



GHOST
PROTOCOL

AD

THE FIELD LIBRARY

DEEP TRACK

INSIDE THE WALLS

Internal and Active Directory

The internal network, Windows and AD,
enumeration, the attack classes, lateral
movement.



Ghost Protocol (Pvt) Ltd · Colombo · ghosts.lk

Security internship training · The Field Library · Edition 1 · 2026

THE GHOST PROTOCOL FIELD LIBRARY · DEEP TRACK

Internal and Active Directory

The internal network, Windows and AD, enumeration, the attack classes, lateral movement.

Ghost Protocol (Pvt) Ltd · Colombo

The Field Library, Edition 1 · 2026

Copyright 2026 Ghost Protocol (Private) Limited. All rights reserved.

Sold as a PDF for the buyer's own reading. Please do not share or resell the file.

The library

The Field Library is a whole shelf, not one book. The Core Path is the spine everyone reads. The rest is depth and breadth, taken on as the work calls for it. The shelf is complete now, and you are reading the one marked here.

A · THE CORE PATH

O The Oath BUILT

I Groundwork BUILT

II The Web BUILT

III The Wider Field BUILT

IV The Work BUILT

V The Craft BUILT

B · DEEP TRACKS

AI and Agents BUILT

Reading Code BUILT

Internal and Active Directory YOU ARE HERE

The Web, Deeper BUILT

Cloud and Containers BUILT

Mobile and APIs BUILT

Reverse Engineering BUILT

Hardware and the Edges BUILT

C · THE OPERATIONS

Red and Purple Team BUILT

OSINT and Recon BUILT

Report Writing Mastery BUILT

The Consulting Craft BUILT

Bug Bounty BUILT

D · THE OTHER SIDE

Detection and Response BUILT

Threat Hunting and Forensics BUILT

Hardening and Architecture BUILT

E · THE GROUND RULES

The Law, Deeper BUILT

Standards and Compliance BUILT

Ethics and Disclosure BUILT

F · COMPANIONS

The Reference Pack BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

- Opening 5
- 1** The Internal Network 6
- 2** Windows and Active Directory 11
- 3** Enumeration 17
- 4** The AD Attack Classes 21
- 5** Lateral Movement and Privilege Escalation 28
- Worked answers 34

Already inside



This scope had no login page and no front door to knock on. The client handed you a laptop already plugged into their office network and a single low-privileged account, and asked the only question that matters on an internal test: if someone got this far, how far could they get.

BLINK "We start inside? That feels like it should be against a rule."

SOL "It is the rule. A real attacker gets a foothold from a phish or a stray laptop, and the useful question is never how they got in, it is what the inside lets them reach. So the client puts you inside on purpose, under paper, and you show them the path from one tired account to the keys to the whole place."

One green eye opened. Wyrms remembers internal tests that went too loud and took a payroll server down at the worst hour.

WYRM "quiet. it is live."

This book is the internal network and the directory that runs it: how it proves who you are, and how that proof is turned against it, carefully, on a network full of real people's work.

CHAPTER ONE

The Internal Network

An internal test does not start at the front door. It starts inside, with a foothold someone handed you, and asks a different question: once an attacker is in, how far do they get? This chapter sets the frame and draws the scope line for a surface where one tool can touch a whole company.

Volume III looked at a network from outside and named the internal vantage point in a paragraph: a visitor on the office LAN, a compromised laptop, a position that assumes a foothold and asks how far it reaches. This book is that paragraph taken to depth. Internal testing, and the Windows networks almost every organisation runs it on, is a surface of its own, with its own protocols, its own attack classes, and a scope line that is harder to hold than any you have met so far.

The web methodology in Volume II is still under you, and the discipline from Volume I still rules: understand the mechanism before you touch it, verify every finding against evidence you can show. What changes is the shape of the engagement and the size of what a single command can reach.

Not a bigger web test

A web test lives inside one application, over HTTP, depth first. You edit a request, you watch one response, and the blast radius of a mistake is usually one site. An internal test lives on a corporate network full of Windows machines that trust each other through a central authority, and it works breadth first: many hosts, many protocols, a web of accounts and permissions that was built over years by people who have mostly left. The question is no longer "how is this one application built." It is "given a starting position inside, what can a determined attacker reach, and how fast."

That difference is not a matter of scale. It is a matter of kind. The valuable findings on an internal test are rarely a single broken input. They are paths: this ordinary user can reset that service account's password, that service account is an administrator on this server, that server has a domain administrator logged in. None of the links is exotic. Chained, they walk a standard employee account to control of the whole network in an afternoon. Learning to see those chains, and to prove them without wrecking anything, is the work of this book.

The assumed-breach Frame

Most internal engagements start from **assumed breach**: the client gives you a starting position rather than making you earn it from the perimeter. You are handed a standard domain user account, or a network port in a meeting room, or a build of a corporate laptop, and the test begins from there. It can feel like cheating. It is the opposite.

The reasoning is honest risk thinking. Perimeters are breached: a phished password, a vulnerable VPN appliance, a contractor's infected machine, a planted USB. Spending a two-week engagement trying to get that first foothold tells the client one thing (whether the perimeter held this fortnight) and leaves the far more expensive question untouched: when someone does get in, and eventually

someone does, is it one laptop lost or the entire company. Assumed breach puts the budget where the real damage is. It asks what the inside is worth to an attacker who already has a toe in it, which is the question that actually keeps a business owner awake.

A test can be scoped at different levels of assumption, and the level is written down before you start: no credentials (you plug in and start from the network alone), a standard user account, or a specific low-privilege host. Each answers a slightly different "what if." None of them is a licence to roam. The assumption is the start of the story, not the end of the scope.

What a Foothold is

A **foothold** is your initial position of access on the internal network: the thing you have been given, or the first thing you take, from which everything else is reached. On an assumed-breach test it is the account or host the client provided. On a test that begins at the network, it is the first credential or session you obtain, often from traffic the network hands you without being asked (Chapter Four). The foothold is almost never the goal. It is the floor you stand on to reach the next rung, and the discipline is to know exactly which rung you are allowed to reach for.

Keep the foothold honest in your notes. Record how you got it, when, and what it can do, because the client's whole interest is the distance between that floor and the ceiling you reach. A report that says "from a standard HR user account, in six hours, we reached Domain Admin, here are the eleven steps" is worth more than any list of missing patches, because it is the attack the client is actually buying protection against.

Scoping an internal test

Scope on an internal test is not one line of URLs. It is a short contract about a whole environment, and because the tools reach so far, the out-of-scope list matters as much as the in-scope one. The law and the stop-and-report triggers are Volume O; the paperwork itself is Volume IV. Here is the shape of what that paper settles before the first command.

WHAT THE SCOPE PINS DOWN	WHY IT HAS TO BE EXPLICIT
The starting position (no creds, a named user, a named host) and how it is provided	It defines what "the test" even is, and stops a disagreement later about whether you were handed too much or too little
In-scope domains, subnets, and hosts, named	A corporate network shares cable and address space with things that are not the client's to authorise
Explicitly out of scope: named production systems, other tenants, anything you must not touch	Flat networks put the medical-records box one hop from your test user; "I could reach it" is not "I was allowed to"
Password spraying and lockout: whether it is permitted, and the account-lockout threshold	Guessing passwords can lock out real staff and halt a business. You must know the policy before you spray, or you do not spray
Destructive and high-risk actions: DoS, actions against domain controllers, mass changes	The DC is the heart of the network. A mistake there is an outage, not a finding

WHAT THE SCOPE PINS DOWN	WHY IT HAS TO BE EXPLICIT
Data handling, the test window, and the stop-and-report contacts	Internal networks hold real personal data under the PDPA; see Volume O for when you stop and who you call

**SOL SAYS**

On an internal test the client often says "test the whole network, go wild." Do not take that as the scope. Take it as the opening of a conversation that ends with named subnets and a written list of what you will not touch. "Go wild" is how a junior justifies the scan that hit the hospital's billing server sharing the building's address block. The words that protect you are the enumerated ones, and you get them in writing before you plug in.

Staying in scope on a flat network

A **flat network** is one with little or no internal segmentation: once you are on it, you can reach almost everything on it. Many real networks are flat, and finding that out is often a finding in its own right, because it means one phished laptop can touch the domain controller, the finance share, and the backup server alike. For the attacker it is a gift. For you it is a hazard, because the same flatness that makes the attack easy makes it trivially easy to step on something you were never authorised to touch.

The tools make this worse, exactly as Volume III warned about scanners. A port sweep pointed carelessly covers a whole range. Worse, some internal techniques are not aimed at a target at all: a tool like Responder sits on the wire and answers broadcast name-resolution requests for the entire segment, so it collects credentials from any machine on the subnet that happens to ask, including ones outside your scope. A tool that passively poisons a broadcast domain does not read your Rules of Engagement. You hold the line, by choosing what you run and where you point it, not by trusting the tool to stay inside.

■ THE LINE

Everything in this book is for your own lab or for a network you hold a written Test Authorisation for, naming the exact in-scope hosts and subnets. On an internal engagement two cautions are specific to the surface. First, a broadcast-level tool (name-resolution poisoning, relay listeners) can capture credentials from machines you were never authorised to touch, because it answers the whole segment: treat running one as touching every host that answers, and confirm the segment is yours. Second, password spraying can lock real people out of real accounts: you do not spray until the ROE permits it and you know the lockout threshold. Scanning, poisoning, or spraying a host you were not given is unauthorised access, an offence under the Computer Crime Act No. 24 of 2007 (Volume O). Confirm the targets against the written scope, point the tool at exactly those, and record what you ran and when.



whose subnet?

The listener you are about to start will answer every broadcast on the wire, and the wire runs past three tenants who never signed anything. "It only listens" is not a defence when it listens to everyone. Confirm the segment is in scope before you bind to it, not after the capture names a stranger.

■ EXERCISE

Build a small Active Directory lab you own and can break safely: one Windows Server as a domain controller and one domain-joined Windows client, as virtual machines on a host-only network that can reach nothing but each other and your Kali box. (Microsoft's evaluation ISOs are free for this, and GOAD, the open "Game of Active Directory" lab, automates a richer version.) Create a standard, non-administrative domain user and log in as that user: this is your assumed-breach foothold. Write down, in two lists, what that ordinary account can already see about the domain, and what it cannot. You are not attacking anything yet. You are learning to stand on a foothold and look around before you move, which is the whole posture of an internal test.

■ VERIFY IT

"The network is flat" is a claim, and like every claim in this work it needs evidence you can show, not an impression. Prove it with reachability you captured: from your in-scope foothold, show that it can open a connection to hosts on different parts of the network that a segmented design would have separated (a connection to the DC, to a server share, to a database port), each a recorded request and response. "It felt flat" is not a finding. "This test user reached these three systems across what should be three zones, here are the connections" is.

■ ON YOUR FEET

You are hired for an internal, assumed-breach test with a standard domain account. On day one you confirm the network is flat: your test user can reach the domain controller, the finance file server, and a host holding medical records, none of them segmented. The ROE names "the internal corporate domain" as scope. You notice the client's offices share a building, and the address range your scanner would sweep also contains hosts belonging to a separate company upstairs on the same block. What do you confirm, and with whom, before you run a single scan, and what do you make sure your tools never point at?



WHAT WYRM KEEPS

An internal test starts from a foothold and measures the distance to the ceiling. The best findings are paths, not patches. The scope line is hardest here, because one tool can touch a whole company.

- Assumed breach is honest risk thinking: perimeters fail, so the paid question is what the inside is worth to an attacker already holding a toe in it.
- A foothold is your initial access, recorded with how and when you got it; the value is the distance from it to the crown.
- Internal scope pins the starting position, the named in-scope hosts, the explicit out-of-scope systems and tenants, the spraying and lockout rules, and the stop-and-report path.
- On a flat network one hop reaches everything, which is both the finding and the danger. Broadcast tools answer the whole segment, and spraying can lock out real staff: hold the line by what you run and where you point it.