tracesecurity

GRC Simplified... Finally.

TRACESECURITY WHITE PAPER

Missed Aspects of Vulnerability Management

Protecting Your Organization from Common Low-Risk Vulnerabilities

Bethany Ward

TraceSecurity Information Security Analyst

Executive Summary

Following a penetration test or vulnerability scan, an organization will often have a handful of issues marked as low-risk. Most IT departments will be quick to mitigate high- and medium-risk vulnerabilities. However, when it comes to low-risk vulnerabilities, organizations often let the issues linger, or worse, dismiss them all together.

Believe it or not, these seemingly dismissible low-risk vulnerabilities can lead to large security breaches. From default credentials on an alarm system to an open Microsoft® share, the simplest security flaws can at times be more dangerous to an organization than a well-crafted exploit.

This white paper highlights common low-risk vulnerabilities most organizations consider non-threatening, and as a result, often fail to address in their remediation activities.

Common Low-Risk Vulnerabilities

Insecure Protocols

Supporting remote access to data servers, routers, and other types of systems is a necessity for most organizations today. Remote access protocols such as HTTP and Telnet are still in common use for administrative functions due to their simplicity of application, but they can pose a serious threat as they transmit all network traffic in cleartext. This means that any malicious attacker that intercepts the transmission between a remote user and a system is privy to all of the information passed between the two, such as authentication credentials, in an easy-to-read format. This is referred to as a “man-in-the-middle” attack.

Encryption, even at the lowest level, has become paramount with the increase of man-in-the-middle technologies. Capturing network traffic is cheap and easy thanks to low-cost equipment, open source software, and extensive free training materials. It is safest to assume that any and all traffic sent across the network can be intercepted and thus should be protected. The simplest way to protect against man-in-the-middle attacks is to use encrypted protocols, such as HTTPS or SSH, anytime remote access is required.

Weak Encryption

While any encryption is a step-up from cleartext, utilizing weak algorithms and cipher suites can make it easier for an attacker to unencrypt data. As technology progresses, computers become faster and more efficient. As a result, the time and cost associated with breaking data encryption continues to decrease. For example, at one time it was standard for symmetric cryptographic algorithms to use key sizes of 40 bits and asymmetric encryption to use 512 bits. In fact, until 1998, it was illegal to export cryptosystems outside the U.S. that used larger key sizes. These key sizes can be broken in a matter of seconds by today’s computers. Now, the National Institute of Standards and Technology (NIST) does not allow anything smaller than 112 bits for symmetric cryptographic algorithms and 1024 bits for asymmetric. Both of these key sizes are thought to become disallowed in the near future.

In order to keep up with technological advancements and newly discovered security threats, the level of encryption accepted by an organization should support the highest level of security possible. This is especially true in the case of online banking services and remote network device administration. A review of the encryption used, including both key sizes and cipher suites, on an annual basis can help keep data safe in today’s evolving threat landscape.

Default Credentials

Even if the strongest encryption is enabled on every remote access protocol, it is still a simple matter for an attacker to access a system if the factory set credentials are never changed. It is extremely common for hardware and software systems to be initially configured with a simple, default set of credentials. These default credentials are often available via online databases that provide username and password pairs, detailing products down to the model and version number.

Even if the default password is not uniform across all devices but is instead a serial number placed on a sticker on the physical system, the potential for an easy compromise exists. An unauthorized employee, third-party vendor or even a successful social engineer could easily take a photo of the sticker and leave the facility with the information needed to access the system.

Policy and procedure should require default passwords to be changed for any new hardware or software introduced into an organization's network. To further enhance system security, default accounts should also be deleted and replaced with unique usernames.

Simple Passwords

Changing a password to "123456" or "letmein" will barely slow a malicious attacker down. As stated previously, capturing network traffic in transit is simple. It is slightly more difficult to read an encrypted password but far from impossible. Most encryption algorithms have identifiable patterns, and numerous tools exist to identify what algorithm has been used on the data captured. Once the type of algorithm used has been identified, an attacker can determine the password by encrypting a list of common passwords with the same algorithm and comparing the output. The largest known password file in existence is 32 million strong. With the addition of rulesets that manipulate the passwords into common reconfigurations, billions of possibilities can be attempted within a matter of minutes.

When a password is set on a system or application, it should be capable of standing up to these types of brute-force attacks. Using multiple character sets (such as lowercase letters, uppercase letters, numbers and symbols) and enforcing a minimum length (eight or more characters is standard) can help prevent a successful attack. Avoid using easy to guess components, such as names, seasons, or pop culture references.

No Lockout Policy

An attacker could skip the hassle of sniffing network traffic and decrypting login information by running a password attack against the login prompt itself. Using gathered or known usernames and a dictionary of passwords, the attacker could try each combination until one grants them access to the system. There are numerous tools to automate this process, making it one of the simplest attack vectors. This type of attack is also one of the easiest to guard against. For any system or application that requires a login, the account should be set to lockout after a certain number of invalid attempts, which will slow or halt a password attack.

The most secure option is to permanently lock the account so that it cannot be used until an administrator physically reactivates it. However, if this is not a viable option (there is only one account for the system or the account in question is the administrator), a time limit can be effective. For example, if an account that only allows three failed login attempts remains locked for 12 hours, an attacker could only try up to six passwords per account per day.

Open Access

Secure protocols, strong encryption, complex passwords, and stringent lockout policies are all completely useless layers of security if the device requires no authentication. This often occurs on systems and applications that are only accessible from the internal network. An opinion commonly held by even diligent Information Security Officers is that if a system is only available internally, it is safe. This is a dangerous assumption that leads to critical files being openly shared with anyone who has access to

the network, whether authorized to view the information or not. Not all files and information should be available to all employees. For instance, a marketing specialist does not need access to customer account information, just as a teller does not need access to payroll information. Allowing employees access to confidential information that is not necessary for their job function increases the spread of damage a rogue employee could inflict.

In the event external layers of security fail, the information housed on the internal network is accessible to a malicious attacker. If a zero-day vulnerability is exploited or a social engineer is successful in gaining access to the network, the lack of internal security controls means the attacker will be able to steal a lot more information — and do a lot more damage — before they are discovered. Adding authentication requirements to access this data, even from inside the organization, provides an extra layer of security that can protect sensitive information and systems in the event internal network access is achieved.

Dismissed Equipment

There are certain categories of equipment that are dismissed when it comes to assessing security risk, leading to potential openings in the network. While critical servers and network devices might be locked down tight, printers, IP phones, and music players are often considered low-priority or low-risk and left with lax security controls. However, these low-priority systems can reveal sensitive information and/or provide a gateway to more critical systems.

For example, a copier that is used to send scanned documents via email can be used to redirect all scanned or copied documents to the attacker's email address. A Windows® XP machine that is only used to play music for the branch is an open door for a hacker. A dedicated attacker will look for the weakest link, and organizations often forget to consider that their simplest systems are part of the network of assets that require protection.

Conclusion: Minimize Security Threats

Patching critical vulnerabilities and keeping abreast of new exploits is a critical part of the threat mitigation process. Common, low-risk vulnerabilities may seem at first glance to be the least of an organization's problems; however, given the right circumstances, a successful exploit of these vulnerabilities can produce disastrous results. In most cases, mitigating the risk associated with a low-risk vulnerability is as simple as changing a password or a configuration setting.

A thorough review of security settings on each asset on an organization's network may be tedious but can ultimately prevent dangerous security breaches. Regular vulnerability scanning can help automate the security auditing process and assist organizations in keeping up with new threats. In addition, annual active penetration testing can reveal risks that automated systems miss, as well as demonstrate the possible dangers of a successful exploit. The key is to review all of the results of a security assessment and not simply the most alarming ones.

The most sophisticated, metal reinforced doorway is as useful as a beaded curtain if no one remembers to turn the lock.

tracesecurity
GRC Simplified... Finally.

About TraceSecurity

TraceSecurity is a leader in cloud-based cybersecurity solutions that help organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. TraceSecurity's award-winning TraceCSO is a revolutionary solution that dramatically streamlines the management of IT governance, risk and compliance (GRC) programs. It accomplishes this by tightly integrating and automating all eight critical IT GRC components: Risk Management, Compliance Management, Audit Management, Vendor Management, Incident Response Management, Vulnerability/Patch Management, Policy Management and Training Management. Most important, it provides built-in security and compliance expertise that most organizations lack. Because of its unique architecture and cloud delivery, TraceCSO deploys rapidly and reduces the cost of GRC management by as much as 80%.

With market experience that spans over 2,000 customers, TraceSecurity offers the insight, products, professional services and partners to support the security and risk management efforts of organizations of all sizes across all industries.

To learn more about TraceSecurity,
call 877-275-3009 or visit www.tracesecurity.com.