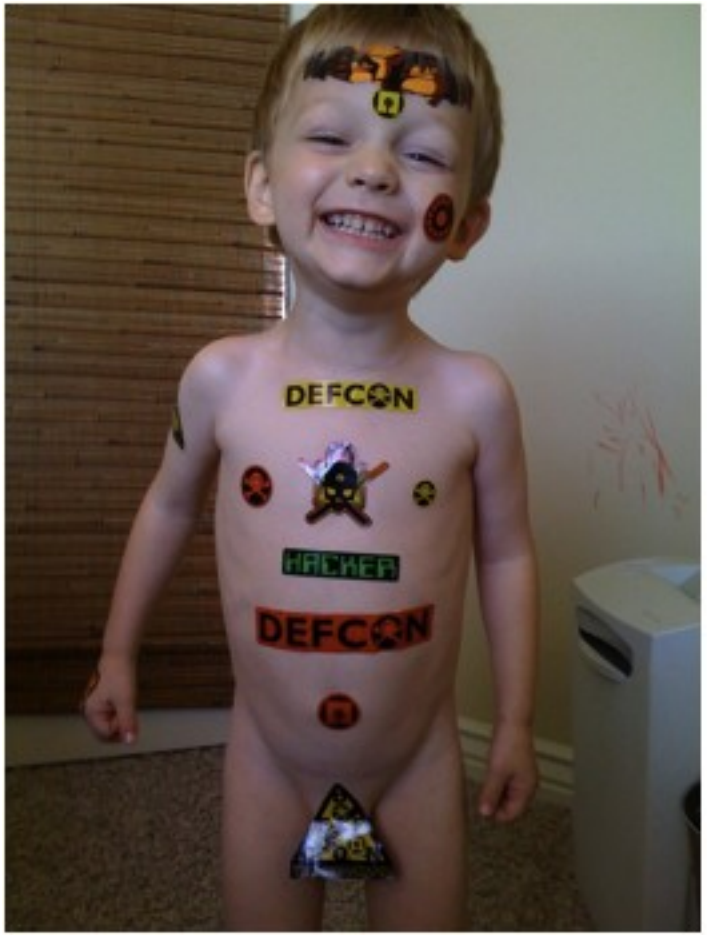
A Day in the Life of a Penetration Tester

Married 11 Years

The Boys



Formal Education

AS in General Education

BS in Technology Education

- Computer Science minor
- Electrical Engineering minor

MBA in International Technology

Certifications

GCFA	GIAC Certified Forensics Analyst (GCFA)
GCIH	GIAC Certified Incident Handler
CISSP	Certified Information Systems Security Professional
SFCP	SourceFire Certified Professional
CCNA	Cisco Certified Network Associate
LPIC1	Linux Professional Institute Certification Level 1
LCI	Linux Certified Instructor (Sair Linux/GNU)
LCP	Linux Certified Professional (Sair Linux/GNU)
Security+	CompTIA
Linux+	CompTIA
A+	CompTIA

Professional Experience

New Horizons – Instructor (Linux & Cisco)

Meeas Technology – Owner

Linux Networx – Support Technician II

ITT Technical Institute – Instructor (ISS)

JetBlue Airways – IT Security Architect

InGuardians – Senior Security Analyst

Interests & Hobbies

Rock Climbing

Canyoneering

Spelunking

Hiking

Hunting

Cycling

Falconry

A Real Play-by-Play Pen Test

- A Large International Bank
- Internal Penetration Test
- Approximately 200,000 IPs
- 2 Pentesters Onsite
- 5 Days to Complete
- Empty Classroom

Monday 9am

nmap across all 196,608 IPs in our scope

- Port sweeps across 6 TCP ports
- Found 8000+ hosts
- performed reverse lookups for live hosts

nmap -sS -n -v -p 22,23,80,443,445,3389 --reason -oA cur/6-TCP-196 10.10.0.0/16

- About 12 minutes per class B

Monday 2pm

Started Qualys sweep for SNMP across all subnets

- found multiple printer and a few Windows machines were readable
- completed in about 12 hours

Started Nessus scans on highly populated segments in the datacenter

- discovered a server vulnerable to MS06-040

Monday 5pm

Started qualys scan for standard ports across all subnets

- scanned 196,608 IPs for 1800 tcp ports, 180 udp ports, and all vulnerabilities
- completed on 8/27/08 in the early morning hours (36 hours)
- found 7232 hosts, 25948 confirmed vulns, 12292 potential vulns, & 114954 infos

Monday 6pm

Owned a Win2000 Server via MS06-040 exploit

- discovered LMHASH was enabled on all servers
- obtained 10 local account hashes
- cracked 8 passwords from wordlist & incremental attack with john (8 hours)
- one of the accounts was a renamed local admin for all servers, but not workstations

Tuesday 10am

Used the local admin account and fgdump on all servers in 2 of the 3 subnets

- obtained 319 cached domain credentials (6 hours)
- obtained 10 password from wordlist attack with john (10 hours)
- one of the accounts was "user-D", who had limited domain privileges

Tuesday 12pm

Call came in saying our Qualys scan knocked over some scheduling servers

- paused scan around 12pm
- worked for 2 hours to bring up a transparent firewall to prevent scanning of port 1721
- started scan back up around 2pm

Wednesday 10am

Owned a Solaris server with sadmind

- obtained 39 un-salted crypt hashes
- cracked 14 passwords from wordlist attack with john
- cracked 2 password from incremental attack with john

Wednesday 12:30pm

Used "user-D" domain credentials, added our own VM host to nt_a domain

- used MS Admin Pack to navigate the AD tree for information
- identified all 22 accounts with full domain admin access

Wednesday 2pm

Owned a Win2000 Workstation with RPC-DCOM & MS06-040

- obtained 2 local account hashes
- cracked both accounts with john ("Administrator":"admin" & "Guest":"")
- determined this was a non-standard configuration

Owned a XP Pro with RPC-DCOM exploit

- couldn't pull hashes & couldn't figure out why

Wednesday 2:30pm

Owned another 2000 Pro with MS06-040

- pulled LMHASH for two accounts
- cracked "local-V" and confirmed that it was the local admin account renamed
- discovered that it was an old password and that this machine had missed the update
- discovered "local-D" is a local service account with admin rights, but we were unable to crack it

Thursday 11am

Tried pulling SAM database physically with a bootable Linux CD, but HD was encrypted

- discovered all workstations (and servers?) use full disk encryption

Next 12 hours were long and frustrating!

Thursday 7pm

Decided to purchase full LMHASH tables for ophcrack ($99) and started download (3 hours)

- cracked local-D with ophcrack XP-Special table (~15 minutes)
- Used it to obtain current hash for "local-V"
- cracked "local-V" with ophcrack XP-Special table (~2 minutes)

Thursday (Friday 1am)

Started fgdump from all workstations across whole IP scope

- discovered cached hashes for 3 domain admins
- failed to discover likely workstations of the domain admins (probably logged off)

Friday 10am

Discovered AV was blocking many of our tools

- modified all needed binaries to bypass AV
  - used LordPE to alter binaries
    - usually shrinks the binary (pulls out Nulls, etc...)
  - Used hex editor to change exposed copyright strings

Friday 12pm

Started using pexec to push/run whosthere.exe on all workstations through the whole scope

- obtained LMHASH values for 6 of the domain admins
- cracked them with ophcrack
- used them to run fgdump on domain controller
- Harvested ~20,000 usernames, most with LMHASH

Lessons Learned

- Use whatever resources you have available
  - Like the 15 computers in the room
- Don't waste your time with john for LMHASH
  - Use ophcrack/rcrack
- fgdump is CPU intensive on large DC's
  - Have it skip cache and history dumps
- Don't kill fgdump before it finishes!!! Especially on domain controllers for large enterprises. ;-)
  - If you do, call Tom!

Contact Information

Justin Searle
justin@meeas.com
801-784-2052
@meeas
Also on LinkedIn and Facebook