How Not To Get Hacked - let's be careful out there

by Aaron Grothe
Security+/CISSP/NSA
IAM/NSA IEM/CySA+/PenTest+

Disclaimer

Anything I say in this talk might not represent the views and/or opinions of Infogroup. I am speaking only for myself.

Felt the need to add that just in case :-O

Introduction

"You don't have to run faster than the bear to get away. You just have to run faster than the guy next to you" - Jim Butcher

These steps aren't going to prevent you from getting hacked. They do however work at reducing the possibility of you're being hacked. What follows is a list of things to consider.

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Deploying Honeypots/Honeynets

A Honeypot is a machine that simulates a machine on your network. It is designed to look interesting and see what people are doing on your internal network.

An example of this is a Raspberry PI setup to mimic an open ftp server. It logs everything that attempts to access the machine so you can see how/what is scanning your network.

There are several options in this space. You can roll your own, deploy a hardware device, or buy a VM.

Deploying a Honeypot/net (contd)

A Honeynet is a series of machines that form a network. E.g. Webserver, application, database.

Ideally information will be logged such as what IP is connecting, time, etc. This can help with log correlation to figure out where the attack is coming from.

An example of a basic Oracle database honeypot could be as simple as open ports (22, 1521, 1630, 3938, 1158, 5520) and others. Any attempt to connect to these ports from another machine could be interesting.

Deploying a Honeypot/net (contd).

The level of sophistication for the simulated machines can range from an open port to an entire simulated service.

Fred Cohen created the deception toolkit years ago which pretended to be relatively complete machines.

There are services such as Canary which produce small devices you deploy on your network that have easy web based setup tools.

Don't Host if You Don't Need To

I maintain the internet infrastructure for the NEbraskaCERT group. As part of this we maintained an e-mail server, e-mail list server, webserver and in the distant past credit card processing.

Over time we've reduced the number of services we host ourselves and are using other services to reduce our vulnerabilities.

E.g. we quit doing credit card processing years ago when the costs/concerns of PCI compliance started adding up. We moved to paypal as an acceptable choice to reduce our vulnerability to attack.

Don't Host if You Don't Need To

We still host a maillist service, but that is only used for internal lists (Board of Directors, Security Professional Training class, etc…) Other lists are now being run on an external service in this case mailchimp.

Last year for the first time in 20+ years our webserver was hacked. How did this happen? We host websites for several other Omaha security groups. One of them used Drupal which they didn't keep up on the patches for. So we got attacked and compromised by a webcrawler looking for vulnerable versions of Drupal. Fortunately they were only running Monero coin mining and cleaning them up was relatively easy.

Don't Host if You Don't Need To.

One of our plans for this year is to move our website to Wordpress. We're either going to use an external service to host our Wordpress or deploy Wordpress with the Wordfence security plugin, automatic updates turned on and the minimal services required to host our website. Potentially with the website in an entirely different account and machine than our mail lists.

There are many companies that will host your site and handle the security/updates/backups/etc for your website and other services. Why are you still hosting your own?

Centralized Logging

Dump all the logs from your boxes to a centralized server. This can be something as advanced as Splunk or Elasticsearch Stack or as simple as syslog-ng dump to a remote machine.

There are also services available that are able to process logs and provide a good interface to them. Usually a customized version of Elasticsearch stack.

Many large breaches are the result of logs not being analyzed. Examples of this are the Experian hack and the Signapore Health System attack.

Centralized Logging.

This is one you can roll your own for if you have sufficient expertise or buy a service for.

Having the system and application logs at least will help you provide information to the authorities about attacks.

Companies such as Loggly, Logz and others exist. Splunk is awesome if you can make a business case for it. This is something you can start small and build over time.

Segment Network

This one is amazing to me. There are three private non-routable ip address blocks available in IPv4.

10.0.0.0 - 10.255.255.255 (16,777,216) addresses.
172.16.0.0 - 172.31.255.255 (1,048,576) addresses.
192.16.0.0-192.168.255.255 (65,536) addresses

So almost 18 million available private addresses and most companies continue to have no real plan for how to segment these. True depending on netmasks and settings you may need to setup routes to have machines be able to see each other. Still no reason to just mix stuff randomly.

Segment Network.

IPv6 has a private address space of almost 19 billion trillion addresses so feel free to spread out a bit.

Many companies I've dealt with in the past just randomly add machines to a network segment until its full and then move on to the next one.

The inverse of this with many, many vlans can be almost as bad where everything is so segmented you almost end up having to have a vhub type of situation so anything can to talk anything else.

Try To Only Use Supported Packages

A developer needs a Python package E.g. python-gpg. There are at least 4 different ways to install this package

1. Install from the vendor's distribution if available
2. Install using the python pip tools for package management
3. Grab the latest version from the git repo
4. Grab a tarball/zip and install the package with the setup command

Which of the above deal with possibility of potential security issues in the installed package.

Try To Only Use Supported Packages.

The packages on the last slide were listed in what I believe to be the best to worst steps. There are other options as well such as installing additional software repos through options such as PPAs, Snap packages, flatpak and so on.

The point here is that every package installed should have its lifecycle considered as part of its installation. Many packages aren't updated in a timely fashion and this can lead to problems.

E.g. Apache Struts and Equifax

Have your Security Team be known

Many users will have a split second where they pause before doing something bad with regards to security.

Having your security team be known is important because that increases the chance that the person will reach out and ask a question for confirmation etc.

It is amazing how many companies security teams have no contact with the endusers and the users have no way to contact them.

Have your Security Team be known.

Ask yourselves the following questions?

If I get a suspected phishing message who do I send it to?
I have a security question how do I ask?
Can I name who runs the security team at my company?
Can I name anybody on the security team?

There is a mindset that thinks the security team should be totally unknown and operating independently of the rest of the company. I do not subscribe to this and have found it to be of limited used in the real world.

Security Awareness Training Program

This one works together with the last suggestion pretty well. The Annual Security Awareness Training Program is a great time to introduce your team.

The goal here is to put together a simple program that every user does on annual basis. Typically 30-45 minutes in length with a simple quiz at the end.

There are a variety of companies that will handle this as a service for you where you put in your custom content along with their boilerplate and they handle the registrations, people doing the course, scores, certificates, etc.

Security Awareness Training Program

The goals of this are as follow

- Increase security awareness amongst your employees
- Provide an auditable event saying every employee completes security awareness training
- Make sure your employees are aware of the security escalation process

Security Awareness Training Program.

One tip on the Quiz make sure it is correct

- For a lot of users this will be the ONLY interaction they will ever have with your security team
- Make sure that the training is accurate
- E.g. having the wrong answers or explanations on the quiz will confuse the end users
- Recently was e-mailed a couple of slides from a company's quiz and it was directly contradicted by the content of the presentation

Review Firewall Rules.

This is an annual review of all the firewall rules. Every firewall rule should exist for a reason and if the reason doesn't exist any more they should be removed.

It is amazing how many companies add firewall rules and they are allowed to live long after the reason for that rule to exist is long gone.

Ideally the rules will require annual signoff by the departments/people who requested them.

Sign up for Have I Been Pwned.

HaveIBeenPwned.com is a service that you can put your e-mail address in to see if it has been compromised. E.g. if you enter my e-mail address ajgrothe <at> yahoo.com, you'll see my account is used as a login for services such as dropbox, linkedin and others. This means I should change my password for these services and any where that I share that password.

HaveIBeenPwned.com also offers a domain wide version of this service as well. E.g. I can sign up nebraskacert.org and be notified when any @nebraskacert.org e-mail adress is detected by the service.

Shodan.

Shodan is a search tool that looks for exposed services such as printers, desktops, IoT, etc.

You can sign up for a free developer account and explore. It can be worth it to see what you have that is exposed to the internet.

You can also do a lot of the same things by doing nmap-diffs over time as well. Shodan however provides a nicer front end to the services.

Recon-NG

Recon-NG is a tool available either Standalone or as part of the Kali Linux distribution.

It allows you to do things such as figure out what subdomains you have exposed to the internet, LinkedIn accounts that reference your domains, pgp keys present in the mit pgp keyring and so on.

One amazing thing about Recon-NG is that it doesn't hit your companies assets instead hitting services such as bing, linkedin, etc. So it won't show up in any logs, ips systems, etc at your location.

Recon-NG.

Recon-NG is also an easily extensible tool that is written in python. You can add custom modules to look for things that are of interest to your company.

Shadow IT

One of the biggest security/hacking implications caused by Cloud computing is the rise of Shadow IT.

Shadow IT is what happens when developers/users/managers are able to create IT infrastructure in the cloud that may or may not be in compliance with your company's IT policies.

With free accounts and free credits available for a lot of services anybody can theoretically start their own IT department.

Shadow IT.

How to fight Shadow IT

- Determine why there is a need/desire for it (no pun intended). Is your internal IT group unable to meet needs.
- Consider setting up internal cloud broker self services such as OpenStack, VMware cloud, etc.
- Make sure the issue is clearly laid out in your security policies and adressessed in your security awareness training
- This one seems pretty obvious but I've seen it enough I feel it needs to be included. Don't reimburse people for Shadow IT.

Review Cloud Service Security Options

Amazon's AWS, Microsoft's Azure services and Google's Cloud services all offer additional security features that are available.

Some examples

- You can set default encryption on S3 buckets so that all objects are encrypted when stored in a bucket
- Virtual disks used by Windows VMs in Azure can be set to be encrypted automatically
- AWS artifacts provides a repository for compliance documentation

Review Cloud Service Security Options

Cloud Services are using security as one of the ways to differentiate between themselves.

This is interesting as the cloud providers are continuing to also provide their own versions of the services provided by other vendors. E.g. AWS Artifact -> Azure Service Trust Platform

Summary

The previous tips will hopefully give you some ideas of how to reduce your risk of being hacked. Hopefully, everybody got a couple of ideas out of this talk :-)

Added together they should hopefully help you think a bit differently about security. There are an eclectic mix but reflect a bit of my 30+ years of doing Computer Security.

Thank you for listening.

Any questions?