Enabling effective Hunt Teaming and Incident Response

—

(with zero budget and limited time)

whoami

Jeff McJunkin, Senior Technical Analyst
Counter Hack Challenges
Certifications: Yes*

*CISSP, CCNA, GSEC, GCED, GPEN, GCFA, GCIH, GMOB, GXPN, GREM, GCIA, hopefully soon GSE

What do I do?

- Expert witness (digital forensics)
- TA (and soon, *here in Portland*, teach!) for SANS
- Create challenges to help people learn offensive and defensive security
  - (SANS NetWars Tournament)
- Background in systems / network administration


SANS
NETWARS
TOURNAMENT

Disclaimer on tools

- I will discuss specific tools
- I’m not paid to endorse these tools

They’re just examples that I’ve found to work well

(Well, usually)

What is hunt teaming?

Step 1) Assume compromise

(It turns out this is very realistic)

What is hunt teaming?

Step 1) Assume compromise

(It turns out this is very realistic)

Step 2) Find your compromised hosts

What is hunt teaming?

Step 1) Assume compromise

(It turns out this is very realistic)

Step 2) Find your compromised hosts

Step 3) Find how they were compromised (forensication time!)

What is hunt teaming?

Step 1) Assume compromise

(It turns out this is very realistic)

Step 2) Find your compromised hosts

Step 3) Find how they were compromised (forensication time!)

Step 4) Set up preventative and detective controls

What is incident response?

Step 1) Notice an incident. Example incident sources include...

- Help desk notices malware on system
- Network team notices lots of outbound traffic from a usually-quiet machine
- Your university is featured on https://krebsonsecurity.com/

Step 2) Hair on fire, stop the bleeding!

What is incident response?

Step 1) Notice an incident. Example incident sources include...

- Help desk notices malware on system
- Network team notices lots of outbound traffic from a usually-quiet machine
- Your university is featured on https://krebsonsecurity.com/

Step 2) Hair on fire, stop the bleeding

Step 3) Learn, implement detective and preventative controls

Note the difference

Hunt teaming is **proactive.**

Incident response is **reactive.**

Learning how you're owned proactively is preferred, but we ***all encounter surprises.***

What do we prepare for?

- Prevention, prevention, prevention
- Penetration testers?
- Things that make our bosses upset (Critical Nessus findings)
- Antivirus
- Patching
- Compliance
- Protecting The Perimeter

An aside on compliance...

- Compliance is probably a net positive
- HIPPA, PCI, CJIS, etc.
- But sometimes we can focus too much on compliance and miss focusing on **security**

What actually happens?

Focus on **DATA**, not anecdotes.

The Verizon Data Breach Report is perhaps the best source of actual compromise data we have in this industry.

	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31–33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44–45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48–49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Figure 2.

Security incidents by victim industry and organization size

What actually happens? - Target 2013 Breach

40 million credit cards stolen

What weaknesses were used?

- Third-party network access
- No review of security logs
- Lack of segmentation

What actually happens? - Home Depot 2014 Breach

56 million credit cards stolen

What software was used?
Details are still forthcoming, but…

- Malware that scraped RAM for credit card information
- Same malware family as Target!
- Likely Domain Admin-level access by the attackers
- Current indications: Attackers targeted self-checkout lane computers

But those examples are too big, and not us!

Good point. **Here's a smaller, local example:**

C&K Systems, Inc.

C&K Systems, Inc.

- Who are they?
  - Third-party payment vendor for Goodwill
- What happened?
  - No details yet
- Who else was affected?
  - Two other unnamed clients

Notice a growing tendency for “watering hole” attacks

C&K Systems, Inc.

How long until they noticed the breach?

C&K Systems, Inc.

How long until they noticed the breach?

18 MONTHS.

Cyber Kill Chain

RECONNAISANCE

WEAPONIZATION

DELIVERY

EXPLOIT

INSTALLATION

COMMAND AND CONTROL (CIC)

ACTIONS or OBJECTIONS

Usually Exfiltration

Today’s attacks versus Yesterday’s defenses

- How do you detect memory-only malware?
  - Never touching the hard drive
- What logs are normal from your machines?
  - I.e., do you have a baseline to compare against?
- How often do you review these logs?
- What if the attacker has “gone native”?
  - Example: No “hacker tools”, just PowerShell and valid credentials

A useful thought exercise…

Imagine if there were no anti-virus.

Imagine if all your computers had unpatch-able known exploits.

(Not too difficult, given XP and Server 2003's end of life)

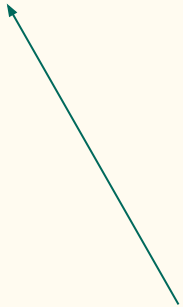
Where do we stand a chance?

1. Exploit
2. Installation (persistence)
3. Command and Control
4. Exfiltration (...maybe)

What's the difference?

Prepare, hunt, respond, learn

Prepare, hunt, respond, learn



Get useful data ahead of time (program execution, centralized logging, persistence, evidence of pivoting)

Prepare, hunt, respond, learn

Assume compromise. Act accordingly.

Prepare, hunt, respond, learn

Find evil and exterminate it.

Prepare, hunt, respond, learn

Red team is threat emulation, blue team should be able to describe red team’s actions

Mind the gap

- How do you track persistence?
- How about new program execution?
- How about data exfiltration? Full packet capture?

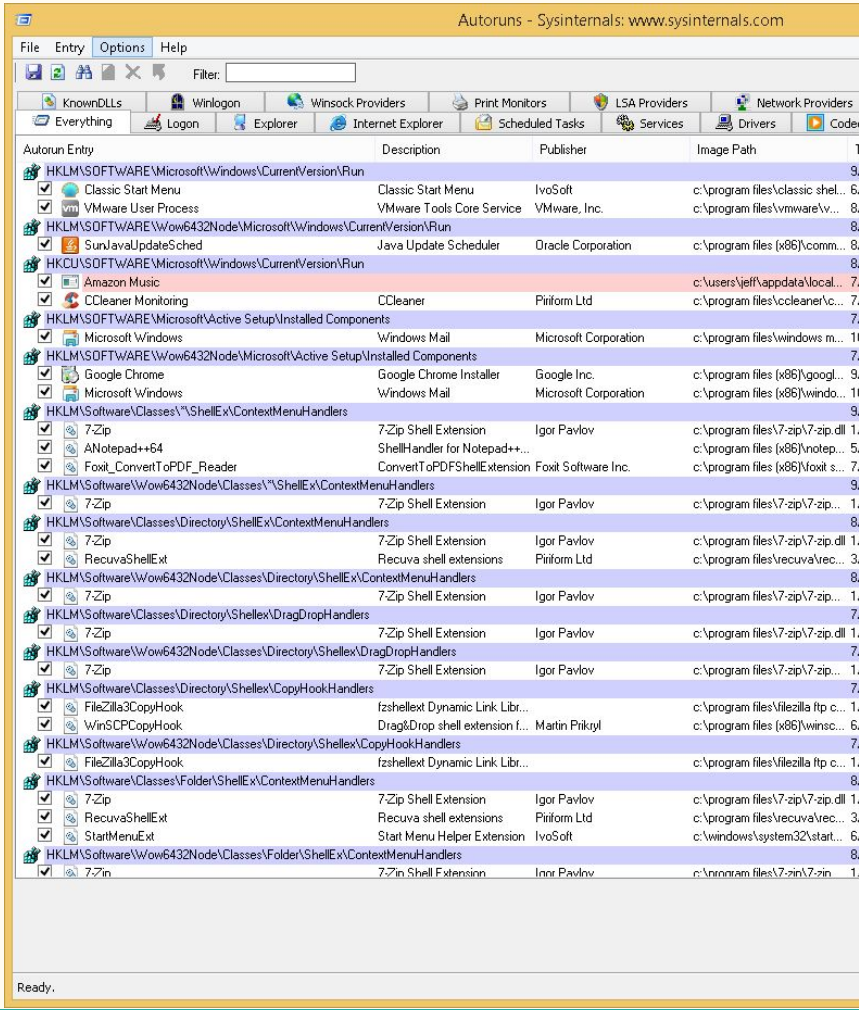
Persistence

How many methods of persistence do you know of?

Persistence

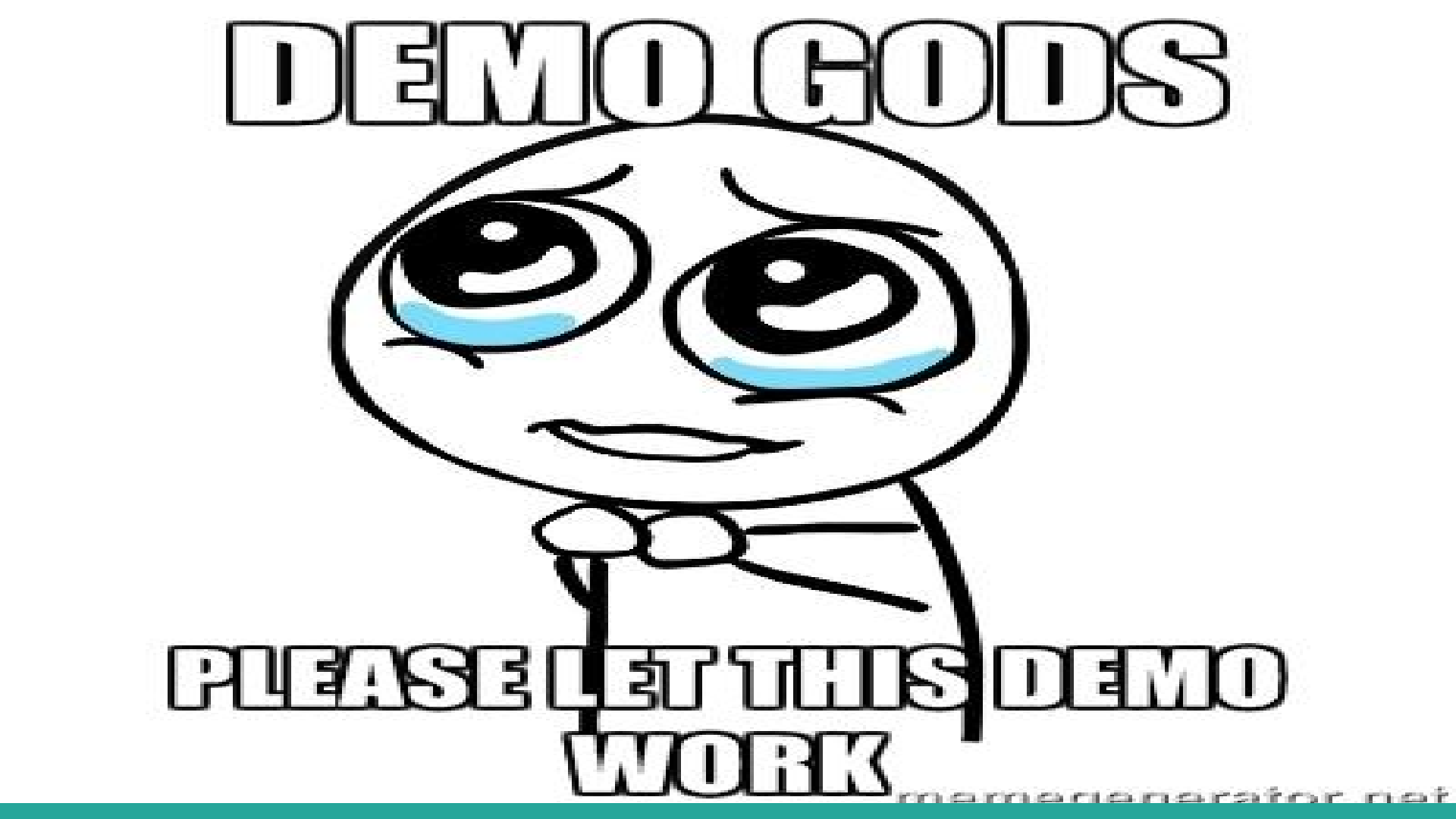
How many methods of persistence do you know of?

I promise Sysinternals Autoruns knows more.



Centralized Persistence Tracking?

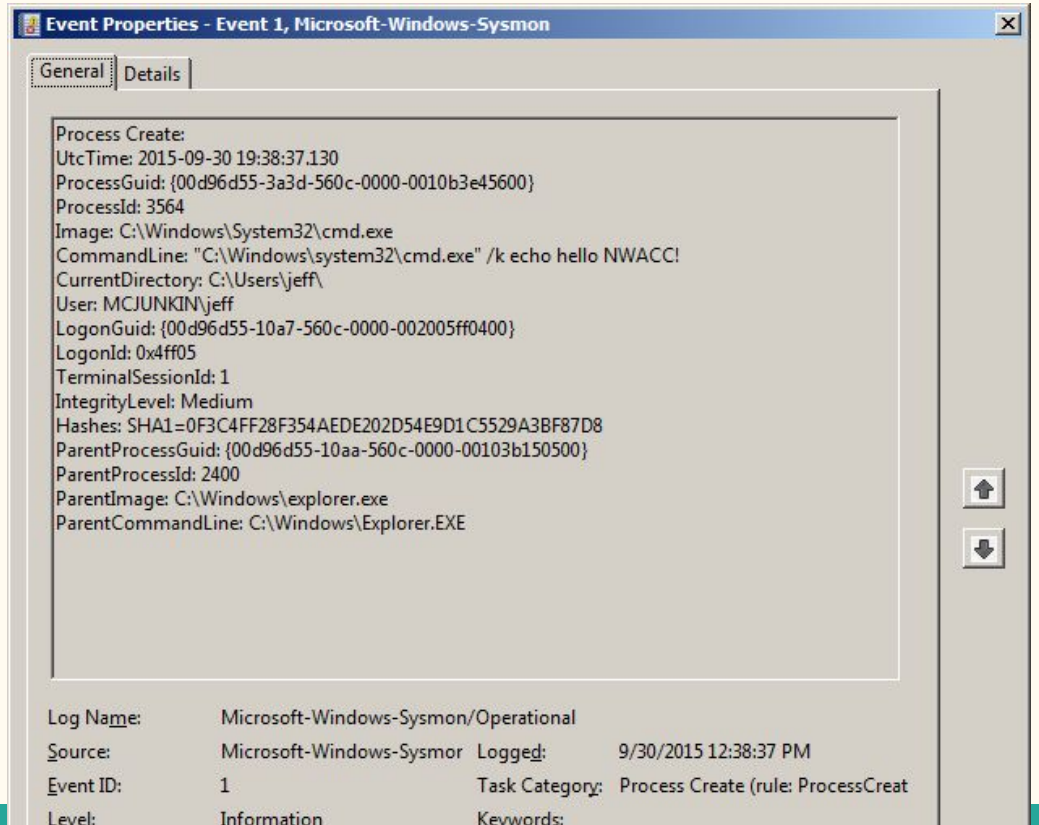
1. Scheduled Task via Group Policy (autorunsc.exe to plain text file on file server)
2. Diff most recent and second-most recent files.
3. Email upon difference.


DEMO GODS
PLEASE LET THIS DEMO WORK

Tracking program execution

- Ever heard of Carbon Black?
  - For many shops, Sysinternals Sysmon is equivalent.
  - For free.

Example event of program execution



Centralized logging?

Step 1) Get your Windows Event Logs to one server (Event Log Forwarding).

Step 2) Get your centralized Windows Event Logs into something easier to work with.

(Splunk, ELK, SexiLog)

Use NXLog Community, not Snare. Snare is now dead to me.

Data exfiltration

- How many spare desktops do you have?
- Install Security Onion on one, set up a SPAN port mirroring your outbound traffic

NWACC 2014, by Jesse Martinich and Christina Kaiseramn!

Snort / Suricata / Bro are their own presentations

Questions?

I'll be around for the rest of the day as well.

Don't want to ask here? Send me an email:

jeff@counterhack.com or jeff.mcjunkin@gmail.com