DRGONF1Y

ACTIVE DIRECTORY ATTACK PATHS

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

2026 THIRD EDITION • INSTRUCTOR EDITION

DRGONF1Y

CYBERSECURITY CONSULTING LLC

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

DRG0NF1Y CYBERSECURITY CONSULTING LLC

BOOK PREVIEW

ACTIVE DIRECTORY ATTACK PATHS

2026 Third Edition / Instructor Edition

A practical field manual for assessment, attack-path validation, CRTP preparation, GOAD labs, detection, defense, and reporting.

DISCOVER - ENUMERATE - VALIDATE - BREAK THE PATH

Inside the complete 245-page edition

- Active Directory foundations and attack-path reasoning
- BloodHound, SharpHound, and PowerView verification workflows
- Kerberos, ACL, GPO, delegation, LAPS, AD CS, DCSync, and trusts
- Hybrid Microsoft Entra identity paths and control-plane analysis
- Expanded GOAD labs, annotated commands, and screenshot sourcing
- Detection references, field cards, worksheets, and bibliography

ABOUT THIS SAMPLE

This promotional preview contains selected, nonconsecutive pages.
It excludes complete exercises, appendices, and the separate Instructor Answer Key.
All offensive material is for authorized labs and sanctioned assessments only.

Copyright, Scope and Responsible Use

This book is written for defensive security professionals, penetration testers, red-team students, system administrators, and learners working in intentionally vulnerable laboratories. Commands and procedures must be used only against systems for which you have explicit authorization.

The objective is to teach the security mechanics behind Active Directory attack paths and how to eliminate those paths. Production assessments should follow written rules of engagement, change-control requirements, privacy obligations, evidence-handling requirements, and stop conditions.

Instructor-edition note: student-facing labs remain evidence-driven and authorization-scoped. The detailed solutions, scoring notes, and facilitation guidance are maintained in the separate Instructor Answer Key so the main manual can still be distributed as a study/reference text.

Methodology

The book combines three complementary models: MITRE ATT&CK for behavior classification; BloodHound attack-path reasoning for graphing abusable identity relationships; and Microsoft guidance for least privilege, privileged-access tiering, Windows LAPS, service-account hygiene, PKI, and hybrid identity. Product behavior and attack-path edge semantics change over time, so tool-specific conclusions should be checked against current official documentation.

The core operator loop

```
SCOPE
  ↓
DISCOVER → ENUMERATE → GRAPH → HYPOTHESIZE
                          ↓
                      VALIDATE
                          ↓
                   NEW ACCESS
                          ↓
                 RE-ENUMERATE
                          ↓
            HIGH-VALUE / TIER 0
                          ↓
          EVIDENCE → REPORT → RETEST
```

Contents

How to Use This Field Manual

Use this edition in two modes: sequential study and rapid operator lookup. LEARN explains the security model; FIELD focuses on validation and evidence; LAB turns the concept into GOAD/CRTP-style practice; DEFEND pairs each transition with telemetry and remediation; REPORT language prevents overstatement.

Notation and Visual Legend

Marker	Purpose
LEARN	Concept, protocol, or security model
FIELD	Manual verification, command context, evidence
LAB	Authorized GOAD / CRTP-style exercise
DEFEND	Detection, hardening, remediation
REPORT	Publication-ready finding language
CAUTION	Prerequisite, scope, or overstatement warning

Legal and Authorization Note

All commands and procedures are intended for intentionally vulnerable labs or systems for which you have explicit written authorization. Production assessments should follow rules of engagement, privacy obligations, change control, evidence minimization, and stop conditions.

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.

Attack-path thinking

```
LOW-PRIV USER
   │
   ├─ group membership
   ├─ writable object
   ├─ reusable credential
   ├─ privileged session
   ├─ GPO / delegation / certificate path
   ▼
INTERMEDIATE CONTROL
   ▼
TIER 0 / DIRECTORY CONTROL
```

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.

9. BloodHound Attack-Path Analysis

Lab-build normalization. *The current upstream GOAD configuration places* `jeor.mormont` *and the* `Night Watch` *group in* `north.sevenkingdoms.local`*, while* `joffrey.baratheon` *belongs to the parent* `sevenkingdoms.local` *domain. The upstream topology names* `WINTERFELL` *at* `192.168.56.11`*; it does not define a host named* `KINGSREGARD`*. This edition therefore treats* `192.168.56.12 (KINGSREGARD)` *as the supplied course alias and requires hostname discovery before any command is run. GOAD providers and forks can assign different addresses. Validate the local build instead of forcing a public walkthrough's labels onto it. See the official GOAD configuration and official topology.*

LEARN | Why this matters

BloodHound turns separate Active Directory facts into a graph of relationships. A user, group, computer, domain, organizational unit, Group Policy Object, certificate authority, or cloud identity becomes a node; membership, session, administrative control, delegation, and object-control relationships become edges. The result answers a question that a flat inventory cannot: **what sequence of permissions and trust relationships could connect the access already held to a higher-value objective?**

An attack path is a hypothesis, not proof of compromise. A displayed edge means that the collected directory or host data satisfied BloodHound's rule for that relationship. Exploitability can still depend on network reachability, authentication policy, service state, token refresh, replication delay, endpoint controls, or missing context. Likewise, an analyst-applied **Owned** or **High Value** flag is a triage annotation; it is not evidence that the principal was compromised or that the asset is inherently critical.

For the GOAD exercise, keep the forest boundary visible. `NORTH\jeor.mormont` and `NORTH\Night Watch` are child-domain objects. `SEVENKINGDOMS\joffrey.baratheon` is a parent-domain

object. A cross-domain path can be valid, but the node names, trust direction, and authentication context must be recorded exactly.

FIELD | Discovery and validation workflow

1. **Confirm the target identity before collection.** Query SMB, DNS, and LDAP to map `192.168.56.11` and `192.168.56.12` to their actual hostnames and domains. Record disagreements as lab-build variance.
2. **Time-synchronize the operator host.** Kerberos authentication and some session relationships are unreliable when clocks differ. Record the time source and offset.
3. **Collect directory relationships first.** Use SharpHound's documented default collection set for a baseline. Add session collection only during an approved observation window because sessions are transient and repeated polling creates additional traffic.
4. **Preserve the raw package.** Hash the ZIP before importing it. The package is source evidence; the BloodHound database is a working copy.
5. **Mark only verified starting access as Owned.** Do not mark every known password or every lab account indiscriminately. Record how the access was validated.
6. **Run focused path queries.** Start from the controlled principal, then examine paths to designated high-value nodes, domain controllers, certificate services, or other exercise objectives.
7. **Validate each edge outside the graph.** Use LDAP, native administration tools, or a second collector to confirm ACLs, group scope, sessions, SPNs, delegation attributes, and host reachability.
8. **Rank paths.** Prefer paths with stable edges and a small number of controlled transitions. Treat session-only paths as time-sensitive and destructive changes as higher risk.
9. **Document rollback before testing a control edge.** Record original memberships, owners, security descriptors, SPNs, or GPO links before any approved mutation.

FIELD | Tool and command examples with multi-sentence flag annotations

Run the following only inside the named GOAD range or another environment for which you have written authorization.

```
nxc smb 192.168.56.11 192.168.56.12
dig @192.168.56.11 _ldap._tcp.dc._msdcs.north.sevenkingdoms.local SRV
```

The SMB probe is used here for identity validation, not broad exploitation. Its response should expose the server name, domain label, SMB signing state, and operating-system context. The DNS SRV query asks the known NORTH DNS/DC address which systems advertise the domain-controller LDAP service; use the returned names to correct local name resolution before Kerberos testing.

```
.\SharpHound.exe `
  --Domain north.sevenkingdoms.local `
  --DomainController WINTERFELL.north.sevenkingdoms.local `
  --CollectionMethods Default `
  --OutputDirectory C:\ProgramData\BH
```

`--Domain` limits the directory scope to the NORTH child domain. `--DomainController` pins LDAP queries to the verified controller instead of relying on automatic discovery. `--CollectionMethods Default` uses SharpHound's supported baseline set; consult the installed build's `--help` because available methods evolve. `--OutputDirectory` separates evidence from the operator's working directory and makes hashing and transfer easier. SharpHound CE usage and flags are documented by SpecterOps and in the flag reference.

```
.\SharpHound.exe `
  --Domain north.sevenkingdoms.local `
  --CollectionMethods Session `
  --Loop `
  --LoopDuration 00:15:00 `
  --OutputDirectory C:\ProgramData\BH-session
```

`Session` collects volatile logon relationships rather than repeating the full baseline. `--Loop` intentionally polls during a bounded observation window, while `--LoopDuration 00:15:00` ends collection after fifteen minutes. Repeated session collection is noisier and should be tied

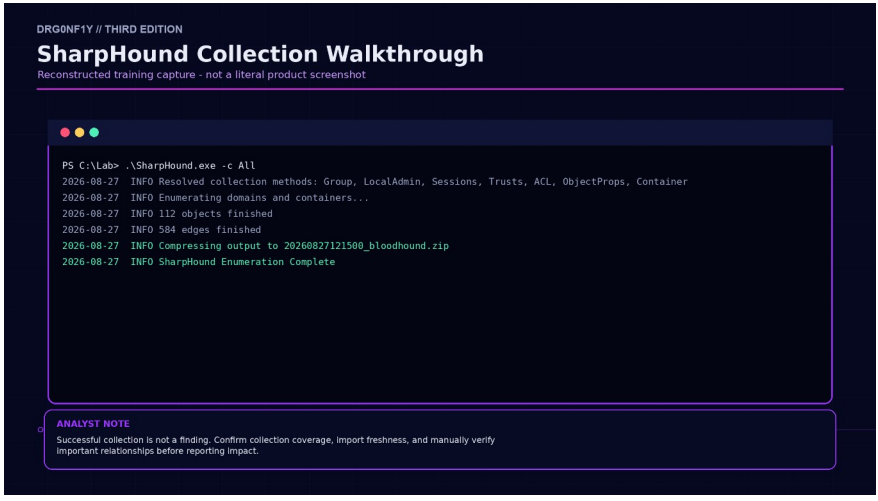


Figure 9.3. SharpHound training illustration - collection workflow and representative console output (reconstructed).

Figure 9.4. PowerView training illustration - recognizing a dangerous WriteDACL ACE (reconstructed output).

22. AD CS / Certificate Services

LEARN | Why this matters

Active Directory Certificate Services (AD CS) issues certificates that can support TLS, code signing, encryption, device identity, smart-card logon, and Kerberos authentication. When an enterprise CA and its templates are integrated with Active Directory, directory permissions and template settings decide who can enroll, what identity can be placed in a certificate, whether approval is required, what purposes the certificate supports, and how long it remains valid.

An AD CS attack path exists when configuration and permissions combine to let a principal obtain or create an authentication certificate for a more privileged identity, modify a template or CA to enable such enrollment, enroll on behalf of another principal, or abuse a vulnerable web-enrollment relay path. The template name alone is not the finding. The analyst must prove the complete condition set: published template, effective enrollment right, authentication-capable EKU or purpose, subject-name behavior, approval/signature settings, CA policy, and a valid mapping path.

Certificates are durable credentials. Resetting the user's password does not necessarily invalidate an already issued certificate. Incident response must consider revocation, CA logs, template repair, account containment, and ticket invalidation. Microsoft's AD CS overview and certificate-template concepts are the design baseline.

Do not assume every GOAD provider deploys the same CA, CA hostname, or vulnerable template. Discover the local build. `WINTERFELL` at `.11` is the NORTH controller in the upstream topology, not automatically the CA. The supplied `.12 (KINGSREGARD)` label must be verified before it is used as a CA or web-enrollment target.

25. Hybrid AD / Microsoft Entra Identity

LEARN | Why this matters

Hybrid identity connects on-premises Active Directory to Microsoft Entra ID so users and applications can share identity data and authentication workflows across both environments. The security boundary is no longer only the forest. Synchronization servers, connector accounts, federation or authentication agents, cloud roles, application service principals, device identities, and attribute mappings can connect an on-premises compromise to cloud access-or a cloud compromise to on-premises administration.

The standard GOAD lab is an on-premises training forest and does **not** natively provide a Microsoft Entra tenant or Microsoft Entra Connect Sync server. This chapter is therefore an extension overlay. Keep GOAD evidence and hybrid-extension evidence separate. Do not claim that `north.sevenkingdoms.local`, WINTERFELL, or the supplied KINGSREGARD alias is synchronized unless live connector scope and cloud attributes prove it.

Common synchronization models include Password Hash Synchronization (PHS), Pass-through Authentication (PTA), and federation. PHS synchronizes a derived representation of the on-premises password hash through Microsoft Entra Connect; the connector requires directory replication permissions that make the Connect server and its accounts high-value assets. Microsoft documents the required PHS permissions and Connect account permissions.

Version currency is a security requirement. Microsoft states that all Connect Sync services will stop working after **September 30, 2026** if they run a version below **2.5.79.0**. Because this manuscript is dated

30. Troubleshooting, Decision Trees and Operator Checklists

Use this chapter to separate environment failure from technique failure. DNS, time, authorization, collection freshness, and lab provisioning explain many apparent tool failures.

30.1 Troubleshooting field guide

Symptom	Verify first	Then verify	Avoid assuming
Kerberos failure	DNS/FQDN/realm	Clock, KDC, ticket cache	Bad password
LDAP failure	DC and 389/636 reachability	Bind identity, TLS, search base	Directory is down
WinRM failure	5985/5986 reachability	Listener/service/ auth/local rights	Credentials are invalid
SMB auth succeeds; admin fails	Authentication	Local Administrators/effec tive rights	Valid = admin
BloodHound path missing	Collection version/methods	Freshness, host/session/ACL coverage	No path exists
PowerView returns nothing	Domain/search base/object identity	Permissions/module version	Object absent
GOAD step fails	VM/DC/DNS state	Provisioning and join order	Technique wrong

FIELD | BloodHound and SharpHound collection gaps

Record collector version, methods, and timestamp. Session, local-admin, ACL, AD CS, delegation, and Entra relationships depend on collection support and reachable data. “No path” can mean no currently collected path. Re-collect after privilege changes or when host visibility improves.

30.2 What do I do next?

Starting condition	Decision path
I have credentials	Validate domain/local context -> enumerate groups, shares, SPNs, ACLs, GPOs, delegation, LAPS/gMSA, AD CS, trusts -> collect graph data -> compare two candidate paths.
I have local admin	Classify host -> sessions/services/tasks/secrets -> higher-tier intersections -> local credential uniqueness -> re-enumerate AD.
BloodHound shows no path	Refresh collection -> inspect outbound control -> inbound high-value control -> trusts/AD CS/delegation/LAPS -> manual ACL review.
GenericWrite	Target class -> exact writable attributes -> security consequence -> minimal proof.
GenericAll	Target class -> target-specific consequence -> ACE/inheritance -> minimal proof.
WriteDACL	Verify ACE -> minimum manufactured right -> before/after ACL -> cleanup.
WriteOwner	Verify ownership -> original owner -> ownership-to-DACL bridge -> cleanup.
SPN found	Account privilege -> password age/encryption -> representative TGS -> offline audit only within ROE.
LAPS exposure	Reset vs query vs read vs decrypt -> managed scope -> encryption state -> minimum validation.
Delegation	Type -> SPNs -> object control -> represented identity/service -> prerequisites.
AD CS exposure	CA/template -> enrollment -> auth purpose -> subject/SAN -> issuance barriers -> ACLs -> endpoint protections -> certificate mapping.
DCSync rights	Required replication-right combination -> expected principal? -> representative proof -> stop bulk extraction.

32. GOAD Field Notes and Screenshots

LEARN | Why this matters

Field notes are the bridge between operator activity and a defensible report. A screenshot without its command, time, target, identity, and interpretation is decoration. A command transcript without a hypothesis or result is difficult to review. This chapter defines an evidence workflow that lets another authorized analyst reproduce the finding, distinguish observed facts from assumptions, and verify that lab changes were removed.

GOAD walkthroughs vary by version, provider, fork, addressing, and author. Public images can help teach interface recognition, but they are secondary illustrations-not evidence from the student's lab. Every harvested image must be checked for the correct domain, object, host, edge direction, command version, and hidden sensitive data. Record the source URL, author, access date, license or permission status, and whether the figure was cropped or annotated. Do not republish a public-blog screenshot merely because Google Images displays it.

Use the course normalization throughout the notebook:

Course label	Required live validation	Identity rule
`192.168.56.11 (WINTERFELL)`	SMB/DNS/LDAP should confirm WINTERFELL and NORTH	Treat as NORTH controller only after validation
`192.168.56.12 (KINGSREGARD)`	Record the actual SMB/AD hostname; KINGSREGARD is a supplied alias	Use the discovered FQDN in Kerberos and LDAP commands
`jeor.mormont`	Resolve in `north.sevenkingdoms.local`	Use `NORTH\jeor.mormont` or the NORTH UPN

Course label	Required live validation	Identity rule
`Night Watch`	Resolve group scope, category, and membership in NORTH	Do not infer ACL control from membership
`joffrey.baratheon`	Resolve in `sevenkingdoms.local`	Use `SEVENKINGDOMS\joffrey.baratheon` or the parent-domain UPN

FIELD | Discovery and validation workflow

1. **Open a case record.** Assign assessment ID, operator, authorization reference, UTC start time, lab snapshot ID, source IP, and tool versions.
2. **Create the target map.** Resolve IP, hostname, FQDN, domain, role, and time source. Preserve both requested aliases and discovered names.
3. **State the hypothesis.** Example: "Jeor's effective NORTH memberships create a path to remote access on WINTERFELL."
4. **Capture the command before the result.** Record exact flags, authentication identity, cwd, and output file. Replace passwords with `<REDACTED>` before publication, not by damaging the raw restricted evidence.
5. **Capture enough screen context.** Include the terminal prompt or application title, target, domain-qualified object, relevant result, timestamp where available, and tool/version context. Crop irrelevant secrets, not explanatory context.
6. **Record an interpretation line.** State what the result proves, what it does not prove, and the next validation step.
7. **Cross-validate material claims.** Use a second source: BloodHound plus LDAP, Certipy plus template DACL, ticket request plus SPN query, or GPO link plus `gpresult`.

33. Guided Lab 1 – Reconnaissance to Domain Map

Objective: build a defensible domain map without relying on a walkthrough. Use only your isolated GOAD network or another explicitly authorized lab.

Step 1 – Establish network context

```
ip addr
ip route
sudo nmap -sn 192.168.56.0/24
```

Step 2 – Identify AD service patterns

```
sudo nmap -Pn -sV -p 53,88,135,139,389,445,464,636,3268,3269,3389,5985,5986
192.168.56.30-31
```

Step 3 – Resolve domain services

```
dig @192.168.56.30 _ldap._tcp.dc._msdcs.<DOMAIN> SRV
dig @192.168.56.30 _kerberos._tcp.<DOMAIN> SRV
```

Step 4 – Build the map

- Record every DC FQDN and IP.
- Record the DNS domain/realm.
- Record SMB signing and remote-management surfaces.
- Do not label a system a DC from one port alone; corroborate multiple AD services.

Exercise 33-A

Explain why 88/tcp + 389/tcp + 445/tcp + 3268/tcp is a stronger DC signal than 445/tcp alone.

45. GOAD Screenshot Walkthroughs

These walkthroughs are designed for live teaching. Figure 45.1 uses the real lab screenshot already present in the manuscript; Figures 45.2-45.6 are reconstructed from lab notes and are intentionally labeled training captures so students learn stable diagnostic patterns rather than a brittle exact UI.

45.1 Confirmed WinRM foothold

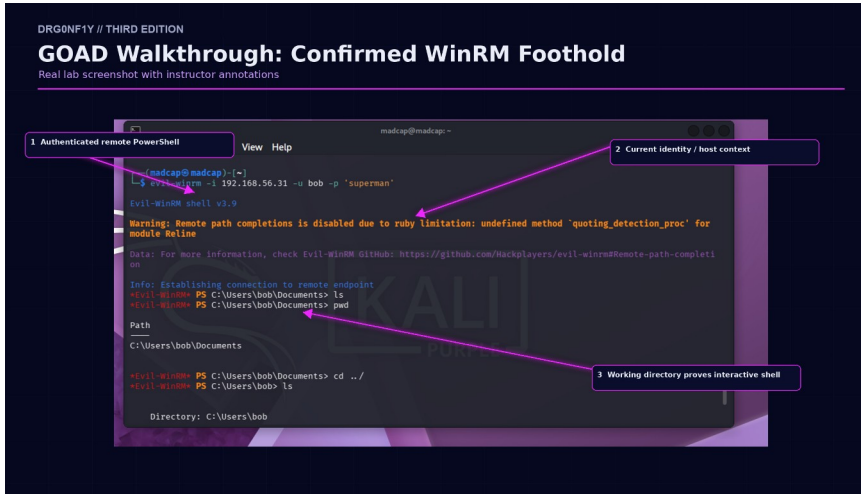


Figure 45.1. Real GOAD WinRM screenshot with instructor annotations.

- What is proven: the target accepted WinRM authentication and an interactive PowerShell session exists.
- What is not proven: local administrator, Domain Admin, or credential material on the host.
- Next: record whoami /all, hostname, local Administrators, sessions, and domain context before deciding on escalation.

46. Detection Event Encyclopedia

This chapter is a field-oriented event reference for attack-path transitions. Event IDs are not detections by themselves. Effective monitoring combines audit policy, SACL coverage where required, object/identity context, baseline behavior, and correlation across multiple events. Microsoft Defender for Identity currently requires a defined set of domain-controller and AD CS events; use current Microsoft guidance when designing production collection.

46.1 Coverage matrix

Attack-path transition	Primary event families	What to correlate
Kerberos authentication / roasting	4768, 4769, 4771	Account, client address, service/SPN, encryption type, request volume, failures.
NTLM / remote validation	4776, 4624/4625, 8004	Source host, logon type, target, protocol, unusual admin origin.
Privileged logon / session exposure	4624, 4648, 4672	Privileged identity on lower-tier host, explicit credential use, logon type.
Group / account control	4728/4729, 4732/4733, 4756/4757, 4738, 4742	Actor, target member/object, before/after privilege.
ACL / directory modification	4662, 4670, 5136	WRITE_DAC/ WRITE_OWNER/write-property, DN, attribute, old/new value, SACL scope.
Remote execution / persistence surface	4688, 4698, 7045	Parent/child process, task/service name, source identity, target host.

Attack-path transition	Primary event families	What to correlate
SMB / share interaction	5140, 5145	Share/path, source address, access requested, admin-share use.
AD CS	4870, 4882, 4885, 4887, 4888, 4890, 4896	CA/template changes, requestor, disposition, privileged certificate issuance.
DCSync / replication	4662 + replication context	Replication GUIDs/rights, non-DC source, domain-root ACL changes.

46.2 Event 4624 - successful logon

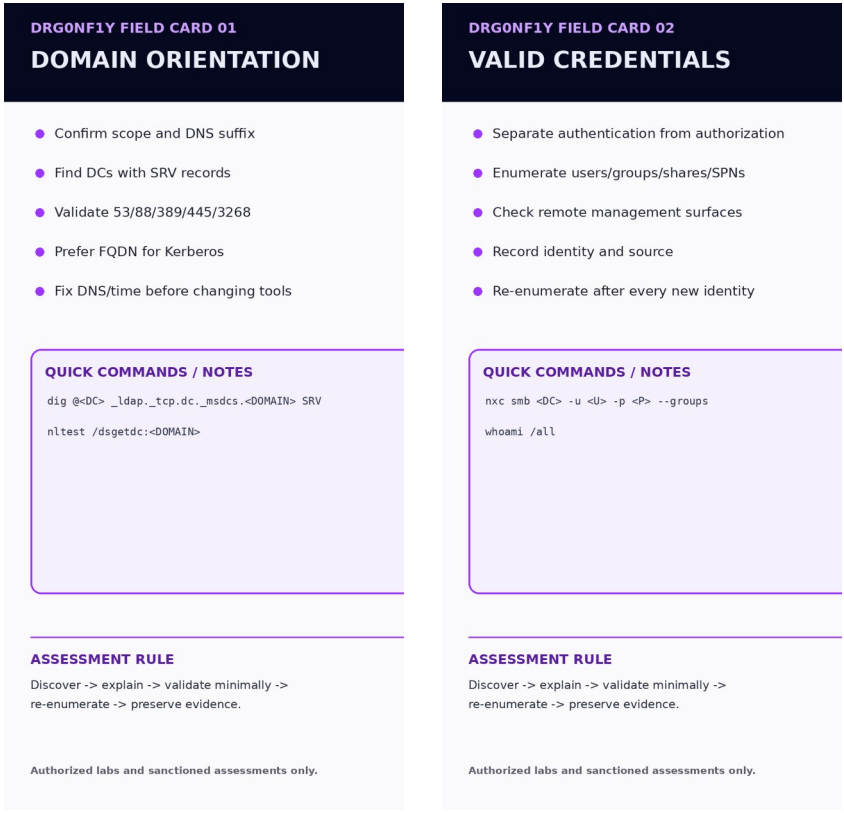
Field	Instructor / analyst guidance
What it records	Records a successful logon on the system that accepted it.
Attack-path relevance	Remote services, privileged-session exposure, cross-tier administrative access.
Useful fields	Account, Logon Type, source address/workstation, authentication package, target host.
High-signal pattern	Privileged identity authenticating to an ordinary workstation or unexpected remote-admin source.
Benign / limitation	Expected admin tooling, service accounts, jump hosts, and management platforms can be noisy.

46.3 Event 4625 - failed logon

Field	Instructor / analyst guidance
What it records	Records a failed logon attempt on the target system.
Attack-path relevance	Password spraying indicators, bad credentials, troubleshooting authentication vs authorization.

47. Printable Operator Field Cards

The ten cards below are designed for two uses: quick-reference pages inside the book and a separate print-ready PDF. They are intentionally concise. A learner should be able to use them without turning them into a command checklist detached from reasoning.



Field cards 01-02 - print-friendly quick reference.

DRG0NF1Y FIELD CARD 03

BLOODHOUND TRIAGE

- Mark Owned only when controlled
- Review outbound object control
- Review inbound control to Tier 0
- Check collection freshness
- Manually verify critical edges

QUICK COMMANDS / NOTES

```
Shortest paths are hypotheses

Evidence beats graph screenshots
```

ASSESSMENT RULE

Discover -> explain -> validate minimally -> re-enumerate -> preserve evidence.

Authorized labs and sanctioned assessments only.

DRG0NF1Y FIELD CARD 04

ACL CONTROL

- Identify source SID + target DN
- Check direct vs inherited ACE
- Resolve object type
- Name the exact writable action
- Capture before state / cleanup

QUICK COMMANDS / NOTES

```
Get-DomainObjectAcl -Identity <T>
-ResolveGUIDs

dsacls "<TARGET_DN>"
```

ASSESSMENT RULE

Discover -> explain -> validate minimally -> re-enumerate -> preserve evidence.

Authorized labs and sanctioned assessments only.

Field cards 03-04 - print-friendly quick reference.

CONTINUE THE PATH

Purchase the complete professional edition

The complete book contains 245 pages of practical Active Directory guidance, 50 chapters, attack-path diagrams, GOAD labs, detection references, field cards, case studies, reporting templates, appendices, and instructor material.

2026 THIRD EDITION / INSTRUCTOR EDITION

Available from DRG0NF1Y Cybersecurity Consulting LLC

Secure checkout and private delivery at drg0nf1y.com.

AUTHORIZED TRAINING AND ASSESSMENT USE