# DRGONF1Y

# ACTIVE DIRECTORY ATTACK PATHS

A PRACTICAL FIELD MANUAL FOR ASSESSMENT, EXPLOITATION, DETECTION & DEFENSE

**2026 FIFTH EDITION - REVISION 5.1**

PRACTITIONER EDITION


DRGONF1Y

CYBERSECURITY CONSULTING LLC


BLOODHOUND • KERBEROS • AD CS • LAPS • DELEGATION • HYBRID IDENTITY

*THE ORIGINAL VISUAL IDENTITY WITH A CLEARER ROUTE INTO THE BOOK*

# F-02 Title and Learning Contract

**DRG0NF1Y ACTIVE DIRECTORY ATTACK PATHS**

2026 Fifth Edition Revision 5.1 - Practitioner Edition

This field manual teaches security reasoning through evidence, prerequisites, manual verification, minimal authorized proof, cleanup, detection, remediation, and retest. Commands are representative and version-sensitive; installed help and primary documentation remain authoritative.

```
Discover -> Enumerate -> Validate -> Control -> Prove -> Clean up -> Report
```

| Reader promise | How Revision 5.1 supports it |
|---|---|
| Find the next page | A visible table of contents maps physical pages, chapters, decision libraries, references, and appendices. |
| Know how to read | Page 9 explains learning, field, lab, defensive, and reporting modes. |
| Know what to do next | Page 10 routes common lab results to the correct methodology or attack-path family. |
| Keep the original identity | The illustrated shield-and-dragon cover is restored; only the edition badge is updated. |

**Version decision.** This is Revision 5.1 because it corrects navigation and reader workflow without adding a new major attack-path family.

*AUTHORIZATION IS A PREREQUISITE*

# F-03 Copyright Scope and Responsible Use

Copyright (c) 2026 DRG0NF1Y Cybersecurity Consulting LLC. All rights reserved. Fifth Edition Revision 5.1 publication build.

This book is for defensive security professionals, penetration testers, red-team students, administrators, instructors, and learners working in intentionally vulnerable laboratories or explicitly authorized assessments. Use commands and procedures only against systems for which the operator has authorization.

| Boundary | Required practice |
|---|---|
| Scope | Record domains, forests, subnets, identities, techniques, and exclusions before testing. |
| Minimal proof | Prove the security-boundary change with the least disruptive reversible action. |
| Secrets | Keep passwords, hashes, tickets, keys, certificates, and dumps out of publication screenshots. |
| Cleanup | Track every changed object, file, listener, route, credential artifact, and rollback verification. |
| Claims | Separate demonstrated capability, supported inference, and untested hypothesis. |

**Responsible-use rule.** If authorization, rollback ownership, or the stop condition is unclear, pause before
changing state.

*START WITH THE ROUTE THAT MATCHES YOUR CURRENT EVIDENCE*

# F-04 Table of Contents - Book Map


| Section | Purpose | Physical pages |
|---|---|---|
| Part I - Foundations | AD model, rights, Kerberos/NTLM, Tier 0 | 11-17 |
| Part II - Assessment methodology | Scope, recon, black box, PJPT, atlas, CRTP, DNS, authenticated enum, BloodHound | 18-154 |
| Part III - Credential/Kerberos | Passwords, roasting, stores, hash/ticket paths | 155-181 |
| Part IV - Authorization/control | ACLs, groups, GPO, local admin, sessions | 182-214 |
| Part V - Enterprise AD | LAPS/gMSA, delegation, AD CS, DCSync, trusts, hybrid | 215-273 |
| Part VI - Detection/reporting | Detection, evidence, remediation, practice, troubleshooting | 274-289 |
| Part VII - Visual guide/labs | Diagrams, GOAD notes, six guided labs | 290-315 |
| Part VIII - Advanced/reference | AD CS, hybrid, cases, exercises, simulation, endnotes, index | 316-344 |
| Appendices | Linux, BloodHound, Windows, IF-THEN, MITRE, worksheets, glossary, bibliography | 345-357 |
| University HB Chain revision | Reusable chain patterns, validation, defense, cleanup | 358-400 |


**Navigation.** The PDF bookmark panel mirrors the specialized routes. The next four contents pages provide physical page numbers for chapters and decision libraries.

*FOUNDATIONS, ASSESSMENT METHODOLOGY, AND CREDENTIAL PATHS*

# F-05 Table of Contents - Chapters 1-14


| Chapter | Title | Page |
|---|---|---|
| 1 | AD Security Model | 11 |
| 2 | Rights, Privileges, Permissions | 13 |
| 3 | Kerberos and NTLM | 14 |
| 4 | Tier 0 and Privileged Access | 16 |
| 5 | Scope and Rules of Engagement | 18 |
| 6 | Reconnaissance | 19 |
| 7 | DNS and Domain Orientation | 140 |
| 8 | Authenticated Enumeration | 141 |
| 9 | BloodHound Attack-Path Analysis | 142 |
| 10 | Password and Secret Hygiene | 155 |
| 11 | Kerberoasting | 158 |
| 12 | AS-REP Roasting | 165 |
| 13 | Credential Stores and Session Exposure | 167 |
| 14 | Pass-the-Hash and Ticket Paths | 179 |


**Start rule.** With zero credentials, use Chapter 5 for scope, Chapter 6 for recon, then enter the Black Box
Methodology at page 21.

*AUTHORIZATION, ENTERPRISE CONTROL PLANES, DEFENSE, AND PRACTICE*

# F-06 Table of Contents - Chapters 15-30


| Chapter | Title | Page |
|---|---|---|
| 15 | GenericAll and GenericWrite | 182 |
| 16 | WriteDACL and WriteOwner | 189 |
| 17 | Group Membership and Password Control | 196 |
| 18 | GPO and OU Control | 203 |
| 19 | Local Administrator and Session Paths | 210 |
| 20 | Windows LAPS and gMSA | 215 |
| 21 | Kerberos Delegation | 217 |
| 22 | AD CS and Certificate Services | 224 |
| 23 | DCSync and Replication Rights | 232 |
| 24 | Trusts and Multi-Domain Paths | 239 |
| 25 | Hybrid AD and Microsoft Entra | 241 |
| 26 | Detection Engineering | 274 |
| 27 | Evidence and Attack-Path Reporting | 276 |
| 28 | Remediation and Retest | 278 |
| 29 | CRTP and GOAD Practice Program | 279 |
| 30 | Troubleshooting and Decision Trees | 281 |


**Edge rule.** Use Chapters 15-25 only after a live ACL, service, delegation, certificate, replication, trust, or
hybrid prerequisite is verified.

*VISUAL LEARNING, GUIDED LABS, ADVANCED TOPICS, REFERENCES, AND TEACHING MATERIAL*

# F-07 Table of Contents - Chapters 31-50 and Appendices


| Chapter | Title | Page |
|---|---|---|
| 31 | Attack-Path Diagrams | 290 |
| 32 | GOAD Field Notes and Screenshots | 294 |
| 33 | Guided Lab 1 - Reconnaissance | 303 |
| 34 | Guided Lab 2 - Authenticated Enumeration | 305 |
| 35 | Guided Lab 3 - Kerberos | 307 |
| 36 | Guided Lab 4 - ACL Attack Paths | 309 |
| 37 | Guided Lab 5 - AD CS | 311 |
| 38 | Guided Lab 6 - DCSync | 313 |
| 39 | AD CS Deep Dive | 316 |
| 40 | Hybrid Identity Deep Dive | 318 |
| 41 | Case Studies | 321 |
| 42 | Exercises and Answer Key | 332 |
| 43 | CRTP-Style Final Simulation | 335 |
| 44 | Instructor Edition Orientation | Instructor only |
| 45 | GOAD Screenshot Walkthroughs | Instructor only |
| 46 | Detection Event Encyclopedia | Instructor only |
| 47 | Printable Operator Field Cards | Instructor only |
| 48 | Instructor-Led Capstone | Instructor only |
| 49 | Formal Endnotes | 337 |
| 50 | Topic Index | 341 |
| A-G | Appendices and quick references | 345 |


**Edition note.** Chapters 44-48 appear only in the Instructor Edition. Student and Practitioner editions route directly from Chapter 43 to Chapters 49-50.

*THE SHORTEST ROUTE FROM AN OBSERVATION TO THE CORRECT FIELD CARD*

# F-08 Table of Contents - Decision Libraries


| Cards | Coverage | Pages |
|---|---|---|
| B-01 to B-10 | Scope, interface, discovery, services, AD roles, DNS | 21-30 |
| B-11 to B-20 | Time, SMB/LDAP/RPC/web, users, AS-REP, first credential | 31-40 |
| B-21 to B-30 | Authenticated inventory, shares, roasting, AD CS, BloodHound, shell, privilege | 41-50 |
| B-31 to B-41 | SQL, relay, GPO, delegation, pivots, domain proof, recovery, reporting | 51-61 |
| P-01 to P-08 | PJPT route, pass-the-password, Golden and Silver tickets | 62-69 |
| P-09 to P-16 | GPP cpassword, LLMNR/NBT-NS, Responder, mitm6 | 70-77 |
| P-17 to P-24 | Token impersonation, file transfer, integrated PJPT chain, sources | 78-85 |
| A-01 to A-06 | Credential-free enum, roasting, PtP/PtH/PtT/PtC | 86-91 |
| A-07 to A-13 | ACL model and full WriteOwner-to-PKINIT chain | 92-98 |
| A-14 to A-20 | GPO/GPP, relay, RBCD, delegation, managed secrets, DCSync, tickets | 99-105 |
| A-21 to A-27 | Trusts, built-in operators, token privileges, service ACLs, secret sources | 106-112 |
| A-28 to A-36 | Tasks/services, SQL, movement, AD CS, troubleshooting, pivot, closure | 113-121 |
| 6A to 6R | CRTP result-driven field upgrade | 122-139 |
| HB revision | Portable multi-stage chains and defensive validation | 358-400 |


**If the test succeeds:** you have a named observation. Jump to its card, verify prerequisites, and perform minimal proof.
**If the test fails:** you do not yet have evidence. Return to B-01 and advance sequentially until a gate produces it.

*CHOOSE A READING MODE, THEN FOLLOW RESULTS RATHER THAN CHAPTER ORDER*

## F-09 How to Use This Book

| Mode | What to do | Best starting point |
|---|---|---|
| Learn | Explain the protocol, security boundary, prerequisite, and failure states in your own words. | Chapters 1-4, then the relevant chapter |
| Black-box lab | Begin with no assumed credentials and follow B-01 through the first validated branch. | Page 21 |
| Technique lab | Choose one P or A card; satisfy every prerequisite; use an inert proof and exact cleanup. | Pages 62 or 86 |
| Exam practice | Use the evidence ledger and decision cards; hide answer material and enforce a stop timer. | Pages 9-10, then page 21 |
| Defend | For each transition, identify telemetry, a path-breaking remediation, and a retest query. | Chapter 26 and each card's defense row |
| Report | Convert the chain into evidence, impact, limits, cleanup, remediation, and retest statements. | Chapter 27 and A-36 |

Working loop: Question -> Evidence -> Prerequisite -> Minimal proof -> Cleanup -> Next branch

| Page element | Meaning |
|---|---|
| Trigger | The observation that justifies opening this path. |
| Prerequisites | Conditions that must already be true; unmet conditions are stop gates. |
| Manual verification | Native or independent corroboration before mutation. |
| If it succeeds / fails | The next page family or diagnostic question; do not repeat a successful invasive action. |
| Evidence and cleanup | What to retain, protect, reverse, and independently verify. |

**Do not read linearly during a lab.** Use the contents to learn; use the decision libraries to operate. Re-enumerate after every new identity, credential, token, host-control level, route, or domain boundary.

*ONE RESULT SHOULD PRODUCE ONE DEFENSIBLE NEXT QUESTION*

## F-10 How to Run a Lab - IF Result THEN Route

| Observed result | Next route |
|---|---|
| No confirmed domain or DC | B-04 to B-10: interface, discovery, services, AD role, DNS |
| Domain known; no credential | B-11 to B-18: time, anonymous services, sourced users, AS-REP |
| Valid username or credential | B-19 to B-25: ledger, protocol matrix, LDAP/shares/roasting/AD CS/BloodHound |
| Password, hash, ticket, or certificate | P-02/P-03 and A-05/A-06: validate artifact against compatible protocols |
| BloodHound ACL edge | B-27 and A-07: verify live owner, DACL, group token, property, and target |
| WinRM/RDP/SMB execution succeeds | B-29 and A-30: obtain the least disruptive shell; run foothold baseline |
| MSSQL authentication succeeds | B-31 and A-29: separate login, impersonation, sysadmin, OS token, and links |
| Relay prerequisites are present | B-32, P-11 to P-16, A-15: analyze first; select one source/target/action |
| GPP or GPO control is found | P-09/P-10, B-33, A-14: separate cpassword, GPC, GPT, gPLink, and scope |
| AD CS condition is found | B-24/B-34 and A-31 to A-33: verify end-to-end issuance and mapping |
| New identity, host admin, or subnet | B-35 and A-35: repeat only affected discovery and authenticated gates |
| DCSync or Tier-0 proof succeeds | A-19 and A-36: stop active exploitation, clean up, preserve evidence, report |

**Lab rhythm**

1. Record scope, source host, time, tool version, identity, target, and question.
2. Run the least invasive discovery or verification step.
3. Classify success, failure, and what the result does not prove.
4. Perform one minimal authorized proof; stop when the objective is met.
5. Clean up, verify restoration, re-enumerate changed boundaries, and write the finding.

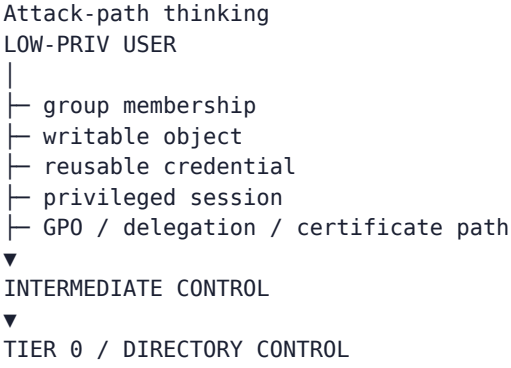
**If the test succeeds:** the result changes capability. Update the ledger and follow exactly one named route.

**If the test fails:** the result does not change capability. Diagnose reachability, DNS/time, authentication, authorization, protection, or tool syntax.

# Part I - Active Directory Foundations 1. AD Security Model

Active Directory Domain Services is an identity and authorization system. Users, computers, groups, services, policies, certificates, and administrative relationships become security principals or securable objects connected by permissions. Attack paths emerge when a principal that begins with limited trust can traverse those relationships toward a higher-value identity or control plane.

- Authentication answers: who are you?
- Authorization answers: what may you do?
- A security principal may be a user, computer, group, or service identity.
- An object ACL can create a privilege path even when no software vulnerability exists.
- A domain compromise is usually a chain of relationships, not one exploit.




## Assessment questions

- What identities exist?

- What can each identity control?
- Where can each identity authenticate?
- Where is it administrator?
- What secrets or sessions become exposed when a host is controlled?
- Which paths reach Tier 0?

Facilitator checkpoint

- Have the learner identify the current identity and distinguish authentication from authorization.
- Require one manually verified edge before accepting a graph-derived path.
- Ask which evidence is demonstrated, inferred, or still missing.
- Record the least-invasive next validation step and the stop condition.

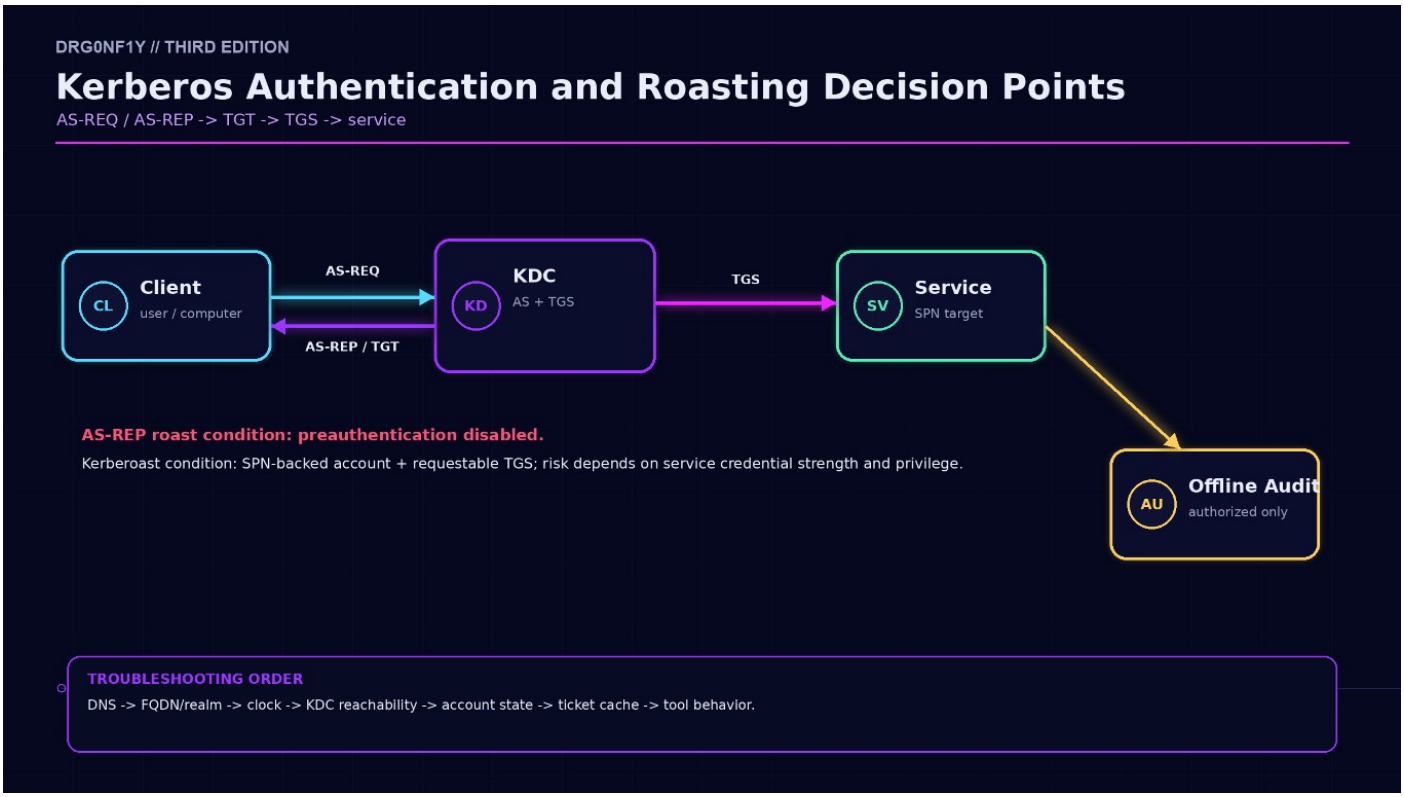
# 2. Rights, Privileges, Permissions and ACLs

Windows terminology matters. Rights or privileges are system-wide capabilities assigned to principals. Permissions are object-specific access controls represented by ACLs and ACEs. Effective access depends on group membership, inheritance, explicit allow/deny entries, ownership,

```
and sometimes powerful user rights.
Concept                                 Example                                 Security question
                                                                                Does the token provide a
User right / privilege                  SeBackupPrivilege
                                                                                system-wide capability?
                                                                                Which object and attribute
Permission                              Write property on AD user
                                                                                can be changed?
ACL                                     DACL on group/GPO/OU                    Who is allowed or denied?
                                        Principal + right +                     Is the entry direct or
ACE
                                        inheritance                             inherited?
                                                                                Can ownership be converted
Owner                                   Object owner
                                                                                into permission control?
```

## Native inspection

```
whoami /priv
whoami /groups
dsacls "<DISTINGUISHED_NAME>"
Get-Acl "AD:<DISTINGUISHED_NAME>" | Format-List
Microsoft emphasizes that highly privileged groups and accounts can
affect the entire forest. The practical lesson is to identify both obvious
privileged groups and less-obvious delegated permissions that lead to
them.
```




# 3. Kerberos and NTLM

Figure 3.1. Kerberos authentication and ticket flow.

Kerberos is the preferred domain authentication protocol. NTLM remains relevant for compatibility and can become a lateral-movement risk when privileged credentials are reused or exposed. A tester should understand the protocol state before selecting tools.

| Artifact | Purpose |
|---|---|
| TGT | Proves a principal has authenticated to the KDC and can request service tickets. |
| TGS | Service ticket for a particular SPN/service. |
| SPN | Maps a service instance to an account. |
| NTLM material | Password-derived authentication material used by NTLM-based flows. |
| PAC | Authorization information carried in Kerberos tickets. |

Kerberos troubleshooting order

1. DNS
2. FQDN / realm spelling
3. Clock synchronization
4. KDC reachability
5. Account status
6. Ticket cache / credential validity
7. Only then change technique/tool

```
Kerberos troubleshooting worksheet
•    Realm/FQDN and DNS resolution verified.
•    Client and KDC time synchronization verified.
•    KDC reachability and account status verified.
•    Ticket cache state recorded before changing tools.
```

# 4. Tier 0 and Privileged Access

Figure 4.1. Tier 0, Tier 1, and Tier 2 privileged-access model.

For AD DS, Microsoft's current tier model separates Tier 0, Tier 1, and Tier 2 administrative identities, workstations, and managed assets. Tier 0 is the identity control plane: compromise of a Tier 0 asset or identity can enable control of the directory. The central rule is to never administer a more trusted tier from a less-trusted host.

| Tier | Typical examples |
|---|---|
| Tier 0 | Domain controllers; Enterprise Admins/Domain Admins/Administrators; AD CS when it can issue or manage authentication for privileged identities; Microsoft Entra Connect Sync infrastructure and other assets that can control AD. |
| Tier 1 | Enterprise application/member servers and the identities/workstations that administer them. |
| Tier 2 | End-user workstations and the identities/workstations that administer them. |