

PROTECT:  
Financial Services & Banking

---

- Vulnerability Program Review
- Penetration Testing Services



DEER BROOK

---

CYBER | TECHNOLOGY | SOLUTIONS

68 Main Street, Kennebunk, ME 04043 (207) 387 - 0396 [www.Deer-Brook.com](http://www.Deer-Brook.com)



DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Maine's Premier Veteran Owned & Staffed Cybersecurity Company

- ✓ Vulnerability Management Services
- ✓ Network Penetration Testing
- ✓ CIS & NIST 800-53, 800-171 Assessments
- ✓ Digital Forensics
- ✓ Software Development Reviews
- ✓ Application Security Assessments
- ✓ Software Code Security Reviews
- ✓ Technology Reviews

## SERVICES

### Vulnerability Management Assessment

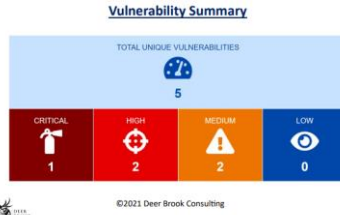
Deer-Brook can review and validate your institution's Vulnerability Management program. We will review your Vulnerability Management policy, program, and standards as well as how you manage accepted vulnerabilities that cannot be reasonably fixed. Our network scans results will be reconciled with yours to find any discrepancies.

### Network & System Penetration Testing

Our expert team will perform penetration tests against all exploitable vulnerabilities we identify. We can also review your Active Directory for anything that can present a threat to your network and data.

### Advisory Services

Your Deer Brook team includes an account representative, a policy and control expert, a Senior Cyber Pen Tester, and team of specialists who have everything cyber covered. If you have any questions regarding security, or technology; feel free to bounce those questions off us. Consider Deer Brook an advisory extension of your team. We are happy to advise on security matters anytime.



### PRIVILEGED ACCOUNT OBSERVATIONS

Severity	Description	Count	Resolution
Critical	Members of the Administrators and Domain Administrators accounts are vulnerable to brute forcing.	4	Implementing a one of the following controls against Active Directory utilizing tools such as Metasploit or Powercat/Powercat, attacks can remove vulnerable accounts. Admins/Domain Admins through specially crafted authentication packets. Once removed an attacker can then brute force over the backoffice and acquire potentially high-level credentials on the domain.
High	Number of administrative accounts without the flag "This account is sensitive and cannot be managed".	25	Remove this flag on all sensitive objects. This account is sensitive can be impersonated by sensitive accounts and might. Best practice dictates all administrative accounts have this set to true.
Medium	Percentage of administrative accounts that are inactive.	20%	Administrative accounts that haven't received a login event in at least 6 months or have been created more than 6 months ago with no logs, are considered inactive. Best practice dictates high-privileged administrative accounts be maintained. If an account is not required, it should be removed or renamed.
Low	Number of administrative accounts with passwords older than 90 days.	3	Best practice dictates administrative account passwords should be changed at least every 90 days, preferably every 60 days. However, periodic rotating or temporary accounts are often created then forgotten about. Compromise tool provides an attacker with long-term persistence with low likelihood of detection.

©2021 Deer Brook Consulting

### LOCAL ADMINISTRATION: REMOTE CODE EXECUTION VIA JNDI REFLECTION (CVE-2015-1635)

**Description:**  
 Remote code execution (RCE) is a critical vulnerability in Active Directory. It allows an attacker to execute arbitrary code on the target system. This vulnerability is caused by a combination of factors, including the use of JNDI for LDAP queries and the presence of a specific LDAP entry in the Active Directory database.

**Vulnerability Score:**  
 CRITICAL

**CVSS: 9.8 (AV:N/AC:L/AU:N/C:CR/I:N/AE:C)**

**References:**  
 - [https://www.exploit-db.com/exploits/10111/](#)  
 - [https://www.exploit-db.com/exploits/10112/](#)

**Steps for Remediation:**  
 1. Verify if the vulnerable LDAP entry is present in the Active Directory database.  
 2. Remove the vulnerable LDAP entry.  
 3. Enter the malicious JNDI LDAP query into the Metasploit Meterpreter console.  
 4. Verify the connection back to the remote host system.

```

msf5 > use multi/ldap/remote_code_execution
msf5 multi/ldap/remote_code_execution > RHOST=10.10.10.10
msf5 multi/ldap/remote_code_execution > RURI=ldap://10.10.10.10:389/ou=Users,dc=example,dc=com
msf5 multi/ldap/remote_code_execution > EXEC=cmd.exe /c ipconfig /all
msf5 multi/ldap/remote_code_execution >
  
```

# REPORTING

Executive Summary

The report details the engagement and provides recommendations for enhancements to your Vulnerability Management program if needed. Scan results are provided and organized by specific vulnerabilities – critical, high, medium, and low.

Vulnerability Summary

Provides unique vulnerabilities and which systems they were identified on.

Configuration Issue Summary

As part of our penetration tests, we evaluate configurations and controls running in Active Directory through unique lenses – stale objects (user or computer), privileged accounts, and weak passwords.

Remediation Recommendations

Remediation instruction is included in Deer Brook reports, and we are happy to rescan your systems as you remediate your critical and high rated findings, or any that you cannot check yourself.

Client Communications

*Deer Brook will be your partner during the engagement and then after. Our team will notify you when field work starts and stops each day. If any critical vulnerabilities are found, we will contact you right away and not wait until the report draft is ready.*