

Using traffic anomalies to detect zero-days

Implementing a Network-based Intrusion Detection System (IDS) for Control Systems

SCADAhacker.com

Think like a *hacker* ...

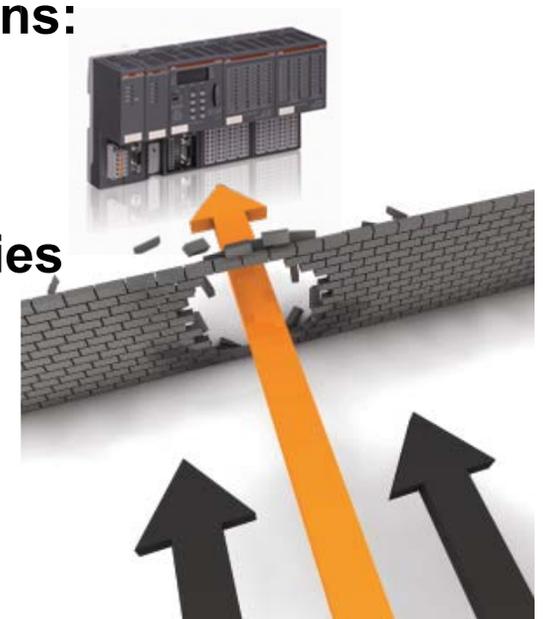
To secure industrial control systems and protect critical infrastructure





Control Systems are Under Attack

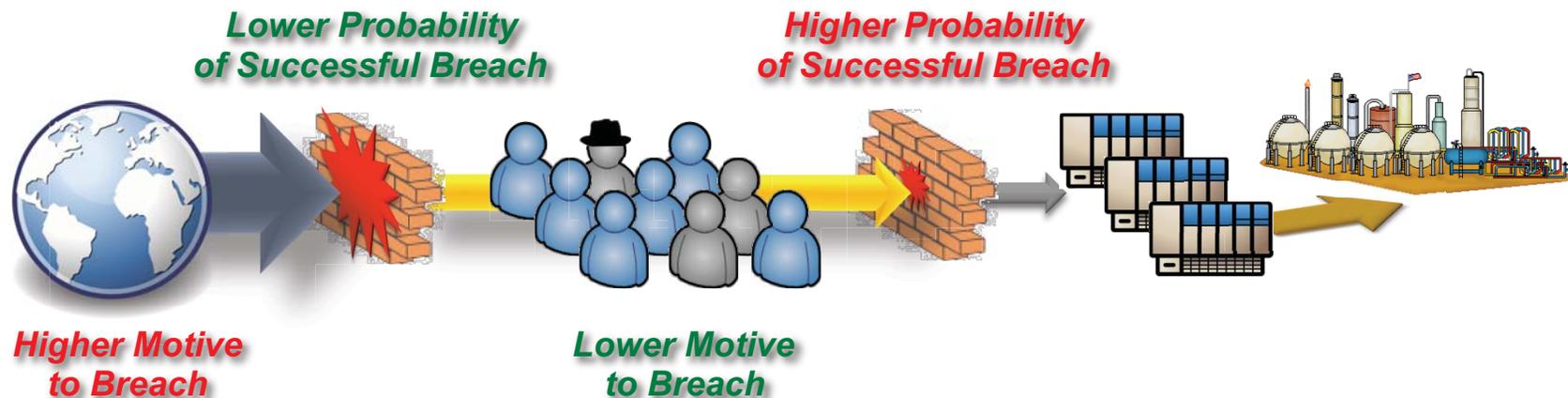
- ICS platforms are becoming an obvious target for attacks
- “Security Researchers” focusing on ICS because it is easy money/fame (little malicious intent)
- Attacks are targeting not only Windows hosts, but controller platforms as well
- Actors with intent have access to the weapons:
 - Download exploits for free (Italian list, Metasploit)
 - Purchase tool kits (Immunity+Gleg)
 - Directed where to look for more vulnerabilities
- Most systems have many exploit opportunities
- Patching is an issue for many companies
 - Patch deployment requires plant downtime
 - Vendor only patches most current version
 - Patch releases are slow
 - Upgrading to latest version may not be an option





Control Systems are Interconnected to other “Less Secure” Networks

- **Control systems are at risk ...**
 - not because they are connected to the Internet, but because
 - they are connected to enterprise networks that are connected to the Internet
- **Concerns rising over the increasing threat from “insiders”**
 - “Insiders” are not necessarily more hostile, they just have more access

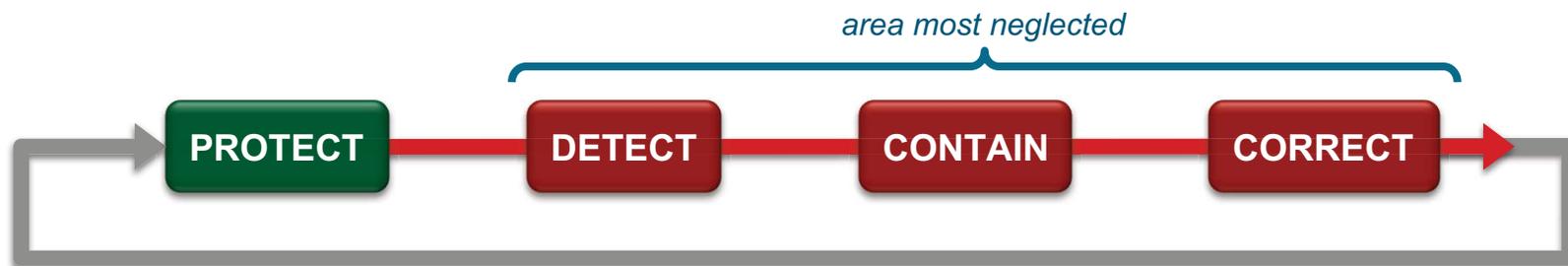


Think like a *hacker* ...



Current ICS Security Practices are Insufficient

- **Once the logical perimeter of the ICS is breached, it is only a matter of time for the ICS to be completely compromised**
 - Firewalls are not as common as most people think
 - Routers are very easy to penetrate
 - Very few architectures implement any perimeter defense-in-depth
- **Most security programs are not risk based**
- **Security controls implemented tend to focus entirely on “prevention”, with little offered to address “detection” and**



Think like a *hacker* ...



New Technologies Act as Game Changer

- **Objectives considered when considering a new security technology:**
 - Resides at the lowest level of the ICS architecture, where devices are most vulnerable
 - Does not affect network or device performance or availability
 - Is implemented external to existing ICS-specific devices
 - Supports ICS-specific protocols
 - Detects “inside” and “outside” attacks
 - Can be used against previously unknown vulnerabilities (zero days)
 - Looks for what is “known good” rather than “known bad” (whitelisting)
 - Detects attempted attacks
 - Supports forensic analysis
 - Integrates with existing security infrastructure (SIEM/SEM, syslog)
 - Affordable
 - Scalable

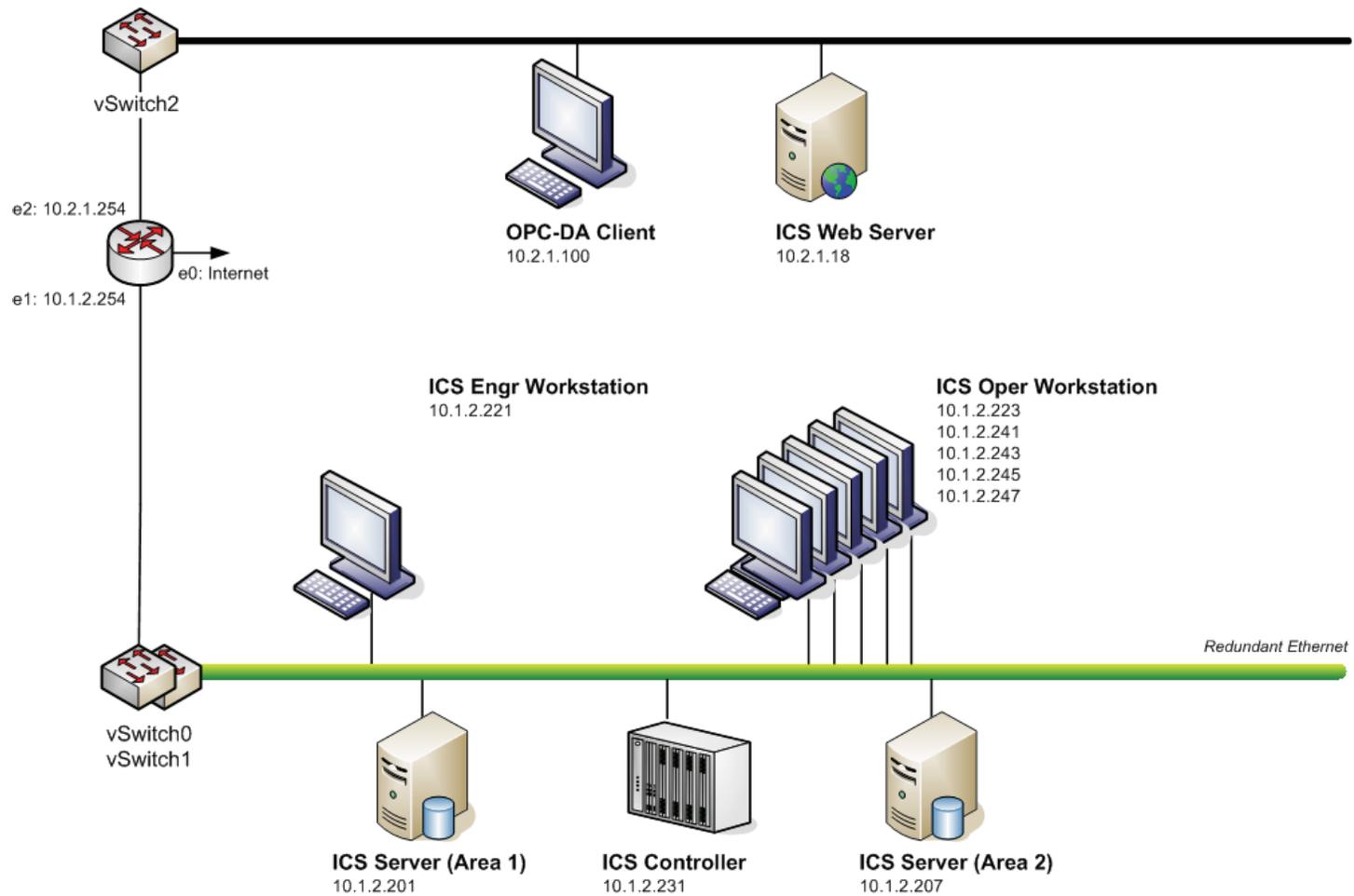


Implementing Intrusion Detection based on Network Behavior

- **Network-based Behavior Analysis**
 - Implemented on core Intrusion Detection platform (SNORT or SURICATA)
 - Simplification through elimination of content inspection (preprocessors) and all previously configured rules
 - Utilizes passively collected network traffic (Wireshark)
 - “Sensors” deployed on any network segment under evaluation
 - Events maintained in industry standard SQL database
- **Steps required to implement an NBA-IDS:**
 1. Collection of “normal” network traffic from all network segments
 2. Mapping of normal traffic flow patterns
 3. Analysis of client-server communications
 4. System definition
 5. Rule Development
 6. Testing
 7. Commissioning



Reference Architecture



Think like a *hacker* ...



Collection of Network Traffic

- **Configure “span” or “port mirroring” on each switch to collect PCAP file of network traffic via Wireshark**

```
C2950# configure terminal
C2950(config)# monitor session 1 source interface range fastethernet 0/1 - 23
C2950(config)# monitor session 1 destination interface fastethernet 0/24
```

- **Merge individual PCAP files into a consolidated file for analysis**

```
root:# merg pcap -w outfile.pcap infile1.pcap infile2.pcap ... infilen.pcap
```

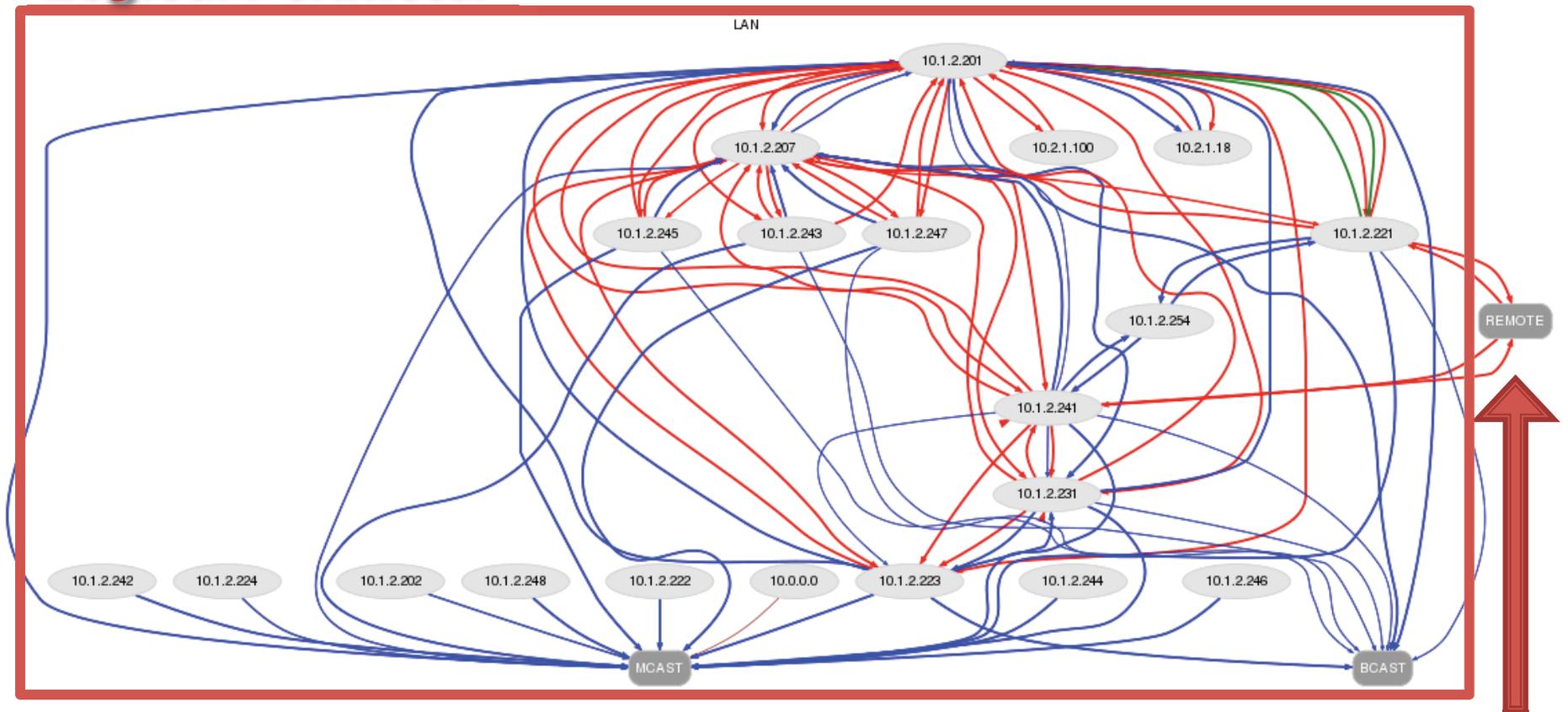
- **Import into Safe Mapping and Reporting Tool (SMART) for analysis**

```
root:# ./smart.pl -N "ICS Behavior Analysis" -L "^10\.1\.|^10\.2\.|^" -r outfile.pcap
```



Mapping of Traffic Flow Patterns (All Communications)

Logical Perimeter



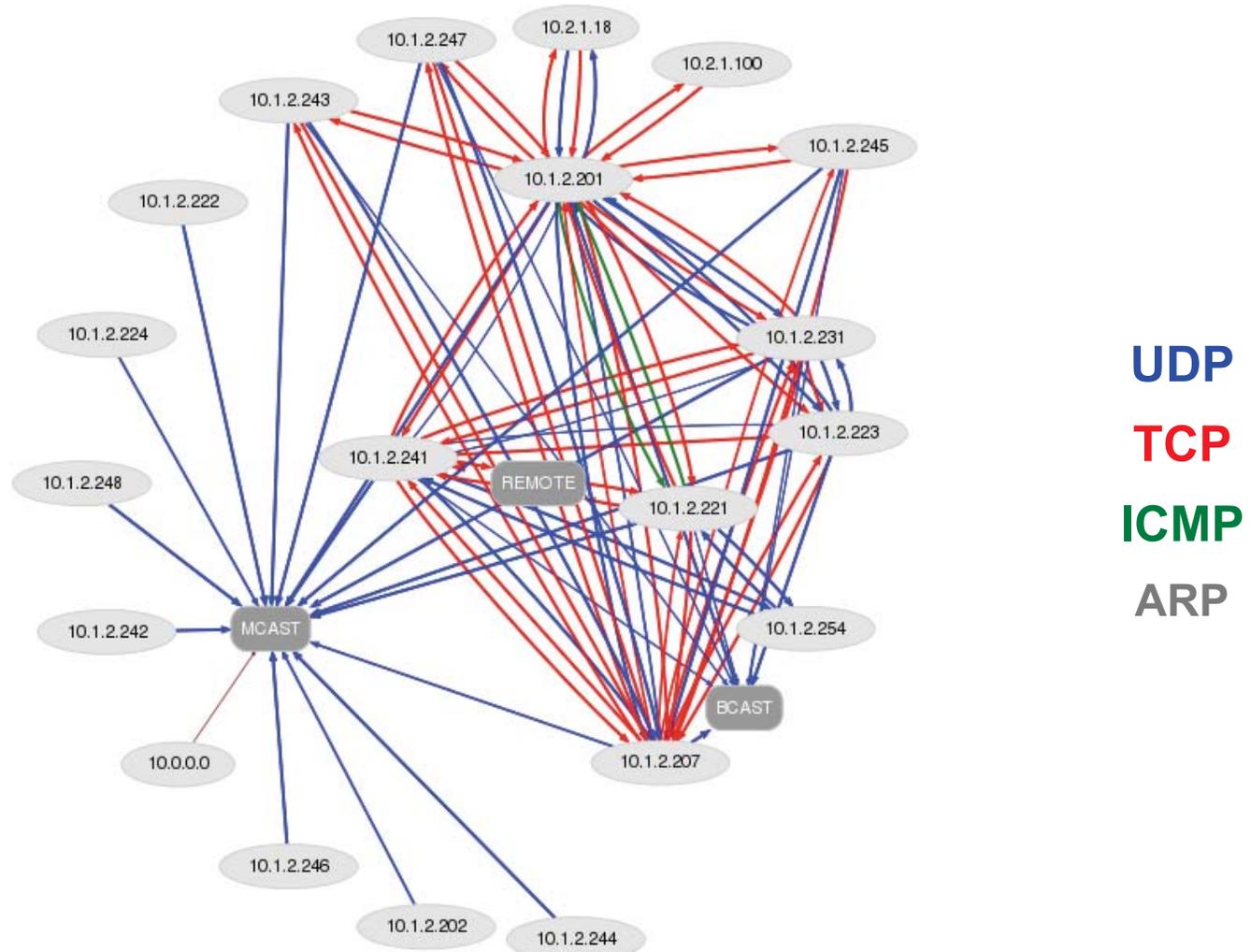
UDP TCP ICMP ARP

External Comms

Think like a *hacker* ...



Mapping of Traffic Flow Patterns (All Communications)

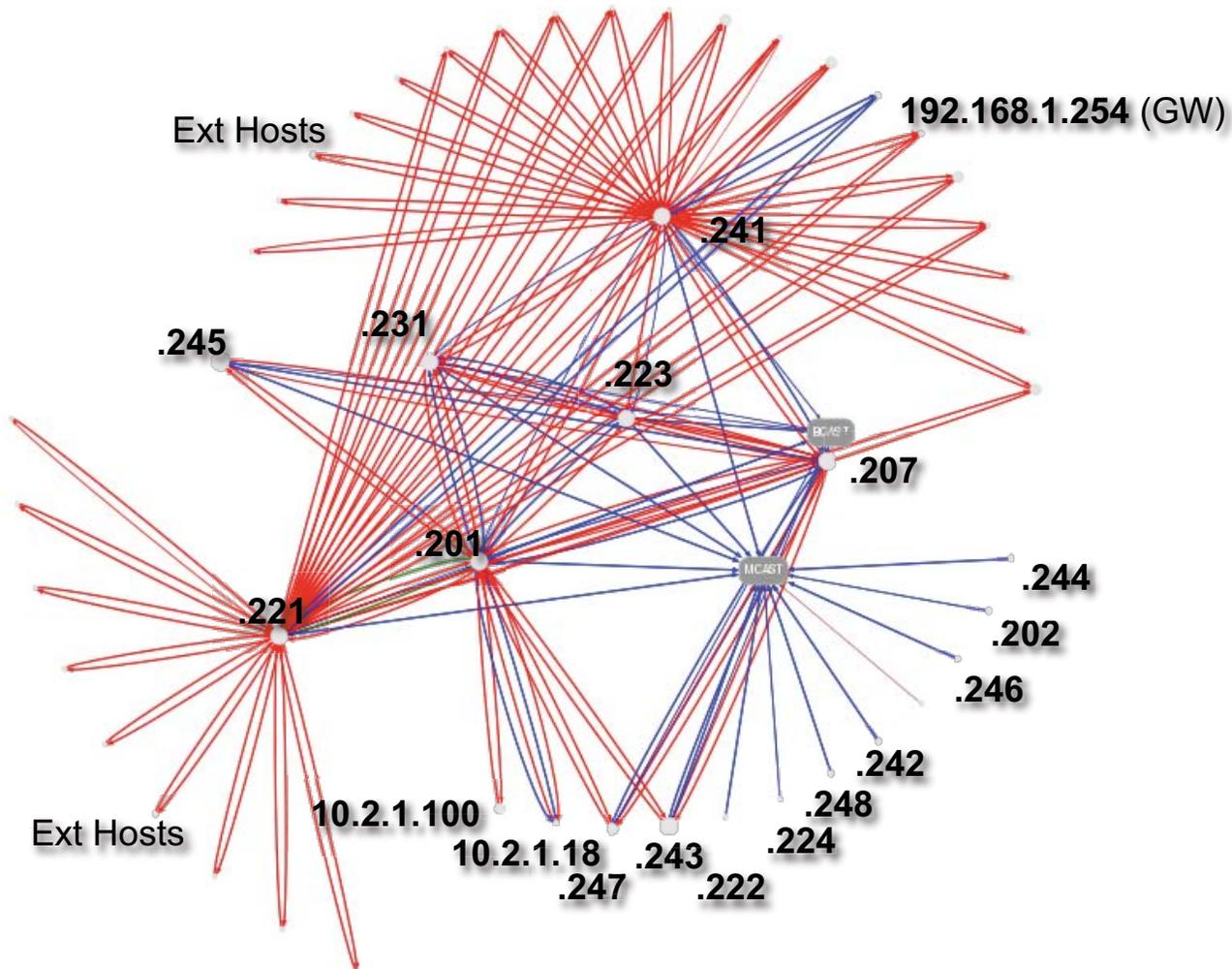


UDP
TCP
ICMP
ARP

Think like a *hacker* ...



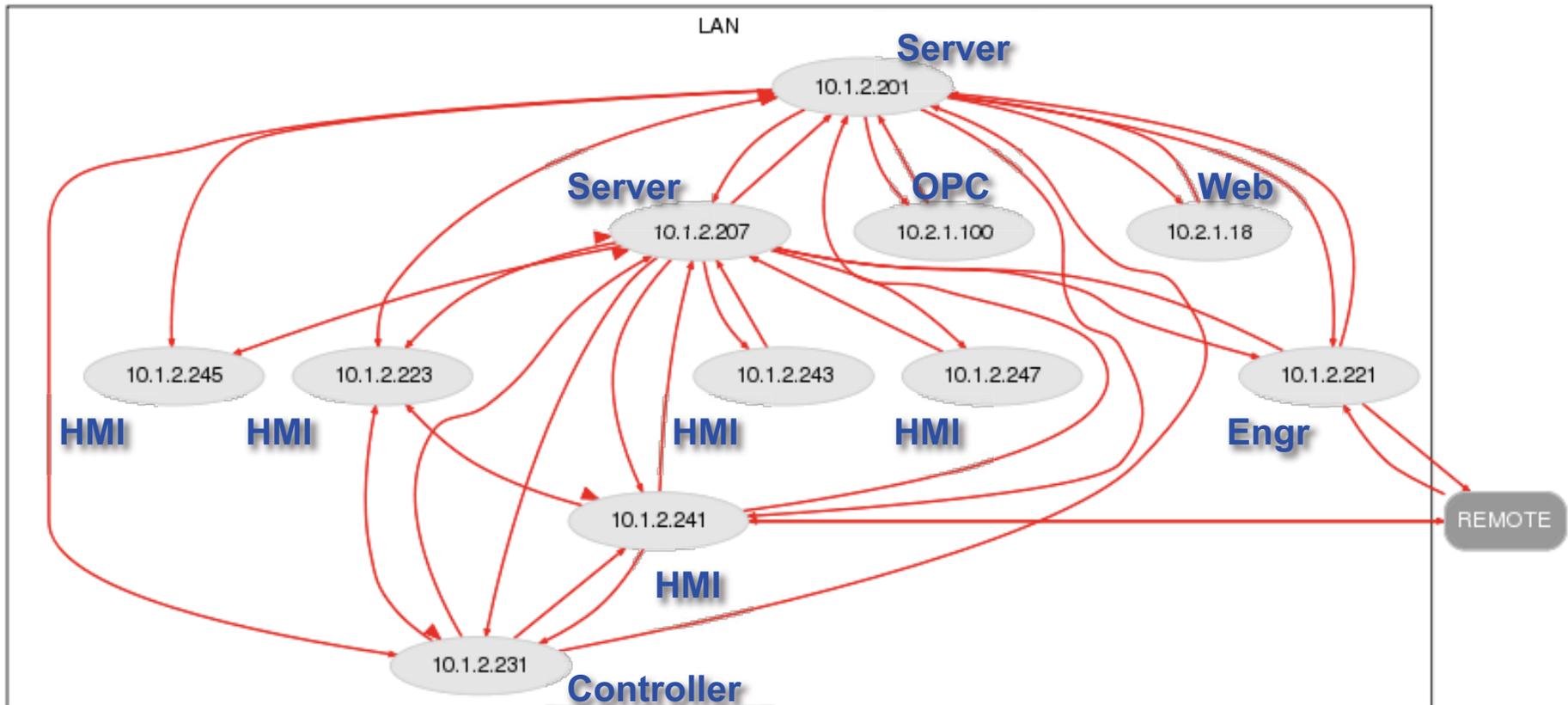
Mapping of Traffic Flow Patterns (All Communications)



Think like a *hacker* ...



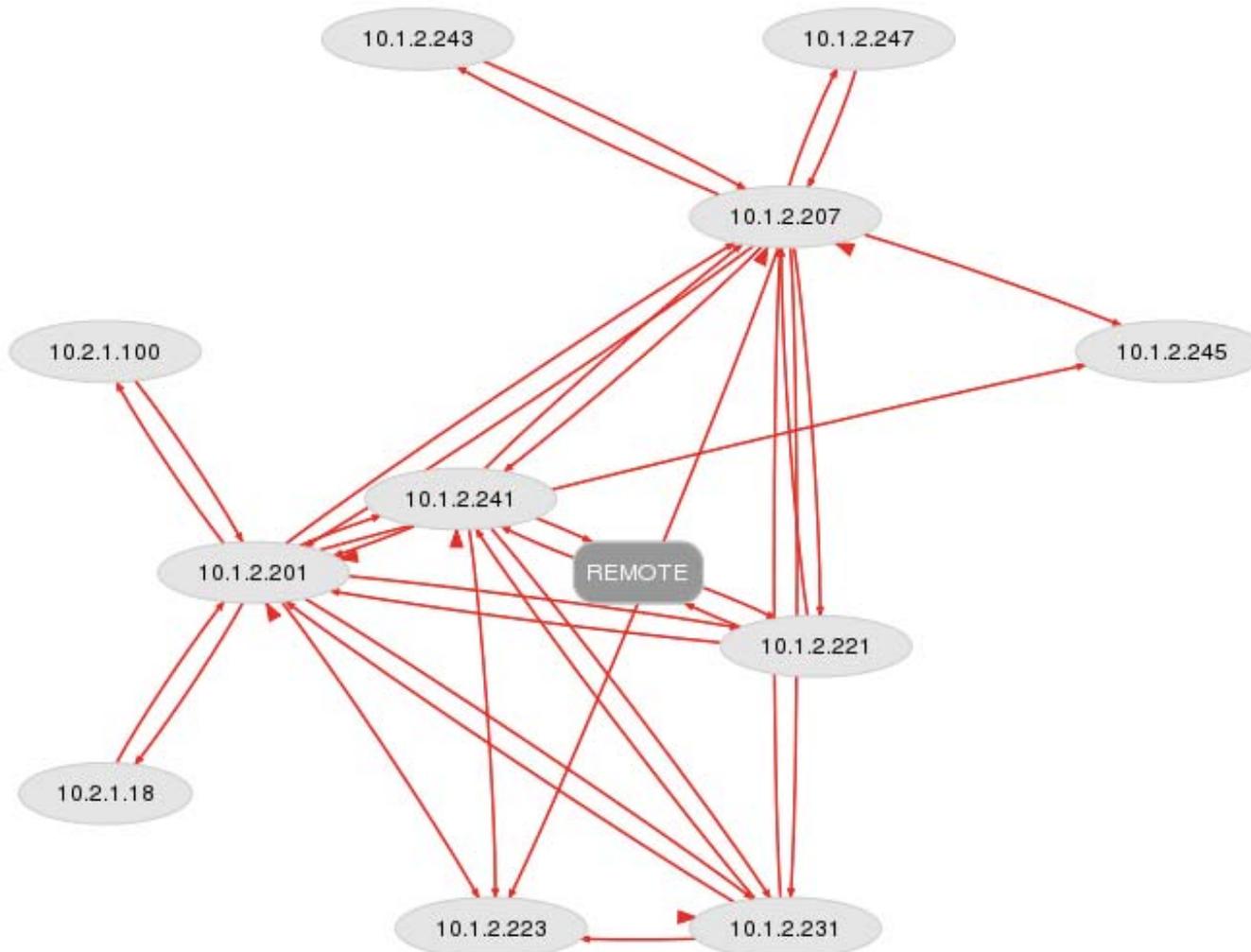
Simplified View of Communications (Established TCP Traffic)



Think like a *hacker* ...



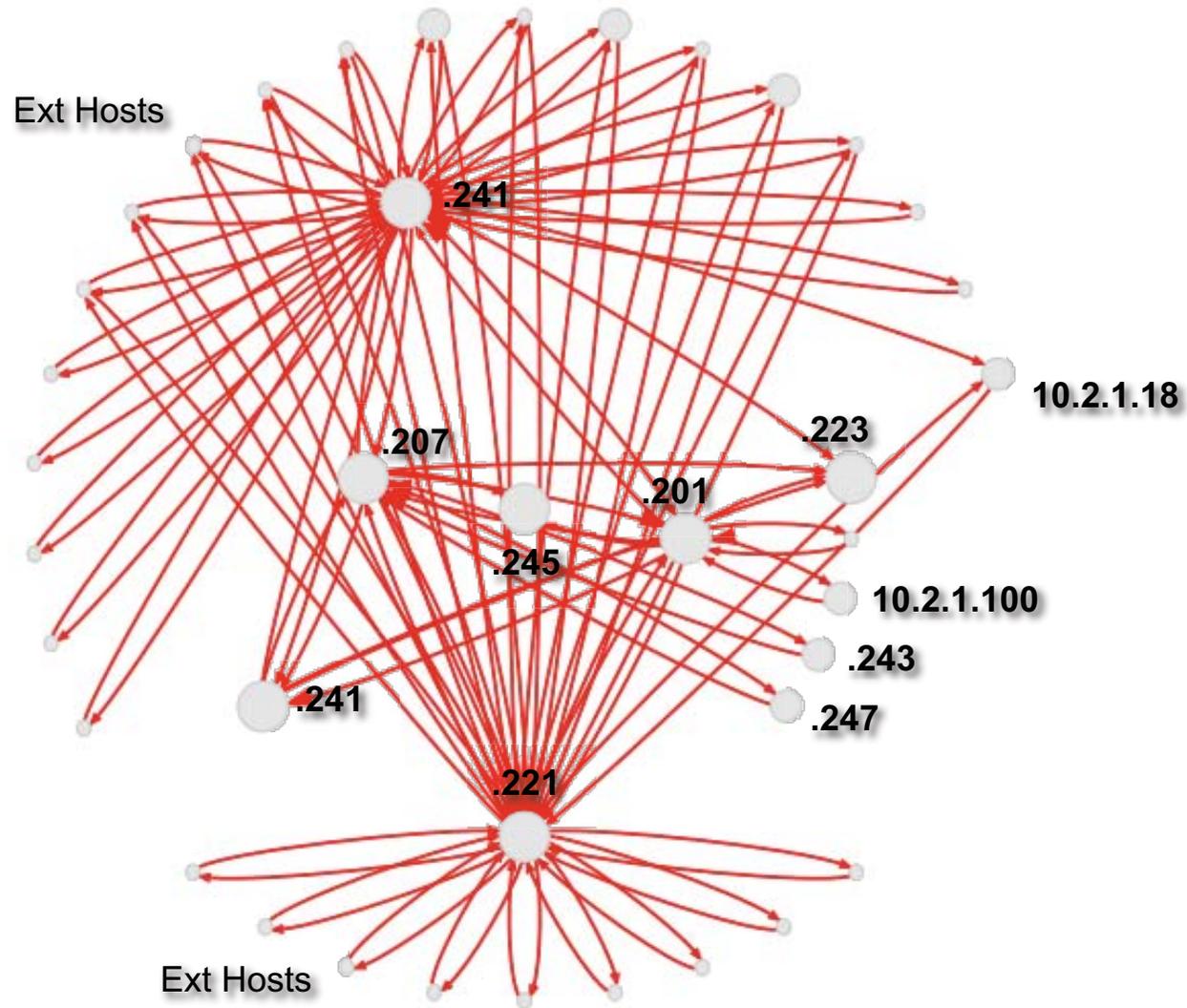
Simplified View (Established TCP Traffic)



Think like a *hacker* ...



Simplified View (Established TCP Traffic)



Think like a *hacker* ...



Analysis of Client-Server Communication

SMART: Local Servers (All Servers)

srcIP	name	srcMAC	srcPORT	proto	description
10.1.2.223		00-0c-29-5f-1b-38	1077	tcp	
10.1.2.223		00-0c-29-5f-1b-38	135	tcp	
10.1.2.223		00-0c-29-5f-1b-38	1040	tcp	
10.1.2.245		00-0c-29-5b-c8-d2	1045	tcp	
10.1.2.245		00-0c-29-5b-c8-d2	135	tcp	
10.1.2.245		00-0c-29-5b-c8-d2	3456	tcp	
10.1.2.245		00-0c-29-5b-c8-c8	1045	tcp	
10.1.2.245		00-0c-29-5b-c8-c8	135	tcp	
10.1.2.221		00-0c-29-87-1f-b1	135	tcp	
10.1.2.221		00-0c-29-87-1f-b1	1098	tcp	
10.1.2.221		00-0c-29-87-1f-a7	135	tcp	
10.1.2.221		00-0c-29-87-1f-a7	1098	tcp	
10.1.2.201		00-0c-29-76-c9-82	135	tcp	
10.1.2.201		00-0c-29-76-c9-82	55556	tcp	
10.1.2.201		00-0c-29-76-c9-82	5012	tcp	
10.1.2.201		00-0c-29-76-c9-82	50000	tcp	
10.1.2.201		00-0c-29-76-c9-82	5002	tcp	rfe 5002/tcp # Radio Free Ethernet
10.1.2.201		00-0c-29-76-c9-82	2910	tcp	
10.1.2.201		00-0c-29-76-c9-82	5013	tcp	
10.1.2.201		00-0c-29-76-c9-82	50003	tcp	
10.1.2.201		00-0c-29-76-c9-82	5001	tcp	
10.1.2.201		00-0c-29-76-c9-82	12321	udp	
10.1.2.247		00-0c-29-a0-a1-a2	135	tcp	
10.1.2.247		00-0c-29-a0-a1-a2	1044	tcp	
10.1.2.243		00-0c-29-79-ad-d2	1043	tcp	
10.1.2.243		00-0c-29-79-ad-d2	135	tcp	
10.1.2.243		00-0c-29-79-ad-dc	1043	tcp	
10.1.2.243		00-0c-29-79-ad-dc	135	tcp	
10.1.2.254		00-0c-29-10-bd-aa	53	udp	domain 53/udp
10.2.1.100		00-0c-29-10-bd-aa	135	tcp	
10.1.2.231		00-0c-29-06-97-9a	1065	tcp	
10.1.2.231		00-0c-29-06-97-9a	135	tcp	
10.1.2.231		00-0c-29-06-97-9a	55553	tcp	
10.1.2.241		00-0c-29-72-c9-89	1044	tcp	
10.1.2.241		00-0c-29-72-c9-89	135	tcp	
10.1.2.241		00-0c-29-72-c9-89	139	tcp	netbios-ssn 139/tcp # NETBIOS session service
10.1.2.241		00-0c-29-72-c9-93	139	tcp	netbios-ssn 139/tcp # NETBIOS session service
10.1.2.241		00-0c-29-72-c9-93	1044	tcp	
10.1.2.241		00-0c-29-72-c9-93	135	tcp	
10.1.2.241		00-0c-29-72-c9-93	137	udp	netbios-ns 137/udp

650,000 Packets
2,500 Unique Sessions
40 Connections

Think like a *hacker* ...



Analysis of Client-Server Communication (Allowed Connections)

	DESTINATION								
	Op Sta	Eng Sta	ICS Srv	PLC	OPC Clt	OPC Srv	Web Srv	Web Clt	Win Srv
Op Sta			✓	✓					✓
Eng Sta			✓	✓		✓	✓		✓
ICS Srv				✓		✓	✓		✓
PLC	✓	✓	✓			✓			
OPC Clt						✓			✓
OPC Srv			✓						✓
Web Srv			✓						✓
Web Clt							✓		
Win Srv									

SOURCE

Think like a *hacker* ...



Analysis of Client-Server Communication (Prohibited Connections)

DESTINATION

SOURCE

	Op Sta	Eng Sta	ICS Srv	PLC	OPC Clt	OPC Srv	Web Srv	Web Clt	Win Srv
Op Sta		X	✓	✓	X	X	X	X	✓
Eng Sta	X		✓	✓	X	✓	✓	X	✓
ICS Srv	X	X		✓	X	✓	✓	X	✓
PLC	✓	✓	✓		X	✓	X	X	X
OPC Clt	X	X	X	X		✓	X	X	✓
OPC Srv	X	X	✓	X	X		X	X	✓
Web Srv	X	X	✓	X	X	X		X	✓
Web Clt	X	X	X	X	X	X	✓		X
Win Srv	X	X	X	X	X	X	X	X	

Think like a *hacker* ...



System Definition – Networks & Hosts

snort.conf

```
# Network Definition
ipvar ICS_NET [10.1.0.0/16,10.2.0.0/16]
ipvar ENT_NET !$ICS_NET
ipvar HOME_NET $ICS_NET
ipvar EXTERNAL_NET any

# Host Definition
ipvar ICS_SERVERS [10.1.2.201/32,10.1.2.207/32,10.2.1.18/32,10.1.2.223/32]
ipvar ICS_OPSTATIONS [10.1.2.221/32,10.1.2.241/32,10.1.2.243/32,10.1.2.245/32,
    10.1.2.247/32]
ipvar ICS_ENGRSTATIONS [10.1.2.221/32]
ipvar ICS_CONTROLLERS [10.1.2.231/32]
ipvar OPC_SERVERS [10.1.2.201/32,10.1.2.207/32]
ipvar OPC_CLIENTS [10.2.1.100/32]
ipvar ICS_WEB [10.2.1.18/32]
ipvar ICS_MULTICAST [224.0.0.105/32,225.7.4.103/32]
ipvar SERVERS [$ICS_SERVERS]
ipvar CLIENTS [$ICS_ENGRSTATIONS,$ICS_OPSTATIONS]
ipvar ICS_COMPOSITE [$ICS_SERVERS,$ICS_OPSTATIONS,$ICS_ENGRSTATIONS,
    $ICS_CONTROLLERS,$OPC_SERVERS,$OPC_CLIENTS,$ICS_WEB]
```

Think like a *hacker* ...



System Definition – Communications

snort.conf

Communication Definitions

```
portvar OPC_DA_PORTS [135,5000:5100]
portvar MODBUS_TCP_PORTS [502]
portvar HTTP_PORTS [80,50000]
portvar SSH_PORTS [22]
portvar SMB_PORTS [139,445]
portvar ICS_UDP_PORTS [53,135:139,12321]
portvar ICS_PORTS [1433,2909:2910,3456,50000:50005,55550:55560,$OPC_DA_PORTS,
    $MODBUS_TCP_PORTS,$HTTP_PORTS,$SMB_PORTS]
```

Rules Definitions

```
include $RULE_PATH/local.ics.rules
include $RULE_PATH/vulnerability_exploit.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/scan.rules
```

Think like a *hacker* ...



Rule Development

- **All SNORT / SURICATA “rules” consist of two (2) components:**

- Rule Header

- action

- alert, activate, dynamic, log, pass ▪ protocol
ip, tcp, udp, icmp ▪ addresses
source/destination ▪ protocol ports
source/destination ▪ direction

->, <>

- Rule Options

```
alert icmp any any -> any any (msg:"ICMP Ping Echo Request"; itype:8; sid:1000001;)
```

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"Web-Misc http directory traversal"; flow:to_server,established; content:"..|5c|"; classtype:attempted-recon; sid:1112; rev:6;)
```



Rule Development – Host-to-Host Communication

local.ics.rules

```
# These required ESTABLISHED connections (3-way handshake successful)

alert tcp $ICS_OPSTATIONS any -> $ICS_SERVERS !$ICS_PORTS (msg:"ICS Suspicious
Activity - Invalid Communications - HMI-to-Server"; flow:established,to_server;
classtype:misc-activity; sid:3100201; rev:0;)

alert tcp $ICS_ENGRSTATIONS any -> $ICS_SERVERS !$ICS_PORTS (msg:"ICS Suspicious
Activity - Invalid Communications - Engineering Stations-to-Server";
flow:established,to_server; classtype:misc-activity; sid:3100202; rev:0;)

alert tcp $OPC_CLIENTS any -> $OPC_SERVERS !$OPC_DA_PORTS (msg:"ICS Suspicious
Activity - Invalid Communications - OPC Client-to-Server";
flow:established,to_server; classtype:misc-activity; sid:3100203; rev:0;)

alert tcp ![$ICS_ENGRSTATIONS,$ICS_OPSTATIONS,$ICS_SERVERS] any -> $ICS_CONTROLLERS
any (msg:"ICS Suspicious Activity - Invalid Communication between Unknown Host
on ICS Net and Controllers!"; flow:established,to_server; classtype:misc-
activity; sid:3100204; rev:0;)

alert tcp !CLIENTS any -> !$SERVERS $SMB_PORTS (msg:"ICS NETBIOS-SMB Illegal
Network Request - Potential Data Collection"; flow:established,to_server;
classtype:misc-activity; sid:3100107; rev:0;)
```

Think like a *hacker* ...



Rule Development – Host-to-Host Communication

local.ics.rules

```
# These required ATTEMPTED connections (SYN flag set; 3-way handshake incomplete/  
unsuccessful)  
  
alert tcp ![$ICS_ENGRSTATIONS,$ICS_OPSTATIONS,$ICS_SERVERS] any -> $ICS_CONTROLLERS  
$ICS_PORTS (msg:"ICS Security Breach - Inside/Outside Attempt to Connect to  
Valid Port/Service - check detailed log for further information"; flags: S;  
classtype:misc-activity; sid:3100205; rev:0;)  
  
alert tcp $SERVERS any -> $CLIENTS any (msg: "ICS Suspicious Activity - Illogical  
TCP Communication - Possible Virus/Attack in Progress"; flags: S;  
classtype:misc-activity; sid:3100206; rev:0;)  
  
alert udp $SERVERS any -> [$CLIENTS,!$ICS_MULTICAST] any (msg: "ICS Suspicious  
Activity - Illogical UDP Communication - Possible Virus/Attack in Progress";  
classtype:misc-activity; sid:3100207; rev:0;)
```

Think like a **hacker** ...



Rule Development – Information Gathering

local.ics.rules

```
alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP ECHO REQUEST";
  itype:8; classtype:misc-activity; sid:3100101; rev:0;)

alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP PING *NIX";
  itype:8; content:"|10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|"; depth:32;
  classtype:misc-activity; sid:3100102; rev:0;)

alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP PING Microsoft
  Windows"; itype:8; content:"abcdefghijklmnop"; depth:32; reference:arachnids,
  159; classtype:misc-activity; sid:3100103; rev:0;)

alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP PING LINUX/
  *BSD"; dsize:8; id:13170; itype:8; reference:arachnids,447; classtype:misc-
  activity; sid:3100104; rev:0;)

alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP Traceroute";
  icode:0; itype:30; classtype:misc-activity; sid:3100105; rev:0;)

alert icmp !$ICS_COMPOSITE any -> $ICS_COMPOSITE any (msg:"ICS ICMP Traceroute
  undefined code"; icode:>0; itype:30; classtype:misc-activity; sid:3100106; rev:
  0;)
```

Think like a *hacker* ...



Testing and Validation

- For the purposes of this demonstration, the following commands were executed from a

```
# Nmap scan
root:# nmap 10.1.2.201

# Ping
root:# ping 10.1.2.201

# SMB/CIFS File-Sharing Connection
root:# mount -t cifs -o username=user,password=pass //10.1.2.201/share /mnt/smb

# Attempt to connect to valid port not used by ICS server
root:# nc 10.1.2.201 3389

# Attempt to connect to valid port used by ICS controller
root:# nc 10.1.2.231 55555

# Attempt to connect to invalid port
root:# nc 10.1.2.201 49999

# Attempt to connect to valid port used by ICS server
root:# nc 10.1.2.201 50000
```



Results from Control Network “Inside” Attack – Known Host

- 1 Nmap
- 2 Ping
- 3 SMB/CIFS (tcp/445)
- 4 RDP (tcp/3389)
- 5 Connect to Controller (tcp/55555)
- 6 Connect to Server (tcp/49999)
- 7 Connect to Server (tcp/50000)

1,6
4,6

ST	CNT	Sen...	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1053	eth1	2.15894	2011-06-01 15:50:14	10.1.2.247	63782	10.1.2.201	5900	6	ICS Security Breach - Inside Attempt to Connect to Invalid Port/Service - chec...
RT	2	eth1	2.16947	2011-06-01 15:51:05	10.1.2.247	55028	10.1.2.201	3389	6	ICS Suspicious Activity - Invalid Communications - HMI-to-Server

Think like a *hacker* ...



Results from Control Network “Inside” Attack – Unknown Host

- 1 Nmap
- 2 Ping
- 3 SMB/CIFS (tcp/445)
- 4 RDP (tcp/3389)
- 5 Connect to Controller (tcp/55555)
- 6 Connect to Server (tcp/49999)
- 7 Connect to Server (tcp/50000)

1,4,6
1,3,5,7
2
2
3
5
5

ST	CNT	Sen...	Aler...	D...	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1048	eth1	2.16...	2...	10.1.2.18	63765	10.1.2.201	587	6	ICS Security Breach - Outside Attempt to Connect to Invalid Port/Service - check detailed log for fu...
RT	33	eth1	2.16...	2...	10.1.2.18	63765	10.1.2.201	445	6	ICS Security Breach - Outside Attempt to Connect to Valid Port/Service - check detailed log for furt...
RT	10	eth1	2.18...	2...	10.1.2.18		10.1.2.201		1	ICS ICMP PING *NIX
RT	10	eth1	2.18...	2...	10.1.2.18		10.1.2.201		1	ICS ICMP ECHO REQUEST
RT	19	eth1	2.18...	2...	10.1.2.18	51711	10.1.2.201	445	6	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection
RT	1	eth1	2.18...	2...	10.1.2.18	54936	10.1.2.231	55555	6	ICS Security Breach - Inside/Outside Attempt to Connect to Valid Port/Service - check detailed log ...
RT	2	eth1	2.18...	2...	10.1.2.18	54936	10.1.2.231	55555	6	ICS Suspicious Activity - Invalid Communication between Unknown Host on ICS Net and Controllers!

Think like a *hacker* ...



Results from Enterprise Network “Inside” Attack – Authorized Host

- 1 Nmap
- 2 Ping
- 3 SMB/CIFS (tcp/445)
- 4 RDP (tcp/3389)
- 5 Connect to Controller (tcp/55555)
- 6 Connect to Server (tcp/49999)
- 7 Connect to Server (tcp/50000)

SGUIL-0.7.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: administrator UserID: 2 2011-06-01 16:33:08 GMT

RealTime Events Escalated Events

ST	CNT	Sen...	Aler...	D...	Src IP	SPort	Dst IP	DPort	Pr	Event Message	
1	RT	1	eth1	2.20...	2...	192.168.11.50	10.1.2.201		1	ICMP PING NMAP	
1,2	RT	11	eth1	2.20...	2...	192.168.11.50	10.1.2.201		1	ICS ICMP ECHO REQUEST	
1,4,5,6,7	RT	1088	eth1	2.20...	2...	192.168.11.50	63849	10.1.2.201	443	6	ICS Security Breach - Attempt to Connect to ICS Network from Outside/Enterprise Network - ch...
1,5	RT	1057	eth1	2.20...	2...	192.168.11.50	63849	10.1.2.201	443	6	ICS Security Breach - Outside Attempt to Connect to Invalid Port/Service - check detailed log f...
2,7	RT	31	eth1	2.20...	2...	192.168.11.50	63849	10.1.2.201	80	6	ICS Security Breach - Outside Attempt to Connect to Valid Port/Service - check detailed log for ...
3	RT	10	eth1	2.22...	2...	192.168.11.50		10.1.2.201		1	ICS ICMP PING *NIX
5	RT	19	eth1	2.22...	2...	192.168.11.50	58069	10.1.2.201	445	6	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection
5	RT	1	eth1	2.22...	2...	192.168.11.50	49284	10.1.2.231	55555	6	ICS Security Breach - Inside/Outside Attempt to Connect to Valid Port/Service - check detailed ...
5	RT	2	eth1	2.22...	2...	192.168.11.50	49284	10.1.2.231	55555	6	ICS Suspicious Activity - Invalid Communication between Unknown Host on ICS Net and Contr...

Think like a *hacker* ...



The Million Dollar Question ... “Would this have detected Stuxnet???”

SGUIL-0.7.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: administrator UserID: 2 2011-06-01 23:06:23 GMT

RealTime Events Escalated Events

ST	CNT	Se...	Alert ...	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	11	eth1	3.278	2011-06-0...	10.1.2.201	2630	10.1.2.221	3456	6	ICS Suspicious Activity - Illogical TCP Communication - Possible Virus/Attack in Progress
RT	292	eth1	3.279	2011-06-0...	10.1.2.201	3087	10.1.2.231	139	6	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection
RT	3	eth1	3.283	2011-06-0...	10.1.2.201		10.1.2.231		1	ICMP L3retriever Ping
RT	3	eth1	3.311	2011-06-0...	10.1.2.201	3093	10.1.2.231	1130	6	ICS Security Breach - Inside Attempt to Connect to Invalid Port/Service - check detailed log for furthe...

YES !!!

Think like a *hacker* ...



The Million Dollar Question ... “Would this have detected Stuxnet???”

View: signature Sensor: All Sensors Status: --

Start: 2011-06-01 17:45:00 End: 2011-06-01 18:10:00 submit reset

M-D/H	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	EVENTS	%
06-01																									309	100%

click the cell again to go back

Report Period: Between Wednesday Jun 1, 2011 17:45:00 and Wednesday Jun 1, 2011 18:10:00 (0.02 days)
Report Filter(s):
Distinct Event(s): 4
Total Event(s): 309
Last Event: 11-06-01 18:04:19 (5.75 minutes ago)
Query Time: 0.004 seconds

visuals map create ip2c

Count	Src	Dst	Signature	SigID	Proto	Last Event
292	1	2	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection	3100107	TCP	11-06-01 18:04:19
11	1	1	ICS Suspicious Activity - Illogical TCP Communication - Possible Virus/Attack in Progress	3100206	TCP	11-06-01 18:04:03
3	1	2	ICMP L3retriever Ping	466	ICMP	11-06-01 18:04:03
3	1	2	ICS Security Breach - Inside Attempt to Connect to Invalid Port/Service - check detailed log for further information	3100303	TCP	11-06-01 18:04:03

status: -- submit reset

M-D/H	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	EVENTS	%
06-01																									292	100%

click the cell again to go back

Report Period: Between Wednesday Jun 1, 2011 17:45:00 and Wednesday Jun 1, 2011 18:10:00 (0.02 days)
Report Filter(s): ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection
Distinct Event(s): 2
Total Event(s): 292
Last Event: 11-06-01 18:04:19 (6.37 minutes ago)
Query Time: 0.004 seconds

visuals map create ip2c

Count	Last Event	Source	Destination	Signature	SigID
191	11-06-01 18:04:19	10.1.2.201	10.1.2.221	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection	3100107
101	11-06-01 18:04:03	10.1.2.201	10.1.2.231	ICS NETBIOS-SMB Illegal Network Request - Potential Data Collection	3100107

Think like a *hacker* ...



The Million Dollar Question ...

“Would this have detected Stuxnet???”

10.1.2.201_3087_10.1.2.231_139-6.raw - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.2.201	10.1.2.231	TCP	3087 > 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000071	10.1.2.231	10.1.2.201	TCP	139 > 3087 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000113	10.1.2.201	10.1.2.231	TCP	3087 > 139 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.000148	10.1.2.201	10.1.2.231	NBSS	Session request, to SCE01R3102<20> from EPKSR3102<00>
5	0.000211	10.1.2.231	10.1.2.201	NBSS	Positive session response
6	0.000500	10.1.2.201	10.1.2.231	SMB	Negotiate Protocol Request
7	0.000938	10.1.2.231	10.1.2.201	SMB	Negotiate Protocol Response
8	0.001568	10.1.2.201	10.1.2.231	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
9	0.002298	10.1.2.231	10.1.2.201	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10	0.002661	10.1.2.201	10.1.2.231	SMB	Session Setup AndX Request, NTLMSSP_AUTH, User: \
11	0.003359	10.1.2.231	10.1.2.201	SMB	Session Setup AndX Response
12	0.003680	10.1.2.201	10.1.2.231	SMB	Tree Connect AndX Request, Path: \\SCE01R3102\IPC\$
13	0.003799	10.1.2.231	10.1.2.201	SMB	Tree Connect AndX Response

Frame 1 (62 bytes on wire, 62 bytes captured)

- Ethernet II, Src: 00:0c:29:76:c9:82 (00:0c:29:76:c9:82), Dst: 00:0c:29:06:97:9a (00:0c:29:06:97:9a)
- Internet Protocol, Src: 10.1.2.201 (10.1.2.201), Dst: 10.1.2.231 (10.1.2.231)
- Transmission Control Protocol, Src Port: 3087 (3087), Dst Port: 139 (139), Seq: 0, Len: 0

Complete forensic data for each packet!

Think like a *hacker* ...



SCADAhacker.com

Think like a *hacker* ...

Additional Information:

joel@SCADAhacker.com

www.SCADAhacker.com

@SCADAhacker

+1.623.476.9667

