November 4, 2016
ACME Company

Security Assessment Report

Contents

Executive Summary

With every security assessment, our goal is to identify the information security related strengths and weaknesses of the organization and its infrastructure so that we can celebrate the positive and identify the areas that may have opportunities for improvement. In the case of your specific assessment, we identified some positive characteristics and strengths as follows:

- Most of the network configuration exhibited a concerted effort to minimize risks and appropriately limit access to the needed services.
- The network related user credential controls seemed very strong in that we were unable to successfully extract a single set of user names/passwords even though we tried via numerous types of coercion. This indicates that the organization has placed a high value proposition on protecting this type of sensitive information.

Although the previous area indicates that the organization has taken strides in properly securing and protecting its infrastructure and data, there were some short-comings identified which have the potential to be damaging to the organization including:

- The public web site is experiencing performance related issues which are revealing details about the site and the server configuration via overly verbose error messages.
- A substantial SQL injection flaw on the acme.com web site which allowed us to extract information about the server and database.
- A weak overall defense to email and phone based social engineering attacks. The weaknesses resulted in high-risk activities such as clicking on unknown links and disclosing various pieces of potentially sensitive information.

Overall we believe the organization has the potential to greatly improve its existing security posture by implementing the recommended remediation steps.

By the Numbers

6	4	2	6/10
Vulnerabilities	High Risk	Strengths	Security Posture

Project Scope

Perform a comprehensive external security assessment and penetration test of the publicly - accessible/internet accessible information systems infrastructure of the ACME Company (ACME) which will include the following:

- Perform a network penetration test on the following publicly accessible IP addresses:

  169.254.0.1-2
  169.254.0.10-14

- Perform a social engineering assessment on the following employees:

John Smith	*Cindy Johnson*	*Carolyn Furr*
Frank Lowder	*Trent Brooks*	*Brandon Smith*

- Perform a web application penetration test on the following domains:

  http://www.acme.com
  https://www.acme.com
  https://partners.acme.com

Information Security Strengths

We identified the following information security related strengths:

Good Job

Minimal Network Exposure

Network Infrastructure

Most of the network configuration exhibited a concerted effort to minimize risks and appropriately limit access to the needed services.

Good Job

Strong Network User Credentials

Network Infrastructure

The network related user credential controls seemed very strong in that we were unable to successfully extract a single set of user names/passwords even though we tried via numerous types of coercion. This indicates that the organization has placed a high value proposition on protecting this type of sensitive information.

Network Vulnerabilities

We identified the following network related vulnerability:

High Risk

N1. Firewall TCP Rule Bypass

169.254.0.1

We identified an issue with your firewall related to the handling of specially crafted TCP packets. A typical TCP 3-way handshake which establishes a connection looks like:

Client (SYN) -----> Server

Server (SYN ACK) -----> Client

Client (ACK) -----> Server

A firewall monitors the incoming packets and checks for either an existing established connection, or if the packet is the initiator of a 3-way handshake, it will verify that a rule allows access and then process the packet accordingly. In the case of this vulnerability, it has been discovered that your firewall will always pass packets if a certain TCP flag is present (typically FIN or RST which are usually sent to end an established connection). The problem arises when we set the FIN or RST flag in the initial packet of a 3-way handshake. This creates an unusual combination of flags (for example, SYN + RST means to both start and reset the connection). After your firewall passes the packet because of the RST flag, the destination server will process the packet as a 3-way handshake initiator (SYN) allowing us to effectively bypass the firewall rules.

Open Ports

We identified the following open ports:

IP Address	Open Ports
169.254.0.1	443 (HTTPS – Cisco SSL VPN)
169.254.0.2	25 (SMTP)
169.254.0.10	80 (HTTP – ACME Public Site) 443 (HTTPS – ACME Employee Portal)
169.254.0.11	443 (HTTPS – ACME Partner Portal)
169.254.0.12	443 (HTTPS – Outlook Web Access)
169.254.0.13	21 (FTP)
169.254.0.14	*No open ports*

Web Application Vulnerabilities

We identified the following web application vulnerabilities:

High Risk

W1. SQL Injection

http://www.acme.com/account/user.cfm?userID=

A substantial SQL injection vulnerability was discovered on the user.cfm page which allowed us to collect information about the server including local IP address (10.10.10.11), SQL user accounts (sa, webadmin), user databases (ReportServer, ACME, ACMEPartners), table names, column names, data, etc. In addition, we were able to create objects (note a new table called 'MyData') and update existing table data (note the 'John Smith' user in the USE_User table now has a middle name of 'Xervant'). It is worth noting that the SQL user didn't have permissions to perform OS level functions which prevented us from interacting directly with the Windows OS.

Medium Risk

W2. Information Disclosure

https://www.acme.com/ registration

The site provides an error message indicating an invalid account number (*Account number was not found*). This information could be used in conjunction with a social engineering type attack to gain access to customer account information.

Low Risk

W3. Click Jacking

http(s)://www.acme.com

https://partner.acme.com

The site does not implement the X-Frame-Options header so the entire site is susceptible to a Click Jacking attack which involves malicious content being sent to the user with an invisible frame overlaying your site.

Social Engineering Vulnerabilities

We identified the following social engineering vulnerabilities:

High Risk

S1. Information Disclosure

General Information

Once we established a baseline trust with the targets, they disclosed numerous pieces of general information which is very useful to a would-be attacker. Some of the significant disclosures that we received included:

- Helpdesk hours of operation
- The helpdesk team are the only ones who could reset a password
- The helpdesk manager's name

High Risk

S2. Clicking Link to Unknown/Unverified Web Site

Highly Targeted Attack

The targets were approached with high-probability user-focused scenarios such as information about a performance issue with their new sports car or an invitation to connect via a social media site. The attack scenarios were very successful usually resulting in numerous clicks. The payload of these particular attacks was to visit a potentially infected web site (although we re-directed the user to a real site once they hit our targeted site).

Social Engineering Thoughts

As with any security assessment, it is important to have specific goals in mind as you go through the social engineering assessment process. With social engineering, the goal should never be to identify the employee(s) who are susceptible to a social engineering attack, because we are all potentially vulnerable in our own ways. The better approach is to assess if you as an organization are fostering the right kind of culture that is naturally defensive to this type of attack regardless of the position or technical knowledge level of the employee. Of course, it is typically easier to convince a non-technical employee to take the bait, but that is to be expected. It is also safe to assume that the bad guys know this fact very well and will likely target those employees with whom they feel they can be successful. With that being said, our focus should be to identify the types of attacks that were successful and then create controls that will help to mitigate that type of attack in the future regardless of which employee may become the chosen target.

In almost every case, the best way to defend against social engineering attacks in general is to:

- Create clear and concise policies to address the areas of concern.
- Educate your staff on those policies.
- Educate your staff on basic computer security concepts on a regular basis (it is important to be creative with this process to help the listener retain the information).
- Help your staff to be a little paranoid by educating them about the risks on a regular basis (monthly emails, etc). *One of my personal favorite sayings is:* ***it's not paranoia if the threat is real.***
- Regularly test the effectiveness of your security training efforts and adherence to policies by performing social engineering assessments on an ongoing basis.

It may seem a little self-serving to suggest ongoing social engineering assessments, but in actuality it will generate an increased defensive posture that you are not likely to achieve through education and policies alone. This metamorphosis occurs because the targeted employees will make it their goal to 'beat' the social engineering assessment team. Since the employees will not necessarily know when an assessment is taking place, they will tend to develop a natural heightened awareness of attack scenarios and their defensive nature will dramatically increase which will directly translate into a much more security conscious employee.

Network Remediation Recommendations

Firewall TCP Rule Bypass

169.254.0.1

1. Apply the latest patches from your firewall vendor to each firewall.
2. Ensure that only non-routable IP addresses are used behind the firewall:
   - 10.0.0.0 – 10.2255.255.255
   - 172.16.0.0 – 172.31.255.255
   - 192.168.0.0 – 192.168.255.255
3. Consider upgrading all firewalls to devices that use stateful inspection type packet filtering.

Web Application Remediation Recommendations

SQL Injection

http://www.acme.com/account/user.cfm?userID=

1. Since the site is a Cold Fusion based site, use the *cfqueryparam* function to parameterize all input parameters.
2. Consider using the *isNumeric()* function to validate all integer based input.
3. To add layers of security and minimize potential impact in the event of an accidental SQL Injection exposure, modify your SQL user account (webadmin) so that it only has the minimally required permissions on the database (ideally 'execute only' for the required stored procedures).

Information Disclosure

https://www.acme.com/registration

1. Update the code so that you always return a general error message.
2. Consider implementing a temporary page block for IP addresses after a number of failed attempts.

Click Jacking

http(s)://www.acme.com

https://partner.acme.com

1. Implement the X-Frame-Options header:

ASP.Net

Update the Global.axa file to include the following in the Application_BeginRequest method:

HttpContext.Current.Response.AddHeader("x-frame-options", "SAMEORIGIN")

IIS 7

- Open IIS Manager and navigate to the site you want to add the header to
- In **Features View**, double-click **HTTP Response Headers**
- On the **HTTP Response Headers** page, in the **Actions** pane, click **Add**
- In the **Add Custom HTTP Response Header** dialog box,
  - type *x-frame-options* in the **Name** box, and
  - type *SAMEORIGIN* in the **Value** box
- Click Ok

Apache

Add the following to your site's configuration:

Header always append X-Frame-Options SAMEORIGIN

Social Engineering Remediation Recommendations

Information Disclosure

Social Engineering

4. Create a written security policy outlining what types of information could be disclosed (and what should never be disclosed), to whom it can be disclosed, and under what circumstances it can be disclosed.
5. Educate staff members on the requirements of the policy.
6. Create an atmosphere of verification first, and then helpfulness. It is human nature to want to help and it is a significant part of our role in IT, but there should be some type of verification that can be performed before any information is disclosed to someone (such as asking for an Employee ID or PIN, etc).

Clicking Link to Unknown/Unverified Web Site

Social Engineering

1. Adopt a 'no click' policy unless the link has been verified.
2. Educate staff on techniques of verifying a link:
   a. In most modern email clients such as Outlook, you can move the mouse over the link in question and it will show the actual link in a popup tooltip message and in the status bar (typically at the bottom) of the mail client.
   b. Another option is to simply right click the link and choose the 'Copy Link' option. You can then 'Paste' the link into a basic text editor (such as Notepad) to reveal the actual link before following it.
3. Educate staff on the basics of HTML to help them understand there is no correlation between the text displayed for an HTML link and the actual destination address of that link.
4. Educate staff on the basics of Internet addressing including:
   a. IPv4 Addressing Notation
   b. IPv6 Addressing Notation
   c. Decimal equivalents of IP address notations
   d. Domain Name System (DNS) basics (name resolution, etc)