SecureSet Capstone Day 1

Article Summary

**Article 1:** ACME Company Reports Massive Data Breach- SOC Has Little To No Understanding Why

Observations:

1. A Medium-sized company was breached
2. Manufacturer of phone cases with contracts with major corporations
   1. Apple, Samsung, HTC
3. The company holds some of these device manufacturers’ intellectual property on new phone models- including size, buttons, camera placement and more.

Questions:

1. Is there a specific APT or group that targets companies like ACME?
2. What about targeting larger corporations?

Article 2: ACME Company Responds to Data Breach- Hires New CISO after E. Fudd Quits

Observations:

1. Elmer Fudd, previous CISO quits for unknown reasons
2. Wiley E Coyote brought on as new CISO

Questions:

1. Elmer Fudd, insider threat?

Article 3: Fresh ACME CISO Fires Out of House Security Operations Center

Observations:

1. The new ACME CISO, Wiley E Coyote, fired the outsourced security company: Cyber Security Stooges.
2. The company was the single point of failure for the breach and directly managed by E. Frudd.
3. The now-disgraced CISO, Frudd was not available to comment on the recent breach.
4. Coyote said “While I regret the decisions made by my predecessor, I am not willing to comment on any reasons he may have left or the cause of the breach

Questions:

1. Fudd and Coyote both refuse to comment on Fudd’s quitting or the reason for the breach. Was the breach due to Fudd’s incompetence or his malicious actions?

Article 4: Cyber Security Stooges Responds to the ACME Breach

Observations:

1. Cyber Security Stooges are a small, but growing Security Operations Center who had ACME as one of their accounts for 3 years.
2. They explained “This was as far as we were able to investigate- a zero-day vulnerability. We shouldn’t be under any scrutiny, there was nothing we could do.
3. Larry spoke positively of Frudd, saying “I always thought he had his head on straight for security. The plans we implemented seemed to be fault-proof, so we had little communication with him.”

Questions:

1. Stooges spoke positively of Fudd, yet they had little communication?

Article 5: ACME CISO Unveils In House SOC

Observations:

1. Wiley E Coyote has announced the creation of an in house Security Operations Center.

Questions:

Article 6: Another ACME Update: Coyote Hires Road Runner Corporation

Observations:

1. ACME’s Buford T. Justice SOC
2. Their per diem rates make it so that problems are still able to be tackled in a cost-effective way- while being able to use them as little as an organization needs

Questions:

1. Is ACME in financial trouble?

Initial Questions for Gary

1. What specific info was exfiltrated?
   1. They are not sure what was exfiltrated and would like for us to find out.
2. Are they still possibly in the network?
   1. As far as they know they are no longer in.
3. Do we have a contact in the new SOC? (Buford T. Justice SOC)
   1. Assume yes, any questions for SOC will go to Gary.
4. Do we know of any APT’s or groups that target companies like ACME or larger corporations that they are partnered with?
   1. No visibility and need us to determine.
5. Where is the intellectual property from any other companies located?
   1. On local servers
6. What was Fudd’s behavior like before he quit?
   1. Not allowed to talk about too much as it is an HR issue, but was acting suspicious and was let go.
7. What IP’s can we scan with the vulnerability scanner?
   1. Pull data and give to us. TBD
8. What is the site to scan?
   1. Pull data and give to us. TBD
9. Do we have backups?
   1. No, not at this time, provide recommendations.
10. What are the critical assets?
    1. Something they would like to get from us as a recommendation during the brief.
11. What, if any, compliance regulations do ACME have to adhere to?
    1. Production company, Sarbanes-Oxley, PCI-DSS
12. What 3rd party or in house software are they using?
    1. Pull data and give to us. TBD
13. Do you have a patch update document?
    1. Pull data and give to us. TBD
14. Can we get access to any of the other servers or stations?
    1. Pull data and give to us. TBD
15. Can we have a network diagram?
    1. All the same VLAN, recommendations during the brief.
16. Can we have access to any and all logs?
    1. Pull data and give to us. TBD
17. What if any crypto is Acme using?
    1. Not sure!
18. What is the budget for the project, if any?
    1. Sent on Slack
19. Do we need to sign and upload the MOU?
    1. Sent on Slack

Notes:

* Vulnerability Scanner UN and PW:

Username: administrator

Password: ArrakisTheDesertPlanet1!2@

Change password of the vulnerability scanner

Network architecture - change it

Recommendations & Tasks

* New network diagram - Ryan
  + Pricing (asked the question on Slack of budget considerations), Created Diagram
* Vulnerability assessment - Andrew & Dillon
* Production companies compliances - Alex
  + PCI-DSS & Sarbanes-Oxley
* Backups - Matthew
  + Research
* Threat analysis - Attached documentation to GitHub

|  | Echo |
| --- | --- |
| Vulnerability Scan Ubuntu 16.04 | 172.16.1.16 |
| Honeypot Ubuntu 16.04 | 172.16.0.248 |
| Windows 2012 Active Directory | 172.16.0.255 |
| Windows 2012 Spiceworks | 172.16.0.253 |
| Ubuntu 18.04 | 172.16.1.0 |
| Ubuntu 16.04 Machine 1 | 172.16.0.254 |
| Win10 Machine 1 | ? |
| Win10 Machine 3 | 172.16.0.251 |
| Ubu-14.04-GA-Alpha | 172.16.0.249 |
| Linux | 172.16.0.250 |
| Ubuntu 16.04 Machine 2 | 172.16.0.252 |
| Win 10 Machine 2 | 172.16.1.17 |
| Win 10 Machine 4 | 172.16.1.15 |

SecureSet Capstone Day 2

Tasks:

1. Identify vulnerabilities from the scan conducted yesterday.
2. SMB/CIF on one system, likely point of entry
3. Cross-reference list from the scan with APTs.
4. Crack username and password lists on the systems.
5. Identify vulnerabilities within systems, find logs and research incident breach
6. ID the potential exploited system, find the attack and contain.
7. Get answers to questions from Acme Co. CISO
   1. Can we change default usernames and passwords?
      1. Recommendation to do in the briefing.
   2. What is the ACME Co budget for the breach?
      1. No budget, Make Low, Medium and High-cost COAs.

* Identified SMB and CIFS as a known vulnerability within Ubuntu Machine 16.04

<https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-36408/Microsoft-Server-Message-Block.html>

SecureSet Capstone Day 3

* 1. Perpetrator used Directory Traversal, Enumeration, XSS and then a vulnerability scan on 14 Dec 17 to find the vulnerable areas in Acme Co.
  2. Then conducted a phishing campaign using GoogleUpdateSetup.exe to install a possible RAT or virus of some kind into the system.
  3. Then on 16 Dec 17 used an ICMP flood on port 53 to mask the probing for open ports on the system.
  4. Then you can see a malware communication with a command and control server through DNS.
  5. After that possibly used the vulnerable SMB/CIFS system to open a shell using port 22 and exfiltrate data.

SecureSet Capstone Day 4

Tasks:

1. Finish analysis of systems
   1. Breakdown systems by person
   2. FU Rootkit installed in Ubuntu 16.04 Machine 2
2. Correlate data from the logs analysis on Day 3 to the physical machines & determine the affected machines
3. Make an excel sheet of all users
   1. Ask Acme Co, for list?
4. Finish compliance standards and write up the report
5. Make recommendations to Acme Co. to fix open breach vulnerabilities & build servers.
   1. Build servers - Active Directory and Spiceworks

Notes:

* Windows 10 machine 4
  + network connection hacked
  + Spotify installed(3rd party software permissions)
  + Crypto miner
  + Disable webcam light
  + Ethical hacking tutorial(web link)
* Ubuntu 16.0.4
  + machine 2 vmlinuz.old should be removed
* Windows 10 machine 1
  + No system 32. Can’t run anything
  + Missing critical files

Final Recommendations

1. Change network architecture to….
2. Compliance standards
3. Update all machines

Machines

Ubuntu 18.0.4

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin

systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin

syslog:x:102:106::/home/syslog:/usr/sbin/nologin

messagebus:x:103:107::/nonexistent:/usr/sbin/nologin

\_apt:x:104:65534::/nonexistent:/usr/sbin/nologin

uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin

avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin

usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin

dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin

rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin

cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin

speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false

whoopsie:x:112:117::/nonexistent:/bin/false

kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin

saned:x:114:119::/var/lib/saned:/usr/sbin/nologin

pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin

avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin

colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin

hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false

geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin

gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false

gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false

administrator:x:1001:1001:administrator,,,:/home/administrator:/bin/bash

sblackburn:x:1002:1002:Susan Blackburn,,,:/home/sblackburn:/bin/bash

triddle:x:1003:1003:Tom Riddle,,,:/home/triddle:/bin/bash

dennis:x:1004:1004:David Ennis,,,:/home/dennis:/bin/bash

lduval:x:1005:1005:Leslie Duval,,,:/home/lduval:/bin/bash

nwrangler:x:1006:1006:Nick Wrangler,,,:/home/nwrangler:/bin/bash

elsad:x:1007:1007:Elsa Drawl,,,:/home/elsad:/bin/bash

bwittacker:x:1008:1008:Bill Wittacker,,,:/home/bwittacker:/bin/bash

rmattis:x:1009:1009:Rachel Mattis,,,:/home/rmattis:/bin/bash

Ubuntu machine 2

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false

systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false

systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false

systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false

syslog:x:104:108::/home/syslog:/bin/false

\_apt:x:105:65534::/nonexistent:/bin/false

messagebus:x:106:110::/var/run/dbus:/bin/false

uuidd:x:107:111::/run/uuidd:/bin/false

lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false

whoopsie:x:109:117::/nonexistent:/bin/false

avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false

avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false

dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false

colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false

speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false

hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false

kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false

pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false

rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false

saned:x:119:127::/var/lib/saned:/bin/false

usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false

sblackburn:x:1001:1001:Susan Blackburn,,,:/home/sblackburn:/bin/bash

triddle:x:1002:1002:Tom Riddle,,,:/home/triddle:/bin/bash

dennis:x:1003:1003:David Ennis,,,:/home/dennis:/bin/bash

lduval:x:1004:1004:Leslie Duval,,,:/home/lduval:/bin/bash

nwranger:x:1005:1005:Nick Wrangler,,,:/home/nwranger:/bin/bash

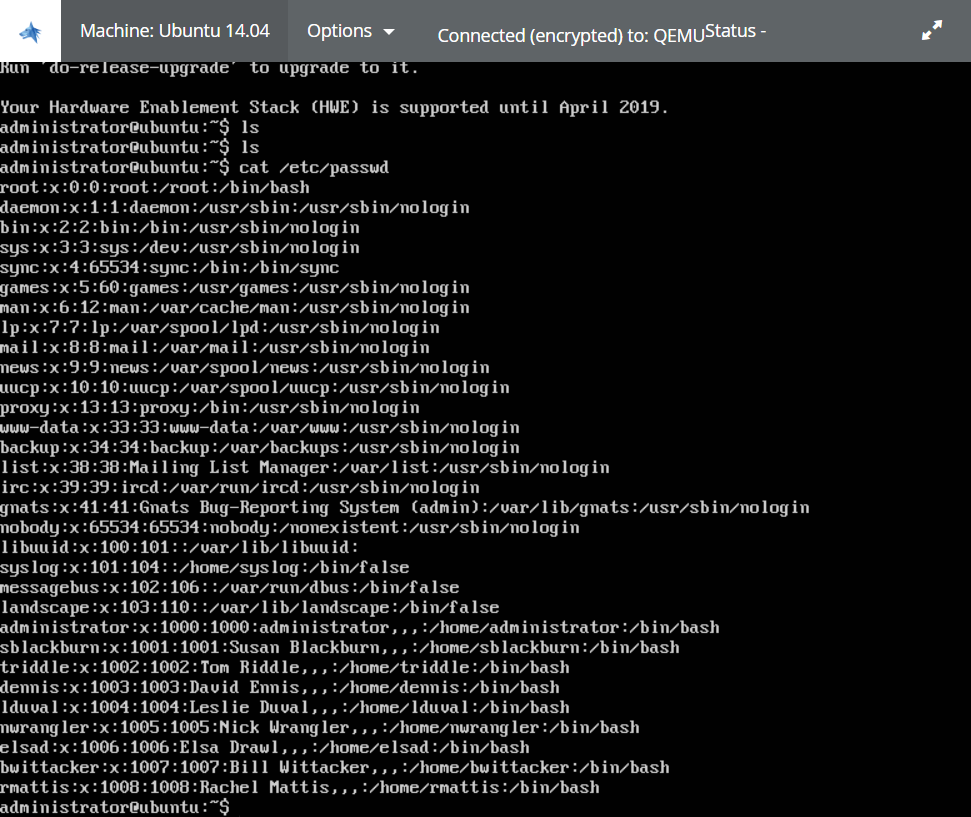
elsad:x:1006:1006:Elsa Drawl,,,:/home/elsad:/bin/bash

bwittacker:x:1007:1007:Bill Wittacker,,,:/home/bwittacker:/bin/bash

rmattis:x:1008:1008:Rachel Mattis,,,:/home/rmattis:/bin/bash

administrator:x:1009:1009:Administrator,,,:/home/administrator:/bin/bash

Ubuntu 14.0.4



SecureSet Capstone Day 5

Tasks:

1. Finish analysis of systems, Linux/Ubuntu
2. Build recommendation list for the Acme CISO
3. Build network diagram and finish cost analysis for the brief
4. Build briefing slides for the C-suite

* Ubuntu machine 2 -> Network -> SecureSet -> Share -> Rootkit!!
* Ubuntu machine 2 -> 4thelulz is empty
* Linux -> upgrade -> backup server
* Ubuntu 14 -> upgrade -> file server(Data at rest encryption)

Recommendations:

1. Change Admin Username and Passwords
2. Update/patch all machines
3. Reimage, update/patch all machines that cannot be fixed with a simple patch
4. Create and implement Active Directory, set policy to change password upon 1st login attempt
5. Create and implement Spiceworks server and setup to manage the system and helpdesk