UNIVERSITY OF PLYMOUTH

Ethical hacking demo

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

Learning outcome checklist

LO1: Tell difference between passive and active footprinting [1]

LO2: Ensure not breaking the law while practicing active footprinting

LO3: Understand the key concepts of Maltego [2,3]

LO4: Conduct level 1 footprinting with Maltego [4,5]

LO5: Scan the open ports using nmap/

Zenmap [8,9]

LO6: Scan vulnerabilities with Nessus [6,7,10]

Further reading

1. https://en.wikipedia.org/wiki/Footprinting
2. https://docs.maltego.com/support/solutions/articles/15000035722-introduction-to-maltego-standard-entities#entity-properties-andvalues-0-2
3. Schwarz, Klaus, and Reiner Creutzburg. "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools-Part 3: Maltego." *Electronic Imaging* 2021.3 (2021): 45-1.
4. https://www.maltego.com/blog/beginners-guide-to-maltegomapping-a-basic-level-1-network-footprint-part-1/
5. https://www.maltego.com/blog/beginners-guide-to-maltegomapping-a-basic-level-1-network-footprint-part-2/
6. https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/
7. https://koayyongcett.medium.com/introduction-to-nessus-and-hands-on-practice-to-scan-the-network-34c8048090fc
8. https://nmap.org/book/zenmap-scanning.html
9. https://nmap.org/book/zenmap-results.html
10. https://docs.tenable.com/nessus/Content/ScanResults.htm

Activity

1. What is the aim of the 1st phase of cyber kill chain?
2. What can be source of information for phase 1 of cyber kill chain?

Open Source Intelligence (OSINT)

- Reconnaissance tools
  - Maltego
  - Nessus
  - Nmap/ Zenmap (nmap GUI)
  - theHarvester
  - Sherlock

Footprinting

- The technique used for gathering information about computer systems and the entities they belong to [1]
- Activity: difference between passive vs active footprinting and example?
- Techniques includes, but not limited to:
  - whois.domaintools.com
  - ipinfo.io
  - tracemyip.org
  - www.netcraft.com
  - https://www.reversewhois.io
  - Google
  - Traceroute
  - Maltego

Maltego

- Maltego CE (community version)
- Transform: bits of code which can be run to generate information based on information we already have.
- Entity: the information generated by the transform or provided by us
- Machines assemble transformations usinga script to automate tasks intelligently.

38.951633,-77.14462
www
www.maltego.com
Maltego

Source of image: [2]

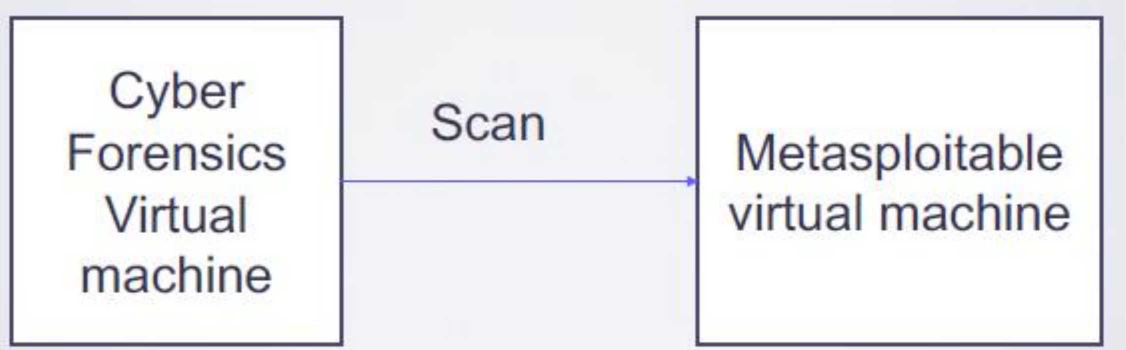
Footprinting with Maltego - Example

Consider University of Plymouth, find out

1. DNS names currently or previously used by the organization;
2. Mail exchange servers used by the organization;
3. Email addresses of the organization’s network administrators;
4. The netblocks that these IP address belong to;
5. The companies owning these netblocks.

Port scanning

- A method of determining which ports on a network are open and could be receiving or sending data
- **Important**: only use the internal IP address in SMB101 (which should start with 192.168) for these tests to avoid breaking law.


Cyber Forensics Virtual machine
Scan
Metasploitable virtual machine

Port scanning with Zenmap/ nmap

- Nmap is a port scanner that discovers the active host by network scanning
- Port scanning with zenmap/ nmap to the Metasplotable VM and identify

1. Opening ports
2. Running services (application name and version) this host is providing.
3. Operating systems and OS versions
4. Firewall in use.

Vulnerability scanning

- The process of identifying security weaknesses and flaws in systems and software running on them.
- Vulnerability scanning with Nessus to the

Metasplotable VM and identify the critical vulnerabilities. Utilise the critical vulnerability in VNC to control the target VM.

Vulnerability scanning with Nessus

- Nessus is a vulnerability scanner which scans ports like Nmap and looks only for the specific weakness of the system against a known host.

UNIVERSITY OF
PLYMOUTH

Dr Hai-Van Dang

hai-van.dang@plymouth.ac.uk

Centre for Security, Communications & Network Research

www.plymouth.ac.uk/cscan