Global Information Assurance Certification Paper

GCIH – Certification and Security Training

Practical submission – Option 1 (Illustrate an Incident)

By Robert J. Shimonski
January 2, 2001

Executive Summary

1. This report will document an actual incident that took place at the organization I am currently working for and I have sanitized this information to protect my organization and myself. To quickly describe the Incident – it was an attack on one of our core routers and a Unix DNS server. Our intruder(s) tried to access one of our routers and access one of our DNS servers.

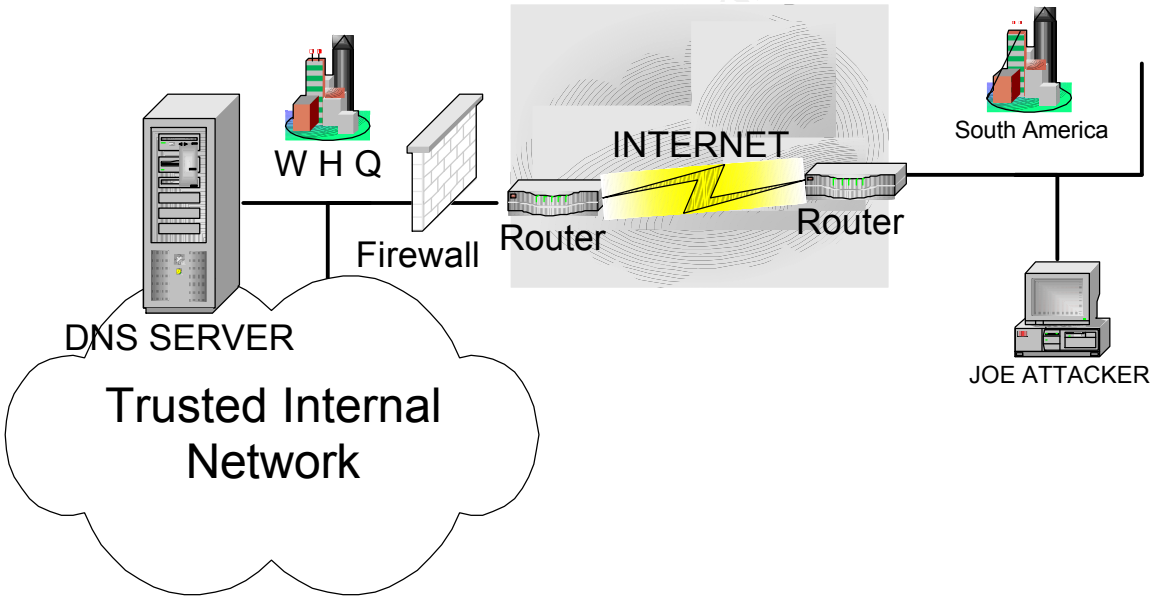
2. The most important piece of information that I can share with you is how our security team was able to work with us (Internetworking Design Group) and how quickly we were able to thwart the attempt – together. If there is perhaps, one thing I had learned well was that teamwork makes for a better success rate.

3. It had started with a crossover from standard router logins to a new system using TACACS+. We had implemented CiscoSecure ACS on all our routers. This now enabled us to monitor and log who was accessing our routers and switches. This works very well because with the standard router login – you had to keep the passwords a secret. This was difficult because you wanted to keep the passwords hard to guess (Therefore, implementing a good password policy) and you wanted to keep them under lock and key. Well the two in my opinion do not mix. With the hundred thousand other things you had to remember in a day people wound up doing the obvious – keeping passwords on a cheat sheet in the wallet or other ways to jot down passwords in order to remember them. This became ridiculous so we implemented a sure fire way to by pass this. We implemented CiscoSecure, which ties into the SAM database of the PDC. Now, all you had to do was log in with your username and password that you use for logging into your workstation. We still kept the Enable Secret password intact (thank the maker) because we felt that it was a 2-way security blanket. We asked ourselves, “What would happen if an Admin turned bad changed a password on the domain – logged in with another persons credentials (Like me!) and then performed an attack and hid the evidence?” this is of course a possibility. Therefore, the Enable Secret stayed in tact and the passwords were updated in following with the current password policy. Now with this kind of power, we can give levels of access to top level help desk to do basic tests, and completely log what’s going on all while keeping the privileged level of commands safe and sound. In addition, when someone has to log into something with their username, they are less likely to play with what they are

not supposed to be playing with in fear of being logged and found out. You can say we felt safer – but we were by far not stupid to think that we were invincible – remember the risk levels?

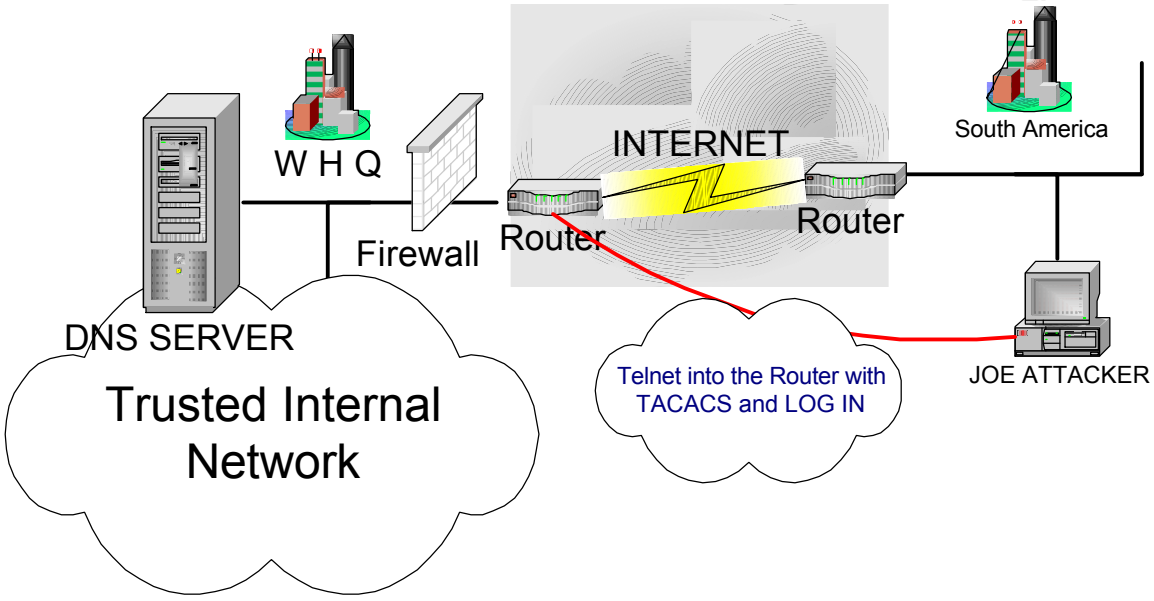
4.Now on to the attack that we caught – the intrusion we detected. This was a common problem – internal LAN users trying to gain access to something they should not be accessing. Of course, there are accidents. How many times I meant to telnet into one router, mistyped the IP Address, and wound up in a Unix server or something else – very common. The factor here is, they actually tried to log in. What also made this attack very, very interesting was that it was from another country aimed at out World Head Quarters Location. For the last piece that was very spooky indeed was that the person knew our manager. Before we go into the break down of the attack, lets look at the infrastructure.

Note: This is a mock drawing to hide the real details of our network – but it is pretty much a close enough replica to give you the idea:

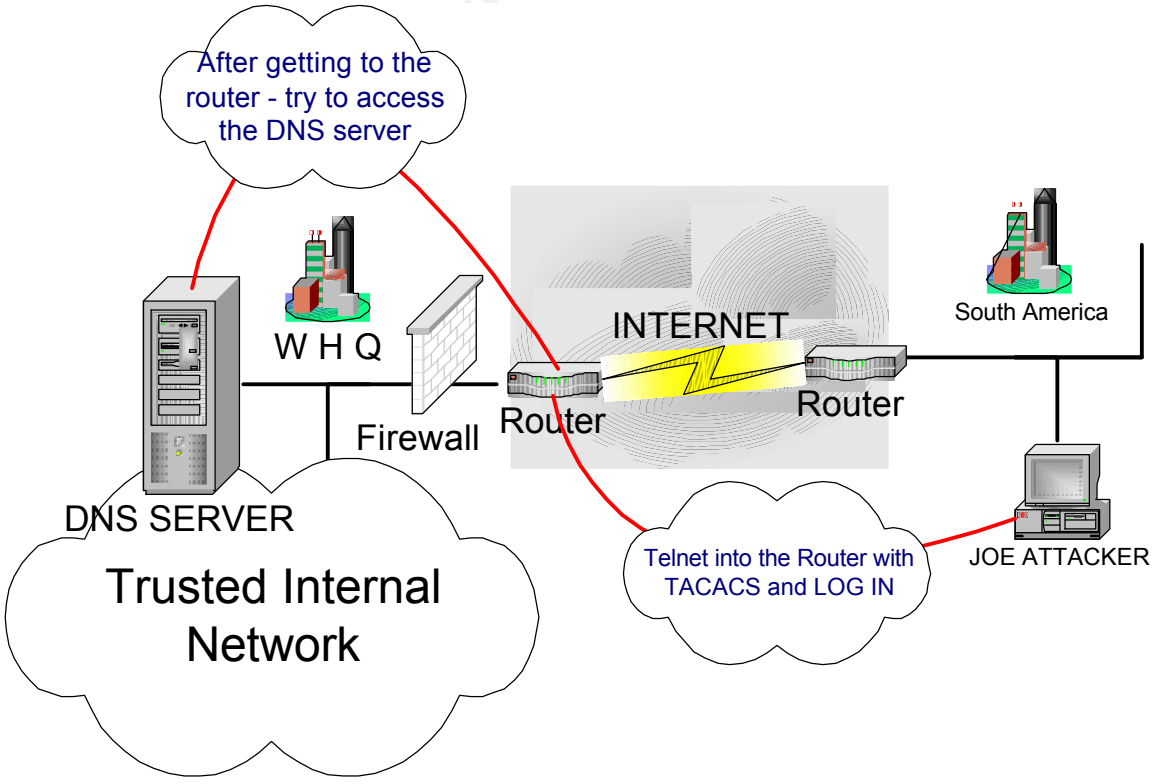


5. The attack was simple. First, someone In the South America location new how to telnet to access a router – and they new what a router was, a DNS server and UNIX. This tells me they have basic competency. You basic untrained user is not going to get this far by accident. The attacker was able to log in (this means they used someone else's ID – meaning they had access to User Manager for Domains or its equivalent to change passwords, and they were able to get all the way to looking at the ARP table and planning an attack on our DNS server) Like I said before, if we did not keep those hard to guess enable secret passwords intact – God knows what could have happened. Finally, the way we busted this guy was we checked the logs on a tool we used to mimic User Manager – and we tied everything down to times from logs. Between us, the security team and the incident plan we had it took a total of 2 hours to find exactly what we were looking for and thwart the attacker.

6. Detail of attack diagram:



Step 2 would be to access the Server – or view the ARP cache and see what can be found:



Now Lets look at the Steps used and the plan that we followed via SANS.

The Six Stages of Incident Handling

To sum up what we had followed – let's look at the six steps of incident handling and quickly review each one – then look at them under a magnifying glass to coincide with the incident outlined above.

Preparation

A checklist as per SANS and how we followed it:

- Establish policy and post warning banners
- Develop management support for an incident handling capability
- Select incident handling team members and organize a team
- Develop an emergency communications plan
- Provide easy reporting facilities
- Conduct training for team members
- Establish guidelines for interdepartmental cooperation
- Pay particular attention to relationships with system administrators and network managers
- Develop interfaces to law enforcement agencies and other computer incident response teams

1. For my Incident, preparation was key to a quick resolution to the attack. If well prepared, anything becomes easier. Our first step was to follow the established policy. This was the easy part. Our main security team had already put out a well-defined incident handling policy and one of the major points to it was to alert them of a possible incident immediately. (We did) This of course was after we made sure it was a possible attack by checking logs and coming to the most basic of conclusions – we had been attacked some how. We of course had management support. The team had already been pre selected. We have our own Security Analyst

based group and they make up the main team. A few select administrators, programmers and Networking personnel (Like me) are a small handful of others that make up the secondary team members. This maps to the interdepartmental cooperation guidelines.

2. We are all tasked with knowing the policy and making a big effort in supporting it. We had established a policy with the Security team and posted warning banners on all the routers, switches and Unix Servers. We Developed management support for an incident handling capability and selected incident handling team members and organize a team for both a primary (Main Team) and a secondary (Us and a few Unix Administrators) team for immediate response. We also developed an emergency communications plan for times like this and it was utilized when the attack was caught – we walked next door – and verbally spoke with the Team Management. We all carry emergency pagers if needed and this was the secondary way of getting someone you needed ASAP. We of course train each other whenever possible but we also offer training for team members via SANS or any other vendor where security training is offered and enforced.

Identification

A checklist as per SANS and how we followed it:

- Assign a person to be responsible for the incident
- Determine whether or not an event is actually an incident
- Be careful to maintain provable chain of custody
- Coordinate with the people who provide your network service (ISP)
- Notify appropriate officials

1. Identification came immediately – we noticed through the checking of logs and watching Tacacs+ well, that we were having an Intrusion problem. As per our in shop policy – we are to constantly look over logs and monitor everything by a set of in depth procedures. We noticed that someone had tried to log into one of our routers at a strange time. Since it was South America, the time zones were off and the time the attacker logged in was 2 hours out of working hours range (8-6 PM) therefore, that was our first red flag. The next flag that went up was the fact that the user logging in was a user from up in WHQ. (Our managers User ID) Why would our manager (Who normally doesn't log into the routers all that often) – be logging into a router, outside the DMZ at a weird time. We

realized later that the attacker had access to User Manager and changed the Managers password to get him into the router – he was not able to do much harm because we had the enable secret still intact.

2. The final nail in the coffin to send us to the security team ASAP was the fact that the IP address that was logged was from a specific subnet that was located only in South America. So why would our manager, who hardly logs into the router very often, be logging into the router on non working hours from South America. OK – we said, someone may be attacking us. What was funny about what I had said earlier about the Attacker knowing our manager is because he figured that it wouldn't look so obvious if the "manager" of the WAN group was logging into a router and probably wouldn't be questioned and some of the passwords tried were his first name and his nickname. Information that you needed to either have investigated a little or know the person. Remember – A persons nickname usually can't be found in the Microsoft Exchange server Global Address book.

3. Lastly, when the guy was caught – we did verify that it was an old worker involved with projects dealing on the WAN side of the house years ago. (And very disgruntled about certain issues) Once we were certain it was an incident, we ruled out the ISP – didn't seed to involve them and we followed the chain – called the security Analyst team (the Main one) and they went into action with us.

Containment

A checklist as per SANS and how we followed it:

- Deploy the on-site team to survey the situation
- Keep a low profile
- Avoid, if possible, potentially compromised code
- Backup the system
- Determine the risk of continuing operation
- Continue to consult with system owners
- Change passwords

1. Once the Onsite team had arrived, they questioned us about the incident. We gave them all the information in the paragraph above (Un-sanitized of course) and they began to survey the situation. Keeping a low profile was easy. There was really no way for the attacker (Unless he had an inside source) to know we were on to him. We found out through logs and

Mainly Tacacs+ that our manager tried to log into a router and failed. (NT has a nice feature that you can set that if you fail 3 times with your password – you lock yourself out but since the attacker changed it for his own attack efforts – the manager never knew the difference) that was another way to realize something was fishy – our manager had to have his password reset in the morning.

2. For this incident, there was no code to compromise but we had to keep all the logs sacred and untouched for evidence. We backed up our NT servers (With TACACS and CISCOWORKS installed) and we had all our evidence right there. We also saved the running configuration on the effected router. The risk of continued operation was of no concern after everything was backed up and since this was a major core router – operation HAD to continue. Passwords on the router of course did not have to be changed – having a great password policy and TACACS is what saved us with this incident.

Eradication

A checklist as per SANS and how we followed it:

- Determine cause and symptoms of the incident
- Improve defenses
- Perform vulnerability analysis
- Remove the cause of the incident
- Locate the most recent backup

1. The cause of the incident was simple to figure out. The main target was the DNS server that was on that segment. Why? – because he admitted it. He was going to try finding information and he claimed to want to do a Zone Transfer. We had every failed attempt he performed on log file. (And he knew it too – once he realized he was caught) he never knew we were on to him because the security team played it so smooth. They waited to call down there and were discreet in their investigating. To destroy any possible way for this to happen again – the Security team analyzed the situation. They asked us if there was anyway we could prevent this from happening again and we came up with a solution together. We decided to disable telnet from that subnet to those routers. We were also able to put tighter control on who had access to User Manager. We had logging

on so no matter what – we were going to trace this down somehow but still – how can you tighten up a little was the point for future eradication.

2. Removing the cause of the incident was easy – we removed the attacker from employment and pressed charges. Nice to know we have banners on all the router, switches and Unix servers telling you very nicely to go away or we will try to punish you. Our most recent backup was of the Configuration on the router in CiscoWorks 2000 RME and the server was backed up on tape.

Recovery

A checklist as per SANS and how we followed it:

- Restore the system
- Validate the system
- Decide when to restore operations
- Monitor the systems

1. Since no major damage was done, we were able to not have to restore anything. The damage was minimized due to the policies and procedures we already had in place. This works well when you have to explain to higher management what happened – always nice to say, "Well we thwarted the attack from the onset and because of our excellent highly trained staff – we minimized damage to nearly nothing" This is of course until next time, and the attacker finds a newer – better way into our network. Unfortunately, when your network grows and you find yourself in piecemeal – you wind up with 10 DMZ's and a God-awful amount of things to monitor.
2. We restore the system to normal operation and the security team validated it. We decided that for monitoring purposes we were going to audit the Hell out of the South America location. This would do two things for us. First, we want to know if anyone else is involved, so we want them to try. This way we can bait them. Our Systems always stayed operational (7000 series core routers cant be contained at whim and this incident did not warrant the containment or isolation of this router) nothing was damaged and all the logs were backed up. We decided to turn up

the heat on monitoring for this location and follow our normal monitoring procedures for the rest of the locations.

Follow Up

A checklist as per SANS and how we followed it:

- Follow up on the incident
- What were the lessons learned?

Follow Up and Lessons Learned

Our follow up was simple. We just monitored the logs as normal and tightened security on the South America location. We think the attacker was alone – or that they know where on to them (their buddy disappeared) so the follow up was an easy one. Just business as usual and tighter analyzing and security of that specific location.

Since we had a great team with a policy and a plan already in place – the attacker really had little chance of success. We could not imagine what could have happened if that were not the case. What would have happened? We would have had an attacker in one of our CORE routers with access to God knows what. Lessons Learned? Well briefly – read the above and tell yourself what would have happened if you didn't have an Incident plan in place – if you didn't have a good security policy.

Notes:

For at least one operating system involved in the incident describe in detail the process used to back up the system. This should include descriptions of the hardware, commands, and any problems that you ran into.

1. The only Operating System that was involved in the incident was the Cisco IOS and its configurations. The IOS is never really backed up. It takes but a few minutes to "flash" a brand new one onto the flash memory.
2. If we wanted to discuss something that really needed to be backed up – was the running configuration and the startup configuration. I discussed

that we had used CiscoSecure as our method of securing our routers – but how do we back them up? We use another piece of Cisco's family of Network Management software called Resource Manager Essentials or RME for short. This is an application snap in for CiscoWorks 2000.

3. We have CiscoWorks programmed to continually at assigned intervals go out and take a snap shot of the configurations. We have at least three different days worth of copies and a nice piece is that if an attacker tried to make changes to the configuration – CiscoWorks has a compare utility which we can use to judge the differences from yesterdays configuration to today's. (We did this when we checked the router over) and no changes were made- If they were we would have known immediately.
4. Our last back up solution is the two redundant NT servers backed up on tape every night. It would be very difficult to lose this data.
5. We also have HP Openview to tell us immediately on collected traps and pings if the router is experiencing problems – especially on our Core routers.

Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence.

1. Our chain of custody was to legally deal with the apprehension of our attacker. I was not involved with this portion but when I interviewed our analysts – they filled me in. To keep sanitized – I will disclose the fact that legal proceedings have already begun to take place.
2. The evidence collected – all logs from the routers and CiscoSecure. All logs relating to the changing of our managers password and the logs from Enterprise Administrator.

References:

- The SANS downloadable modules for the SANS GIAC Incident Handling online course modules, By SANS Authors
- Computer Security Incident Handling Step by Step, A Survival Guide for Computer Security Incident Handling, Stephen Northcutt.
- Cisco Secure User Guide and Reference, Cisco.com
- CiscoWorks 2000 RME User Guide and Online Documentation
- Cisco Online Resources, Located: http://www.cisco.com

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS