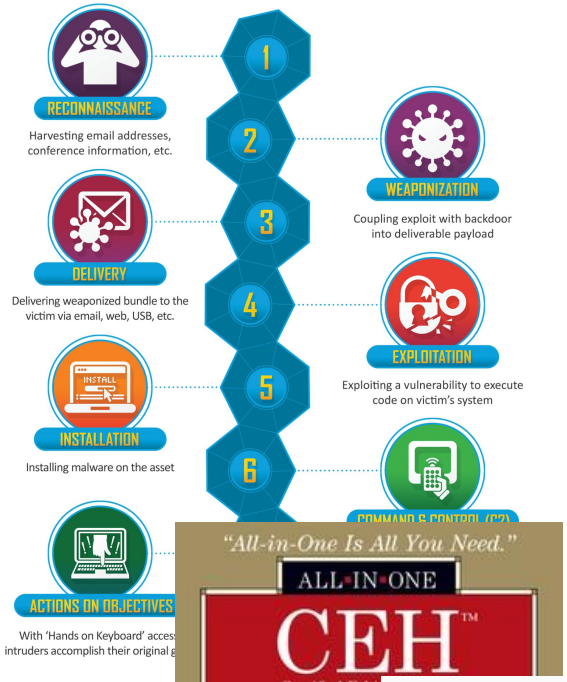
SoK: A Framework for Asset Discovery

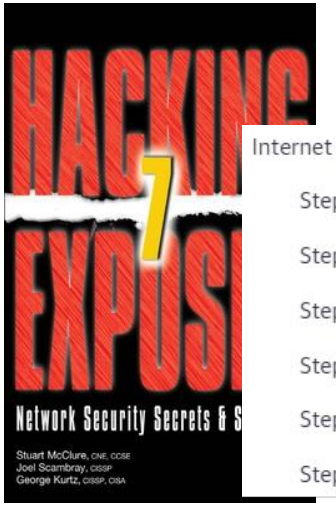
Systematizing Advances in Network Measurements for Protecting Organizations

Mathew Vermeer, Jonathan West, Alejandro Cuevas, Shuonan Niu, Nicolas Christin, Michel van Eeten, Tobias Fiebig, Carlos Gañán, Tyler Moore

2021 IEEE European Symposium on Security and Privacy

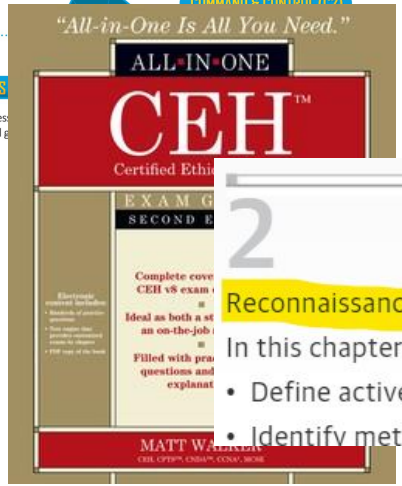
TU Delft Delft University of Technology





Internet Footprinting

- Step 1: Determine the Scope of Your Activities
- Step 2: Get Proper Authorization
- Step 3: Publicly Available Information
- Step 4: WHOIS & DNS Enumeration
- Step 5: DNS Interrogation
- Step 6: Network Reconnaissance



CHAPTER 2

Reconnaissance: Information Gathering for the Ethical Hacker

In this chapter you will

- Define active and passive footprinting
- Identify methods and procedures in information gathering

MITRE | ATT&CK®

TACTICS

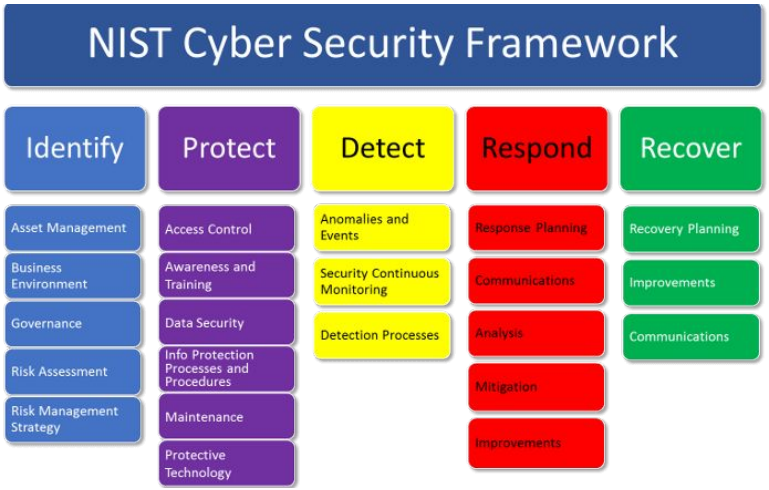
Enterprise

Reconnaissance

Resource Development

Asset management

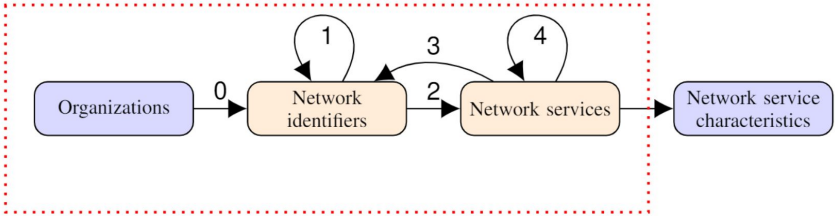
- The bedrock of good security posture
- NIST Cybersecurity framework; ISO/IEC 27001



https://www.givainc.com/blog/index.cfm/2019/7/24/5-key-changes-made-to-the-nist-cybersecurity-framework-v11

Asset discovery

- Assets
  - All network identifiers (e.g., addresses, FQDNs, DNS zone contents)
  - The network services reachable via these network identifiers
- Discovery
  - When the existence of an asset associated with a specific organization becomes known
- Focus on assets discoverable through external network measurements



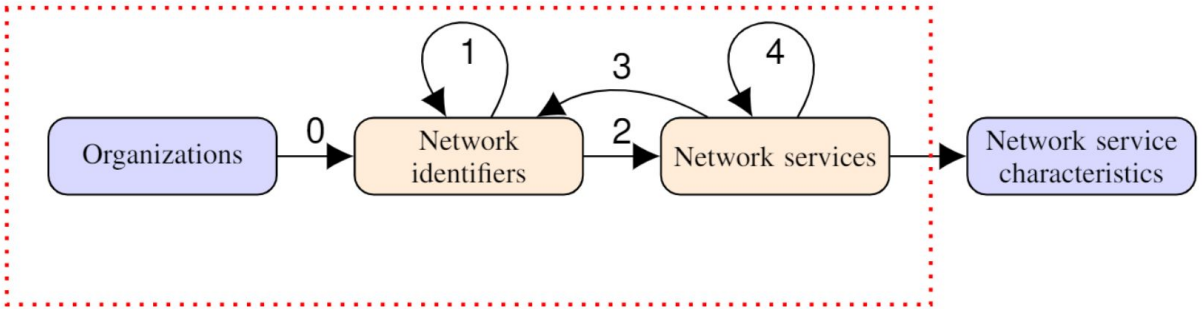
Systematization

- Techniques are scattered throughout the literature
  - Not explicitly advertised as asset discovery

- Selected 93 papers out of 4,100+
  - 14 major security & networking venues
  - Timespan of 5 years (2014-2019)

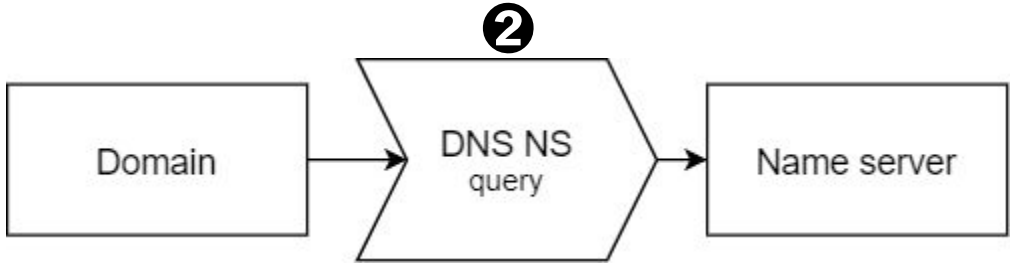
- Extracted asset discovery techniques
  - *Input asset → discovery method → output asset*

Systematization



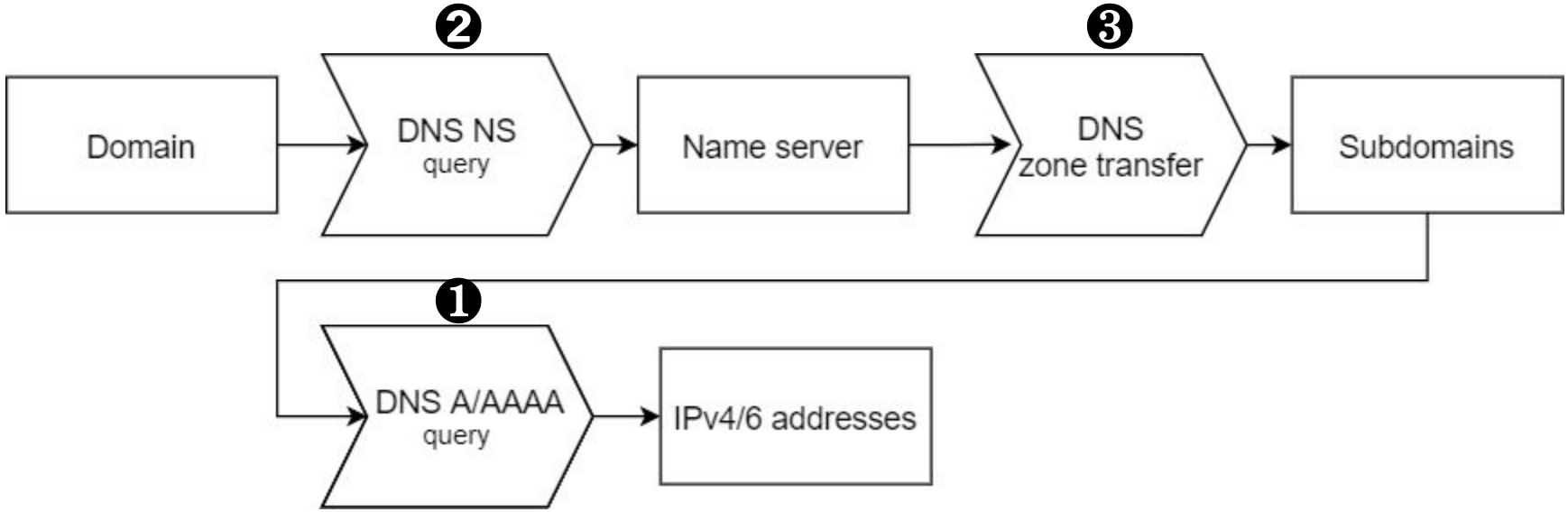
Citation	Edge	Input asset	Discovery technique	Output asset
[34, 117]	1	Domain	A/AAAA records from passive DNS	IPv4/IPv6 addresses
[34]	1	Domain	CNAME record from passive DNS	Domain
[84]	2	IP address	ZMap scan; analyze sigs. in fetched banners	Honeypot
[16]	2	IP address	Search IP in botnet population	*Bot services*
[29]	2	IP/Dom./URLs	Scans of S3 buckets	S3 buckets
[55]	3	Name server	Query open resolver for `v6only` zone	IPv6 address
[87]	4	Name server	Authoritative name server discovery technique	Name server
[31]	4	Name server	DNS query for hostnames under own domain	Name server

Asset discovery chain

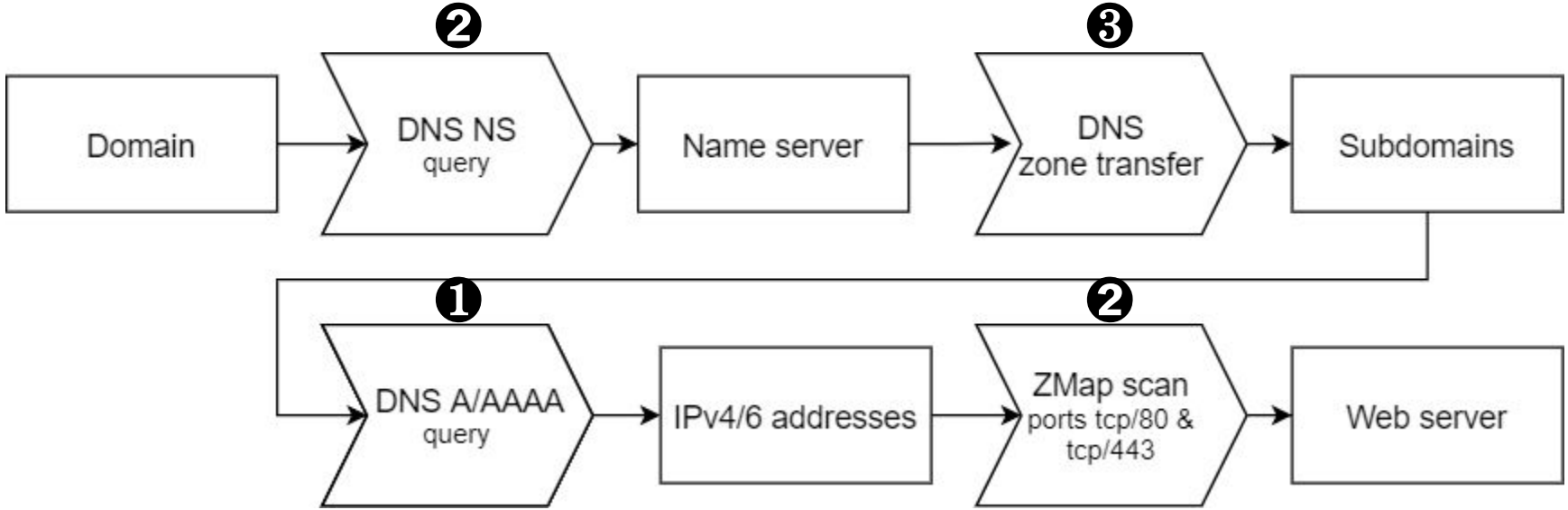


Asset discovery chain

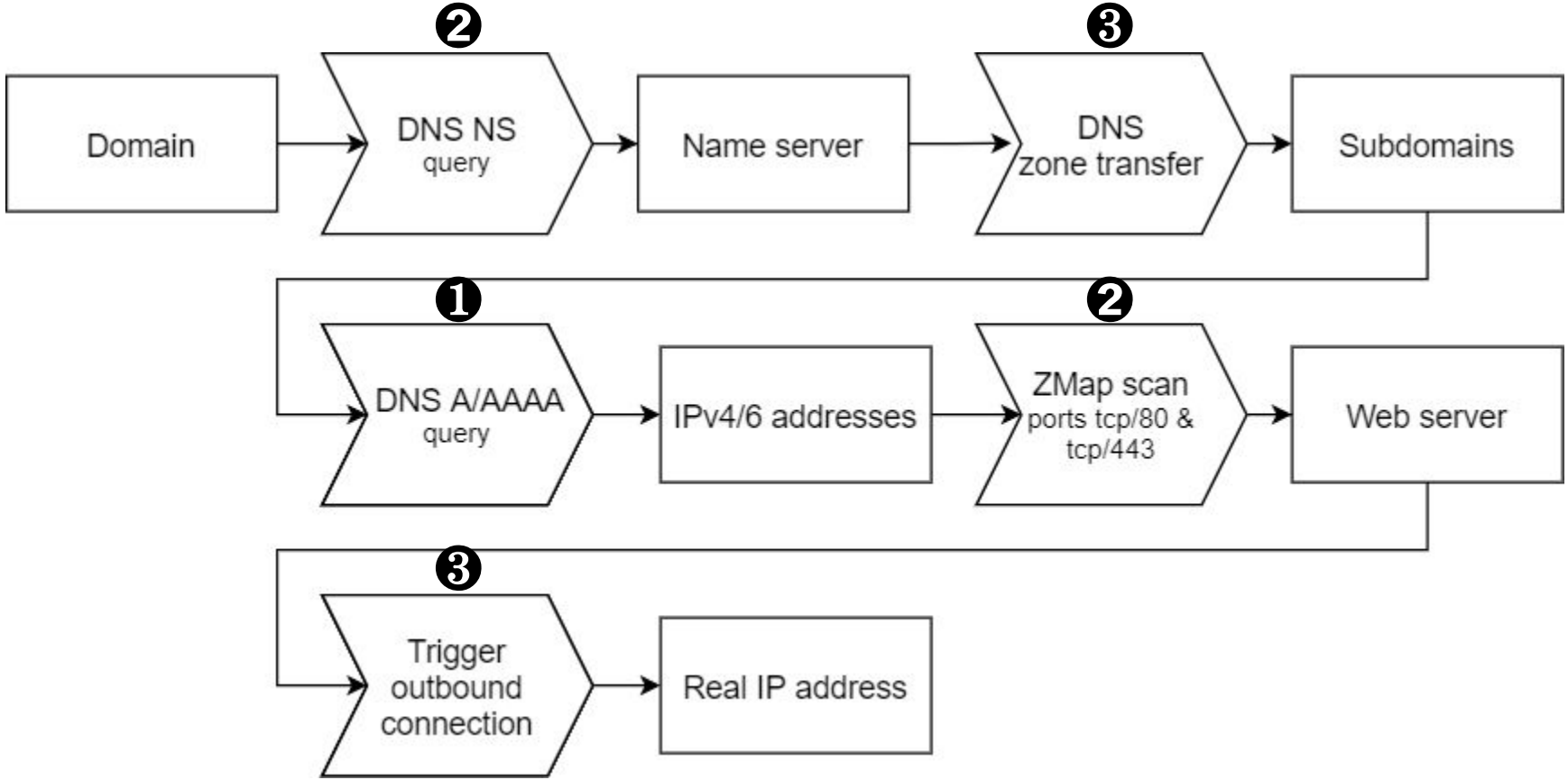
Asset discovery chain



Asset discovery chain



Asset discovery chain



In conclusion

SoK: A Framework for Asset Discovery: Systematizing Advances in Network Measurements for Protecting Organizations

Mathew Vermeer*, Jonathan West†, Alejandro Cuevas‡, Shuonan Niu†,
Nicolas Christin‡, Michel van Eeten*, Tobias Fiebig*, Carlos Gañán*, Tyler Moore†
*Delft University of Technology {m.vermeer,m.j.g.vaneeten,t.fiebig,c.hernandezganan}@tudelft.nl
†University of Tulsa {codiwest,shn5898,tyler-moore}@utulsa.edu
‡Carnegie Mellon University {acuevasv,nicolasc}@cmu.edu

***Abstract*—Asset discovery is fundamental to any organization's cybersecurity efforts. Indeed, one must accurately know which assets belong to an IT infrastructure before the infrastructure can be secured. While practitioners typically rely on a relatively small set of well-known techniques, the academic literature on the subject is voluminous. In**

formation Technology Infrastructure Library (ITIL) and ISO procedures, necessarily contain errors and omissions. Automated techniques to identify these gaps are therefore essential for defenders to adopt.

Asset discovery is not only a defensive activity, but

Acknowledgements

This research was partially supported by the Air Force Research Laboratory (AFRL) under agreement number FA8750-19-1-0152, and by the European Commission through the H2020 program in projects CyberSecurity4Europe (Grant No. #830929), and Safe-DEED (Grant No. #825225). The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of AFRL or the U.S. Government.