Splunking DarkTools - A Pentesters Guide To Pwnage Visualization

Bryce Kunz, Nathan Bates
Who are we?

- Bryce
- Nathan
Buy now!

- Acquired!
Hole in One!

- Execs Happy!
VS. the little guy!
Stubborn

- As a Mule!
Swoop In

I will PWN YOU!

Into a Secure State!

- To Save The Day!
Chaotic

- Lacks Integration
- Unnecessarily Hard
- Weak Scaling
Pirate Skelton's agree, it's **easy** & **scalable**!
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!

MQ

Gator Console

Project A

1. Find Sub Domains
2. Find IP Addresses
V. Validate Target

Deliverances

Project B

Gator Console

Blacklist of IPs
Whitelist of IPs
Graylist of IPs

Splunk
HTTP Event Collector (HEC)

1. Enable HEC
2. Generate Token
3. POST
4. Received
5. Indexed
HEC POST

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":"1499928119449hcobwltkfnqtnjgwgtbconodklovmqru",
  "uniq_target_id":"1499941726162nhshtgmkoolfhffaguyiflclfbuhqj"
  
'}
Auto Pilot

- Find All Open TCP Services

- {  
  - domain: “example.com”,  
  - ip: “1.1.1.1”  
  - openTcpPort: “80”  
  - service: “http”  
  - }

Gator Console

Project A

Find Sub Domains

Find IP Addresses

Find Open TCP Ports

Find Services of Open

MQ

Deliverances

Smokey

Gator Console

Project B

Splunk
Auto Pilot

- Dispatcher sends target to modules

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

Deliverances

Bandits

Project A
Gator Console

Project B
Gator Console

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

- Expandable Bandit Modules

MQ

Bandits

Anon FTP Check
Find Web Resources
Test TLS/SSL
UDP Proto Scan
HTTP Options
Whois IP
Web Server Checks
SSH Try Creds
Etc…”

Gator Console

Project A

1

D

D

Gator Console

Project B

2

I

I

3

P

P

4

S

S

5

S

Splunk
Template Bandit

- `do_work_son()` – Place logic within the try

```python
def do_work_son( sProject, sUniqSelectorId, sUniqTargetId, sDomain, sIp, sProtocol, sOpenTcpPort, sTcpService):
    try:
        # Logic here
    
```

- `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
```
Making the Data more Usable

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

- All In One
Distributed

- Deployed to Multiple Servers
Hipster Skelton's agree,
  - it’s easy & scalable!
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:
