Twitter Thread by Tinker ■

Tinker ■
@TinkerSec

Singing the Blues:
Taking Down an Insider Threat

"I had all of the advantages. I was already inside the network. No one suspected me. But they found my hack, kicked me off the network...

...and physically hunted me down."

Many pentests start from the outside, wanting to see how the perimeter might be breached.

This pentest started from the inside. My client wanted to assume they had already been breached, and, if breached, how far could an attacker go.

Could they stop me once I was inside?

So they snuck me in. Disguised me as a new employee. Gave me a work computer, an ID badge, an account in their system... hell, I even had a cubicle w/my assumed name on it.

The only person who knew who I really was was their CISO. Everyone else thought I was Jeremy in Marketing.

During most of the first morning, I completed onboarding, made introductions, and completed menial tasks.

But I had to act quick. I only had a week onsite. I had to hack their network while not raising suspicion.

So I set about it.

You have to understand... most "Internal Pentests" are straight forward. The hard part is breaching the network, but once you're inside, it's a target rich environment. End of Life computers, default passwords, everyone a Local Administrator...

On most Internal Pentests, I generally get Domain Admin within a day or two. Enterprise Admin shortly thereafter. The rest of the time spent in mop-up and proofs of impact.

Narrator: "But this time was different. This time, Tinker was in for a surprise."

I set up my work computer and made it look like I was actually working.

I would use my work computer for research, for seeing how other workstations were configured, but I wouldn't use it to launch attacks from directly. I didn't want things to get back to me.

Instead, I brought in a rogue device. A personal laptop, loaded with Linux and a mess of hacking tools.

I plugged it into the network and got an IP address. Their Network Access Control (NAC) wasn't fully set up across their environment. Everyone at a cube was trusted.

I started my usual approach.

Captured packets and analyzed them with wireshark, changed my rogue computer's MAC and hostname to blend into their environment and look like their standard equipment.

Poisoned the local subnet with Responder to trap hashes and crack passwords.

I got lucky pretty quickly. Captured a solid handful of hashes. I was on their standard employee subnet, so many user accounts were logging in, opening up internet browsers, and throwing authentication hashes around.

I started cracking these with my 8 GPU cracking rig, but...

Something was off.

I can go through an 8 character password, all combinations upper/lower/number/symbol, in a short amount of time (NetNTLMv2).

Most normal passwords (single word, capital first letter, ending with a number or symbol), I crack instantly.

But not here.

I could've run "net accounts" on my workstation to query Active Directory directly & see their password policy, but decided to look elsewhere first. I didn't want to set off any alerts or logging.

I navigated through the company's intranet and found their Security Requirements.

They required a minimum of 12 characters with upper, lower, number, symbol.

They were moving from passwords to pass phrases...

I changed my cracking rulesets to use a dictionary with longer words, capitalized the first letter, ended with num/symbol.

And got a few!

Alright! Let's go!

I immediately try to log in remotely to the user's workstation with their own password...

And am blocked.

What the...? This always works...

Password is correct. But access is denied.

I checked myself. Start from basics. Do it right.

I spent some time hunting the Domain Controller. The VoIP phones served up a web page config file and gave the DC's address.

I pulled Group Policy Preference, accessed AD through LDAP, looked through their group rights/privs.

After reading through the massive amount of settings, I realized that they had limited remote access to only a small number of IT personnel, and even that was only a few.

I hadn't cracked any of those passwords.

They had implemented a Least Access Model...

Who does that?

Well screw you. I don't need to log into their workstation.

I'll log into their email!

So I do. I search for "password" in their emails, in their Skype Conversations, check their Outlook Notes section and Drafts.

I find a lot of personal passwords: Bank, PTA, Amazon...

But no corporate passwords.

I *did* find a recent email sent out by Corporate Information Security stating that email was going to implement MultiFactor Authentication in a week's time.

Well then... got lucky, didn't I?

I next went to their Single Sign On portal.

Every internal app, in one tidy space. A hacker's dream!

I click on one of the applications. It requires MultiFactor Authentication. So did the next one. And the next!

What sort of locked down prison is this?! A hacker's nightmare!

I see they're using Citrix.

It's behind MFA, but fine. I'll deal with that.

Citrix will get me remote access to an internal server. I need to hop onto an internal box. Get away from my rogue device and actually start pivoting.

I click on it. It asks me to enter a 6 digit pin.

There's a button that says "Click for MFA token" and gives a slightly redacted phone number (xxx)xxx-5309.

I bring up the email account (that didn't require MFA) and search for "5309". I find a signature of the user with their full phone number.

I call the phone number.

A woman answers.

"Good afternoon, Pam. I'm Josh from IT. We're about to migrate your Citrix instance to a new server. I'm going to send you a 6 digit number. I'll need you to read that off to me. As a reminder, IT will never ask for your password."

I already had her password.

She gave a hesitant, "Okay..."

I clicked on the "Click for MFA token" button and stated, "Alright, I've sent you the number. You should get a text. Please read it to me."

She said, "Umm, alright. Got it. It's 9-0-5-2-1-2."

"Thanks! Please stay off Citrix for about two hours!"

The 60sec timer was counting down. I typed the number into the MFA section and clicked OK.

And I log in.

Fuck you, MultiFactor Authentication!

Once in, I see... nothing. NOTHING!

This user didn't need Citrix, so her Citrix linked to NOTHING.

I had hacked into a broom closet.

Ok. This is ridiculous.

I can maybe crack a long password, but only if I get lucky and capture the right hash. Even with a cracked password of a tiny group of people, I have to bypass MFA. Each attempt, especially with a secured group, runs the risk of detection.

Damnit...

I go through everything else. I start running more & more aggressive scans, but they're still necked down below standard threshold for detection. I try every network and service based attack I know. I get some small things here and there, but no foothold.

I'm getting desparate.

I'm at the end of the 2nd day. I'm usually in databases at this point. I'm usually going through the CEO's email at this point. I'm usually taking pictures of people through their web cam at this point.

Fuck it. I'm going to break into the IT shack. I'm going to steal laptops.

I stay late.

Tell my new coworkers that I'm going to finish the Annual Security Training for my onboarding.

They nod. Everyone leaves.

The cleaning crew comes through. And leaves.

I'm alone.

I head to the IT/Helpdesk room. Find the door.

I look around and then go for it.

We'll pause here for a moment. I've got some other work to do. I'll be back in a couple of hours to finish out the story.

So there I was... about to break into the IT shack & steal laptops.

I had already tried various things to my own employee laptop, but I was not local admin and the disk was fully encrypted.

My goal was to find an old unencrypted laptop that had a common local admin hash on it.

I scanned the hall looking for anyone close by. I scanned the ceiling for security cameras.

I opened my mouth slightly and tilted my head to hear if anyone is coming from around the corner.

Nothing. I was clear to proceed.

I approached the door expecting to pick the lock, mess with electronic badge access, or pop a door of the hinges, but found a door stop wedged between the door and the frame.

Well there's a bit of good luck.

The door *did* have electronic access control & a solid backup lock on it. The hinges were security hinges.

But someone left it pried open that night.

I cracked the door & peered in expecting to see someone inside.

No one.

Fuck it. Seize the day. I opened the door & entered.

I had no idea why the door was propped open, but 80% of my job is user error, 56% is skill, 63% is adaptability, 90% is abusing "features", and a solid 80% is luck.

Only about 1% involves math...

Anyhow. #HailEris

I also didn't know if anyone was coming back soon, so I went to work.

I saw stacks of laptops in a corner. Various ages, makes, and models.

I weighed the risks of staying and getting caught in the the IT shack, or having a pile of laptops at my desk.

I chose my desk.

So there I am, hauling armloads of old laptops from the IT shack to my cubicle, a small Leaning Tower of Pisa forming under my desk.

Once I have a solid pile, I methodically try to boot each one from USB. Hoping to find a single laptop that doesn't have Full Disk Encryption.

I have a live USB of Kali with the program 'samdump2' on it.

I stick the USB in one, boot it up, try to mount the harddrive.

And get more and more frustrated as each one has FDE enabled.

Finally, after 30 laptops, I find three that are half ripped apart with clear harddrives.

Using 'samdump2', I pull the local NTLM hashes out of SAM and compare them.

I find a nonstandard local admin account called "ladm" on those three machines. Each hash is the same.

Oh thank Eris... They aren't using LAPS. They're sharing the local admin across boxes.

I crack this hash fairly easily. It was and the year was a couple years back.

Improper disposal of information assets. Gotta love it.

I tried using the creds to log into machines remotely & got the same error as before. Even local admin couldn't log in remotely... wtf!

I used the creds to log into my own work laptop, and it worked!

It bypassed Full Disk Encryption! A master key!

Ok.. okay! I can use this!

But when I logged with the administrative account, I noticed something odd...

I didn't have permissions to view the user area of the harddrive.

What? They limited access EVEN TO LOCAL ADMINS!?! Damn.

I needed to elevate privileges to System. I tried every trick I could think of.

Finally I ran a check for Unquoted Service Path vulnerabilities and found some! But the output said that my local admin user did not have permissions to write to the needed folders. Come on!

By this time, I'm hurting. I'm fatigued. Coming at the end of a second 17 hour shift. My brain is numb.

This was yet another dead end. Another series of hard fought, successful hacks, only to end with no access.

I had to get home. Get some sleep. Start again the next day.

The next day, I go over everything. Making sure I didn't miss anything. I check every thing that I can check. Scan everything I can scan. Do everything I can think of.

Small things here and there. Nothing worthwhile.

I call a colleague. A fellow member of the @Dallas_Hackers.

I finish telling him what I've tried and end on the "Unquoted Service Path" vulns. Told him how I got my hopes up and the output showed I didn't have privs.

He asked, "Did you try to exploit it anyway?"

I stopped.

I hadn't.

In my fatigue, I believed the output & hadn't tried.

Well. Here's to Entropy!

I attempted to write to the folder. The same folder that Windows told me I didn't have privs to write to.

And I successfully wrote to the folder.

Damnit Windows... lying to me again.

But cool. Fucking awesome. A new lead.

My colleague wrote up a quick malware loader executable in C pointing to a powershell payload I put together.

I tested it on my box (a risk) and it seemed to work fine.

It was a convoluted attack.But all I had.

I would:
- Set up a listener on my rogue device.
- Gain physical access to a laptop in the office.
- Log in w/localadmin creds.
- Upload the two-stage malware to the "Unquoted Service Path"
- Log out.
- Wait for user to log in & trigger.

Lunch Break was coming up. I smiled away invites to go out to eat from my new coworkers and hung back a bit.

I planned first to target IT while they were at lunch and pop one of their boxes.

But as I walked by the IT area I noticed that they were all at their desks! Eating lunch in front of their computers!

Don't they realize how unhealthy that is!? How lack of work/life separation and lack of breaks adds to stress?!

WHY DON'T THEY EAT LUNCH LIKE NORMAL PEOPLE?!?!

Screw it. I'm going to pop a box. Any box.

I walked around the office and finally found a set of desks that were empty. Accounts Payable / Accounts Receivable. Finance.

Okay. We're hacking into Finance.

I said something to one lovely little old lady that had come back for her purse. Let her know I was IT & upgrading computers. She nodded & smiled a nice smile before leaving.

Angerly, my face filled with spite and malice, I turned towards one of her team's computers & hacked it.

The deed done in less than 30 seconds. I set the chair and mouse back to how I found it. Did a quick once over to ensure everything looked fine. And, walked back to my cubicle.

And sat. Staring at my listener.

Lunch ended at some point. I lacked the will to conversate.

Just as I was about to lose hope, I see:

> Meterpreter session 1 opened

And then...

> Meterpreter session 2 opened
> Meterpreter session 3 opened
...
> Meterpreter session 7 opened

Holy shit!

I ran a quick GETUID and saw:
- NT AUTHORITY\SYSTEM

Oh Fuck Yeah!!!

Alright! Alright! Okay! Umm... Let's Go! Yeah!

Establish quick persistence, dump memory, and start rifling through their file system.

Some AP/AR finance info. Some clear text passwords. Sensitive information, but nothing major.

S'alright. It's a start. A foothold.

And then...

> Meterpreter session 1 closed

I try to hop sessions, but they're all closed. I ping the system, it's not responding. I port scan 445. Nothing. The system is offline.

Fuck. That. Noise.

I get up and begin a beeline towards to Finance department. What happened to my shells?!?!

As I round the corner, I see that lovely old lady talking to the biggest meanest dude wearing an IT polo.

I do a quick "Oh fuuu" & make to turn around when the old lady turns towards me, points a finger directly at me, and shouts "That's him! He was messing with our computers!"

I belted out a high pitched scream and made to run for it.

My back turned from one mean looking blue team, I ran in the opposite direction.

Only to run into two other blue team members. Looking quite pissed off and making it clear that I was in the wrong neighborhood.

I woke up, bloody, in an ergonomic office chair, my hands zipped tied behind me with the same zip ties they used to manage the server ethernet cables.

The head DFIR person stood in front of me, her knuckles raw, a small crew of Intrusion Detection Analysts behind her, grinning.

I croaked out one word... I needed to know...

"How...?"

The DFIR lead leaned down next to my ear and whispered, "No one in Accounts Payable ever runs Powershell..."

Alright... That last part had a bit of dramatization added to it.

But me running around the corner and into the little old lady reporting me to IT's Blue Team was real. They stopped me right there. Confiscated my machine and reported me.

CISO came in, validated my presence.

And the way they had detected me was real, too.

They got an alert that powershell was running on a system that did not belong to the small group of IT and Developers that ran powershell on a normal basis.

A solid, and simple, anomaly detection method.

Key Take Away's
==========

Blue Team:
- Least Privilege Model
- Least Access Model

- MultiFactor Authentication
- Simple Anomaly Rule Fires
- Defense in Depth

Red Team:
- Keep Trying
- Never Assume
- Bring In Help
- Luck Favors the Prepared
- Adapt and Overcome

Cheers.

Thanks for reading.