CC:IIE Grants

• Same grants Mark discussed earlier
• Similar to “Above the Net”
• CC:NIE ==> Science Research
Phase 0

- Linux remote access
- VNC through an HTTP channel
- Federated web SSO ==> connection to a virtualized Linux environment
- Application containers for performance, scalability
- Last year
Linux VM
Apache/Shibboleth SP
NoVNC
Docker Engine
Orchestration

research
data

Same or different
Linux Host

Linux VM
Apache/Shibboleth SP
NoVNC
Docker Engine
Orchestration

websock
websock
websock

authN,
authZ,
request

browser

Dynamic port
noVNC

cfg
Reaction

- Faculty loved it, used it (heavily)
- What about Windows?
  - Some researchers prefer Windows
  - Some data analysis demands Windows
Phase I

- What if there were Docker container?
  - (Xvnc=>Xserver=>RDP client)
- Short-lived domain-joined Windows virtual desktops
- Federated web front-end; dynamic credential assignment
- Dynamic software deployments via Microsoft AppV
- Federated front-end authentication
- Zero-install (researchers hate installations)
Linux VM
Apache/Shibboleth SP
NoVNC
Docker Engine
Orchestration

MySQL

Active Directory
user creds
group memberships
data access
port #s
vm states

SMB Homedirs
grps
Appv

Short-lived Windows VM
fixed user, dynamic cred

XfreeRDP
Xvnc
Websockify

user,port

Linux VM
Appv
grps
websock
websock
websock

authN, authZ, request

Dynamic port
noVNC

browser
Quick Demo 1
Schaufenstern
Enter the Dragon

- APT attacks against HE AD’s, 2013-2015
  - Nation-state actors — maybe China?
- Targeting R1 user credentials
  - Research data
  - Possibly other purposes
Analyze the Dragon

- Consistent MO using MS “convenience”
  - Compromise unprivileged acct/machine
  - Local privilege escalation
  - Await more privileged login
  - Capture credential hashes from memory
  - Pass-the-hash, smash-and-grab vs. DC
Slaying Taming the Dragon

• MO requires:
  
  • Credential exposure to unprivileged windows client
  
  • Credential durability (user, password persist)
  
  • Authorization durability (user, privileges persist)
  
  • Tackle distributed admins, then domain admins
Slaying Taming the Dragon

• Break the APT MO:
  • Move durable privileged creds off Windows
  • Make in-use creds short-lived
  • Make in-use privilege short-lived
• Proconsul…
Quick Demo 2
Proconsul
Ongoing Work

• AD propagation delay issues - adjustments pending

• Consul for Domain Admins, Proconsul for distributed

• Consul database dynamic suppression of automated privilege group management (domain admin squashing)

• Performance, features
  • Windows Audio
  • HW graphics acceleration