Penetration Testing for Today's Global Threats

Network and system vulnerabilities are being discovered and targeted every day. As cyberwarfare and hacking get more intricate and complicated with the integration of AI, it only reinforces the importance of effective penetration tests and network security hardening.

The introduction of Artificial Intelligence (AI) and Machine Learning (ML) provides a faster and more agile enumeration capacity to hacker groups. AI can corelate Open-Source Intelligence (OSINT) such as collections of breached user credentials, searchable databases of detected devices with vulnerabilities, as well as corporate media announcements and employee social media posts and provide corporate doxing reports.

As threat pressure escalates, it's never been more important than now to ensure your networks, devices and users are secured against the myriad of attack possibilities.

Unfortunately, Deer Brook continually detects common and easily remediated vulnerabilities during our vulnerability and penetration test engagements. By comparing the results of our penetration tests to industry norms, we've been able to assemble this collection of common (and critical) vulnerabilities and practices that need to be addressed.

Background

Default Credentials in Use

Leaving the default username and password enabled on a device opens it up to be exploited by all hackers, regardless of their skill.

This is one of the most dangerous mistakes an organization could make, in large part due to resources such as www.defaultpassword.com that catalog default usernames and passwords for over 1800 devices.

It's so easy for someone to look up default credentials for any device, that the device may as well have no credentials at all.

Since 2014, more organizations have become aware and changed their devices' default credentials. The number of devices using default credentials continues to decrease, but the few devices remaining that use default credentials are posing an incredibly dangerous security threat.[1]

Default SNMP, Including Write Ability

Simple Network Management Protocol (SNMP) is how devices on a network communicate with each other, therefore it is notable to stress its importance in an organization's structure.

With this high-level of importance arise permissions and abilities through the SNMP protocol that are very attractive for hackers.

In the wrong hands, SNMP is an entry point for hackers that want to obtain information including Address Resolution Protocol (ARP) tables, usernames, and Transmission Control Protocol (TCP) connections across the SNMP.

Default SNMP settings forego the guessing work for hackers, allowing them to sooner access your network information and prepare to exploit all the vulnerabilities they've identified as a result.

SNMP is a useful tool to monitor your network, but it wasn't developed with the modern day's widespread Internet-use in mind.[2] As a result, valuable tokens and keys (specifically, the Community Key) are transmitted over SNMP as plain-text, and hackers that gain access to your information will have little trouble identifying systems. Additionally, the important device management abilities within the SNMP can allow hackers a wide variety of options, including shutting down your network interface.[3]

SNMP is an important network management tool that can't be replaced, but is extremely vulnerable with its default settings enabled.

SMBv1 With No Signing Required

Developed in the 1980s, Server Message Block (SMB) is a network protocol that allows devices to communicate and share files. Much like SNMP, it was developed for a bygone era of computing. Nowadays, SMBv1's vulnerabilities and exploits are used to propagate malware to all devices on a LAN, regardless of the security settings. SMBv1 is not secure.[5]

SMBv1 is prone to man-in-the-middle attacks, cyberattacks in which a hacker alters communications between two parties. This means that a hacker can tell your network to downgrade its security and leave itself susceptible to more attacks, can view the information your devices are sending to each other on the network, and more.[6]

Infamously, the WannaCry ransomware program leverages SMBv1's vulnerabilities to compromise systems, encrypt files, and spread to other devices on the network.[7] Other threats such as TrickBot and Emotet also take advantage of SMBv1's systemic vulnerabilities.

Unencrypted Management Protocols

SMBv1 is an example of an unencrypted management protocol, but other insecure protocols include HTTP, NTLM, and LLMNR. HTTP in particular isn't insecure by nature but is rather dangerous to use when sending or receiving data.[8]

Unencrypted management protocols leave your organization's data exposed and vulnerable for attacks, and hackers consistently rely on these protocols to unleash their ransomware attacks.

Unpatched Third-Party Software

Third-party software is an undeniable commodity for most organizations, but this software often proves to be a backdoor for hackers if not kept up to date.

In 2019, a two-year study by Ponemon Institute revealed that 60% of the data breaches recorded within that time were due to unpatched software.[9]

If your third-party software is unpatched, you run the risk of data and security breaches, and a potential loss of reputation. It's imperative to keep third-party software patched and up to date, because no matter how stellar a security system is, unpatched external software can do it in.

Unconfigured Printers

The modern printer is a sophisticated computer with print functionality; there's a lot of complex processes and programming under the hood of a printer, to the point where printers have proven to be valuable points of entry for hackers. In 2019, 10% of security breaches affecting organizations had involved a printer in one way or another.[10]

Today's modern printers are deeply integrated into organizations' networks and are considered a connected device. Anyone who can access your organization's internal

network can access your printer, and unconfigured printers are often to exposed to the internet for everyone to access.

Many printers are setup with default settings and are not updated routinely, leaving them exposed to the internet while running on outdated, vulnerable software. Hackers take over these printers by sending them malware, and as mentioned previously, once the hacker has gained access to your printer, they can access the rest of your network.

We often find printers with access to the Internet over ports 80 and 443 as an oversight. It is best practice to deny printer IP addresses outbound traffic to the Internet using a firewall.

Hardening of AD Authentication Protocols

When utilized effectively, Active Directory (AD) authentication protocols serve as a simple, streamlined way for your IT team to manage user and rights management for everyone across your organization. However, a misconfigured, poorly managed, or unpatched AD system is a ticking clock counting down to a security breach.

Networking Equipment with Initial Setup Services Running

Telnet, Remote Desktop Services (RDS), File Transfer Protocol (FTP), Simple Management Block (SMB) and other unnecessary and risky protocols are sometimes left running on network devices after setups.

It is best practice to only enable services that are necessary to operate the device in order for it to fulfill its mission. Should risky protocols be needed for administrative work, they should be disabled when no longer in use.

Kerberoasting

Kerberoasting is a kind of cyberattack that retrieves the password hash of an AD account with a Service Principal Name. The hacker is able to retrieve the hash of the account's password and cracks the hash to reveal the password in plain text. Once the password is cracked, the hacker can log into the account and gain access to all the work systems and networks that are available to the account.[12]

Network Level Authentication Not Required

RDS operating without enabling Network Level Authentication (NLA) leave themselves open to remote code execution attacks and denial of service attacks.

NLA requires any connecting user to first authenticate themselves before they can actually establish a session with a server.

In addition to preventing remote code executions and other vulnerabilities associated with RDS before an actual sign on, NLA also ensures less remote computer resources are being used until the user is fully verified and connected to the server.[13]

Integrated Lights-Out Interfaces

Integrated Lights-Out (iLO) interfaces are often neglected from vulnerability scans under the assumption that, if a server was scanned, the full picture is taken. That could not be further from the truth. iLO interfaces can have vulnerabilities that require updates, just like any other device.

Lessons Learned

With the Deer Brook team's collective experience and studious approach to penetration testing, we've accumulated lots of lessons learned that can benefit any organization immediately:

- Most Internet of Things (IoT) are not segmented away from critical systems or the internet, even if they should be. IoT devices are physical, have processing ability, and can communicate and exchange data with other objects and services over the internet.
    - Additionally, most of these IoT are not updated. This leaves these devices vulnerable to current threats like Log4J that can take total control of systems.
- We've found that Microsoft updates are mostly systematic and provide adequate-enough coverage.
- On average, network devices lag behind all others in terms of firmware updates.
- Third-party software is often neglected by organizations, and in turn is widely targeted by hackers.

    - Additionally, unused and unnecessary software that is used once and forgotten is often the most vulnerable.
- Most of the issues and focus of the security realm hover around servers, but it's important to acknowledge that social engineering is also a popular tactic used by online threat actors. Training against social engineering should be considered alongside server hardening.
- Most of the vulnerabilities we find are related to third-party applications. Specifically, we've found that the most vulnerable applications are those not patched with services like Windows Server Update Services (WSUS).
- Modern tools and services are often patched and updated while older protocols and services are left neglected.
- Eternal Blue and BlueKeep are very popular exploits that are very effective. If you don't have the right protections in place, it's a matter of "when," not "if."
- AD's complexity, combined with default settings that organizations often leave unconfigured, makes it an easier and more popular service to attack compared to any other specific services.

Proposed Solution

To maximize your network security and minimize your vulnerability, Deer Brook recommends a five-pronged approach to security, hardening, and review: a combination of asset management solutions, regular vulnerability scans, remediation SLAs, third-party tests, and firewall reviews.

Asset Management Solution

An asset management solution will help your organization track its assets, maximize utilization, and minimize costs. Specifically, the ideal asset management solution will give you detailed breakdowns of user permissions, usage patterns and compliance, and other details.

An asset management solution will make it clear what you own, so that assets won't get forgotten, neglected, and rendered vulnerable for exploits.

Regular Vulnerability Scans

Vulnerability scans will show you security flaws and vulnerabilities across your organization's networks, systems, hardware, and software.

Performing vulnerability scans on a regular cadence will allow your organization to choose remediation paths for any vulnerabilities exposed, allowing you to keep your security fresh and up to date.

Remediation Service Level Agreements

Vulnerability remediation SLAs outline the process of how your organization patches vulnerabilities, and establishes a level of service that measurement, metrics, and penalties can be created based on.[14]

It's important to develop an SLA that is aligned with business or technology objectives, because there's no one-size-fits-all timetable for all vulnerabilities.

Third-Party Tests

With expertise and industry best practices in mind, third-party penetration tests often find more vulnerabilities than in-house teams.

Additionally, third-party tests can provide detailed breakdowns of security effectiveness, response time, and incident management procedures.

Firewall Reviews

Firewall reviews are important to maintain a firewall's effectiveness as it relates to rules, change management procedures, open ports, and more.

Outdated firewall policies and rules can negatively affect an organization's security and efficiency, but a detailed firewall review will ensure that all policies and rules are up to date.

Conclusion

As an experienced third-party tester, Deer Brook can provide full, effective vulnerability management discovery and tracking services. Deer Brook is also capable of performing efficient, productive firewall reviews.

References

1. "2020 Trustwave Global Security Report" Trustwave. 22 April 2020
2. "Lock IT Down: Don't allow SNMP compromise net…" TechRepublic. 11 April 2001
3. "Reducing the Risk of SNMP Abuse" CISA. 05 June 2017
4. "The protection of information in co…" Proceedings of the IEEE. September 1975
5. "Microsoft network server: Digitally sign communic…" Microsoft. 17 January 2023
6. "Disable SMB v1 in Managed Environments with Grou…" Microsoft. 17 May 2017
7. "WHAT IS WANNACRY/WANACRYPT0R?" NCCIC. 09 June 2017
8. "Insecure Protocols: SMBv1, LLMNR, NTLM, and HTTP…" ExtraHop. 12 May 2021
9. "The 5 biggest dangers of unpatched and unused softwar…" 1E. 26 February 2019
10. "Global Print Security Landscape, 2019" Quocirca. February 2019
11. "Active Directory Security and Hardening: An Ethical Hac…" Delinea. 29 July 2022
12. "Kerberoasting Attacks" Crowdstrike. 01 March 2023
13. "Prevent a worm by updating Remote Desktop Service…" Microsoft. 14 May 2019
14. "Tenable Cyber Exposure Study – Cyber Insurance Report: SLAs and R…" Tenable.

deer-brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS