Testy Penetracyjne

Zbieranie informacji — Metody pasywne

Arkadiusz Chrobot

Katedra Systemów Informatycznych

13 marca 2024

Plan

Wstęp

Kolejną czynnością po planowaniu i określaniu zakresu testów penetracyjnych jest zbieranie informacji i skanowanie podatności. Ten wykład będzie dotyczył pierwszej jej części. To ile informacji należy zebrać zależy od ustalonej metody testowania. W przypadku testów znanego środowiska ta czynność może nawet być pominięta. Wymagane informacje zostaną dostarczone przez właściciela testowanego systemu. Kiedy wykonywane są testy częściowo znanego lub nieznanego środowiska, to należy pozyskać większość lub całość danych koniecznych do prawidłowego przeprowadzenia testowania.

Metody zbierania informacji o sprawdzanym systemie dzielą się na dwie kategorie: *pasywne* i *aktywne*. Do pierwszej należą te sposoby uzyskiwania danych, które nie wymagają bezpośredniej styczności z weryfikowaną infrastrukturą informatyczną, ale korzystają one z publicznie dostępnych źródeł informacji. Z tego powodu są także nazywane „białym wywiadem” lub OSINT od angielskich słów *Open Source Intelligence*.

Metody pasywne

Niecyfrowe źródła informacji

Pasywne metody mogą obejmować nie tylko uzyskanie danych nie tylko z źródeł cyfrowych, ale także fizycznych (np. niedokładnie zniszczone i wyrzucone dokumenty z informacjami niejawnymi) i od ludzi związanych z testowanym systemem (np. pracowników firmy, gdzie jest on zainstalowany). Jeżeli testy penetracyjne mają również dotyczyć zabezpieczeń fizycznych (np. monitoringu CCTV — *Closed-Circuit TeleVision*), to wykonawcy powinni uzyskać ich dane techniczne i informację o lokalizacji poszczególnych elementów.
Wobec pracowników firmy wyposażonej w weryfikowany system można zastosować socjotechnikę, np. *phishing* lub *vishing* (skrót od angielskich słów *voice phishing*, czyli technikę polegającą na wykorzystaniu połączeń głosowych zamiast wiadomości e-mail lub SMS.

Metody pasywne

Media społeczne

Źródłem cennych informacji mogą być treści umieszczane przez pracowników podmiotu, do którego należy weryfikowany system. Dotyczy to zarówno platform specjalistycznych, takich jak LinkedIn, jak i ogólnego przeznaczenia, jak Facebook. Przeglądając profile zatrudnionych osób lub ogłoszenia naboru do pracy ich pracodawcy testerzy mogą się dowiedzieć jakimi kompetencjami dysponują pracownicy firmy, np. w jakich technologiach są ekspertami lub jakich specjalistów brakuje. Jeśli występuje podejrzenie, że pewne dane były publicznie dostępne, ale zostały usunięte, to warto sprawdzić na stronie ▸ Internet Archive, czy przypadkiem nie zostały tam zarchiwizowane.

Metody pasywne

Wyszukiwarki internetowe

Do „białego wywiadu” można także zastosować zwykłe wyszukiwarki internetowe. Istnieje np. poradnik, jak do tego celu wykorzystać Google. Oprócz tego stworzono specjalistyczne wyszukiwarki, takie jak Shodan, Censys lub ZoomEye.org, które umożliwiają wyszukiwanie danych technicznych dotyczących urządzeń podłączonych do Internetu, niekiedy nawet wraz z informacjami o podatnościach jakie w nich występują (podany może być numer CVE lub CWE).

Metody pasywne

Metadane

Znalezione w Internecie pliki mogą zawierać metadane, które także mogą się okazać cenne. Przykładowo, aparaty fotograficzne zainstalowane w smartfonach mogą umieszczać w sekcji *Exif* plików z obrazami współrzędne miejsca, gdzie zdjęcie zostało wykonane. Jeśli celem testów jest samo urządzenie mobilne, to dane o aparacie mogą zdradzić jego model i producenta. Do uzyskania metadanych ze zdjęć można posłużyć się np. poleceniem `exif` (Linux) narzędziami z pakietu *ExifTools* (Windows, MacOS). Podobną rolę dla plików PDF pełni polecenie `pdfinfo`. Z kolei `strings` wyszukuje łańcuch tekstu w plikach binarnych i wyświetla je na ekranie.
Opracowano również specjalistyczne narzędzia, takie jak ▸ FOCA (ang. *Fingerprinting Organizations with Collected Archives*) dla systemu Windows, które wyszukują plik i analizują zawarte w nich metadane.

Metody pasywne

Inne źródła danych

Strony takiej jak ▸ Have I been pwned? mogą dostarczyć informacji, czy w przeszłości dokonano co najmniej jednego udanego włamania do testowanego systemu, lub czy dane jego użytkowników nie zostały ujawnione w wyniku podobnego zdarzenia dotyczącego innych systemów. Jeśli tak, to pentesterzy mogą rozpocząć poszukiwania stron, które zawierałby ewentualną bazę ujawnionych haseł.
Dobrym pomysłem może okazać się sprawdzenie publicznych repozytoriów z kodem używanego lub tworzonego przez firmę oprogramowania. Analiza statyczne ich zawartości może ujawnić istniejące w kodzie podatności, które można wykorzystać w testach.

Metody pasywne

Informacje o domenach

Informację o domenach zarejestrowanych dla testowanego systemu można uzyskać bezpośrednio z rejestrów nazw domen lub odpytując serwery DNS z użyciem odpowiednich narzędzi. Naczelną organizacją zarządzającą domenami jest IANA — *Internet Assigned Numbers Authority*, ale również istnieją cztery centra regionalne, które pozwalają uzyskać informacje o nich:

- AFRINIC – dla Afryki;
- APNIC – dla Azji i rejonu Pacyfiku;
- ARIN – dla Ameryki Północnej, części Karaibów i wysp na Północnym Atlantyku;
- LACNIC – dla Ameryki Łacińskiej i Karaibów;
- RIPE – dla Europy, Rosji i Bliskiego Wschodu oraz części Azji centralnej.

Metody pasywne

Informacje o domenach

W Linuksie można wykorzystać polecenie `whois` do uzyskiwania informacji o określonej domenie z rejestru. Poniżej pokazany jest wynik polecenia `whois mit.edu`.

```
Domain Name: MIT.EDU

Registrant:
        Massachusetts Institute of Technology
        77 Massachusetts Ave
        Cambridge, MA 02139
        USA

Administrative Contact:
        Mark Silis
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
```

Metody pasywne

Informacje o domenach

```
        +1.6173245900
        mark@mit.edu

Technical Contact:
        MIT Network Operations
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6172538400
        noc@mit.edu

Name Servers:
        EUR5.AKAM.NET
        USW2.AKAM.NET
        ASIA1.AKAM.NET
        USE5.AKAM.NET
```

Metody pasywne

Informacje o domenach

```
USE2.AKAM.NET
ASIA2.AKAM.NET
NS1-173.AKAM.NET
NS1-37.AKAM.NET

Domain record activated:    23-May-1985
Domain record last updated: 08-Jun-2021
Domain expires:             31-Jul-2024
```

Uzyskane informacje nie zawsze są tak szczegółowe. Zdarza się, że organizacje rejestrujące domeny po pewnym czasie usuwają z rejestru część danych. Są one jednak ▸ archiwizowane i niekiedy można do nich ▸ dotrzeć.

Do odpytywania serwerów DNS służy kilka różnych narzędzi. Prawdopodobnie najpopularniejszym z nich jest `nslookup` (Linux, MacOS i Windows), które umożliwia zarówno interaktywną jak i wsadową pracę.

Metody pasywne

Informacje o domenach

Slajd zawiera wynik polecenia `nslookup google.pl 8.8.8.8`.

```
Server:                 8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:           google.pl
Address: 216.58.215.99
Name:           google.pl
Address: 2a00:1450:401b:807::2003
```

Metody pasywne

Informacje o domenach

Do pozostałych narzędzi, służących do komunikacji z serwerami DNS zaliczą się polecenia `host` i `dig` (Linux). Slajd zawiera przykładowe wyniki działania tego pierwszego.

Polecenie `host tu.kielce.pl`

```
tu.kielce.pl has address 81.26.0.47
tu.kielce.pl has IPv6 address 2a00:cd80:10::c
tu.kielce.pl mail is handled by 0 mailgw.tu.kielce.pl.
```

Polecenie `host 81.26.0.47`

```
47.0.26.81.in-addr.arpa domain name pointer www.tu.kielce.pl.
```

Zastosowanie `dig` zostanie pokazane na przykładzie uzyskania informacji przy pomocy operacji *transferu strefy DNS* (ang. *DNS zone transfer*), oznaczanego skrótem AXFR. Ten transfer służy do replikowania bazy danych o adresach między serwerami DNS. Z uwagi na istotność tych danych transfer stref w większości serwerów DNS jest albo bardzo dobrze zabezpieczony, albo wyłączony.

Metody pasywne

Informacje o domenach

W przykładzie dotyczącym transferu stref użyty zostanie przykład ze strony ▸ Robina Wooda:

```
dig axfr @nsztm1.digi.ninja zonetransfer.me
```

```
; <<>> DiG 9.11.3-1ubuntu1.19+esm2-Ubuntu <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200        IN        SOA        nsztm1.digi.ninja. robin.digi.ninja.
↪  2019100801 172800 900 1209600 3600
zonetransfer.me.        300        IN        HINFO        "Casio fx-700G" "Windows XP"
zonetransfer.me.        301        IN        TXT
"google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200        IN        MX        0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200        IN        MX        10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200        IN        MX        10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200        IN        MX        20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200        IN        MX        20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200        IN        MX        20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200        IN        MX        20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200        IN        A        5.196.105.14
zonetransfer.me.        7200        IN        NS        nsztm1.digi.ninja.
zonetransfer.me.        7200        IN        NS        nsztm2.digi.ninja.
_acme-challenge.zonetransfer.me. 301
↪  IN        TXT        "6Oa05hbUJ9xSsvYy7pApQvwCUSSGgxvrbdizjePEsZI"
_sip._tcp.zonetransfer.me. 14000 IN        SRV        0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200        IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN        AFSDB        1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200        IN        A        127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN        AFSDB        1 asfdbbox.zonetransfer.me.
```

Metody pasywne

Informacje o domenach

```
canberra-office.zonetransfer.me. 7200 IN A        202.14.81.230
cmdexec.zonetransfer.me. 300        IN        TXT        "; ls"
contact.zonetransfer.me. 2592000 IN        TXT        "Remember to call or email Pippa on +44 123
↪  4567890 or pippa@zonetransfer.me when making DNS changes"
dc-office.zonetransfer.me. 7200        IN        A        143.228.181.132
deadbeef.zonetransfer.me. 7201        IN        AAAA        dead:beaf::
dr.zonetransfer.me.        300        IN        LOC        53 20 56.558 N 1 38 33.526 W 0.00m 1m
↪  10000m 10m
DZC.zonetransfer.me.        7200        IN        TXT        "AbCdEfG"
email.zonetransfer.me.        2222        IN        NAPTR        1 1 "P" "E2U+email" ""
↪  email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.        7200        IN        A        74.125.206.26
Hello.zonetransfer.me.        7200        IN        TXT        "Hi to Josh and all his class"
home.zonetransfer.me.        7200        IN        A        127.0.0.1
Info.zonetransfer.me.        7200        IN        TXT        "ZoneTransfer.me service provided by
↪  Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more
↪  information."
internal.zonetransfer.me. 300        IN        NS        intns1.zonetransfer.me.
internal.zonetransfer.me. 300        IN        NS        intns2.zonetransfer.me.
intns1.zonetransfer.me.        300        IN        A        81.4.108.41
intns2.zonetransfer.me.        300        IN        A        167.88.42.94
office.zonetransfer.me.        7200        IN        A        4.23.39.254
ipv6actnow.org.zonetransfer.me.        7200 IN        AAAA        2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.        7200        IN        A        207.46.197.32
robinwood.zonetransfer.me. 302        IN        TXT        "Robin Wood"
rp.zonetransfer.me.        321        IN        RP        robin.zonetransfer.me.
↪  robinwood.zonetransfer.me.
sip.zonetransfer.me.        3333        IN        NAPTR        2 3 "P" "E2U+sip"
↪  "!^.*$!sip:customer-service@zonetransfer.me!" .
sqli.zonetransfer.me.        300        IN        TXT        "' or 1=1 --"
```

Metody pasywne

Informacje o domenach

```
sshock.zonetransfer.me.        7200        IN        TXT        "() { :]}; echo ShellShocked"
staging.zonetransfer.me. 7200        IN        CNAME        www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A        127.0.0.1
testing.zonetransfer.me. 301        IN        CNAME        www.zonetransfer.me.
vpn.zonetransfer.me.        4000        IN        A        174.36.59.154
www.zonetransfer.me.        7200        IN        A        5.196.105.14
xss.zonetransfer.me.        300        IN        TXT        "'><script>alert('Boo')</script>"
zonetransfer.me.        7200        IN        SOA        nsztm1.digi.ninja. robin.digi.ninja.
↪  2019100801 172800 900 1209600 3600
;; Query time: 41 msec
;; SERVER: 81.4.108.41#53(81.4.108.41)
;; WHEN: Wed Mar 13 01:43:57 CET 2024
;; XFR size: 50 records (messages 1, bytes 2085)
```

Interesujących informacji o domenach mogą również dostarczyć certyfikaty TLS.

Metody pasywne

Adresy IP

Właściciel adresu IP, a także zakres adresów, który jest mu przynależny, może być sprawdzony na stronie ▸ Whois. Zbadanie trasy do hosta z określonym adresem IP, przy pomocy takich poleceń jak `traceroute` (Linux, MacOS), `tracepath` (Linux) i `tracert` (Windows) również może okazać się pomocne. Pozwala ono uzyskać informacje o topologii sieci. Z kolei informację o trasowaniu (ang. *routing*) można uzyskać z serwerów zwanych jako ▸ *BGP looking glasses*.

Metody pasywne

Zbieranie informacji o sieciach bezprzewodowych polega na skanowaniu otoczenia w ich poszukiwaniu. Wiąże się ono z koniecznością przemieszczania, najczęściej przy pomocy jakiegoś pojazdu, dlatego taka czynność w języku angielskim jest nazywana *wardriving*. Zgromadzone dane można np. porównać z informacjami udostępnianymi przez strony takie jak ▸ Wigle.net lub nałożyć na mapę posługując się ▸ triangulacją.

Metody pasywne

Inne narzędzia

Do porządkowania danych pochodzących z „białego wywiadu” można użyć szeregu narzędzi. Przykładowo, *theHarvester* gromadzi wiadomości e-mail, informacje o domenach, nazwy urządzeń sieciowych (ang. *hostnames*), nazwiska pracowników, otwarte porty, banery (informacje tekstowe zwracane przez usługi sieciowe) używając wyszukiwarek internetowych. *Maltego* tworzy mapy relacji między ludźmi i zasobami, z kolei *Recon-ng* automatyzuje zbieranie informacji.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!