Splunking DarkTools: A Pentesters Guide To Pwnage Visualization

Bryce Kunz I Nathan Bales
September 2017 I Washington DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
Who Are We?

- Bryce
- Nathan
Acquired!
Hole in One!

Execs Happy!
Attack Surface

VS. the little guy!
Stubborn

As a Mule!
Swoop In

I will PWN YOU!

To Save The Day!

Into a Secure State!
Lacks Integration
Unnecessarily Hard
Weak Scaling
Pirate Skelton's agree, it's **easy** & **scalable**!
Demo 1
Together Now!

▶ Also needs to be Actionable!
Collaboration
Visualization!

Of Big Data!
Auto Pilot

Multiple Penetration Testers is Easy!

- {  
  - domain: “example.com”,  
  - ip: “1.1.1.1”  
}
Auto Pilot

Ensure targets are within scope!
HTTP Event Collector (HEC)

1. Enable HEC
2. Generate Token
3. POST
4. Received
5. Indexed
curl -k -H "Authorization: Splunk 12345678-1234-1234-1234-1234567890AB"
https://localhost:8088/services/collector/event -d
{
  "project": "DARKGRIFTER",
  "domain": "confluence.darkgrifter.com",
  "ip": "34.251.221.65",
  "protocol": "tcp",
  "port": "22",
  "service": "ssh",
  "selectortype": "target",
  "severity": "INFO",
  "uniq_selector_id": "1499928119449hcobwtknqtnjgwbtconodklovmqru",
  "uniq_target_id": "1499941726162nhs tgtgm hko lflffaguyii clfbuhqj"
}
Auto Pilot

Find All Open TCP Services

- {  
  - domain: "example.com"
  - ip: "1.1.1.1"
  - openTcpPort: "80"
  - service: "http"
- }

Gator Console
Project A

Gator Console
Project B

MQ

1. Find Sub Domains
2. Find IP Addresses
3. Find Open TCP Ports
4. Find Services of Open
5. Smokey

Deliverances

Smokey

Splunk
Auto Pilot

.dispatcher sends target to modules

Gator Console
Project A

Gator Console
Project B

Find Sub Domains
Find IP Addresses
Find Open TCP Ports
Find Services of Open

Smokey

MQ

Deliverances

Bandits

Web Find Resources
UDP Proto Scan
Whois IP
SSH Try Creds

Splunk
Why Splunk?

- Simple & Scalable
- Enterprise Security
- Already in use!
Splunk Setup

- Splunk Install
- Create Index
- HEC
- Install Apps
Bandits

Gator Console
Project A

Gator Console
Project B

Expandable Bandit Modules

Bandits

MQ

1
D

2
D

3
I

4
P

5
S

Anon FTP Check
Find Web Resources

Test TLS/SSL
UDP Proto Scan

HTTP Options
Whois IP

Web Server Checks
SSH Try Creds

Etc…

Splunk
Template Bandit

- **do_work_son()** – Place logic within the try
  ```python
  def do_work_son( sProject, sUniqSelectorId, sUniqTargetId, sDomain, sIp, sProtocol, sOpenTcpPort, sTcpService ):
    goToLogging()
    try:
  ```

- **splunkEvent()** – Sends a JSON object to Splunk
  ```python
  # Whenever you have the result in a JSON like format, send it to Splunk using the splunkEvent() function!
  jEvent = {
    "project": sProject,
    "uniq_selector_id": sUniqSelectorId,
    "uniq_target_id": sUniqTargetId,
    "domain": sDomain,
    "ip": sIp,
    "protocol": sProtocol,
    "port": sOpenTcpPort,
    "service": sTcpService,
    "severity": "LOW",
    "bandit": sNameOfFunction,
    "bandit_status": "Successful",
    "bandit_result": sResult
  }
  splunkEvent(jEvent, sNameOfFunction)  # sSourceTool = sNameOfFunction
  ```
Field Extraction

Before Splunk
- JSON, AutoKV, etc
- Done in python

In Splunk
- Per sourcetype
- Regex, field extraction, etc
- Pros.conf,

Lookups
- Scheduled Searches to combine sourcetypes that output as lookups

GeoIP
- Adding location data to visualize locations
Standalone

Console

Splunk

MQ

Deliverances

Etc...

Bandits

Etc...
Distributed

Deployed to Multiple Servers

Bandits

Deployed to Multiple Servers

Deliverances

Etc…

MQ

Bandits

Etc…

Splunk

Console

Console
DarkTools Demo

Hipster Skelton's agree,

» It’s easy & scalable!
Demo 2
Future Versions

- More Modules w/ Checks
- Data Model for Splunk
- Correlation within Splunk
- Trending within Splunk
- Machine Learning ToolKit (MLTK)
- API for More Integrations
- Etc…
Questions?

@TweekFawkes
@brutes_
Requirements:

- DarkTools App -- https://github.com/brutes1/darktools_bh
- Sankey Diagram App -- https://splunkbase.splunk.com/app/3112/
- TA-geoip -- https://github.com/georgestarcher/TA-geoip
Thank You

Don't forget to rate this session in the .conf2017 mobile app