



# Police Station Pentest

From Zero Access to the Evidence Room

# ■ \$(whoami)

## **TYLER BOOTH, OSCP**

- Sr. Information Security Consultant at CDW.
- I have one cert and wrote a few blog posts on a currently defunct blog (dru1d.ninja). I guess that makes me a bit of an expert, amirite?
- Currently focusing my efforts on running red team operations, managing (and automating) our team's attack infrastructure and various security research projects.



# ■ Background

- My company was contracted to conduct a comprehensive security assessment of a large county in the Mid-Atlantic.
- The client wanted me to focus on both the security of the county and the local police force. The police chief was involved in these decisions; I fortunately didn't get into hot water like the folks at CoalFire.
- This included:
  - External security testing
  - Internal security testing
  - Wireless security testing
  - Social engineering (phishing and physical)
- I cannot reasonably cover my entire methodology. If you believe there are gaps, ask and I will fill them in to the best of my abilities.\*\*\*



# ■ External Path to Compromise

## RECONNAISSANCE

- Initial reconnaissance was performed.
  - I collected a list of employee email addresses and job titles. Public facing pages for government agencies typically have a lot.
    - <https://hunter.io/> helps
    - <https://github.com/vysecurity/LinkedInt> really helps
  - I also identify DNS subdomains and IP ranges using tools like:
    - <https://github.com/aboul3la/Sublist3r>
    - <https://github.com/OJ/gobuster>
    - <https://github.com/trustedsec/hardcidr>

# ■ External Path to Compromise

## EMAIL-BASED ATTACKS

- Initial access was obtained by sending what we call an "imgsrc" attack.
- This allows us to abuse how the Windows version of the Outlook client handles embedded UNC paths in HTML when there is no proper egress filtering in place.
  - Ex. 
  - The UNC path points to an Internet facing server running responder and logo.png doesn't even need to exist.
- A NetNTLM challenge-response will occur and key material will be captured for offline cracking using hashcat or JtR.

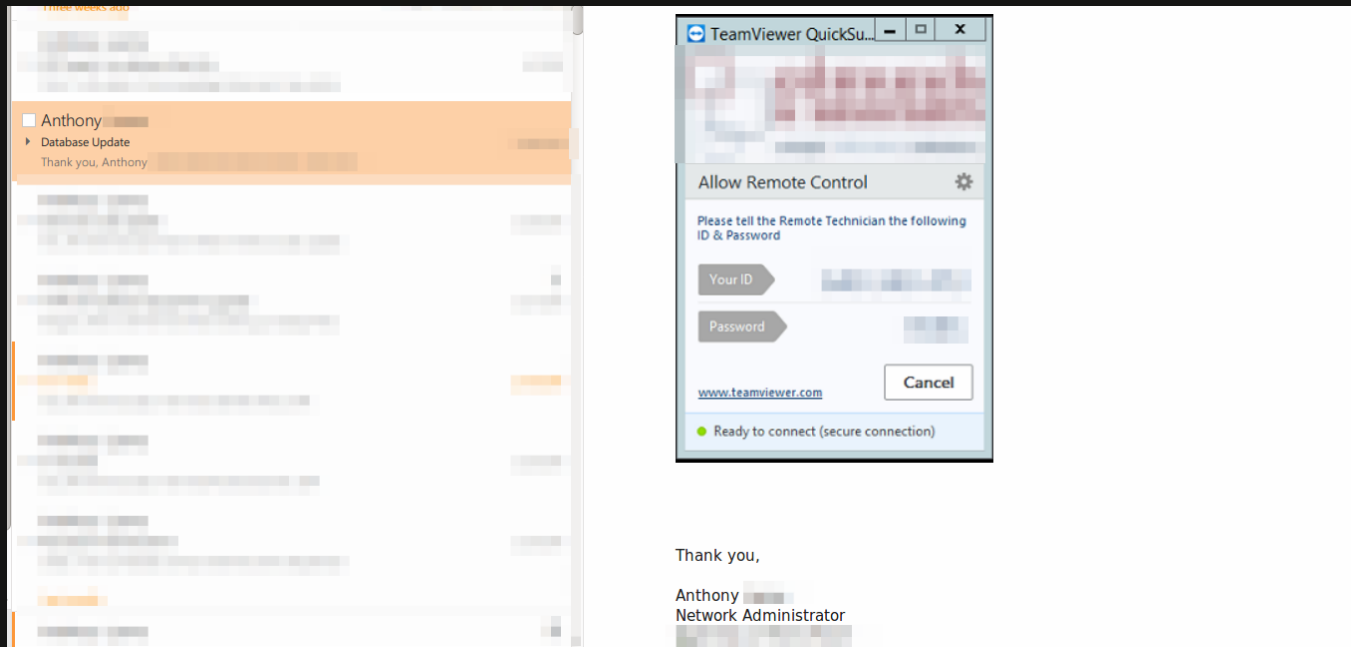
```
[+] Listening for events...  
[SMBv2] NTLMv2-SSP Client : 10.0.0.2  
[SMBv2] NTLMv2-SSP Username : PC-MANTVYDAS\mantvydas  
[SMBv2] NTLMv2-SSP Hash : [REDACTED]
```

(I snagged this sweet screenshot from Google Images)

# ■ External Path to Compromise

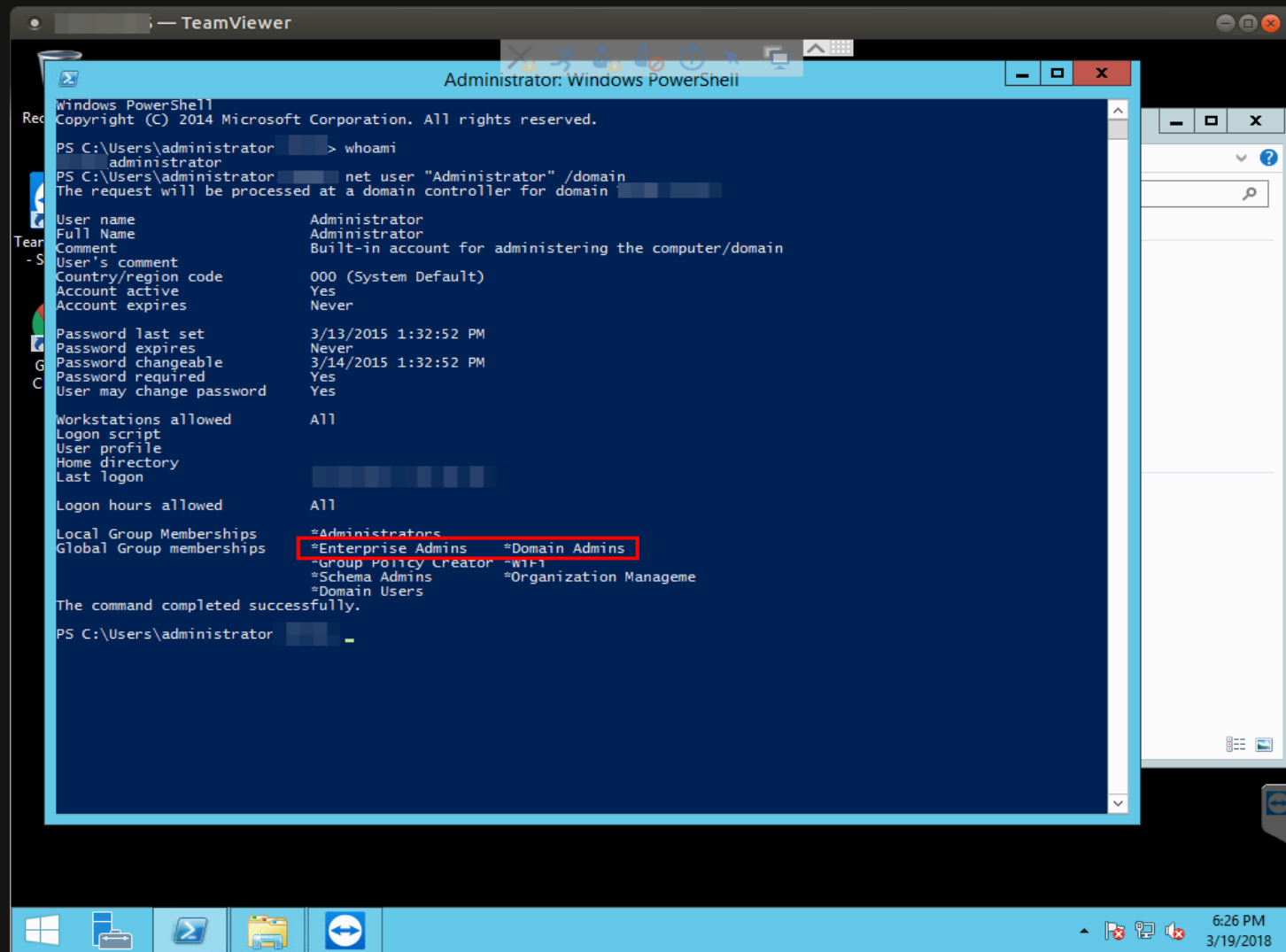
## IMPROPERLY DISTRIBUTED CREDENTIALS

- We've obtained a hash for a user and have logged into their email. However, this user doesn't have VPN access. :(
- There were some emails about a database upgrade from a network admin. This contained static TeamViewer credentials.



# ■ External Path to Compromise

## EASY DA



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator > whoami
administrator
PS C:\Users\administrator > net user "Administrator" /domain
The request will be processed at a domain controller for domain

User name: Administrator
Full Name: Administrator
Comment: Built-in account for administering the computer/domain
User's comment:
Country/region code: 000 (System Default)
Account active: Yes
Account expires: Never
Password last set: 3/13/2015 1:32:52 PM
Password expires: Never
Password changeable: 3/14/2015 1:32:52 PM
Password required: Yes
User may change password: Yes
Workstations allowed: All
Logon script:
User profile:
Home directory:
Last logon:
Logon hours allowed: All
Local Group Memberships: *Administrators
Global Group memberships: *Enterprise Admins *Domain Admins
                        *Group Policy Creator *W1F1
                        *Schema Admins *Organization Manageme
                        *Domain Users

The command completed successfully.

PS C:\Users\administrator >
```




# ■ External Path to Compromise

## NOTHING IS SAFE




- After compromising the entire domain, I set my sights to more interesting endeavors.
  - What's in these database servers?
- I moved laterally to a production database and immediately found something that caught my attention.
  - Tables related to "GuardAll"
  - I had seen this before, but for those who don't know...


**GSR** PX/QX Series Software



- Guardstation is a software package to manage, maintain or monitor your security system enabling configuration, integration and control of our PX/QX equipment.
- All are Windows-based and designed to run on a PC with applications ranging from controlling your access systems, to full remote operation of the system, to the use of integrated maps.
- All variants of the Guardstation are ordered under the same part number and a form filled out to requested the desired features. Each feature is priced individually.

Security Control	Basic software package
Access Control	Enabling full control and management of access system(s)
Interactive Maps	Integrated maps graphical package
Windsor 500 Support	Allowing management of Windsor 500 panels
Polling	Enabling verification of connection to a panel
Remote	Allowing full remote operation of the security system



**Guardall**  
A UTC Fire & Security Company

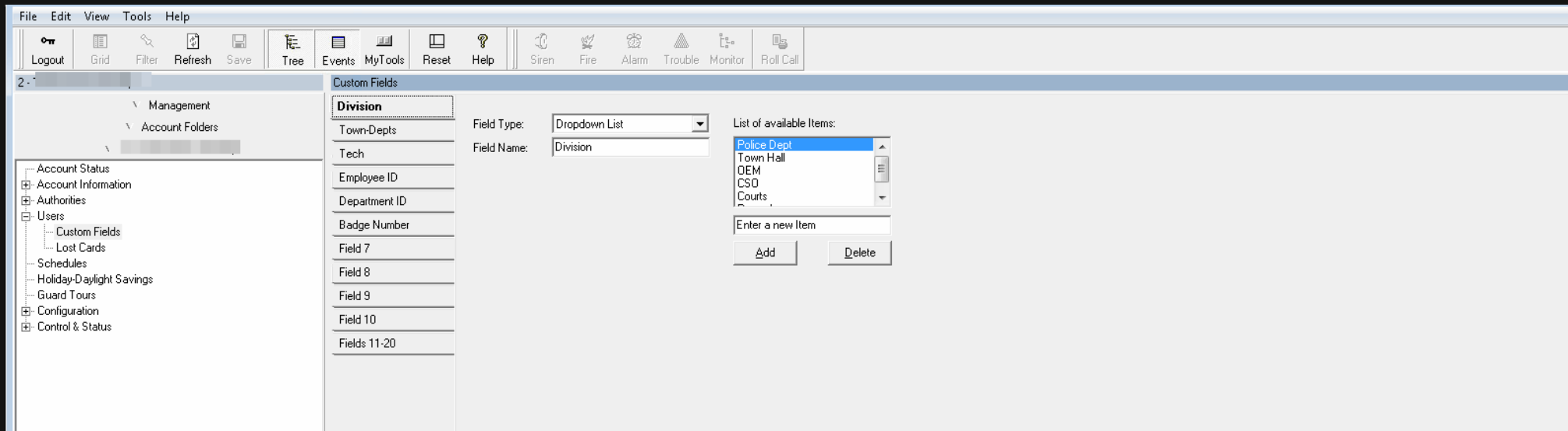
It's in our nature to protect  
**Secure Solutions**



# ■ External Path to Compromise

## NOTHING IS SAFE

- After a bit of messing around, I was able to crack a password that was stored in the SQL database and obtain access to the access control system.



- I then created my own badge with the system and a ProxMark3 I had at home. I'll save this for later. ;)

# ■ Physical Social Engineering

## THE ART OF THE PRETEXT

- When we plan to infiltrate a building, we tend to consider *why* we would be there in the first place.
- I knew from my initial reconnaissance that a specific telecom company serviced the county and its E911 system. This seemed like the perfect way into restricted areas.
- I needed to look the part and procured:
  - A clipboard with a fake work order
  - Some old work boots
  - A toolbelt
  - A telecom company uniform (thanks, eBay!)



# ■ Physical Social Engineering

## HOW THIS ALL ENDED

- I showed up at the police station and was waived in by the officers. They didn't really care to check my backpack or toolbelt.
- I obtained unfettered access to the police department. No one stuck around to watch me, and I was able to use my created badge to access restricted areas.



# ■ Takeaways for Defenders

- *Filter traffic on egress!* Why would you need SMB/CIFS outbound to arbitrary IPs?
- *Implement a more stringent password policy!* Even if key material gets compromised, it'll make it exponentially harder to crack offline.
- *Don't share credentials through insecure channels!*
- *Use privileged access management (PAM) and adhere to the tiered administration model!* Don't let DAs leave the sanctity of the Domain Controllers. Use server admin accounts or workstation admin accounts to manage other assets.
- *Properly vet folks who show up onsite for "business"!* This whole physical infiltration of not one, but two facilities, could have been prevented if someone would've just checked with management before letting me wander around unattended.

# ■ Obligatory Q&A with the Red Team

- Provide me questions and I will provide you answers.
- Thanks for hanging out and listening. Don't forget to tip your waitress.
- Also, obligatory self-plug if you're interested in having something like this happen to you: <https://www.cdw.com/content/cdw/en/solutions/cybersecurity/security-assessments.html>