Bro, I Can See You Moving Laterally

Richie Cyrus
@rrcyrus

Who Am I?

- Defender - Incident Responder @ CME Group

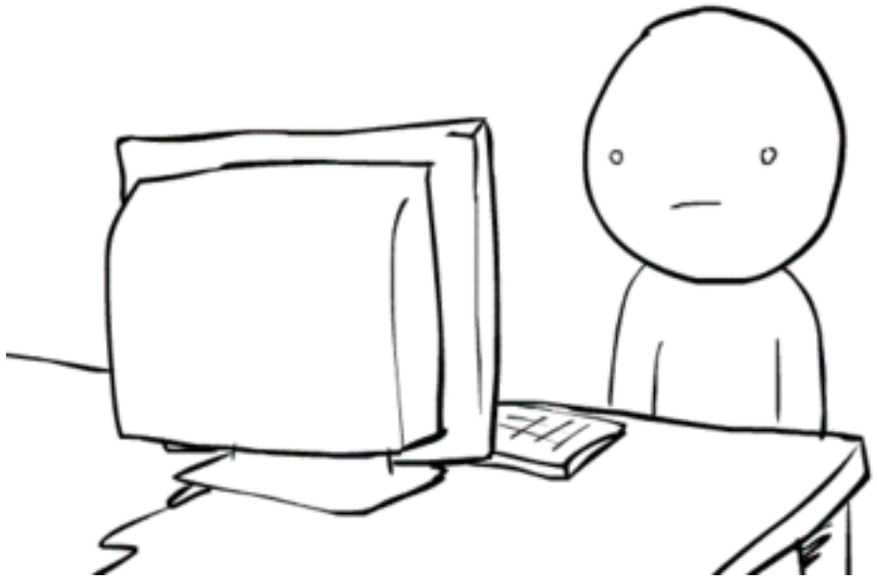
- Network Security Monitoring (NSM) Fanboy

- A healthy obsession with finding malicious activity, and new ways to go about doing so.

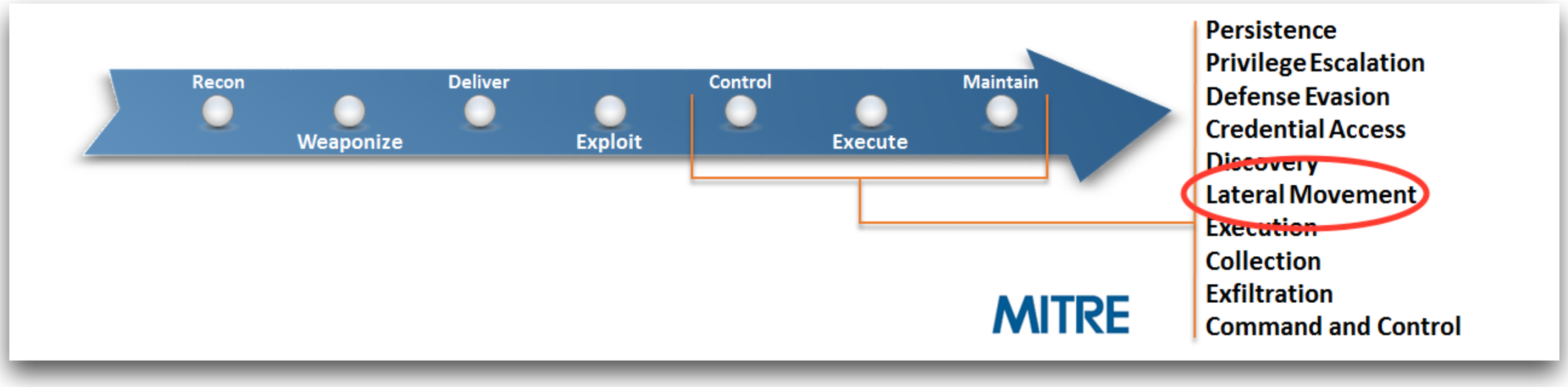
- @rrcyrus

Do You Even “Bro”?

- Bro Logs
- Bro SMB analyzer
- Bro Scripting



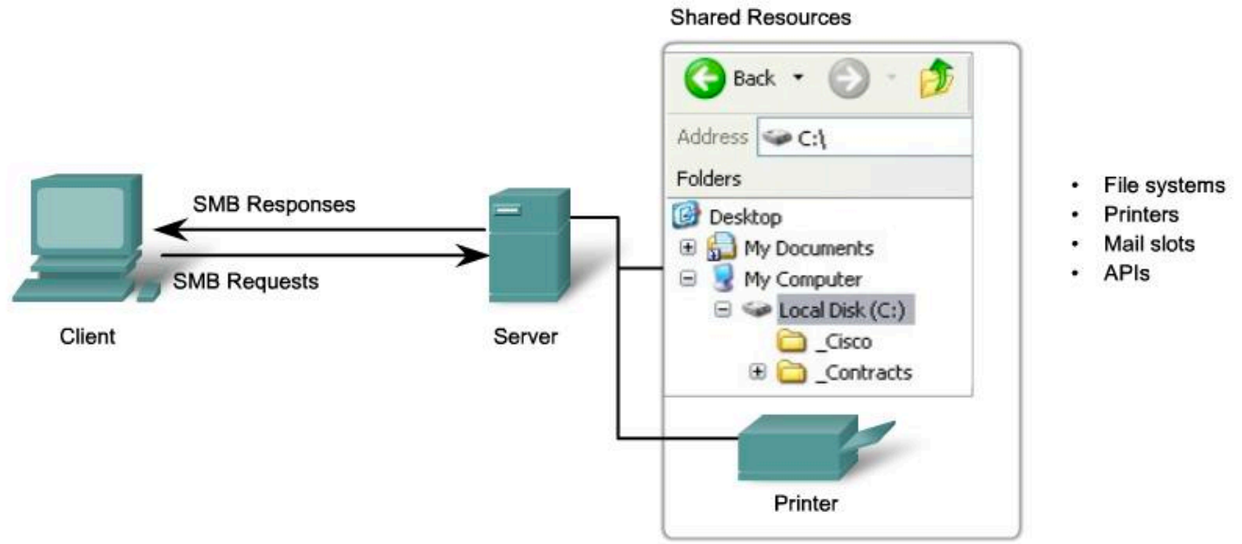
Post Compromise Activity (Lateral Movement)



https://attack.mitre.org/w/images/6/6f/MITRE_attack_tactics.png

SMB Protocol

- Used for File Sharing
- MS-SQL
- Printing, etc.
- SMB Version 2.x

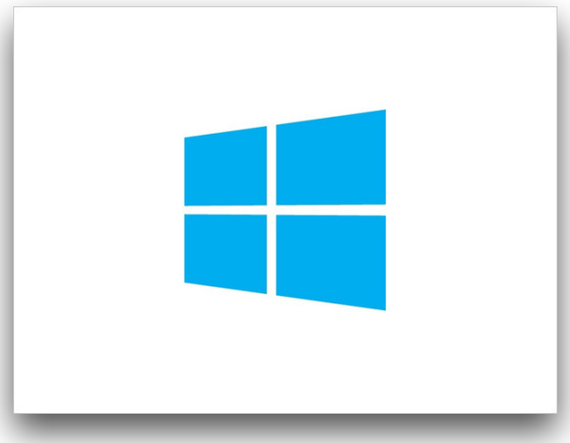


SMB is a client-server, request-response protocol. Servers can make their resources available to clients on the network.

https://4.bp.blogspot.com/

Methods Typically Used

alert tcp any any -> $HOME_NET [139,445] (msg:”ET POLICY PsExec? service created”; flow:to_server, established; content:”|5c 00 50 00 53 00 45 00 58 00 45 00 53 00 56 00 43 00 2e 00 45 00 58 00 45|”; reference:url, xinn.org/Snort-psexec.html; reference:url, doc.emergingthreats.net2010781; classtype:suspicious-filename-detect; sid:201781; rev:2;)



Windows Event Logging:

- Event ID 5140, 5142, 5145, etc

Bro Network Security Monitor

- Metadata - Network Protocols
- File metadata
- Alerting
- ASCII - Easy to grep/ bro-cut, ingest into SIEM

Example of Bro Log

```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2017-02-22-18-00-27
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service dur
ation        orig_bytes      resp_bytes      conn_state      local_orig      local_resp      missed_bytes
    history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_parents  orig_cc resp_cc
 sensorname
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   str
ing   bool    bool    count   string  count   count   count   count   set[string]     string  string  string
1487786361.029448       CJweJe2TJu0KWfFgE6      10.74.151.107   1900    239.255.255.250 1900    udp     -
       6.021858        8643    0       S0      T       F       0       D       18      9147    0       0
       (empty) -       -       secadmin-virtual-machine-eth1
1487786415.366247       CzUdAR3aOEvlZGFdO6      10.74.151.103   5353    224.0.0.251     5353    udp     dns
     5.242362        4870    0       S0      T       F       0       D       24      5542    0       0
       (empty) -       -       secadmin-virtual-machine-eth1
1487786415.366716       CbEVZS1sWYLtbOjnqj      fe80::18f6:e464:f5c9:83cc       5353    ff02::fb        535
3    udp     dns     5.242391        4870    0       S0      F       F       0       D       24      6022
    0       0       (empty) -       -       secadmin-virtual-machine-eth1
1487786416.492791       Cen61x24CbQmwRnja7      10.74.151.116   5353    224.0.0.251     5353    udp     dns
     4.082545        17218   0       S0      T       F       0       D       36      18226   0       0
       (empty) -       -       secadmin-virtual-machine-eth1
1487786416.493333       CmY4TV3ptal4pg8hK9      fe80::bf:e184:4449:8758 5353    ff02::fb        5353    udp
     dns     4.082007        17218   0       S0      F       F       0       D       36      18946   0
       0       (empty) -       -       secadmin-virtual-machine-eth1
:
```

Bro & SMB

- Policy not enabled by default
  - Uncomment policy in /opt/bro/share/bro/site/local.bro

  - smb_cmd.log ,smb_files.log, smb_mapping.log, ntlm.log, dce_rpc.log

Bro Scripting

- Built on C++
- Notice framework: Allows for alerting
- Files Framework: Grabs file metadata

SMB Files to VirusTotal

- VT API key - Free Version
- Uses Files Framework
- Detects known malicious files transferred over SMB

Accessing SMB Admin Shares

- Detects attempts to access IPC$, ADMIN$, C$, D$, etc
- Sends alert to notice.log

Rogue Hostname Detection

SECNET-WINHVA001

DEMO

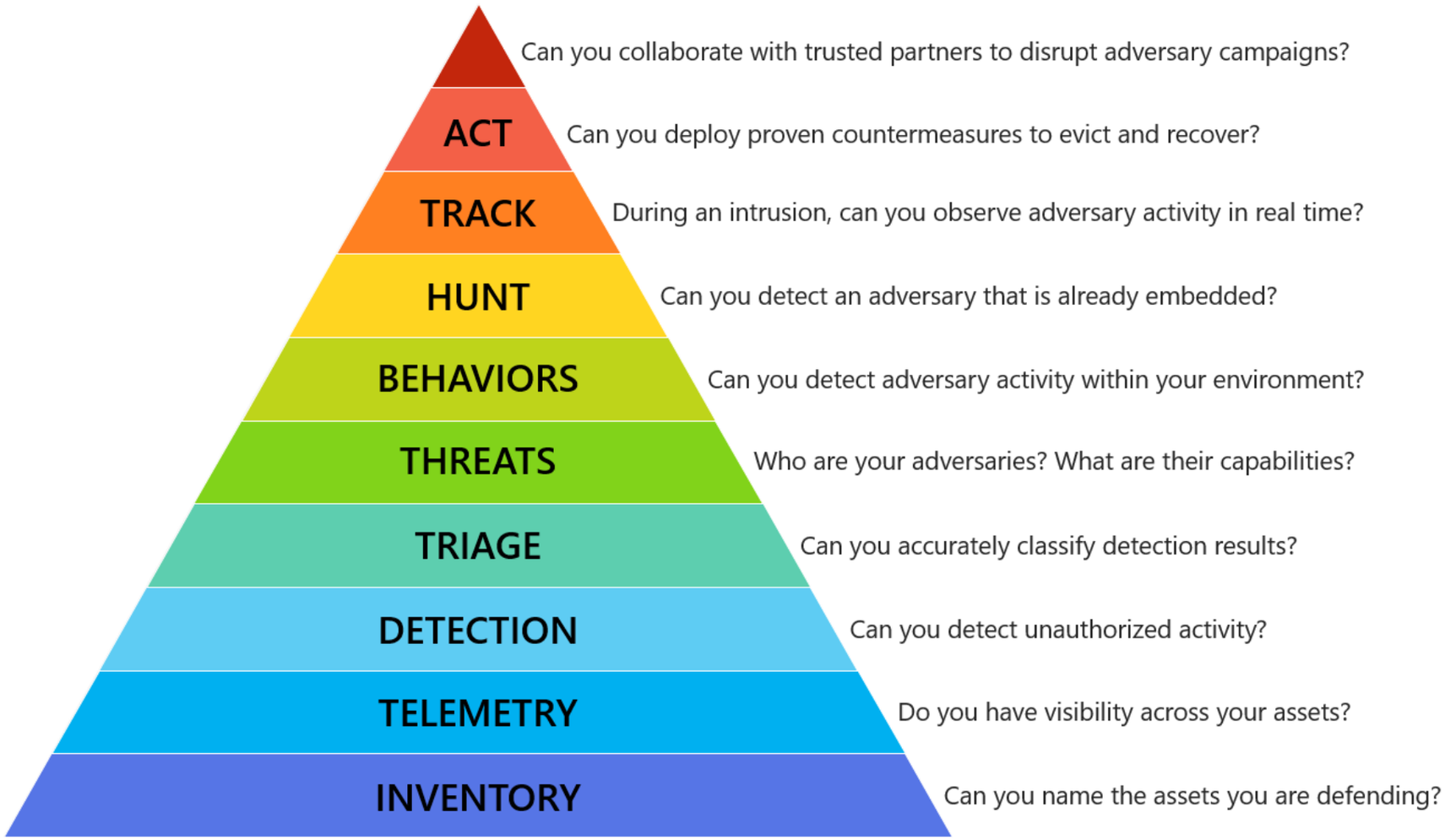
Malicious Attacker

(Post Compromise)

vs

Defender

Bro Detecting the “Bro”



Questions?

- Slides: securityneversleeps.net
- Scripts: https://github.com/richiercyrus/Bro-Scripts
- Twitter: @rrcyrus