
BLUE TEAM PRIMER:
DETECTING A HACKER
Derek Carlin

Table of Contents

About the Book:

Most modern-day businesses are required to have a Penetration Tester or Security Auditor review their systems annually for flaws and holes in their security. The professional tester will generally come onsite and spend on average two to three days on premise for the engagement before departing to write up their report, which will then be handed to IT Security to start remediation efforts.

This book looks at how to maximize the two to three-day window that the Penetration Tester is onsite, focusing not on how the tester finds the flaws, but instead on how the defensive security team can track the tester as they move through the network. The final goal being able to apply these tactical lessons learned to improving continuous monitoring and alerting for adverse behavior.

About the Author:

Derek Carlin is an accomplished Information Security Professional with extensive experience in red team and blue team engagements. With a focus on client satisfaction, he has honed his skills in a variety of industries, including finance, defense, healthcare, and technology.

On the red team side, Derek has led teams of testers with diverse backgrounds and geographical locations, performing a wide range of security testing activities such as penetration testing, vulnerability assessments, password cracking, cloud configuration assessments, and web application assessments. He has also worked in both classified and unclassified environments.

On the blue team side, Derek has worked extensively in this space, with a background running a security operations center for a global company and working as a cloud security architect, and director of cloud security and operations. He has experience designing, implementing, and protecting cloud networks that meet StateRAMP and FedRAMP Moderate standards, and on-premise classified environments that meet the MMM levels of confidentiality, integrity, and availability. Derek has also held roles as a consultant incident responder specializing in cloud environments.

Derek currently holds the following certifications, as well as a Master's Degree in Cybersecurity and Information Assurance:

- Certified Information System Security Professional (CISSP)
- GIAC Certified Intrusion analyst (GCIA)
- GIAC Certified Enterprise Defender (GCED)
- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- CompTIA Security+
- CompTIA Network+
- AWS Certified Cloud Practitioner
- AWS Certified Solutions Architect (Associate)
- AWS Specialty: Security
- Azure Certified Security Engineer

- Azure Solutions Architect: Expert.

Derek's LinkedIn: https://www.linkedin.com/in/derek-carlin-m-s-b674b767/

Derek's Blog: https://shadowknightsecurity.com/

What this book isn't:

This book is not intended to be an all-inclusive record of how to detect every possible technique that a tester could, or will, throw at your environment. Instead it is written to reflect the most common real-world techniques on a general scope. This book is also not geared specifically towards detecting Advanced Persistent Threats or towards telling you exactly how-to setup your SIEM environment.

Why I wrote this book:

I wanted to write this as a general detection and countermeasure methodology using free or open source tools that can be taken, revised, and implemented in environments that have employed proprietary tools (Carbon Black, Cylance, Qradar, Splunk, etc.). Note that not all techniques can currently be detected by FOSS tools and some commercial tools will be recommended. My goal is to have others use this as a foundation to build up their environments and leverage these fundamentals to raise awareness on basic red team tactics from a blue team perspective. Please note that the techniques discussed here are shown inside of a lab environment, and as such will vary from what you will observe on your company networks or in the field. Additionally, I wrote this in a book format instead of multiple blog posts because it seemed the logical course of action.

Introduction:

The Penetration Testers that I've had the pleasure of working with in the past have always been extremely knowledgeable and eager to share their wealth expertise with their clients. It seems however, that most of their clients have solely been focused on meeting compliance requirements instead of looking to maximize their return on investment by hiring these individuals. Leading to hours of skilled labor yielding only one product; the report. The most overlooked opportunity that these professionals can provide is the opportunity to *train your security team*.

If you are able to hire a professional to come in and test your infrastructure and you are *not* capitalizing on the chance to *train* your team, *test your monitoring*, and *improve your detection capabilities*, you are doing yourself a disservice. This book encompasses all of Derek's lessons learned *so far* from a Red vs. Blue perspective and is written as the companion guide to Paul Seekamp's "Internal Security Assessment: Field Guide"; with his permission of course. The book follows the stages of penetration testing and examines popular attack types and situations from a defenders perspective.

RECONNAISSANCE

Reconnaissance

The "Recon" phase, short for reconnaissance, is the first phase in a typical penetration testing cycle. This phase involves gathering as much information as possible about the target system, network, or organization that is being tested. The goal of the Recon phase is to identify all of the hosts in the network and get a lay of the land.

Note: Asset discovery / reconnaissance can also be scoped against public facing assets in a similar manner (DMZ, Cloud, SaaS, etc.); or with specific tools such as Shodan or Censys. For now, we are going to focus our efforts towards operating on a LAN / WAN environment.

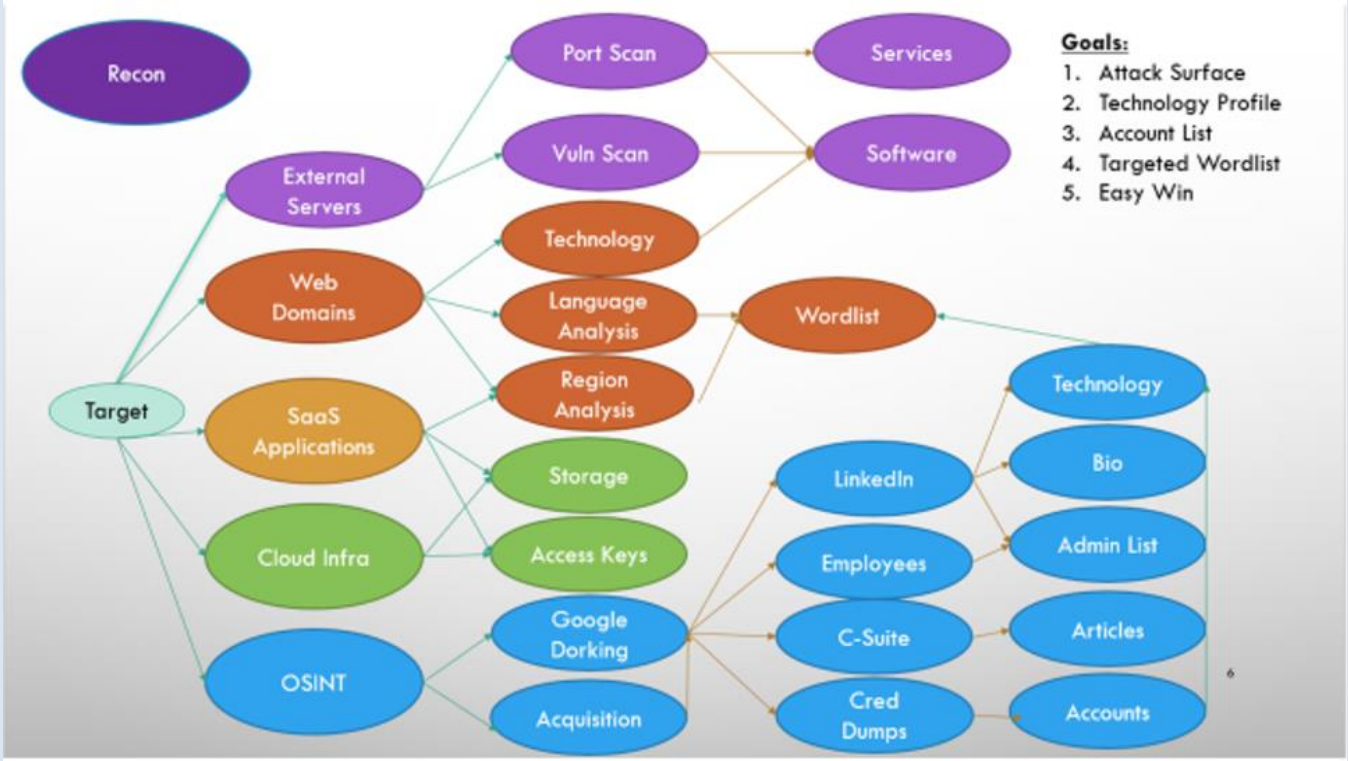


Figure 1.0: Sample External Recon/OSINT Flow.

TCP SYN (Stealth) Scans:

The Threat:

- Utilizing the TCP three-way handshake, common scanners such as Nmap and Masscan are deployed to attempt to get "live hosts" to respond to a simple synchronization request; SYN, SYN/ACK, ACK. Where the host (Penetration Tester's machine) sends a SYN packet to the recipient (target host), which will respond with a SYN/ACK, at which point the host machine will break the connection with a RST (reset) packet. Preventing a full connection from ever being established with the target. The goal here is to get the target hosts to reply with the SYN/ACK response, indicating that there is a live host. The purpose of a SYN scan is to determine what hosts are on the network.

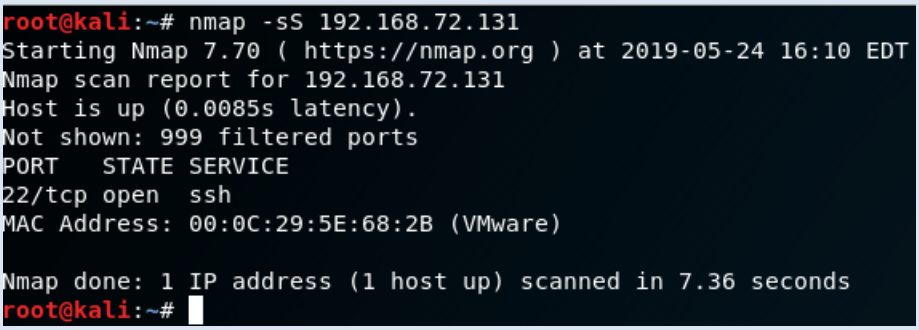
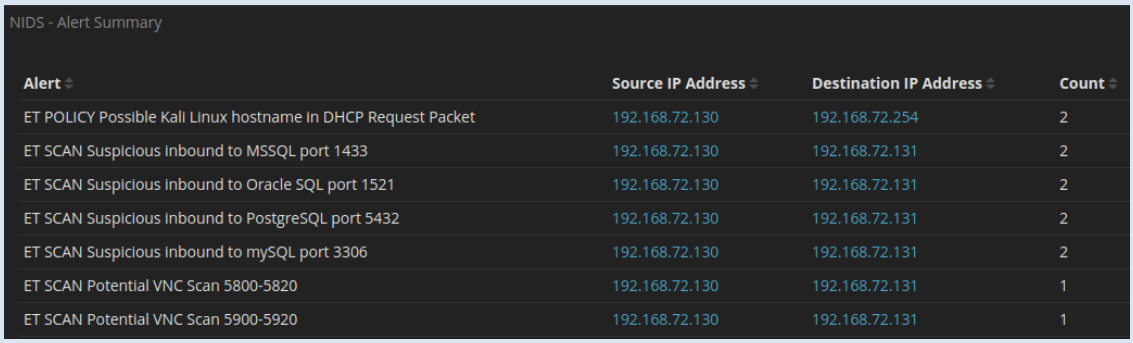


Figure 1.1-A: Nmap TCP/SYN Scan.

The Detection:

- Detection of a SYN scan is relatively simple, as most often these scans will be coupled with quick port scans by default (as with Nmap). It's simple if your enterprise is utilizing any sort of Intrusion Detection system that is; such as Security Onion, which is the open source tool that couples together the ELK stack, Snort (or Surricata) and Bro. Bonus points for detection if the tester is using the default "Kali" Linux hostname like I am in my lab environment. You're looking for the SYN, SYN/ACK, RST combination from one host to one, or many, destination addresses, potentially coupled with multiple of these packet combinations to many ports for each host.



NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	192.168.72.130	192.168.72.254	2
ET SCAN Suspicious Inbound to MSSQL port 1433	192.168.72.130	192.168.72.131	2
ET SCAN Suspicious Inbound to Oracle SQL port 1521	192.168.72.130	192.168.72.131	2
ET SCAN Suspicious Inbound to PostgreSQL port 5432	192.168.72.130	192.168.72.131	2
ET SCAN Suspicious Inbound to mySQL port 3306	192.168.72.130	192.168.72.131	2
ET SCAN Potential VNC Scan 5800-5820	192.168.72.130	192.168.72.131	1
ET SCAN Potential VNC Scan 5900-5920	192.168.72.130	192.168.72.131	1

Figure 1.1-B: Security Onion Port Scan Detection.

The Countermeasure:

- Host-based firewalls can be configured on endpoints to block incoming connections except for certain machines used by administrators; however, this approach is uncommon as it can create more problems than it solves. The recommended countermeasure is detection capability, followed by investigation of why the offending host system is conducting scans. Detection can be conducted by correlating logs from endpoint machines firewall logs, host-based IDS logs, or network-based IDS logs.

Ping Sweeps:

The Threat:

- A ping sweep scan is a network scanning technique used to identify live hosts within a target network. This technique is based on the use of the Internet Control Message Protocol (ICMP) echo request and reply messages, commonly known as "pings". During a ping sweep scan, the scanning tool sends ICMP echo requests to a range of IP addresses in the target network. If a host in the network is alive and responds to the ping, the scanning tool will receive an ICMP echo reply message. The tool can then use this information to identify the live hosts within the network.

```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 23:10 EDT
```

Figure 1.2-A: Nmap Ping Sweep.

The Detection:

- It's tricky / low value to run detection on ping sweeps due to the sheer number of false positives that will be received from network management software that natively utilizes ping. However, in a perfect world of you whitelist all your networking software and write rules to detect sweeps over entire subnets instead of alerting on host to host connectivity the false positives will lower to a manageable rate. Still, running detection here is of low value, but it is important to understand the fundamentals when triaging network traffic of interest; as this could be the starting point of the puzzle.

Destination	Protocol	Length	Info
Broadcast	ARP	42	Who has 192.168.72.131? Tell 192.168.72.130
Vmware_2d:c3:af	ARP	60	192.168.72.131 is at 00:0c:29:5e:68:2b
192.168.72.131	ICMP	98	Echo (ping) request id=0x094b, seq=1/256, ttl=64
192.168.72.130	ICMP	98	Echo (ping) reply id=0x094b, seq=1/256, ttl=64

Figure 1.2-B: Wireshark Ping Sweep Detection.

The Countermeasure:

- Routers and host-based firewalls can be configured to drop ping requests from traffic excluding whitelisted IP addresses belonging to network equipment. Though this is rarely done in practice. The recommended countermeasure is detection capability, followed by investigation of why the offending host system is conducting ping sweeps.

ARP Scans:

The Threat:

- An ARP scan is a third way to discover assets on the local network and is often conducted in conjunction with ping sweeps. The Address Resolution Protocol (ARP) maps physical MAC addresses to IP addresses. ARP sends out broadcast packets to all hosts on the subnet asking, "who has 192.168.6.x?" and, theoretically, the host who has the address will reply. I say theoretically because ARP spoofing is a technique attackers use to impersonate other hosts to intercept traffic.

```
Currently scanning: 192.168.171.0/16   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 480

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.72.131  00:0c:29:5e:68:2b      3     180  VMware, Inc.
192.168.72.2    00:50:56:e0:95:80      3     180  VMware, Inc.
192.168.72.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.72.254  00:50:56:e1:4d:30      1      60  VMware, Inc.
```

Figure 1.3-A: netdiscover ARP Scan.

The Detection:

- This activity can be detected using Wireshark, Security Onion, or other similar network monitoring tools. The activity can be observed by looking for hosts that sequentially broadcast packets looking for sequential IP addresses in the local range.

Source	Destination	Protocol	Length	Info
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.180? Tell 192.168.6.
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.181? Tell 192.168.6.
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.182? Tell 192.168.6.
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.183? Tell 192.168.6.
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.184? Tell 192.168.6.
Vmware_2d:c3:af	Broadcast	ARP	42	Who has 192.168.6.185? Tell 192.168.6.

Figure 1.3-B: Wireshark ARP Scan Detection.

The Countermeasure:

- The recommended countermeasure is detection capability, followed by investigation of why the offending host system is conducting ARP Scans.
- **Note:** ARP scans are often followed by an attacker impersonating the MAC address of another host, possibly for a Mand in The Middle (MiTM) attack.