GUIDEPOINT® SECURITY

ACTIVE DIRECTORY SECURITY REVIEW

Let the Experts Most Familiar With Active Directory Attacks Evaluate Your Implementation to Find the Issues Before the Attacker Does

Active Directory is a crown jewel that attackers will pursue with a laser focus

Your Active Directory implementation is a mission-critical and ever-evolving piece of your IT infrastructure. Access to your AD would allow attackers an unprecedented amount of control in your environment, so it's critical to evaluate and test your implementation.

Good security requires ongoing attention, but some assets are just too important to call it a day at "good". For those assets, the price of excellent security is eternal vigilance.

Access to your Active Directory is a promised land for attackers. Once inside, they can wreak havoc across your environment, develop persistence, and engage in counter-IR that can stretch any incident out indefinitely.

GuidePoint Security's Active Directory Security Review will assess and test your AD implementation to find weaknesses, pinpoint exploits, and recommend improvements to ensure you meet or exceed best practice recommendations. Our offensive security experts will identify misconfigurations and vulnerabilities across your AD that are commonly exploited by threat actors.

- Service Principal Name (SPN) configuration
- Kerberos Authentication
- Domain Functional Levels
- Password Policy
- Share, User, Group, and Computer Permissions
- Null Sessions and Passwords
- Password Reuse
- Domain Trust Configuration
- Server Message Block (SMB) Configuration

Put a Highly-Trained, ELITE Team on Your Side

More than 70% of our workforce consists of tenured cybersecurity engineers, architects and consultants.

Hundreds of Industry and Product Certifications

OSCP OSCE CISSP GWAPT GSE GPEN

GuidePoint Security's expert teams will analyze your Active Directory (AD) data for the following items and show the various impacts of any misconfigurations identified. All RAW data output can be provided upon request.

Detailed analysis of in-scope AD domains to include:

- Domain Computers
- Functional Levels
- Domain Users
- Password Policy
- Default Domain Policy
- File Shares
- Server Principal Names (SPNs)
- User, Group, and Computer Permission Delegations

Analysis of common vulnerabilities and misconfigurations regarding the following:

- Kerberos Delegation
- Local Administrator Password Solution (LAPS)
- FSMO Roles
- Accounts that are sensitive to delegation
- Kerberos encryption type
- Fine-Grained Password Policies
- KRBTGT password changes
- Group Policy Objects (GPOs)
- Trust configuration
- Server Message Block (SMB) Signing
- Domain Controller Null Sessions
- Identify accounts that can have no password applied
- SMB Versions

After analysis is complete, we will provide recommendations to address any discovered misconfigurations and harden your AD against exploitation.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.

GUIDEPOINT® SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132