Active Reconnaissance

Nmap

Active Reconnaissance - Λίγη Ορολογία

Reconnaissance : Η συλλογή πληροφοριών για έναν στόχο, συνήθως υπολογιστή. Χωρίζεται σε Passive και Active.

Active Reconnaisance : Αλληλεπίδραση Επιτιθέμενου-Στόχου μέσω traffic. Σκοπός η συλλογή δεδομένων για το σύστημα (πχ. λειτουργικό, υπηρεσίες που τρέχουν, ανοιχτά ports) και κατ' επέκταση η εύρεση vulnerabilities.

Active Reconnaissance θεωρείται και το απλό **ping** ή **traceroute**, ωστόσο εργαλεία όπως **nmap** ή **nessus** το κάνουν με αυτοματοποιημένο τρόπο και με πιο advanced τεχνικές.

Το Active Reconnaissance παράγει θόρυβο στο σύστημα αν γίνει "επιθετικά"(πολλά πακέτα σε σύντομο χρονικό διάστημα == sus) και έτσι συστήματα IDS (Intrusion Detection Systems) το εντοπίζουν.

Μια αναφορά στο Passive Reconnaissance

Passive Reconnaisance: Συλλογή πληροφοριών για τον στόχο, χωρίς όμως την ενεργό αλληλεπίδραση με αυτόν.

Περιλαμβάνει:

- OSINT (Open Source Intelligence), δηλαδή συλλογή δεδομένων από δημόσιες πηγές (literally googling stuff)
- Μελέτη του source code όταν αυτός είναι διαθέσιμος (π.χ. open source projects), ή των στοιχείων κώδικα που μπορούν να ληφθούν μέσω common μεθόδων όπως ctrl+u σε μια ιστοσελίδα

Με αυτόν τον τρόπο μπορεί κανείς να βρει vulnerabilities στον στόχο, γνωρίζοντας τι τρέχει από πίσω

NMAP (aka to logo στο background)

- Πρόκειται για το go-to open-source εργαλείο active reconnaissance (fun fact, η official ιστοσελίδα διαθέτει λίστα ταινιών που εμφανίζεται το tool https://nmap.org/movies/)
- Preinstalled στα kali, αλλιώς εγκατάσταση με:

```
~$ sudo apt update

~$ sudo apt install nmap
```

- Πραγματοποιεί **port scanning** στον στόχο, βρίσκει τα ανοιχτά ports, τις υπηρεσίες που τρέχουν σε αυτά, ενώ μπορεί ακόμα και να δοκιμάσει διάφορα built-in scripts για τον εντοπισμό vulnerabilities

NMAP - Λειτουργία

Η εντολή, στην απλή της μορφή εξής:

```
~$ nmap <IP>
```

```
┌──(kali㉿kali)-[~]
└─$ nmap 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 06:19 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Το nmap σκανάρει τα 1000 πιο συχνά ports για κάθε πρωτόκολλο (https://stackoverflow.com/questions/56522114/what-are-the-1000-ports-that-nmap-scans-by-default) της target IP. Εμφανίζει τα ανοιχτά ports, το πρωτόκολλο που χρησιμοποιούν (tcp/udp), την κατάστασή τους (open) και την υπηρεσία/πρωτόκολλο που τρέχουν (ssh,http).

Το nmap μπορεί να πραγματοποιήσει και πιο σύνθετες αναζητήσεις όπως θα δούμε παρακάτω

Scan Types

TCP(Default)/UDP scan (-sS/-sU): Target scan με χρήση TCP/UDP πακέτων

Service and Version Detection (-sV): Ανίχνευση είδους υπηρεσίας

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.4p1 Debian 1 (protocol 2.0)
```

Os Detection (-O): Ανίχνευση Λειτουργικού Συστήματος (απαιτεί δικαιώματα root)

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
```

Run NSE Scripts (-sC): Εκτέλεση built-in scripts για εύρεση περισσότερων πληροφοριών και vulnerabilities για τον στόχο

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 b7:43:52:83:09:d6:92:dd:7a:63:8a:d8:f8:13:05:06 (ECDSA)
|_  256 b3:d2:58:ca:cd:92:08:9f:cc:0e:a7:6f:44:cb:18:2d (ED25519)
80/tcp open  http
|_http-title: Apache2 Debian Default Page: It works
```

Όλα τα παραπάνω πλην UDP Scan (-A)

Nmap Switches and other useful stuff

- -p <port>: scan specific port
- -p <start>-<end>: scan all ports in range start-end
- -T0, -T1, …, -T5: από paranoid(αργό, non-detectable) σε aggressive(γρήγορο, detectable) scan types
- -v: πιο verbose output
- -Pn: Port Scanning χωρίς έλεγχο αν ο host είναι up. Χρήσιμο σε περιπτώσεις που ένας server είναι up, αλλά π.χ. δεν έχει ρυθμιστεί να απαντά σε pings
- nmap <IP1> <IP2>: scan both targets IP1, IP2
- nmap 192.168.1.1-192.168.1.255: scan all IPs in range

Resources

Για περισσότερες πληροφορίες σχετικά με το nmap:

- https://www.stationx.net/nmap-cheat-sheet/ (nmap cheatsheet)
- https://shorturl.at/lrFR7 (cookbook on nmap)

Για εξάσκηση:

- https://tryhackme.com/room/furthernmap

Thanks for your Attention!!