Red Wizard

User friendly, automated RT infrastructure

https://github.com/SecuraBV/RedWizard
Goal for today:
Publish the Red Wizard tool
and show you its capabilities
Agenda

• (Short) Intro to Red Teaming
• Red Teaming and infrastructure
• Red Wizard: Introduction
• Red Wizard: Basic Building Blocks
• Red Wizard: Demo Time
• Closing thoughts
Welcome! Who am I?

Ben Brücker
Domain Manager: Red Teaming
@Secura since 2014

Trained Penetration Tester / Social Engineer / Trainer
OSCP, GXPN, GMOB, MLSE
(Short) Intro to Red Teaming
A realistic cyber attack simulation to test the detection, response and mitigation capabilities of the defenders.
Full-Spectrum Operations

Physical Access  Social Engineering  Rogue Devices  (Remote) Network Compromise

Causing (simulated) high impact events
Red Teaming is unforgiving.
Red Teaming and infrastructure
Red vs. Blue
Command & Control Server -> Target
Command & Control Server

Target

Blue Team
Command & Control Server → Relay Server → Target
You have to do this a lot
Introducing: Red Wizard
What is Red Wizard?
Why did we make it?

• Deploying stuff manually is painful
• Must be easily explainable to new team members
• Infrastructure deployer is not always the operator
• Information sharing on how to use an infra costs time
• Spending less time on infra deployment results in more time for our customers
Is it unique? Is it rocket science?
Red Wizard Design Principles

• Simplicity trumps fanciness
• Operational Security (OPSEC)
• Must be robust
• No magical Black Boxes
• Everything must be self-documenting
• Easily extendable
• Preconfigured listeners / phishing profiles
• Log everything

Maturity of the tool?
Technology behind Red Wizard?
• Create a base configuration for all your deployments

• Create a configuration for a new RT campaign

• Create an inventory of systems

• Deploy your infrastructure
Deployment Requirements

• Ubuntu 22.04 on the deployment system
  • (Your laptop or a VM is fine)
• Clean Ubuntu 20.04 on all target machines
  • (Will support 22.04 in the near future)
• 1 deployment user
  • (Configured for key-based SSH access on all machines)
• Deployment user has identical sudo password on all machines
Red Wizard
Basic Building Blocks
C2

Infra Component (Docker)
C2

Infra Component (Docker)

OpenVPN

Relay
C2

Infra Component (Docker)

OpenVPN

Relay

Target

The rest of the internet
Red Wizard
Demo Time
Red Wizard
Closing thoughts
Where to get it?

https://github.com/SecuraBV/RedWizard
Will there be bugs?
Publicly released components

- GoPhish
- Manual Phish
- CobaltStrike
- OSINT
- Web Catcher
- Dropbox (Hardware implant)
What did we not release? What do you have to do yourself?

• Secura’s Red Teaming secret sauce
  • OPSEC patches to GoPhish / Cobaltstrike etc
  • Malleable Profiles
• Other components for proprietary software
• Not all hardenings for our environments
• Relay website-generators
• Server deployment
Future public releases?

- RedElk integration (Red Team SIEM by Outflank)
- MitM Phishing (EvilGinx / Modlishka)
- Support for non-standard relays (domain fronting etc)
- Hardware implants?
Thank you!

https://github.com/SecuraBV/RedWizard

Ben Brücker
ben.brucker@secura.com