Gathering Threat Intelligence through Computer Network Deception

William M.S. Stout

Vincent E. Urias, Han W. Lin

Sandia National Laboratories
Albuquerque, New Mexico

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Outline

- Introduction and Motivation
- The Deception Environment
- Methodology and Operating Modes
- Analysis of an Attack
- Conclusion

INTRODUCTION AND MOTIVATION

Introduction: Defender Needs

- Foremost: tool was an outgrowth of operational needs
- Actionable threat intelligence is needed; gaps exists
  - Modern tools are often are reactionary (signatures, etc.) and do not enable proactive strategies to combat threat
  - Traditional techniques of unplugging compromised boxes, we lose value intelligence into adversary motivation
- As a network defender, there are few/no mechanisms to interact and learn about our adversaries
- Better tools are needed to gather information about our adversaries

Introduction: Intelligence Needs

- More and more threat feeds moving behind the door…
  - Aggregation of smaller feeds (LookingGlass)
  - Mandiant purchase of iSight
- What will the landscape look like 3-5 years from now?
- Closed feeds by disparate vendors
  - Purchase them all?
  - Pick out the relevant threat feeds from the noise?

- Consider: tailored intelligence based on security posture and threat profile
  - Roll-your-own based what is import to you

Motivation

- Predictability in the computing environment is foundational to an adversary's success.
- BUT we can exploit the adversary’s expectation of a homogenous environment through cloud and virtualization technologies.

Motivation

- Through a deception framework:
  - Obscure the real target
  - Devalue information gathering
  - Increase the difficulty of attack planning
  - Cause the adversary to waste time and resources
  - Force the adversary to reveal advanced capabilities
  - Expose adversary intent
  - Limit the scope of the attack
  - Limit the duration of a successful attack

Research Focus Areas

- Endpoint
  - Introspection
  - Reach-in
  - Aging
- Network
  - VM relocation
  - Stream modification
  - File modification
- Environment
  - High-density
  - High-fidelity
  - Traffic generation
  - Tailored deception

THE DECEPTION ENVIRONMENT

The Deception Environment

- Virtualization Environment
- Virtual Machine Introspection
- Software-defined Networking

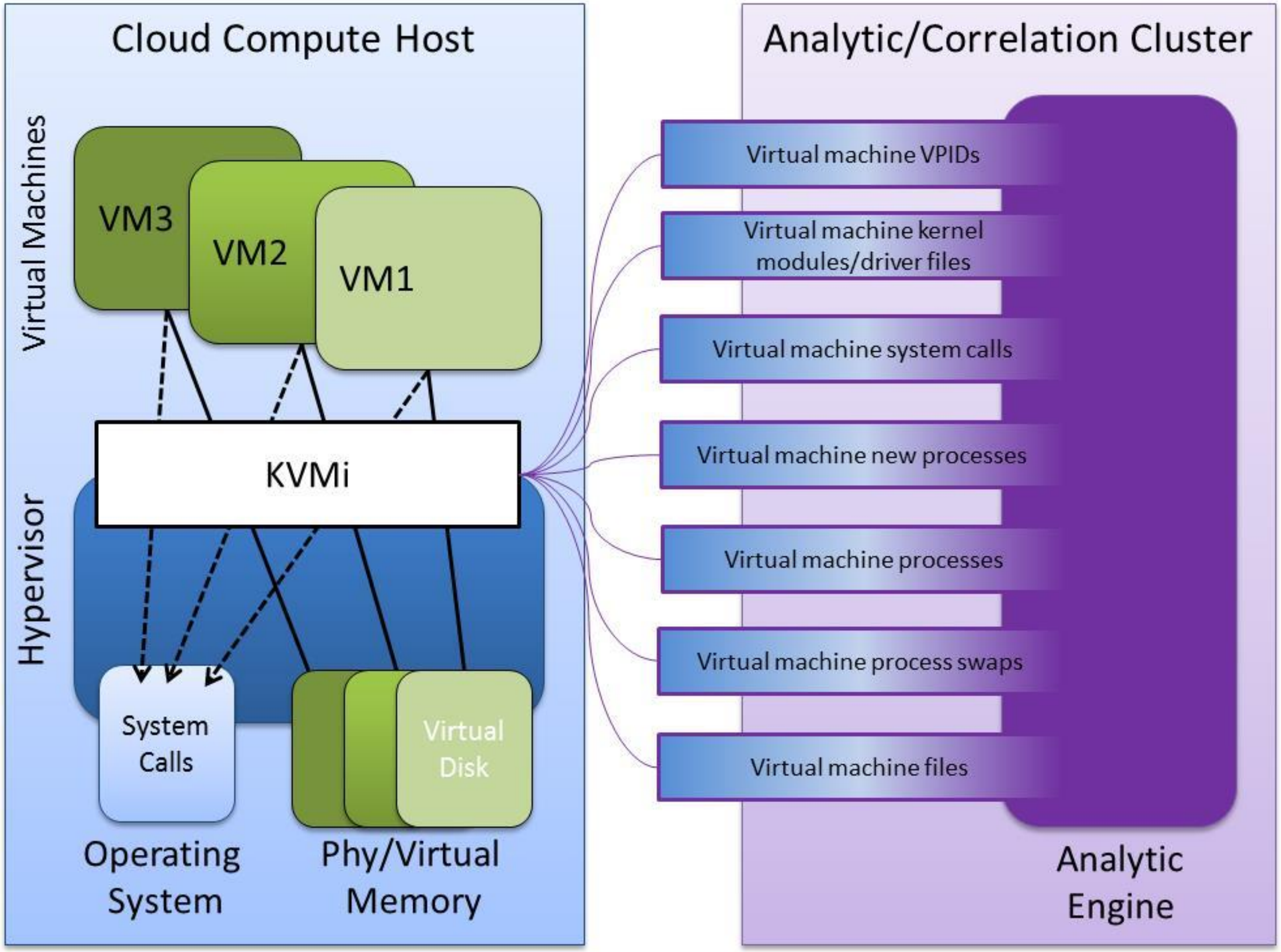
Virtualization Environment

- Emulation/HITL
- High-Density
- Fast boot times
- Automated complex network specification
- Automated service provisioning

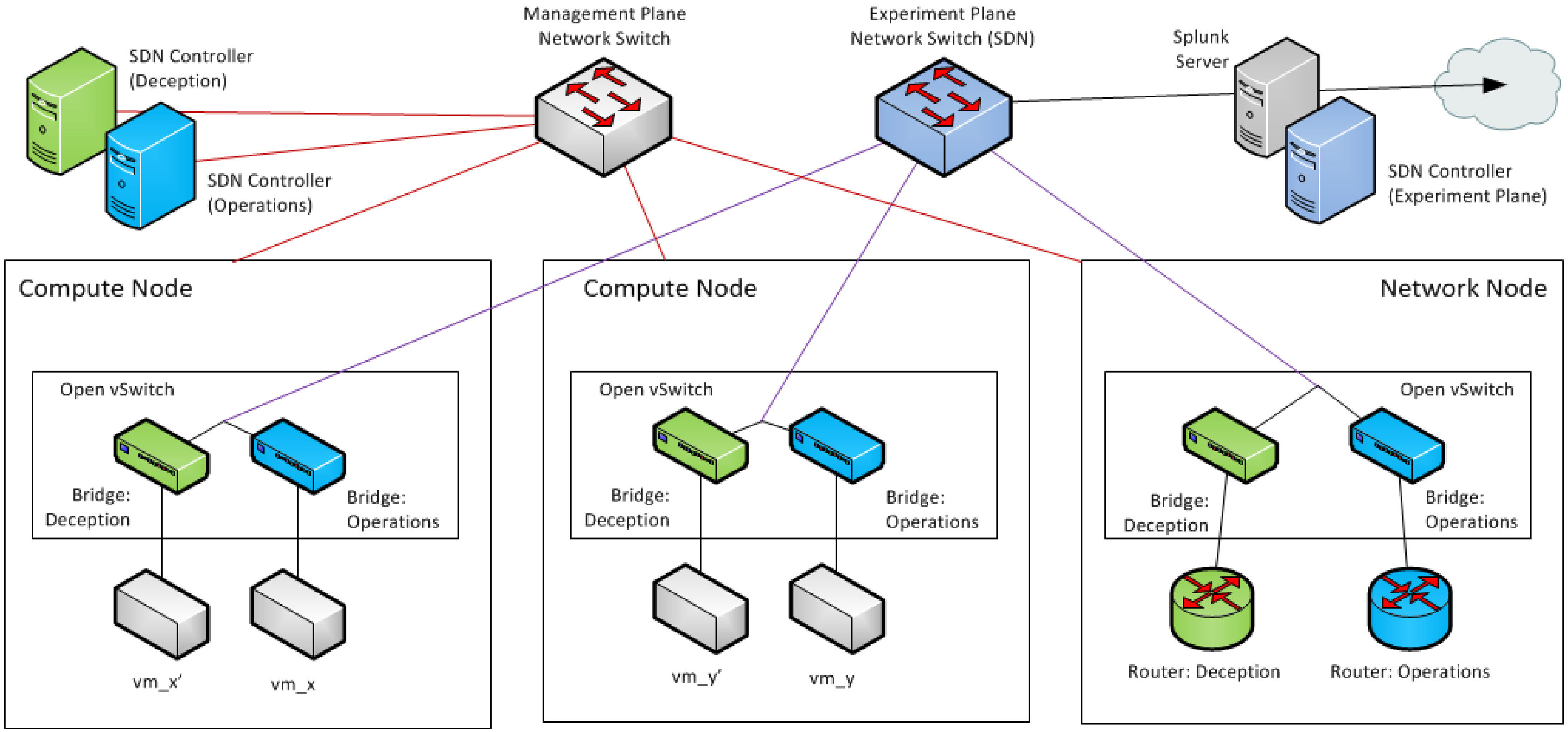
Virtual Machine Introspection

- Modern hypervisors have a hardware-defined structure and must interact with the CPU in a certain way
- By intercepting code execution between an exiting VM and KVM, we get to be the hypervisor before handing control over to KVM (if we give them control at all)
  - We do this by loading a Linux kernel module (KVMi), which finds KVM and hooks the exit handler
  - This can be loaded and unloaded at any time, agnostic of KVM versions
- During this time we control and see all aspects of VM execution
  - VM extended/shadow page tables
  - Read/write VM memory, execution context, register state
- Since we are running at the same level as KVM, we require no ring switching or additional VM exits

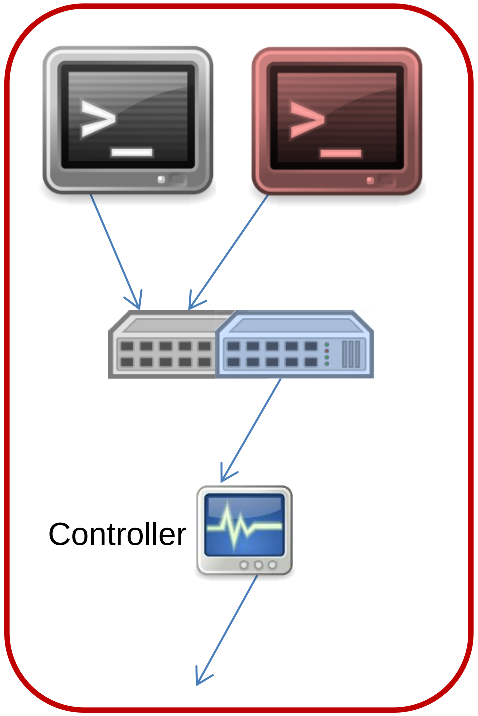
Virtual Machine Introspection


Cloud Compute Host
Virtual Machines
VM3
VM2
VM1
KVMi
Hypervisor
System Calls
Virtual Disk
Operating System
Phy/Virtual Memory
Analytic/Correlation Cluster
Virtual machine VPIDs
Virtual machine kernel modules/driver files
Virtual machine system calls
Virtual machine new processes
Virtual machine processes
Virtual machine process swaps
Virtual machine files
Analytic Engine

SDN Topology



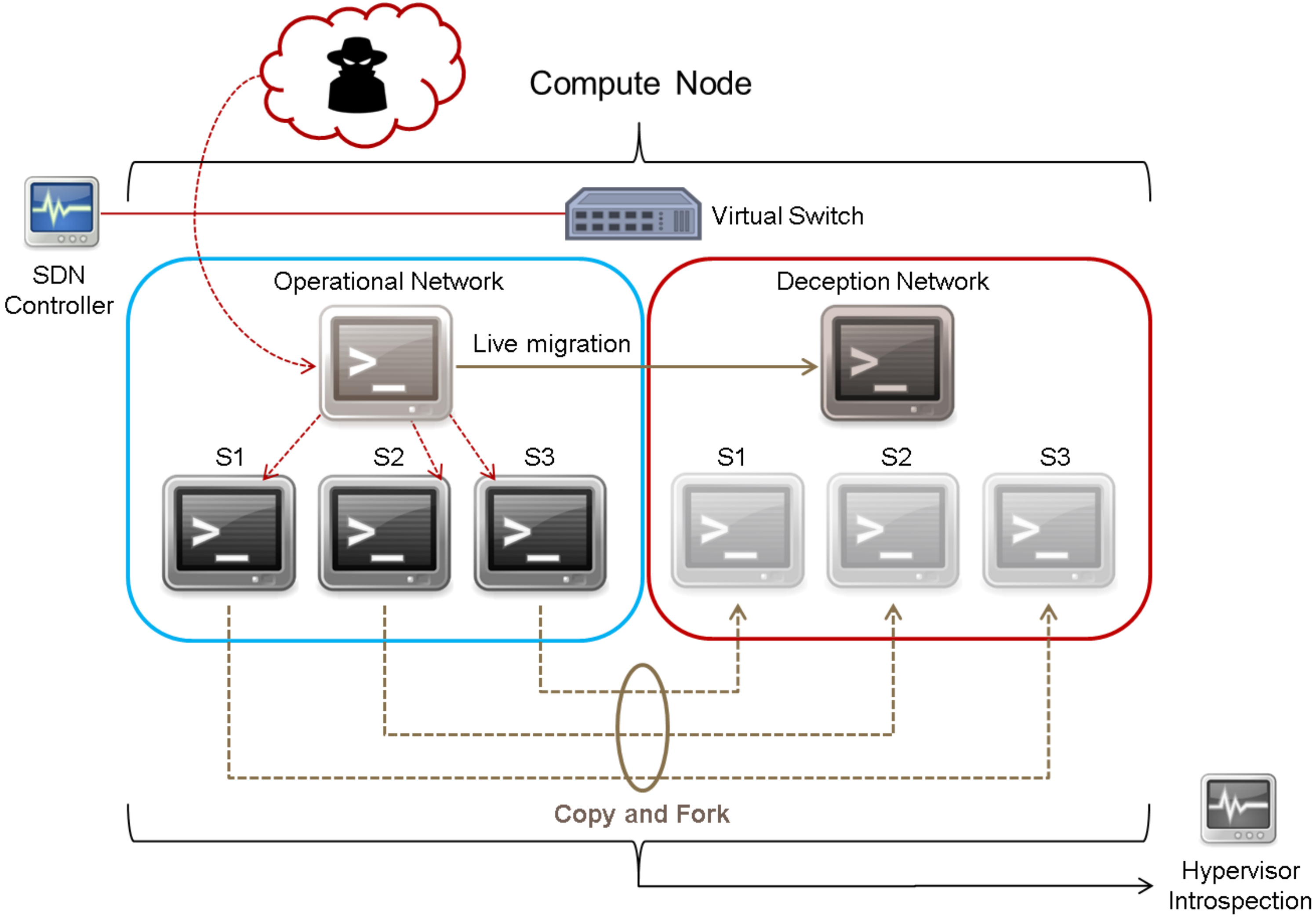
SDN Capabilities



- OVS “pipes” between OVS on guest and resident NIC on host node.
- Custom module for Openflow Controller:
  - Static/reactive flows pass inbound and local traffic.
  - Outbound TCP/UDP inspected and payload intercepted at specified intervals.
- Degradation of service to prevent large file transfer and waste adversary resources for exfiltration.
- Given the MITM presence, we also have the ability to:
  - Watermark images
  - Wrap Executables
  - Modify PDFs and Zips
- OVS L7 DPI
- Modification of perspective (adversary)

METHODOLOGY AND OPERATING MODES

Methodology

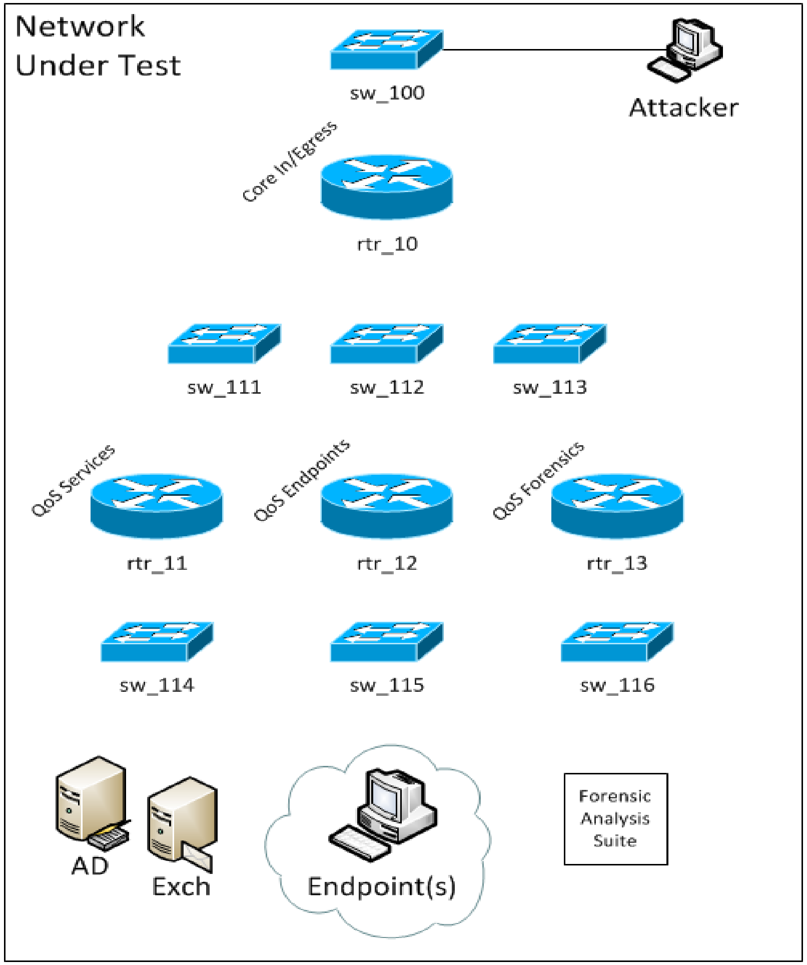


Methodology: Operating Modes

- VM Replacement
  - Migrate flows to a warm VM
- VM Isolation / Quarantine
  - Migrate VM to logically isolated locale
- Forking / Service Migration
  - Fork to new env; patch in former
- Running parallel deception network
  - Full VM migration to Deception Environment

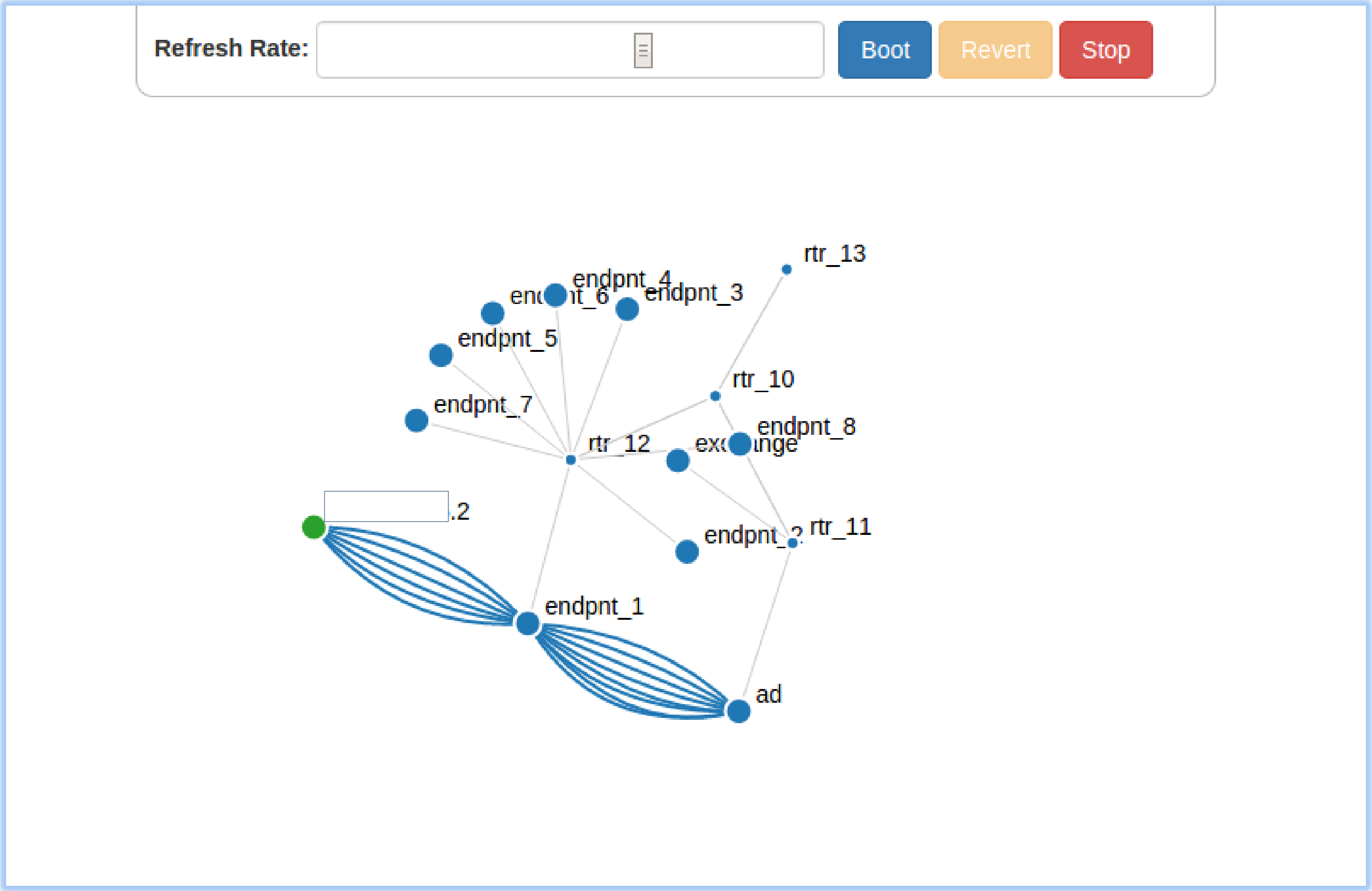
ANALYSIS OF AN ATTACK

Attack Analysis



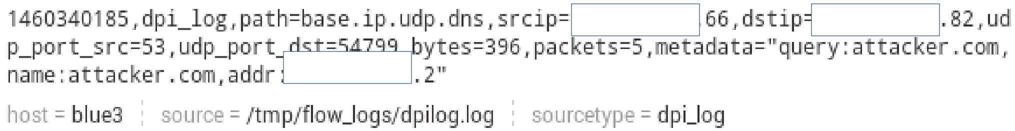
- Small-scale network enclave
  - Three subnets
  - Eight endpoints
  - Two servers
  - Four virtual routers
  - One external attacker

Attack Analysis

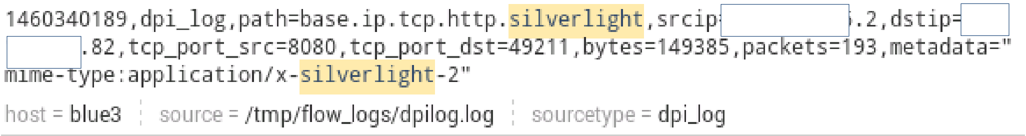


Attack Analysis

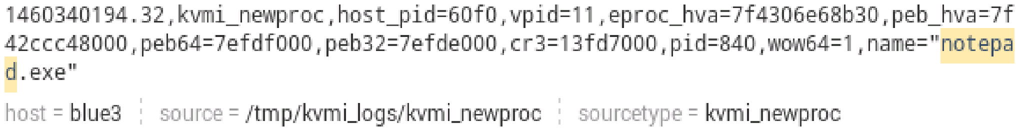
- To start the chain of events, an administrator logs into the Vulnerable Workstation and adds an Administrative share using his Domain Administrator credentials. He then visits a phishing website hosted on the attackers machine ("attack.com"). This is shown in the DPI log below
- The Attacker compromises the machine using a Silverlight Exploit through a XAP file and runs a bind meterpreter on port 2222
- The Attacker then starts a new process notepad.exe and migrates to the process so when the user closes iexplore.exe they don't close the meterpreter session.



```
1460340185,dpi_log,path=base.ip.udp.dns,srcip=[redacted].66,dstip=[redacted].82,ud
p_port_src=53,udp_port_[redacted]bytes=396,packets=5,metadata="query:attacker.com,
name:attacker.com,addr[redacted].2"
host = blue3 | source = /tmp/flow_logs/dpilog.log | sourcetype = dpi_log
```



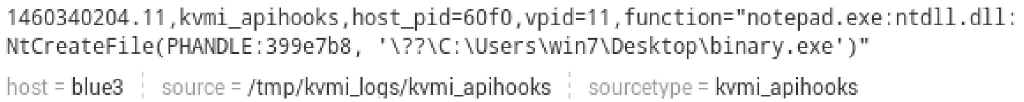
```
1460340189,dpi_log,path=base.ip.tcp.http.silverlight,srcip[redacted].2,dstip=[redacted]
[redacted].82,tcp_port_src=8080,tcp_port_dst=49211,bytes=149385,packets=193,metadata="
mime-type:application/x-silverlight-2"
host = blue3 | source = /tmp/flow_logs/dpilog.log | sourcetype = dpi_log
```



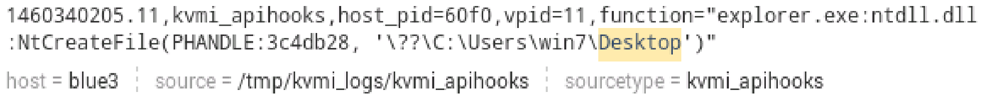
```
1460340194.32,kvmi_newproc,host_pid=60f0,vpid=11,eproc_hva=7f4306e68b30,peb_hva=7f
42ccc48000,peb64=7efdf000,peb32=7efde000,cr3=13fd7000,pid=840,wow64=1,name="notepa
d.exe"
host = blue3 | source = /tmp/kvmi_logs/kvmi_newproc | sourcetype = kvmi_newproc
```

Attack Analysis

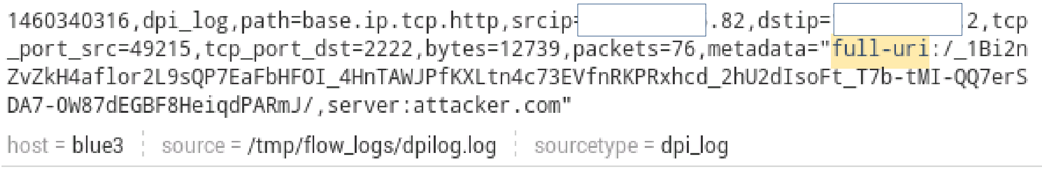
- The Attacker then uploads a binary and executes it. The binary is seen here, and also dumped to from the guest for further inspection.
- The Attacker then downloads a file located on the compromised machine’s desktop to the attacker machine, we see this process started by a walk of the directory tree
- The Attacker then runs hashdump to collect the local SAM hashes on the machine andl loads mimikatz into the meterpreter session to collect passwords located in memory (kerberos, msv, and ssp passwords). As this information is transferred back to the attacker machine, high entropy URIs are seen in the DPI log over a meterpreter bound port 2222.
- Using the new found credential and pivot, the attacker uses psexec to login to the domain controller. When the session is opened, the Attacker again loads mimikatz to collect passwords, as well as hashdump to collect the local and domain password hashes. The UI shows a connection from an external entity (green dot) pivoting at endpnt1, which in turn maintains a connection to the AD server. Again, hashed URIs are shown traversing port 2222 from the AD to the Attacker server, as well as exfiltration communication from the AD to the Attacker over port 3333.



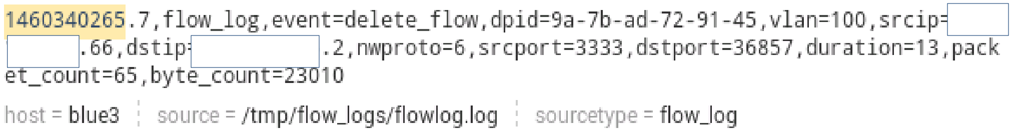
```
1460340204.11,kvmi_apihooks,host_pid=60f0,vpid=11,function="notepad.exe:ntdll.dll:
NtCreateFile(PHANDLE:399e7b8, '\??\C:\Users\win7\Desktop\binary.exe')"
host = blue3  source = /tmp/kvmi_logs/kvmi_apihooks  sourcetype = kvmi_apihooks
```



```
1460340205.11,kvmi_apihooks,host_pid=60f0,vpid=11,function="explorer.exe:ntdll.dll
:NtCreateFile(PHANDLE:3c4db28, '\??\C:\Users\win7\Desktop')"
host = blue3  source = /tmp/kvmi_logs/kvmi_apihooks  sourcetype = kvmi_apihooks
```



```
1460340316,dpi_log,path=base.ip.tcp.http,srcip=[redacted].82,dstip=[redacted]2,tcp
_port_src=49215,tcp_port_dst=2222,bytes=12739,packets=76,metadata="full-uri:/_1Bi2n
ZvZkH4aflor2L9sQP7EaFbHFOI_4HnTAWJPfKXLtn4c73EVfnRKPRxhcd_2hU2dIsoFt_T7b-tMI-QQ7erS
DA7-OW87dEGBF8HeiqdPARmJ/,server:attacker.com"
host = blue3  source = /tmp/flow_logs/dpilog.log  sourcetype = dpi_log
```



```
1460340265.7,flow_log,event=delete_flow,dpid=9a-7b-ad-72-91-45,vlan=100,srcip=[redacted]
[redacted].66,dstip=[redacted].2,nwproto=6,srcport=3333,dstport=36857,duration=13,pack
et_count=65,byte_count=23010
host = blue3  source = /tmp/flow_logs/flowlog.log  sourcetype = flow_log
```

CONCLUSIONS

Conclusions

- Discussed:
  - – Motivation, methodology, technologies
- Use-case and example deployment
- Take aways:
  - – Deception allows an adversary to play their game
  - – Dynamically modify the environment to entice
  - – Correlation of host and network data to gather actionable intelligence, to inform future decisions

Gathering Threat Intelligence through Computer Network Deception

Questions/Comments

William M.S. Stout

wmstout@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP