Tales from the Trenches – Learning from the Misery of Others.

Confessions of a Sh*tty SysAdmin

Andy Thompson, CISSP, GPEN
CyberArk
whoami – Andy Thompson

- Programs Office - Customer Success "¯\_(ツ)_/¯"
- B.S. MIS – Univ of Texas at Arlington
- Credentials:
  - COMPTIA A+ & Sec+
  - (ISC)2 SSCP & CISSP
  - GIAC – Certified Penetration Tester (GPEN)
- DC214 / DHA / ISSA / NTXCSG +++
- Travel-Hacker
- Shitty SysAdmin
WARNING!

• Lots of TLA’s ahead.
• Take notes.
• Quiz later.
First Call Resolution 90%
Helpdesk Level 1
We've got to help her!

Helpdesk Level 2
They're my friends, I've got to help them!

Helpdesk Level 3
I can save him, I have to try!

Sysadmin
Who are you? Go away!

SYSTEM ADMINS
I AM THE KEYMASTER

ARE YOU THE GATEKEEPER?
WE TOOK THE HOSTAGES, SECURED THE BUILDING, AND CUT THE COMMUNICATION LINES LIKE YOU SAID.

EXCELLENT.

BUT THEN THIS GUY CLIMBED UP THE VENTILATION DUCTS AND WALKED ACROSS BROKEN GLASS, KILLING ANYONE WE SENT TO STOP HIM.

AND HE RESCUED THE HOSTAGES?

NO, HE IGNORED THEM. HE JUST RECONNECTED THE CABLES WE CUT, MUTTERING SOMETHING ABOUT "UPTIME".

SHIT, WE'RE DEALING WITH A SYSADMIN.
Availability
Systems Administrator

What my friends think I do

What society thinks I do

What my boss thinks I do

What my users think I do

What I think I do

What I actually do
How I took the name Rainmaker?

¯\_(ツ)_/¯
FREE WIFI
Compliance!
YOU'RE BAD
AND YOU SHOULD FEEL BAD
i've seen things...

terrible things...
Exposed Passwords

If you’re dumb enough to leave your login on a PostIt on your desk, it’s not a hack. It’s barely social engineering. It’s more like natural selection.

- Gilfoyle
DESKTOP PASSWORD: r4ew01s589

Password: I Love Shelflock

"Let me in."
According to Gartner, through 2023 at least 99% of cloud security failures will be the customer’s fault.

https://www.fugue.co/blog/the-human-factor-in-cloud-misconfiguration
IT'S APRIL FOOLS!
18+ FOR ADULTS ONLY
YOU KEEP USING THAT WORD
I DON'T THINK IT MEANS WHAT YOU THINK IT MEANS
TO BE HONEST...
BURNING THE SHIPS
BRAND-JACKING
OPEN THE KIMONO
Hacking is not a crime.
I’ve seen some good things too...
@echo off
echo Easy Ransomware Protection
echo By: Andy Thompson
echo www.MeteorMusic.com
echo @R41nM4kr

assoc .js=poss_bad
assoc .jse=poss_bad
assoc .wsf=poss_bad
assoc .wsh=poss_bad
assoc .hte=poss_bad
assoc .lng=poss_bad
assoc .ps1=poss_bad
assoc .cmd=poss_bad
assoc .bat=poss_bad
assoc .vbs=poss_bad
assoc .vbe=poss_bad

ftype poss_bad=c:\Program Files\Windows NT\Accessories\wordpad.exe %1
Literally, that’s it!
Experience vs. Certification
STEP AWAY FROM THAT NETWORK SERVER!
I'M CERTIFIED!

I SUMMON THE VAST POWER OF CERTIFICATION!

WELL, THIS IS EMBARRASSING; THAT'S ALL I REMEMBER FROM THE CLASSES.
Dragnet video here
uname -s
Checks machine name properties of remote server

uname -s
RENAMEs HOST Solaris
rm -rf /

EDIT .profile TO rm -i TO CONFIRM DELETES!
SysAdmin Quiz

- SLA: Service Level Agreement
- FCR: First Call Resolution
- CIA: Confidentiality
- AAA: Accountability
- WTFBBQ: Availability
Key Takeaways

• Prioritize Security.
• Don’t cut corners.
• Watch the Watchers
• Systems are more vulnerable to misconfiguration vs traditional exploits.
• SysAdmins are people too.
WARNING!

• Risk is EVERYWHERE.
• Learn from these mistakes.
• Don’t let this happen to you.
Parting Advice

• Blame the previous sysadmin.
• Blame the vendor.
• Prepare 3 envelopes.
Thank You!

Andy@MeteorMusic.com
@R41nM4kr
www.MeteorMusic.com