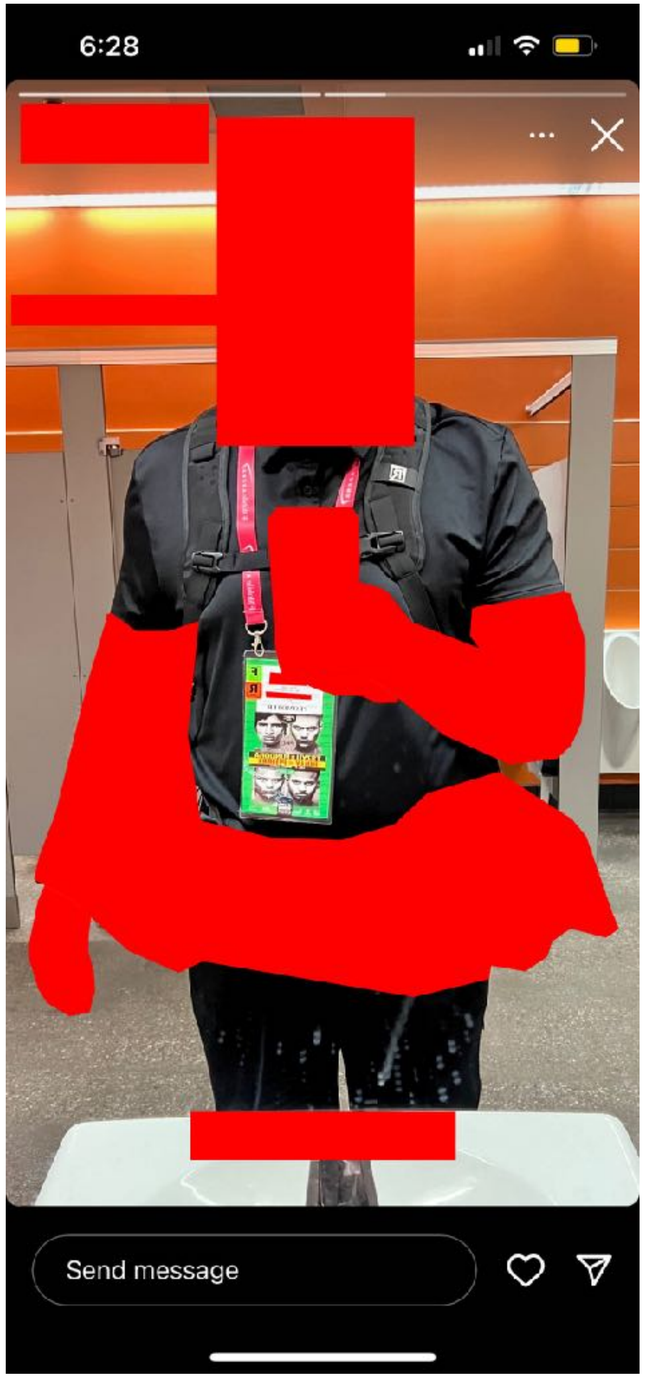
Part 1: Getting in

- Creds through social media
- The media credential, or press pass, process


MANKATO
RIDE
Schell's


6:15
[redacted]
2024 WORLD TOUR
PRESS
PASS
THE ORIGINAL
HARLEM
GLOBETROTTERS
Send message


10:16
[redacted]
FIELD PHOTO
11


6:28
Send message

4:59
UFC 297
SCOTIABANK ARENA
NO FLOOR

NCAA
MEDIA
NCAA DIVISION I
ICE HOCKEY CHAMPIONSHIP
1994
FINALS
1995
1996
FINALS
1997
FINALS
1999
FINALS
2000
FINALS
2001
FINALS
2002
FINALS
2003
FINALS
2004
FINALS
2005
FINALS
2006
FROZEN FOUR
JESS MYERS
FROZEN FOUR
BOSTON
BP

OR...

The media credential, or press pass, process

- OSINT to find publicist/managers (Press releases, Facebook page, IMDB, etc.)
- Identify target outlet/mark
- Why Reporter/smaller outlets are a good example
- Typosquatting, cloning sites and email accounts

4:31
J
Jane Tastad
Today 4:28 PM
Hey Jane, is it okay if I talk about my time at the Reporter and use it as an example for my conference talk?
Delivered
Yes yes and yes

Domain Registration

Register Domain

Buy a new domain at cost.

Domain registration documentation

Search for a domain name

msureperter.com

Search

Review instructions and supported extensions.

msureperter.com

$9.77

Renews at $9.77

Purchase

msu-reporter.com

$9.77

Renews at $9.77

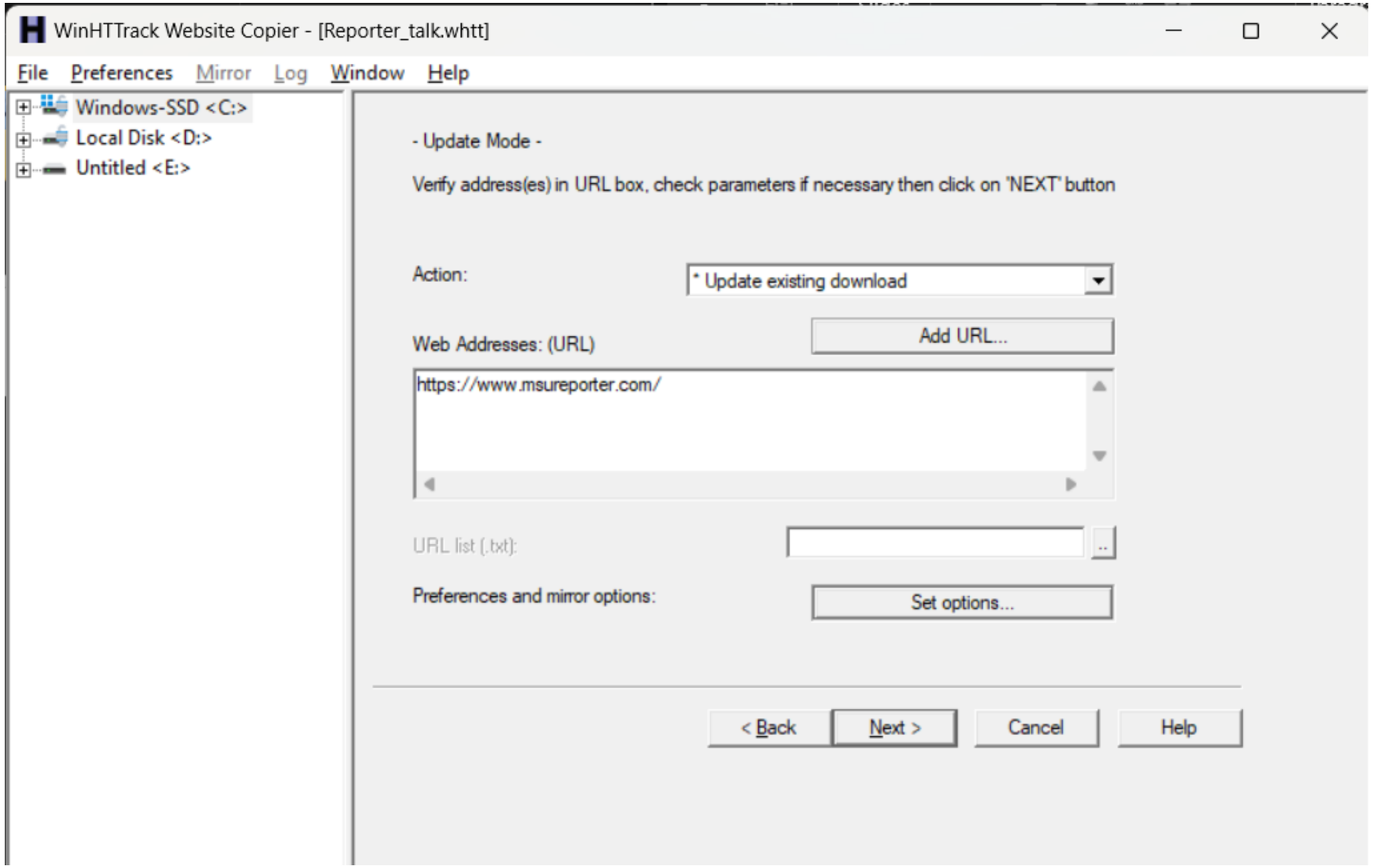
Purchase

thereportermsu.com

$9.77

Renews at $9.77

Purchase


WinHTTrack Website Copier - [Reporter_talk.whtt]
File
Preferences
Mirror
Log
Window
Help
Windows-SSD <C:>
Local Disk <D:>
Untitled <E:>
- Update Mode -
Verify address(es) in URL box, check parameters if necessary then click on 'NEXT' button
Action:
* Update existing download
Web Addresses: (URL)
Add URL...
https://www.msureporter.com/
URL list (.txt):
Preferences and mirror options:
Set options...
< Back
Next >
Cancel
Help

Downloads > Talk > Repo2 > www.msureporter.com >

Sort View ...

Name	Date modified	Type	Size
Today			
xmlrpc0db0.html	6/27/2024 1:30 AM	Firefox HTML Doc...	1 KB
index975a.html	6/27/2024 1:29 AM	Firefox HTML Doc...	1 KB
index.html	6/27/2024 1:29 AM	Firefox HTML Doc...	137 KB
2010	6/27/2024 1:30 AM	File folder	
2016	6/27/2024 1:30 AM	File folder	
2017	6/27/2024 1:30 AM	File folder	
2018	6/27/2024 1:30 AM	File folder	
send-story-idea	6/27/2024 1:30 AM	File folder	
2019	6/27/2024 1:30 AM	File folder	
2020	6/27/2024 1:30 AM	File folder	
2021	6/27/2024 1:30 AM	File folder	
2022	6/27/2024 1:30 AM	File folder	
2023	6/27/2024 1:30 AM	File folder	
2024	6/27/2024 1:30 AM	File folder	
author	6/27/2024 1:30 AM	File folder	
category	6/27/2024 1:30 AM	File folder	

What to do when you have access?

- Play by the book, until you get your moment and deploy your dropbox (prior experience/research helps)
- The less interaction the better: act like you’ve been there or you’re supposed to be there (Bonus tip: being nice always helps :)
- Verify you have good connection. If so, let the games begin!
- Bonus – priv esc: Switch roles (Re: Jayson Street MS badge)

If all goes well…

- Maybe a bonus point: building the relationship with the publicists (= establishing persistence) to get more shows. But don’t worry, you don’t have to work that hard…

ChatGPT

https://chatgpt.com

ChatGPT 3.5

You

Can you help with a writing assignment

ChatGPT

Of course! I'd be happy to help. What specifically do you need assistance with for your writing assignment?

You

Can you write a concert review for a Taylor Swift show from her Eras tour
at the U.S. Bank Stadium in Minneapolis on June 27th

ChatGPT

Concert Review: Taylor Swift's Eras Tour at U.S. Bank Stadium, Minneapolis

On a balmy summer evening in Minneapolis, U.S. Bank Stadium was transformed into a pulsating nexus of music and magic as Taylor Swift took the stage for her highly anticipated Eras Tour. The atmosphere was electric, buzzing with anticipation from a diverse crowd spanning generations, all eager to witness Swift's evolution through her music.

As the lights dimmed and the crowd erupted into deafening cheers, Swift appeared onstage, a vision in sequins and charisma. She opened with "Fearless," instantly captivating the audience with her powerful vocals and infectious energy. The stage design was a spectacle in itself, with elaborate sets and dazzling visual effects that complemented each song's narrative.

Swift seamlessly transitioned between hits from different eras of her career, showcasing her versatility

Message ChatGPT

ChatGPT can make mistakes. Check important info.

Part 2: Attacking networks and pivoting

- Exploiting the traveling folks
  a. Dropbox equipped with ways to connect to multiple networks
  b. LOTs of custom scripts to…
  c. Start detecting new APs when traveling party starts prep
  d. Try to get creds (deauth attacks, social engineering through captive portals)
  e. Connect and pivot to the ‘traveling network’ using creds. Try to establish persistence/exploit right away (depending on scenario)

MakeAGIF.com

Yikes! So what should we do?

- Photogs: don’t post your credentials online pls
- Security companies: work on developing and adding service offerings tailored to publicists/management companies
- Publicists/management companies: talk to security companies and offer tailored training

What’s next on this project?

- Working on a comprehensive demo of the whole attack chain
- Developing tooling/workflow to get it to do more reliable Wi-Fi attacks
- Talk to smarter people and see if they have any ideas

I am here a lot

- https://www.linkedin.com/in/mansoor-ahmad-khan/

Thank you!