GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Strategic and Tactical Considerations in Remote Vulnerability Assessments.

The events of September 11 have shocked the U.S. and the world. President Bush has started to populate his cybersecurity task force. Regardless how you feel about the issues surrounding this move, it signals an awakening concerning information and the internet. Confidentiality, Integrity, Availability, as well as Control, Authenticity, Utility -CIA(CAU)- are important to the market.

To that end, methods of assuring CIA(CAU)(1) are being re-examined. The biggest challenge, mainly because it is the cause most ignored to date, is crackers. Best Practices are an issue under review with diverse views by many economic sectors. We must methodically assess our vulnerabilities thoroughly to secure them. One aspect of this is to look at the system from the end of a wire. Techniques must be applied by the client to ensure Maximum Benefit. We will look at some tactics and strategies used by attackers, and thus, by security engineers. We will examine why one should not examine networks from afar. Remember, computers record.

Crackers or hackers, keeping them at arms length is a matter of knowing your system better than the bad guy. This requires a strategy of Defense-In-Depth. Part of that defense is knowing how the crackers will get in. The SANS (System, Administration, Networking and Security) Institute publishes a consensus document of the top ten vulnerabilities. They (SANS) say "Vulnerabilities are the gateways by which threats are manifested." Incidents.org provides attack information as real time as anyone. The Mitre Corporation maintains a database of vulnerabilities, with ratings. All you need to do apply this knowledge to your system!

Yeah! That's all...

Being in business, you must put information out to the public. People need to know how to come to you for the help that you offer. This applies to everyone from non-profits to government agencies to mom and pops ice cream stand. There are those who track this information for reasons from sales to taxes to "who knows". Of course, when you go outside, you show your face. Everyone makes a mark. This is especially true in computers, except that your tracks may not be immediately visible to you.

For most citizens this is new. Assessing your vulnerabilities is not simple. Experience is a necessary ingredient. A methodical approach may be more important. You must eat the elephant in small bites.

Vulnerability Assessments

If you haven't heard of CERT/CC, go to http://www.cert.org and fix that. They have built a three phase method of internal Vulnerability Assessment (**VA**) called OCTAVE (2). It provides a process for complete Risk Analysis. It involves tuning your resources for your assets. Start your internal VA from here and you'll have an easier time getting Senior Management to sign off on it. It goes far beyond the scope of this paper. It serves here to illustrate the highly focused nature of Remote Vulnerability Assessment (**RVA**), in a comparative sense.

Full VA's require access to everything from the trash through the office to the home phones and computers of every employee in your organizational chart! RVA's focus on what you can learn from your desk. Ok, maybe not YOUR desk. If you understand this, you are well on your way. A complete vulnerability assessment has no limits. If it did, something would be missed. If something is missed, the client (yourself, if performing an internal VA) gets a false sense of security. This may prompt them to drop their guard.

© SANS Institute 2000 - 2005 Author retains full rights.

Conveying false security is the absolute worst thing a security professional can do.

In comparing Full VA to RVA, penetration testing is not between them. Both Penetration Testing and RVA come at your organization from the outside. Both start with a predefined level of knowledge. Both need well defined and expressed procedures. This is more to protect the testers, though the client's understanding determines the value of the testing. The difference is in the deliverables.(3)

A penetration test looks for access. It is a pass/fail proposition. It also has the propensity for a confrontational relationship. The goal is specified at the beginning. It may be to grab a privileged file. It may be to leave a calling card. It may even be to execute a file. Even though several vulnerabilities may be found, a client may only learn that he is vulnerable, not how.

A Remote Vulnerability Assessment investigates an entity from the end of a wire. The process here is to gather all the information possible from outside of an organization, disclose your findings, discuss solutions with management and administration, write a report, and stake your reputation on it. It is part of the deliverable that this report be referenced to third parties. This is a marker in a process of security improvement. You are working with the organization to improve their CIA(CAU).

Historically VA's of all sorts have been a requirement of the Financial, Government, and Bonded Sectors. The government sector is probably the sector most recently conspicuous in their decline of appearances on sites like http://defaced.alldas.de. The government is an obvious target, and they have learned the hard way. Others, hopefully, will take their lead. It doesn't make much sense to invest millions in a store front, only to have it wrested from you by a kid with a keyboard and nothing but time. Even worse, someone altering your carefully crafted product, delivered over the web(4). If you are doing e-business, you need VA.

Ultimately, which one is chosen, or in what order, is up to management. A Full VA can be expensive, in time, planning and money. A penetration test may be required by insurers. Management may want more than a penetration test can tell them. At this point your job is to analyze the prospects needs and guide them toward what they need. This can be the toughest part of the job. However, this paper will focus on RVA.

Discrete Information Gathering

So what can you learn from the end of a wire? One test is to google yourself! Or run a search on your organization. These tools are open to anyone with a browser. If one can determine the name of your CEO, how much would one learn? How about your network administrator? If they have posted to a list, most real search engines will find those posts.

Other initial remote information gathering tools include whois, and Domain Name Service. Unless the client is running their own name service, the client will not have the opportunity to tack these requests. They will not be able to track your search engine lookups either. This is important. This information can be harvested without the target ever knowing. Here, an attacker has an edge.

This tactical advantage gives insight to the attackers process. We will be concentrating on the attacker that prefers to do things digitally, for whatever reason. Crackers won't be very successful unless they have a plan. By and large their plan is the same plan an infantry squad uses when taking an objective. The steps are something like this(5):

1. Broad reconnaissance - choose an objective
2. Targeted probes - find a vulnerability
3. Exploitation of vulnerabilities - :)
4. Occupy and improve the position - patch the hole, hide presence
5. Prepare for combat - gather tools, prepare system

© SANS Institute 2000 - 2005 Author retains full rights.

6. Conduct follow-on operations - recon, probe, etc...

Obviously, once we hit step three, it is too late. Exploiting a found vulnerability takes nanoseconds. Computers will never be smart; only dumb, really really fast. This illustrates the point taught at SANS: "Vulnerabilities are the gateways by which threats are manifested."

Now that have some idea of what the smart intruders do, we can follow their plan to evaluate our own systems. So let's start gathering data...

Strategic and Tactical Considerations

Before you do any testing, get permission in writing! I would cut and paste that a hundred times...

Any security testing seminar worth its salt will tell you about Randall Schwartz. If you read the Camel or Llama book (O'Reilly - PERL) you know him. He ran crack (a Password Cracker) for a large Pentium processor company that shall not be mentioned here, and is now a felon(6). Personally, I am acquainted with an individual who's career was saved by having prior authorization in hand. He was on a business trip when he ran a portion of a VA. The IDS and it's analysts performed zealously. Everyone is happy, now anyhow.

Carnegie Mellon's CERT/CC offers a wealth of well thought out and tested information for the Security Professional. One of these is answering incident calls. CERT is not about to release packet logs, nor would that be very useful. One very useful output from CERT is statistics on how many calls they take. Granted, not every incident is reported, and fewer still are reported to CERT. http://www.cert.org/stats/cert_stats.html gives a look at a staggering trend. The link to CERT gives more complete information.

Incidents Reported to CERT/CC

1990	1999	2000	1Q - 3Q 2001
252	9,859	21,756	34,754

A Vulnerability Assessment is basically an audit of the configuration. External Audits are performed to verify the accuracy of the owning organization's reports. This implies that the Auditors are objective. Objectivity requires, among other things, independence. Professional Auditors have extensive guidelines on independence. In Document # 020.010.010 the ISACA (7) stipulates that prior involvement in anything from development to acquisition of the tested system, may impair independence. This basically disqualifies hardware and software vendors from performing VAs. It also puts limitations on the usefulness of internal audits.

Service Interruption -

Another requirement of RVA is to keep the intended purpose of the system running! If a test might bring down a server, coordinate that time with management. Your manager should be able to point you at the right person to ask. You want a time when the least amount of users are on the system (RFPoison on an NT4.0 Server). Also, depending on the test, you may want the most amount of time to recover (rpc.statd upgrade necessary). With some systems, you may even want to alert Administration, but these are only on poorly developed systems (Proprietary App Servers, etc). Upper Management does not need to be bothered with these details, but Administration needs to be tested. Put this on your list of things to talk to the CIO about (generally).

Prior Knowledge of Tested System -

© SANS Institute 2000 - 2005 Author retains full rights.

A key item is whether the client requires a zero-knowledge test, full-knowledge test, or something in between.(8) This can be a stipulation of an insurer or regulator, or a desire of management, etc. You may never know what inputs are involved in this. It is completely up to the client.

The zero-knowledge and full-knowledge tests are rather straight forward. A partial knowledge test is left completely up to the customer as to what is disclosed before the test. They may have a portfolio of tests to be run, similar to a penetration test. They may give you whois and DNS information. They may be aware that Google has cached their newsgroup postings, and will therefore save your time and their money by providing those documents.

The full-knowledge test is likely to be performed in concert with other parts of a full VA. The Zero-knowledge test is where you earn your money. Whois may give the name of the administrator, or not. If only it were that easy. One place to look is the entity's web site. They may have posted their staff names and assignments. Their location is likely to be there, if that is held back too! Phone Numbers can be googled, and may even reveal a history of sorts from newsgroup and listserv postings.

The update timestamp of the Web Page is important as well. This can be had in netscape or mozilla by clicking on security icon (That little lock at the bottom). This will give you an idea of how closely they watch their server. How old the document is gives some idea as to it's current validity. For instance, if the page is three years old, or more, the Admin listed may be a role account that only looks like a username.

Maximum Value -

As the testing engineer, your job starts as you hammer out the details of the test. Your goal is to impart maximum learning potential to your clients, be they folks you see daily, or the Bank up the street. You need to be clear that part of your report will be based on the raw data received, as well as the analytical process and reaction! If there are any doubts, get an extract of their logs to examine briefly during the follow-up. The client should be setting up their production network to render as much information as possible, while maintaining its intended purpose. They may need some advice in this area. The key is to get them to recognize and handle an incident!

The six steps of incident handling are:

1. Preparation
2. Identification - Detection
3. Isolation - Containment
4. Eradication
5. Recovery
6. Follow-up

Essentially this is an old fashioned BASIC GOTO loop. Once you're done with follow-up, you prepare for the next. However, if identification occurs while on any step, that thread must be triaged and dealt with as well. This is one of the details you should hammer out with management, and administration. Approach it as a training plan. Be aware as well that attackers don't care if the target is involved in intense training. They may well try to capitalize on it. Don't let your guard down.

The value of RVA is limited in this respect. Unless you are on-site, you will have a keyhole view of the organizations response. If the client stipulates a zero-knowledge test, your ability to advise the team is limited by lack of input. Even in a full-knowledge test, your data on the analytical process and handling practices will be second hand. Most items that go unchecked in an RVA are internal. Do you have a switch in a closet in the basement. A client of mine did. Bad logging practices will show at the border, or systems

© SANS Institute 2000 - 2005 Author retains full rights.

compromised by testers, only. Rights, permissions, and other internal controls will go untested. Policies, practices, and procedures will also be left out if not exploited.

The above illustrates the need to integrate this testing with a Full VA. Even in RVA, there is no substitute for being on-site. When the hit comes, your on-site personnel will be there to confirm it. If a real hit occurs concurrently, your people can help coordinate a proper response. Your personnel can be assigned in such a way that those performing the RVA do not actually visit the client until the follow-up meeting. This is no simple task.

Source Obfuscation -

Depending on your assessment of the client's team, or their stipulations, you may find it desirable to exploit the advantage of information gathering possibilities even further! SamSpade (9) is an excellent site for this. The "Safe Browser" will send a get request, and return the full answer in flat ascii text. This information is obtainable with a sniffer, but you have to reveal your IP Address. The best part of SamSpade's Safe Browser output is the Web Server version string. At the least it will tell you if Administration is practicing Defense on Depth by altering the default string. At best it will be the default, giving you a name to search on your favorite exploit depository. Other proxies exist for browsing as well, such as www.anonymizer.com.

By far the feature of SamSpade I use the most is the DoStuff line. That line does a DNS, and whois lookups, and traceroute on any target, from SamSpade's host. This insulates you from DNS lookup packets sent into the client's perimeter. The same goes for traceroute, possibly revealing the IP of their border router. SamSpade also lets you do a wide variety of whois and rwhois lookups, though Steve is tweaking the automation of DoStuff. Another nice feature that is getting better is the clickable subrange in whois. This attempts to resolve ISP's subnetting their huge IP spaces. Getting all of earthlink's address space as an answer doesn't tell you much!

SamSpade's main focus is on anti-spam. Registering (as free as any on the internet) will give you more possibilities. Steve is a generous soul for giving the world this resource. His FAQ is as humorous as any unix man page. He also has a tool for windows, but that is another paper.

And so, without ever firing a packet directly from our own computer, and more importantly, remaining completely legal, we know quite bit about our target. We know their public IP address space. We can find the mail server's IP address. We have their Web Servers IP address, and if we correlate that against the mail server, we will likely find if they use a web hosting service. If they do, then the Web Server is probably off limits. Depending on the web server status just mentioned, the server string may provide some insight. The opportunities to drill even further are abundant.

Test Setup -

The stuff available at SamSpade is information generally required by various processes to make the internet useful. This information travels the internet constantly. It looks normal. If we are to dig any deeper, we may want to consider what we are sending, and more importantly, receiving.

While your getting permission, get it to scan the ports and addresses on their internet connection to your hearts content for the duration of the test. It is thus possible to be sitting on a Hawaiian Beach getting a tan, while billing for your time. A juicy proposition, with foolish undertones.

The NMAP portscanner will send irregular packets to a host to identify the Operating System (more precisely, the TCP/IP stack). I recommend this, or Queso. They are lightweight, customizable, and as stealthy as it gets. Some consider this software in the realm of hackers. They are right. These packets are NOT normal. They are part of the default SNORT alarm suite. They will be keyed upon.

© SANS Institute 2000 - 2005 Author retains full rights.

If you can key on the packets, so can anyone else. Any exploit you perform is traveling across machines over which you have no control. This means passwords, access lists (or stuff bouncing off of them, which is almost as good), your holy grail. Have you ever connected to console port of a Cisco router? That is it's "Root" access point. Unless you are in control of every router between you and the target, someone else is! It is highly improbable that you will notice a Cisco router dumping packets to another system between you and your target. Now all the vulnerability information you are collecting, is being collected by someone else. *This is a major breech of Confidentiality*. One that is very hard to detect!

If you can not detect it, you must assume that it is occurring. If you have a relationship with an ISP, perhaps you can contract with them to connect to the same router your client does. That is a tall order. An easier task would be to get a dial-up account with their ISP. How ever you connect, you are looking to shorten the number of hops. Your goal is to reduce your exposure to clandestine listening.

If this not possible, perhaps you should investigate ways to connect to the outside interface of the constituent's network. This may sound paranoid. I challenge all to deny it is possible, and undetectable.

Assessment Methods -

Within the remote context, testing can take many paths. The client may have a list of required tests. Scanner software entities put out updates often. With VA's, flexibility is required to track down the exposures. It is not enough to know that rexec is running on a host, one should look for trust relationships to gauge the exposure extent. This is in keeping with the Maximum Benefit principle above. Careful planning of tests (attacks) will meet the requirement to try not to get caught.

Once you reach step three in the attack process, the host is compromised. Further attacks are up to the testing team's discretion. Perhaps the client's team has not detected their compromised host yet. Perhaps you want to apply some pressure to make a decision to the client's team. You should, however, avoid beating a dead horse.

There are many packages available to perform a basic security scan on a machine, or range of machines. Kapil Sharma has posted a list of freeware scanners, including SATAN and Nessus.(10) Each has their strengths and weaknesses. There are also tools such as nemesis. Nemesis facilitates crafting each bit in a packet. Just as in computers and networks, the most important hardware is the physical mouse driver. In an interview @ www.insecure.org, Rain Forest Puppy said it well: RFP: "Auditors who walk in and exclusively run ISS or CyberCop aren't doing a thorough job. The majority of the time, the auditors don't understand the security vulnerabilities that the scanners are finding."

The client has information that is his and only his. The Privacy Issues (11) surrounding Employer - Employee relations are different for legal, and each and every employer, at this point. Yes, courts have found that employers own the systems, and may monitor them, and may use what they find, with some stipulations, in court. But, most employers let their employees go far beyond what the courts have held, and legislatures passed. This is not the only issue surrounding client data. If the client should be broken into in the days or weeks that followed, you will need the logs to show it wasn't you. If some other information were to suddenly find itself in the public domain, you will have show that you did not have access, or took "reasonable?" steps to safeguard it. Logs that show it did not leave your premises will help. You may be stuck trying to prove a negative.

One way to avoid getting tangled in customer data issues, and still test the border systems of your client is to install a standard workstation, that has not had any proprietary data added. It should be as similar as possible to a standard workstation. This would be your target. Another is to install a shadow IDS sensor on the internal ethernet segment. A shadow IDS sensor generally has no IP address, and cycles its sniffer

© SANS Institute 2000 - 2005 Author retains full rights.

process and file every hour. It would keep your files managable, and provide you with a log of your activities. It would be filtered to show packets going to and from the attacking IP range(s), or another machine designated between you and the client.

Your best defense may not be your Permission Slip to perform this test in the first place. I doubt a Bank, or their insurers (the Federal Government) would hold you harmless if an incident did occur, and evidence suggested you or no one else were at fault, regardless of any previous agreements between you. Remember, your client may or may not follow your suggestions immediately, completely, or faithfully. This is a sticky wicket! It is necessary to take steps to avoid it.

Generally, an RVA will consist of internet probes and attacks, as well as WarDialing. WarDialing is making your modem call a range of numbers and recording which ones offer a terminal session, or fax machine (a la Wargames). Be careful here. WarDialing may be illegal in your state or locale. You may want to investigate the possibilities with law enforcement, or the legislature on this. Perhaps a license to WarDial is warranted, so the criminals are not the only ones with this in their arsenals.

How far should wardialing go? Companies pay for each incoming line, they should know haw many there are. Beyond that, a Private Branch Exchange (PBX) would be required. Some PBXs will kill a modem if attached, but there are adapters. Don't allow an overconfident admin deter you with that. Generally, any phone number accessible from the outside should be checked. Most WarDialers have a random order function. This is in response to PBXs that log callers that dial too many sequential numbers. One should at least dial every PBX line that is remotely accessible.

The only wardialer I have experience with is a copy of ProComm shareware I got at a HamFest in the '80s. It will randomize a list! It will log connections to data or fax. I don't think it is available, and I have not run a more current version. One that looks interesting is PhoneSweep from SandStorm. They actually hardware license their software as a security precaution. They list some self testing issues, but not much more. They also sell multi modem setups to speed things up!

Follow-Up -

Perhaps the most important step in any test or training is to take the time to meet after, preferably immediately, the exercise. Besides building a team, this will give the testers and administrators the opportunity to talk about events, and compare notes, while the activities are still fresh in their minds. Packet traces and logs of significant events should be available on projector for reference. At least one person should take notes. A leader should be assigned to keep the meeting on track. That leader should attempt to capture three good and three bad things. As the client is paying, stick to his point of view. Your testers can meet as soon after as convenient.

Management should attend for team building. They do have an entirely separate set of issues, so a planned break off should take place. Beyond their own hashing of events, good and bad, schedules for delivery of documents, discussions, and final reports should be set out. It is important to get the client's input to the final report. Issues such as planned upgrades and policy meeting schedules can be accounted for, and included.

Summary -

The object of computers is information. Your information gets around by virtue of your mobile existence. Information has a tendency to propagate.

We have "briefly" discussed Vulnerability Assessments. We looked at a range of focuses. There are many other slices that could be made, including physical, human resource, etc. Generally, however, one entity

© SANS Institute 2000 - 2005 Author retains full rights.

needs to manage the process from beginning to end.

We focused on Remote Vulnerability Assessment (RVA) with in the context of a Full VA, and compared to penetration testing. We looked at some sources to find information in a way that the target would not be aware. We found the line where it doesn't matter anymore, vulnerability exploitation.

Before you do any testing, get permission in writing!

The number of incidents is rising, and with it the number of reports. Hopefully, we can share more Break-In information. Its not your fault, though you may feel responsible. That's why you should have independent folks look at your site.

In order to stay in business you must provide value and take care of your customer. There are considerations that could greatly increase the value you provide. These include: planning dangerous tests around your customer's schedule; planning for your customers statutory requirements; assisting your customers in their on-going training; providing a realistic scenario for that training; and NOT allowing your customers weakness information to fall into the wrong hands. I have not seen the last item preached or practiced on the internet. Additionally, you need to gather records that show your activities, and your safekeeping of any data you capture.

There are many ways to perform these tests. There are many tools. There are not many folks who understand what the tools are telling. And don't forget the modems! Wardialing is a necessary step. Perhaps it should be licensed.

The Army has a principle that if you don't schedule time to capture lessons learned, you won't learn. Both teams need to meet as a whole, and in their respective parts to properly hash out the events. Take good notes, and you'll stay ahead of the crackers.

---
bibliography

To return to your place, locate your reference, and click return.

1. The Basics are the Basics, Winn Schwartau, Interpact, Inc. winns@gte.net (return)
   on the Parkerian Hexad (Donn Parker, CISSP)
   http://www.infowar.com/chezwinn/articles092899/TheBasicsAreTheBasics.shtml
2. OCTAVE, by Christopher Alberts and Audrey Dorofee, SEI Carnegie Mellon (return)
   http://www.cert.org/octave/methodintro.html
3. Guidelines for Developing Penetration "Rules of Behavior", Nancy Simpson (return)
   http://www.sans.org/infosecFAQ/penetration/rules.htm
4. When Trusted Web Sites Go Bad: Another Web Weapon, Daniel F. DeLong, September 28, 2001
   issue of NewsFactor Network (return) http://www.ecommercetimes.com/perl/printer/13829/
5. Elements of a Hack, George Bakos, Vermont National Guard Information Operations Training
   Development Center. (Available by e-mail to bschnzl@bigfoot.com) (return)
6. State of Oregon v. Randal Schwartz, Steve Pacenka, spacenka@lightlink.com. Thanks to host ISP
   Lightlink. (return) http://www.lightlink.com/fors
7. Effect of Involvement in the Development, Acquisition, Implementation or Maintenance Process on
   the IS Auditor's Independence Copyright 2001 Information Systems Audit and Control Association
   (return) http://www.isaca.org/standard/guide5.htm
8. Your First Penetration Test, David Piscitello, Core Competence, Inc (return)
   http://www.tisc2001.com/newsletters/312.html

© SANS Institute 2000 - 2005 Author retains full rights.

9. SamSpade.org Steve@blighty.com http://samspade.org (return)
10. Security Scanners Kapil Sharma, Linux Gazette, (return)
http://www.linuxgazette.com/issue57/sharma.html
11. Electronic Commerce & Law Report, October 10, 2001 Computer Law Association (CLA) (return)
http://www.cla.org/bna6_39.htm

© SANS Institute 2000 - 2005, Author retains full rights.