

Security tools  
Introduction

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

Learning goals



- Explore the landscape of security tools
- Understand a possible taxonomy of these tools
  - To understand key categories of security tools
  - To understand how new tools new tools you encounter connect to existing tools

2 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

Security tool(s)

- Tools to observe, monitor, and/or create/modify bits to ensure that C.I.A. is maintained
- But... a major problem with security tools
  - Dual Purpose/Use

3 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

**WARNING**



**\*\*\* IMPORTANT \*\*\***

- Do not use these tools without:
  - Truly understanding what the tool does and what its side effects may be
  - Getting proper (written) authorization to use the tool in/on the environment you intend to use it in/on

4 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

**Security tools**



- More “silicon snake oil”
- Tools are often sold as things to solve a problem, so that you don’t have to THINK about the problem
- Vendors often make assumptions about technology environment
- Increasingly, tools try to spread into other tools markets
  - One tool does it all

5 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

**A simple taxonomy**

- Blocking tools
- Detection tools
- Probing tools
- Offensive tools
- Just one of many ways to classify these tools
- Some tools span more than one category

6 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

### Topics



- Blocking tools – part I – R  
NACs, ACLs, Firewalls
- Blocking tools – part II – R  
Content checkers, IPSs, WAFs
- Detection tools – R  
File integrity checkers, packet sniffers, IDSs
- Probing tools – R  
Vulnerability, policy compliance, penetration testing
- Offensive tools – R  
Packet generators, brute force, hijacking, fingerprinting

7 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
4	<a href="https://en.wikipedia.org/wiki/File:UK_traffic_sign_562.sv">https://en.wikipedia.org/wiki/File:UK_traffic_sign_562.sv</a>
8	
5	<a href="http://www.kitsch-slapped.com/wp-content/uploads/2011/01/1950-snake-oil-is-wonderful-stuff-500x722.jpg">http://www.kitsch-slapped.com/wp-content/uploads/2011/01/1950-snake-oil-is-wonderful-stuff-500x722.jpg</a>
7	Partial view of Harvard AutoReg screen
7	<a href="http://www.supercool.ac/wp-content/uploads/2011/10/STOPA.png">http://www.supercool.ac/wp-content/uploads/2011/10/STOPA.png</a>
7	Foca, Snort, Hydra logos

8 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---



### Subcategories of blocking tools

- **Devices**
  - Network Access Control (NAC)
- **Packet and format centric**
  - Access Control Lists (ACLs)
  - Firewalls
- **Content centric**
  - Web Application Firewall
  - Content checkers
  - Virus and worm checkers
  - Intrusion Prevention Systems (IPS)

4

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

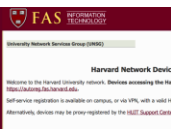
---

---

---

---

### Network Access Control (NAC)



- Network registration systems
- Generally require some form of user computer registration
- Can verify policy compliance before a access
- Ensures endpoints are not vulnerable to attack before enabling network access (patched, have AV, etc.)

5

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

---

---

---

---

### Subcategories of blocking tools

- **Devices**
  - Network Access Control (NAC)
- **Packet and format centric**
  - Access Control Lists (ACLs)
  - Firewalls
- **Content centric**
  - Web Application Firewall
  - Content checkers
  - Virus and worm checkers
  - Intrusion Prevention Systems (IPS)

6

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

---

---

---

---

## Access Control Lists (ACLs)



- Provide programmable, stateless filtering function  
Found in routers, some switches, host-based firewalls
- Filter on:
  - Source/destination/ IP/MAC address/prefix or protocol
  - TCP/UDP source/destination port value
  - Input/output logical or physical port
  - Other header information
- Forward, redirect, discard, count based on filter

7

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## ACLs, contd.

```
#access-list 10 deny 172.16  
#access-list 10 permit host  
#access-list 10 deny 172.16  
#access-list 10 permit any
```

- Advantages:
  - Cheap - present in most routers and many switches, no extra box or extra cost
  - Fast
  - Simple
- Disadvantages:
  - Usually stateless
  - Typically support only static configurations
  - Less flexible

8

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

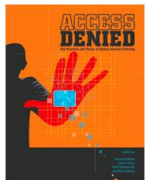
---

---

---

---

## Firewalls



- Can be dedicated hardware or software
- Can be stateless or stateful
- Filter inbound or outbound traffic, or both
- Can take many different actions:
  - Forward, redirect, monitor, discard, drop, notify
  - Combinations of the above

9

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## Application Layer Gateway (ALG)

- The way a firewall understands application protocols  
E.g., SIP (voice over IP) or Active FTP  
both use dynamic ports and IP addresses within data packets
- Can also “open ports” on firewall based on application signaling

10

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## Host based firewalls



- Most operating systems include a simple packet filtering firewall  
e.g. Windows Firewall, iptables, pf  
Should be configured to permit applications  
Disable all other traffic (aka “default deny”)
- Should be enabled  
Provide another layer of defense  
Can be a support nightmare  
Can be subverted by local administrator

11

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## Other firewall functions

- Logging denied traffic  
To see if site is under attack  
May slow things considerably
- Terminate VPN tunnels  
Added function on some firewalls  
Encrypt / decrypt traffic  
Identity-based access

12

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Firewalls, contd.

- **Advantages**
  - Block simple attacks
  - More flexible than ACLs alone
- **Disadvantages**
  - Hard to configure/poorly configured
    - too many holes
  - Configurations can be complex (many rules)
  - Only filter inbound traffic by default
  - Easily tunneled through
    - see RFC 3093

13

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Firewalls, contd.



- **Biggest issues with firewalls:**
  - Break E2E Internet and thus can make deployment of new applications hard
    - can also be an advantage - block unapproved applications
  - Not great at blocking insider threats
    - Not generally in the path for inside to inside traffic
    - Not generally configured to stop someone inside attacking out or malware "calling home" for instructions
  - Provide false sense of security
    - reduced attention to security "inside" because of "firewall protection" – "Crustacean Security"

14

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
5	PacketFence logo
7	<a href="http://media.news.harvard.edu/gazette/wp-content/uploads/2010/04/access_controlled_300_Book_FuII.jpg">http://media.news.harvard.edu/gazette/wp-content/uploads/2010/04/access_controlled_300_Book_FuII.jpg</a>
9	<a href="http://oni-access.net/wp-content/uploads/2011/12/denied-180px.png">http://oni-access.net/wp-content/uploads/2011/12/denied-180px.png</a>
11	IPTables firewall logo
14	<a href="http://cdn.meme.am/instances/500x/57873562.jpg">http://cdn.meme.am/instances/500x/57873562.jpg</a>

15

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---





### Content checkers, contd.



- More use cases:  
Companies want to be sure their employees are not reading or sending “bad” content
  
- Spam Blocking
  
- Data Leak Prevention/Protection (DLP)  
SSN, account numbers, student ID, etc.

4

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

---

---

---

---

### Content checkers, contd.

- Advantages  
Help compliance  
Reduce risk of lawsuits/legal issues  
Protect IP assets
- Disadvantages  
Authoritarian - can be a censorship tool  
Complex - hard to keep up with matching expressions to tag/block, report  
Dumb - Easily avoided by rewording or reformatting or using encryption

5

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

---

---

---

---

### Virus and worm checkers



- Special case of content checker
- Most do a pattern match on features of worm or virus  
Uses “signatures” of features (e.g., bit patterns)  
Good at fighting “yesterday’s attack”  
Patterns must be updated frequently
- Heuristic-based detection becoming more common  
“Learns” to identify malware

6

Copyright © Scott Bradner & Ben Gaucher in 2015

---

---

---

---

---

---

---

---

### Virus and worm checkers, contd.

- Can run:
  - In-line (traffic passes through)
  - On mail server (common)
  - On local host (most common)
- Lots of vendors providing features in this area - e.g.:
  - Implement kernel interface or disk files to see when something "bad" happens - e.g., accessing Windows registry
  - Real time reporting of malware and distribution of signatures when outbreak detected on Internet

7

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Intrusion Prevention System (IPS)



- Goal: block attacks while they are happening
- Inline device (traffic goes through – or doesn't)
  - Differentiates IPS from IDS
- Examines packets, then interrupts sessions/drops packets to block attacks
  - Difficult to implement on robust network architectures
  - Must intercept all paths to be effective
  - Works against network design goals

8

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### IPS, contd.

- Can be stand-alone device or built into routers
- Can use signatures, heuristics, reputation, or content checkers
  - e.g., block access from known bad addresses, check Java/ActiveX for malicious content
- Often integrated into firewalls
  - "Next Generation Firewall"

9

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### IPS, contd.

- **Advantages**
  - Ideally, can block attack before much damage done
  - Respond faster than a human (and may be responding correctly)
- **Disadvantages**
  - Response still takes time
    - by the time filters are applied, attack may be complete
  - False alarms / spoofed traffic can be a self-inflicted DoS enabler

10

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Web Application Firewalls (WAF)

Name	Description
WordPress Exploit Common Exploit	Block cookies, forbid some plugins
General Exploit Safe Request Methods	Denies a GET, POST
General Exploit SPECIFIC CHARACTERS	Denies a character REALLY depends
General Exploit Bogus Graphics Exploit	Denies a

- Similar to a Firewall – but for web applications
  - Can either be an appliance (commercial)
  - Or a server plugin, e.g. ModSecurity for Apache
- Required by some standards (e.g. PCI)
- Detects attacks via the web application level (the webpage)

11

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### WAF, contd.

- **Advantages**
  - Can block many web attacks
    - E.g. SQL Injection, XSS (Cross-site scripting)
  - Allows for quick reaction to emerging threats
- **Disadvantages**
  - May need to be highly customized
  - Can also block legitimate traffic
    - MUST be maintained as the application is modified

12

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

3 "Loose lips might sink ships" by Unknown - <http://www.jtfgtmo.southcom.mil/wire/WirePDF/v9/Issue%20260.pdf>. Licensed under Public Domain via Commons -

[https://commons.wikimedia.org/wiki/File:Loose\\_lips\\_might\\_sink\\_ships.jpg#/media/File:Loose\\_lips\\_might\\_sink\\_ships.jpg](https://commons.wikimedia.org/wiki/File:Loose_lips_might_sink_ships.jpg#/media/File:Loose_lips_might_sink_ships.jpg)

4 <http://www.supercool.ac/wp-content/uploads/2011/10/STOPA.png>

4 <http://s3.amazonaws.com/rapgenius/survey-invitation-spam-filter-300x225.jpg>

4 [https://upload.wikimedia.org/wikipedia/commons/thumb/b/7/70/Censored\\_rubber\\_stamp.svg/2000px-Censored\\_rubber\\_stamp.svg.png](https://upload.wikimedia.org/wikipedia/commons/thumb/b/7/70/Censored_rubber_stamp.svg/2000px-Censored_rubber_stamp.svg.png)

8 [http://www.cisco.com/c/dam/en/us/products/vpndevc/ps5729/ps5713/ps12156/ciscoip\\_large.jpg](http://www.cisco.com/c/dam/en/us/products/vpndevc/ps5729/ps5713/ps12156/ciscoip_large.jpg)

13

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

Security tools  
Detection tools

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

Detection tools

- Packet sniffers  
Parse network traffic  
e.g., Wireshark, tcpdump
- File integrity checkers  
Verify that files have not changed  
e.g., Tripwire, OSSEC
- Intrusion detection systems  
Detect malicious activity, like IPS  
e.g., Snort, Bro

2 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---


---

---

---

Packet sniffers

**TCPDUMP**



- Tool to intercept and decode packets on a network  
Generally have configurable input filters - trigger on particular packet info (e.g. src/dst address or port)
- Original developed for debugging hardware & software
- Can also be used as a spy/wiretapping tool  
e.g., capture all traffic from selected host, save & examine

3 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Packet sniffers, contd.

- **Advantages**
  - Simple, packet-level capture system
  - Very configurable
  - Often include basic root cause analysis and diagnosis
- **Disadvantages**
  - Can themselves be used as attack tools
  - Hard to structure and understand output

4

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### File integrity checkers



- Used to verify that files have not been modified
  - e.g., by a worm, virus, or intruder
- Create cryptographic checksums for each file
  - Saves checksums in a verifiable way (often, hash)
  - Verify checksums periodically to find out if there has been an attack
  - Or, after known attack, to find out what files were changed by attack

5

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### File integrity checkers, contd.

- **Advantages**
  - Easy to find out what files modified in an attack or system upgrade
- **Disadvantages**
  - Hard to establish a baseline
  - Some applications are self-modifying, so difficult to check
  - System/software updates cause wave of alerts
  - Identifies the results of an attack, not the attack
  - Only as accurate as the information provided by the OS
  - Lengthy, difficult tuning process to avoid false positives

6

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Intrusion Detection System (IDS)



- What is an IDS?  
A tool to detect inappropriate, incorrect, or anomalous activity
- Various methods:
  - Signatures – match provided patterns
  - Statistics/Anomalies – look for “unusual” behavior based on defined “normal” traffic
  - Heuristics – “Learn” what’s unusual/wrong

7

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### IDS, contd.



- Host-based IDS (HIDS)  
Typically, software installed on a system  
E.g., OSSEC
- Network-based IDS (NIDS)  
Sample network traffic, but do not block  
Can be inline or on mirror copy of traffic (span)  
E.g., Snort

8

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### NIDS placement

- Inside firewall  
Limits false positives – “cleaner” data
- Outside firewall  
Shows overall interest in attacking site
- Like IPS, need to collect all traffic to be effective
  - Switch port will not work
    - Need hub, switch SPAN port, passive tap
  - Difficult on high-bandwidth links
    - Can’t keep up, special hardware required
  - Difficult in robust network architectures

9

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---



### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
3	TCPDump, Wireshark logos
5	OSSEC, Tripwire logos
7	Snort, BRO logos
8	Snort, OSSEC logos

---

---

---

---

---

---

---

---

Security tools  
Probing tools

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

Subcategories of probing tools

- Vulnerability assessment tools  
Test systems for vulnerabilities
- Policy compliance tools  
Verify system setup matches policy
- Penetration testing tools  
Attempt intrusions  
Verify that vulnerabilities can be exploited  
Report on what must be fixed

2 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---


---

---

Vulnerability assessment tools



- Agent-based (local)  
Software run on host, generally with some level of privilege  
Can report to a server if specific software (e.g., virus checker) is running and software version



- Agentless (remote)  
Poke at known security holes - e.g. open ports  
Verify ACLs  
Infer attack by looking for byproducts (e.g. newly open ports)  
No special rights needed on hosts

3 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Vulnerability assessment tools, contd.

- **Advantages**
  - Finds misconfigurations
  - Verify patch levels (checks file versions)
  - Finds (some) compromised machines
  - Finds vulnerable machines
- **Disadvantages**
  - Finds result of a compromise - afterwards
  - Can crash devices if not “gentle”
  - Looks like an attack to IDS
  - Local checks require privileges on host

4

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Policy compliance tools



- **Many types**
- **Outbound email filters**
  - Tries to stop people from violating corporate policy
  - E.g., who can communicate with the press
- **Web site testers for regulatory compliance**
  - E.g., Sarbanes-Oxley Act, GLB & HIPAA
  - Also, accessibility for people with disabilities



5

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Policy compliance tools, contd.

- **Advantages**
  - Filters can block inadvertent violations
  - Web site checkers can find configuration errors and improperly protected information
  - Automates some compliance
- **Disadvantages**
  - Filters do not generally block deliberate violations
  - Web site checkers can produce very long error lists

6

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Penetration testing tools



- “Pen” Test:  
“A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious cracker.” *Wikipedia*
- Open Source Security Testing Methodology Manual  
Peer-reviewed methodology for performing security tests and metrics  
<http://www.wisecom.org/research/osstmm.html>

7

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Penetration testing tools, contd.



- Two extremes:  
“Black box” - attack with no inside knowledge  
“White box” - attack with insider knowledge
- “White box” test harder but better represents historic threat profile  
Insiders know the security measures and where the important things are

8

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Penetration testing tools, contd.



- Capabilities:  
Can target a particular system  
E.g., a web server, email server  
Can target the network and whatever is on it  
Broad brush  
Can target the user (phishing)  
Email with attached Adobe buffer overflow and trojan  
Unlike vulnerability testing tools, provides a human intelligence behind the attack  
More realistic assessment

9

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Penetration testing tools, contd.

- **Advantages**
  - Find holes in security systems
  - Realistic assessment
- **Disadvantages**
  - Can be used for real attacks
  - Can crash systems
  - A successful run means no security holes were found
    - Doesn't mean there are none - trying to prove a negative
  - If problems are found, then the testing report is a roadmap on how to break in
  - Trade off on cost of a pen test vs. value

10

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

3 Nessus, openVAS logos

5 Foca, WAVE logos

7 OSTMM logo

8

[http://www.slate.com/content/dam/slate/articles/arts/culturebox/2012/09/120906\\_CBOX\\_RedfordSneakers.jpg](http://www.slate.com/content/dam/slate/articles/arts/culturebox/2012/09/120906_CBOX_RedfordSneakers.jpg).CROPArticle 250-medium.jpg

9 Backtrack logo

11

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---



### Hijacking tools



- Subvert protocol security (or lack thereof)
- Layer2 security
  - Switches and spanning tree protocol (STP)
    - Macof, Versinia
  - ARP poisoning
    - Cain & Abel, Ettercap
  - Wireless
    - Rogue and "promiscuous" access points
    - Evil Twin attack

4

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Hijacking tools, contd.

- DNS poisoning
  - Redirect traffic by manipulating DNS mappings
  - e.g., Dnsspoof, Ettercap
- TCP session hijacking
  - Hijack existing TCP sessions
  - e.g., Hunt, Juggernaut
- Secure protocol (HTTPS/SSL, SSHv1) attacks
  - Terminate and proxy encrypted sessions
  - e.g., SSLstrip

5

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Brute force tools



- Password crackers (offline attack)
  - Given encrypted/hashed password, determine input
  - e.g., John the ripper, Cain & Abel, oclHashcat
- login hackers (online attack)
  - Dictionary attack using massive number of connections
  - Easily mitigated through account lockouts and login timers
  - e.g., Hydra

6

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---



---

---

---

### Fingerprinting tools

- Determine “useful” information about a host
  - Operating System
  - Version information, etc.
- Passive methods:
  - Operating systems:
    - POf, NetworkMiner, Satori
- Active methods:
  - Operating system
    - Nmap, Xprobe2
  - Services
    - Amap, Nmap



7 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

### Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
3	Hping logo
4	Ettercap, Cain & Able logos
6	John the ripper, Hydra logos
7	pOf, nmap logos

8 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---



Security tools  
Conclusion

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

WARNING



**\*\*\* IMPORTANT \*\*\***

- Do not use these tools without:
  - Truly understanding what the tool does and what its side effects may be
  - Getting proper (written) authorization to use the tool in/on the environment you intend to use it in/on

2 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---


---

---

---

---

Now what?



- Do all of these tools together make you and your organization secure?
- “situational awareness” is still a key requirement to keep things secure
  - Tools don’t stop sophisticated attacks, they just slow them down
  - Event correlation is tricky
  - Requires outside intelligence

3 Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## Now what?



- Logging helps, but...
  - What is an anomaly?
  - Needle in the haystack
  - Who is actually looking at the logs?
- Attack techniques and capabilities seem to be evolving faster than defense capabilities
- Tools establish a baseline of controls
  - Smart humans need to fill the gaps

4

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---

## Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

2

[https://en.wikipedia.org/wiki/File:UK\\_traffic\\_sign\\_562.sv](https://en.wikipedia.org/wiki/File:UK_traffic_sign_562.sv)

8

3 <http://www.kitsch-slapped.com/wp-content/uploads/2011/01/1950-snake-oil-is-wonderful-stuff-500x722.jpg>

4

"Hacker - Hacking - Symbol" by www.elbpresse.de - Own work. Licensed under CC BY-SA 4.0 via Commons - [https://commons.wikimedia.org/wiki/File:Hacker\\_-\\_Hacking\\_-\\_Symbol.jpg#/media/File:Hacker\\_-\\_Hacking\\_-\\_Symbol.jpg](https://commons.wikimedia.org/wiki/File:Hacker_-_Hacking_-_Symbol.jpg#/media/File:Hacker_-_Hacking_-_Symbol.jpg)

5

Copyright © Scott Bradner & Ben Gaucherin 2015

---

---

---

---

---

---

---

---