



Crossing the Streams with State Machines in IDS Signature Languages

Michael Rash
ShmooCon 2014 FireTalks
<http://www.cipherdyne.org/>
@michaelrash

flowbits Primer

- flowbits allows multiple Snort rules to function as a group for better attack detection
- flowbits criteria can essentially build a *state machine* out of a set of Snort rules
- Example:

```
alert tcp any 143 -> any any (msg:"IMAP login";  
content:"OK LOGIN"; flowbits:set,logged_in;  
flowbits:noalert;)
```

```
alert tcp any any -> any 143 (msg:"IMAP LIST";  
content:"LIST"; flowbits:isset,logged_in;)
```


flowbits Limitations

- ✦ Although flowbits is powerful, it cannot apply across multiple conversations
- ✦ *Does this matter?*
 - ✦ Put another way, would cross-stream flowbits enable better attack detection?

Multi-Conversation Metasploit Modules

- Look for Metasploit modules that require multiple connections/conversations for successful exploitation
- Good approximation derived from multiple calls to any of these three functions within a single module:
 - `connect()`
 - `connect_udp()`
 - `send_request_cgi()`

A Quick Approximation

```
$ cd ~/git/metasploit-framework/
```

```
$ git grep -c "^[[:space:]]*connect" modules |grep -v ":1" |wc -l  
132
```

```
$ git grep -c "send_request_cgi" modules |grep -v ":1" |wc -l  
263
```


Metasploit ContentKeeper Web Remote Command Execution

- `modules/exploits/unix/http/contentkeeperweb_mimencode.rb`
- Exploits the ContentKeeper Web Appliance (versions < 125.10) to acquire remote command execution as the Apache user
- Work flow:
 - 500 Internal error from `/cgi-bin/ck/mimencode` implies vulnerable
 - Script upload via HTTP POST `/cgi-bin/ck/mimencode?-u+-o+spamkeeper.dat`
 - Script execution via HTTP GET `/cgi-bin/ck/spamkeeper.dat`
 - *Multiple HTTP requests are **required** for exploitation even without running the Metasploit `check()` function*

Additional Metasploit Examples

- ✦ SCADA 7-Technologies IGSS Rename Overflow
- ✦ Apache ISAPI DoS
- ✦ Many more...

New Snort Keyword: "xbits"

- "xbits" would allow an xbit to be set on one conversation, and then tested within another conversation (spanning TCP, UDP, ICMP, or any other IP protocol)
- xbits would offer standard flowbits modifiers such as "set", "unset", "noalert", etc. with identical semantics
- xbits would add two new modifiers:
 - "track" - with args "ip_pair", "dst_port", etc. to require tuple matches (or not) across conversations
 - "expire" - force xbit expiration independent of TCP connection close

Metasploit ContentKeeper Exploit Detection

- Set xbit "`Metasploit.ContentKeeper.recon`" on initial HTTP connection (part of the Metasploit check() function)
- Test "`Metasploit.ContentKeeper.recon`" xbit with 'isset' and if it matches, then set xbit "`Metasploit.ContentKeeper.recon_status_is_vuln`" on '500 Internal' webserver response. Track by ip_pair.
- Look for an HTTP POST that uploads the base64 encoded perl script and test "`Metasploit.ContentKeeper.recon_status_is_vuln`" xbit. If this xbit is set, then set xbit "`Metasploit.ContentKeeper.payload_uploaded`" and track by ip_pair.
- Look for an HTTP GET to /cgi-bin/ck/spamkeeper.dat and test the "`Metasploit.ContentKeeper.payload_uploaded`" xbit. If it is set then generate an event "`Metasploit ContentKeeper Web remote code exec`".

Trade Offs

- ✦ Why not just look for requests like “POST /cgi-bin/ck/mimencode?-u+-o+” by themselves?
- ✦ Detection implications - potential false negative increase in exchange for higher confidence true positives, but *definitions become important*
- ✦ IDS engine implications (multi-threaded or not)
- ✦ Performance implications

Final Points

- Application communications by design frequently involve more than single conversations (Bittorrent, VoIP, anything that uses a signaling protocol).
 - Corollary: *Attacks do as well*
 - The Snort signature language itself should therefore contain a built-in ability to link groups of rules across multiple conversations
- Event correlation in the SIEM world is a related technology in some ways

Linux Firewalls

- ✦ Writing 2nd edition now
- ✦ xbits will be covered



Questions?

Michael Rash

@michaelrash

mbr@cipherdyne.org

<http://www.cipherdyne.org/>