Bezbednost Aplikacija
Izviđanje i profilisanje Web servera

Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

Osnovne Aktivnosti napadača

Različiti načini proboja sistema sa ciljem posedovanja sistema

- Sakupljanje informacija o meti
- Identifikacija ranjivosti
- Eksplotacija

Faze penetracionog testiranja

Izviđanje

- pronalaženje javno dostupnih informacija i upoznavanje sa tehnologijama sistema

Skeniranje

- pronalaženje potencijalnih prolaza ili ranjivosti u sistemu primenom automatizovanog ili ručnog skeniranja

Eksploatacija

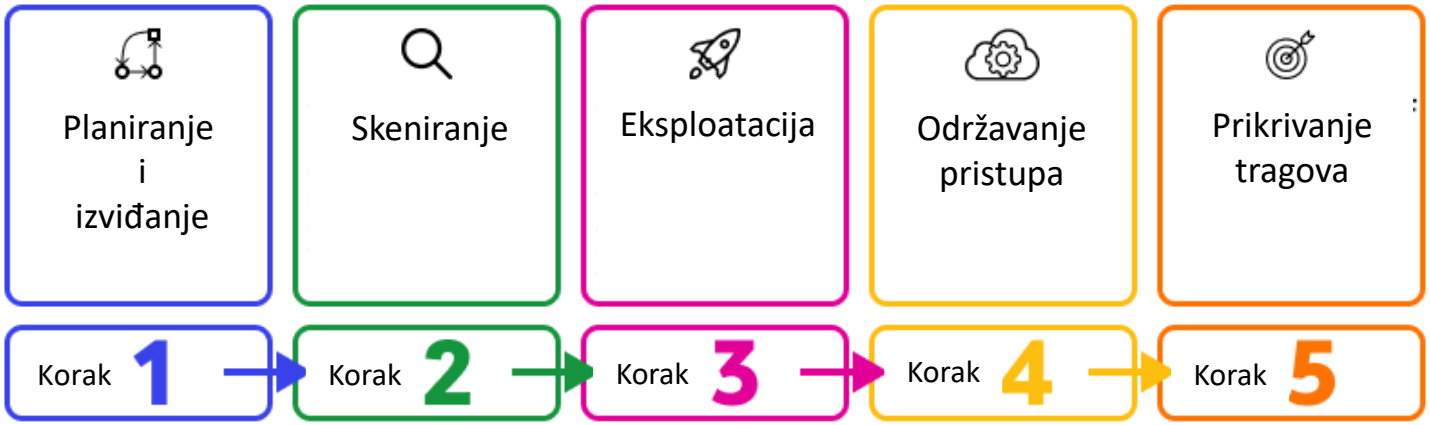
- uključuje kompromitovanje cilja i dobijanje pristupa

Održavanje pristupa

- Eskalacija privilegija na kompromitovanom sistemu, postavljanje ulaza u sistem (back door), kreiranje korisnika,...

Prikrivanje tragova

- Uklanjanje dokaza napada



Faza Izviđanja

Vojni termin – dobijanje informacije o neprijatelju na način koji ih neće upozoriti

Osnovni cilj je sakupljanje informacija

Napadač zlonamerni sadržaj koristi na osnovu informacija sakupljenih u fazi izviđanja

planiranje izviđanje

Cilj Izviđanja

planiranje izviđanje

Identifikovanje IP adresa, domena, poddomena korišćenjem Whois alata

Sakupljanje informacija o meti (ciljni web sajt) iz javno dostupnih servisa (Google, Yahoo, Bing, ...)

Internet Archive (https://archive.org) je digitalna arhiva za sve web stranice na Internetu koja kešira sve internet sajtove od 1996.

Pronalaženje ljudi koji su povezani sa metom pomoću društvenih mreža (LinkedIn, Facebook, Flick, Instagram, Twiter,...)

Određivanje fizičke lokacije mete upotrebom Geo IP baze podataka (https://ipgeolocation.io/ip-location/)

Skidanje web sajta na lokalnom računaru, ručno pretraživanje i kreiranje mapa sajta za razumevanje (https://www.httrack.com/)

Pasivno Vs Aktivno izviđanje

planiranje izviđanje

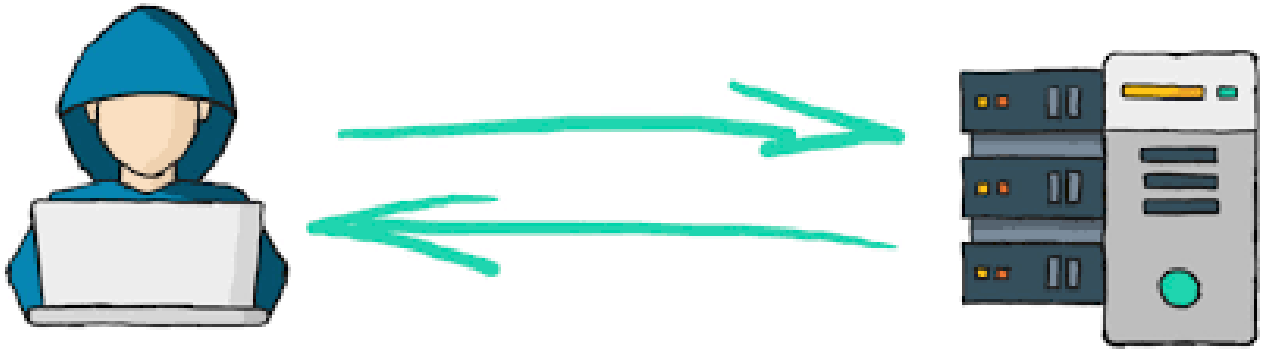
Pasivno izviđanje podrazumeva sakupljanje informacija iz drugih javnih izvora a ne direktno u interakciji sa metom

Pasivnim izviđanjem se izbegava direktna interakcija sa metom

Pasivno izviđanje zavisi od keširanih informacija i poznato je kao Open Source Inteliligence (OSINT) sakupljanje

Interakcija sa metom na način koji neće upozoriti uređaje za prevenciju proboja (firewall ili IPS)

Aktivno izviđanje uključuje pretraživanje ciljnog uređaja kroz javno dostupni sadržaj.



Whois – pronalaženje informacija o domenu

Whois zapis sadrži registracione detalje koje obezbeđuje vlasnik domena registru domena

Sadrži ime, adresu, broj telefona i email adresu osobe koja je registrovala domen.

Whois serverima upravljaju regionalni internet registri (Regional Internet Registry) kao što su (RIPE, ARIN,AfriNic,...)

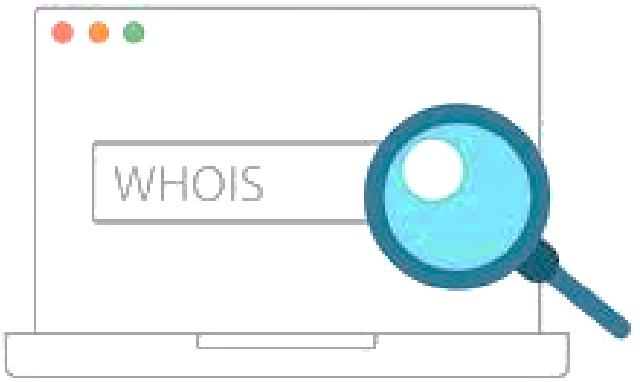
Whois serverima može direktno da se pristupi putem porta 43

Whois Lookup web sajt: https://who.is/whois/vtsnis.edu.rs

Vlasnici domena mogu da blokiraju poverljive informacije.

Whois server može da vrati sledeće informacije

- Datum registracije domena i datum isteka domena
- Kontakt informacije
- DNS server koji je zadužen za domen koji može da se iskoristi za pronalaženje ostalih urađaja u domenu



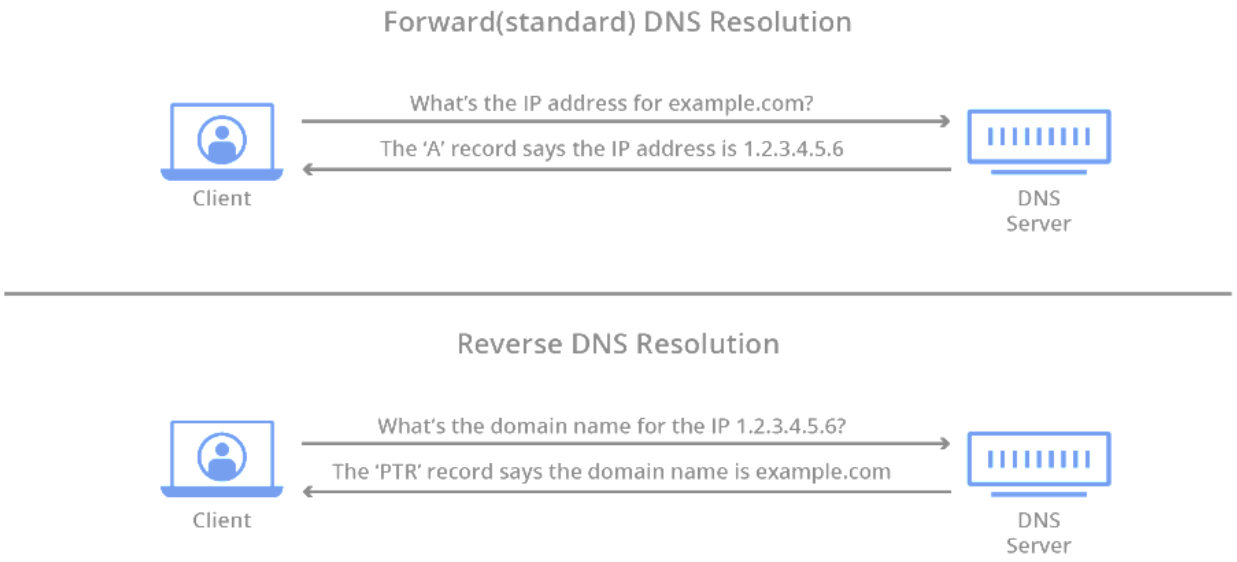
DNS Lookup – pronalaženje povezanih hostova

Poznavanje autorativnog DNS servera za metu može da se upotrebi za pronalaženje dodatnih uređaja u domenu

Na Internetu svaki servis zahteva naziv hosta za identifikaciju servisa koji se nalazi na DNS serveru

Mail server, FTP server koriste DNS za razrešavanje hostova u IP adrese

planiranje
izviđanje



DIG ALAT – Transfer DNS zone

DNS arhitektura zahteva minimalno dva DNS servera, primarni i sekundarni zbog veće dostupnosti servera

Transfer zone je sihronizacija DNS zapisa sa primarnog na sekundarni DNS server

Pogrešna konfiguracija DNS servera može da dozvoli svakom uređaju da zatraži transfer zone i da dobije listu mapiranja svih uređaja i servisa u toj zoni.

Alat koji omogućava transfer zone je DIG (Domain Internet Groper) koji se još koristi za uobičajne DNS upite.

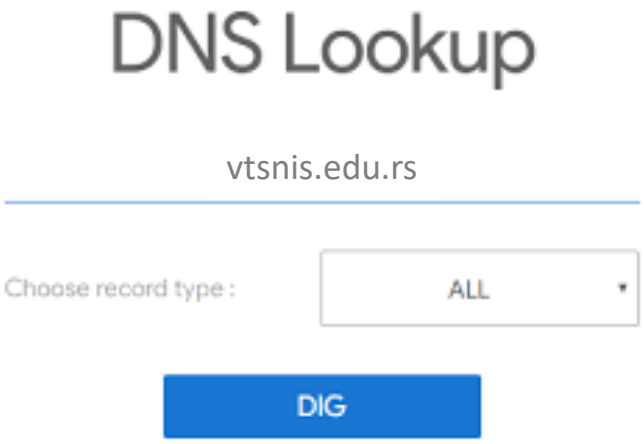
Za transfer zone se koristi TCP port 53.

https://toolbox.googleapps.com/apps/dig/

Ostali alati za popis DNS informacija su:

- *DNSEnum*
- *DNSRecon*
- *Nmap - Napad grubom silom na DNS zapise*

planiranje
izviđanje



Online Alati za pasivno izviđanje

Pretraživači Google, Bing i DuckDuckGo omogućavaju:

- *naprednu pretragu upotrebom filtera u cilju pronalaženja informacija o određenom domenu*
- *određene tipove fajlova*
- *sadržaje u URL adresi*

Shodan (https://www.shodan.io/) omogućava pretragu:

- *naziva hostova*
- *otvorene portove*
- *lokaciju servera*
- *specifična zaglavlja odgovora u servisima*

planiranje izviđanje

Google dorks - Online Alati za pasivno izviđanje

Napredna Google pretraga tzv. Google dorks omogućava konkretniju pretragu na osnovu zadatih parametara i unetih znakovnih nizova

Prikaz svih pdf dokumenata na sajtu vtsnis.edu.rs
site:vtsnis.edu.rs filetype:pdf

Prikaz svih log fajlova koji u sebi sadrže reč password
allintext:password filetype:log

Reference za email adrese definisanog domena
"@akademijanis.edu.rs" -site:vtsnis.edu.rs

Stranice koje sadrže admin u naslovu na sajtu vtsnis.edu.rs
intitle:admin site:vtsnis.edu.rs

Web sajtovi koji pripadaju rs top level domenu i u URL adresi sadrže http
site:.rs inurl:http

Shodan- Online Alati za izviđanje

Shodan je pretraživač koji pomaže pronalazak uređaja (IoT) koji su povezani na Internet i svi servisi koji su pokrenuti na tim uređajima.

Ima svoju sintaksu za izvršenje naprednih i specifičnih pretraga

Po svakoj ključnoj reči prikazuje statistiku npr: top countries, top operating systems, top organizations,...

Pretraga servera koji pripadaju određenom domenu
hostname:imedomena

Pretraga specifičnih tipova uređaja kao što su kamere ili industrijski kontrolni sistemi
server: SQ-WEBCAM

Pretraga otvorenih portova i servisa
port:80,443,8080

Pretraga otvorenog porta 3389 u definisanom opsegu mreže
net:160.99.37.0/24 port:3389

Pretraga operativnog sistema
os:windows xp

Ostali alati za izviđanje

theHarvester

Koristi se za pronalaženje:

- *email adresa*
- *naziva poddomena*
- *virtuelnih hostova*
- *otvorenih portova*
- *imena zaposlenih koji su povezani sa domenom iz različitih javnih izvora*

Maltego

vlasnička aplikacija

Recon-ng radni okvir

koristi veliki broj izvora za sakupljanje informacija

SKENIRANJE – ISPITIVANJE CILJA

U fazi skeniranja koriste se informacije dobijene iz faze izviđanja

Klijent može za potrebe pen testa da obezbedi dodatne ciljeve koji nisu identifikovani u fazi izviđanja.

Kombinuju se metode hakera sa crnim i belim šeširom (test se započinje kao zlonamerni napadač ali se tokom testiranja obezbeđuju dodatne informacije od klijenta koje sadrže tačan prikaz cilja.

Faze prilikom skeniranja cilja uključuju:

- skeniranje porta
- Skeniranje portova i određivanje operativnog sistema
- verzija web servera koja se koristi
- Analiza pozadinske infrastrukture
- Identifikacija aplikacije

SKENIRANJE – NMAP

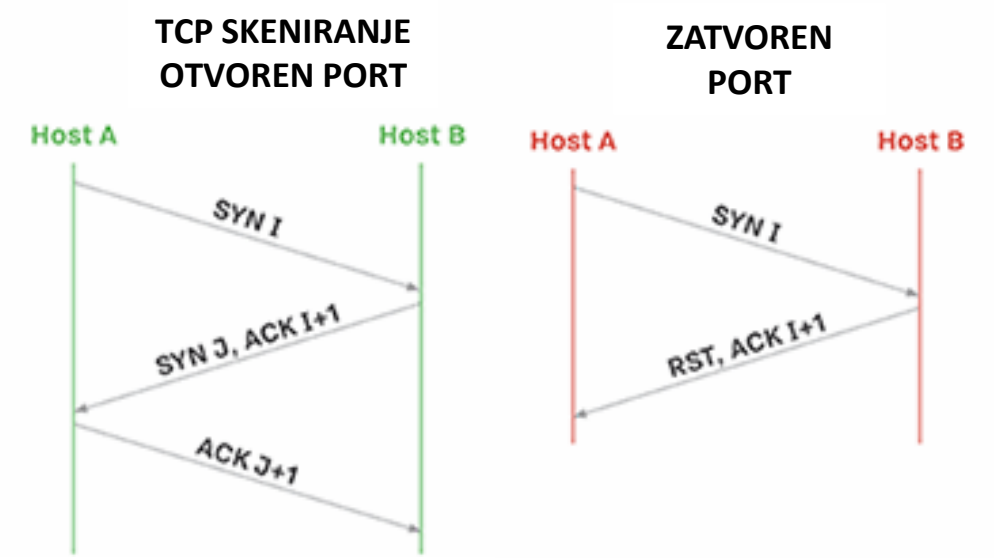
NMAP je najpoznatiji skener porta

Pronalazi otvorene UDP i TCP portove

Podrazumevano, nmap ne ispituje sve portove već 1000 najčešće upotrebljenih portova zbog brzine skeniranja jer ukupno postoji 65535 TCP i UDP porta a aplikacija može da koristi bilo koji.

Radi na principu pokušaja uspostavljanja TCP konekcije na zahtevanom portu.

TCP skeniranje kroz 3 way handshake proces se evidentira na ciljnoj mašini i izvršenje je sporije za razliku od polu otvorenog skeniranja koje se ne evidentira na ciljnoj mašini jer napadač resetuje konekciju pre nego što se uspostavi, manje se troše resursi ali takvu komunikaciju često blokira firewall.



SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

Skeniranje

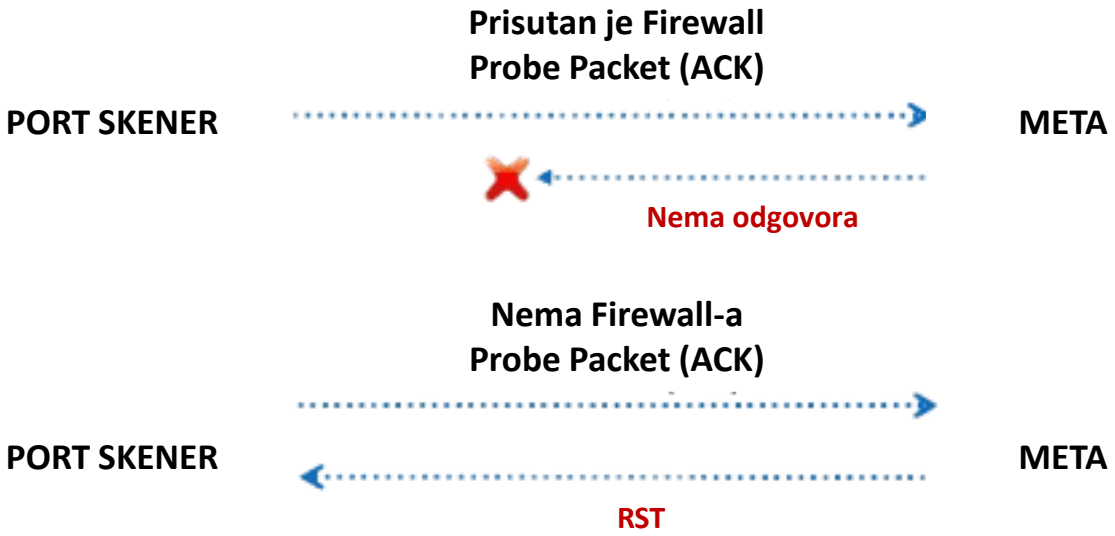
ACK metoda Skeniranja

Koristi se za utvrđivanje da li je meta zaštićena sistemom za filtriranje malicioznog saobraćaja (firewall)

Skener šalje ACK probe (test) paket koji sadrži slučajni SEQ broj.

Ukoliko skener ne dobije odgovor, port je filtriran a uzrok može da bude firewall dok ukoliko RST odgovor stigne znači da je port zatvoren

ACK skeniranjem se ne može utvrditi da li je port na krajnjem sistemu otvoren ili zatvoren jer različiti sistemi odgovaraju različito na nepoželjan ACK



SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

Nepromenjiv izvorni port na firewall-u

Najčešće pravilo na firewall-u dozvoljava ulazni saobraćaj iz spoljne mreže koji potiče iz određenog izvornog porta kao što su 53 (DNS), 25 (SMTP) ili 80 (HTTP).

NMAP pored toga što nasumično selektuje izvorišni port, može da bude konfigurisan da koristi određen izvorišni port i da na taj način zaobiđe pravila firewall-a.


```
root@bt:~# nmap --source-port 53 scanme.nmap.org

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-01 22:56 BST
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9929/tcp open  nping-echo

Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
```

SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

Prilagođena veličina paketa

Skeneri uglavnom šalju pakete određene veličine

Moderni Firewall sistemi imaju pravila za odbacivanje takvih paketa

NMAP skener sadrži opciju da šalje pakete rezličite veličine


```
root@bt:~# nmap --data-length 25 192.168.1.64

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-02 11:51 BST
Nmap scan report for Blackbox.home (192.168.1.64)
Host is up (0.00021s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
MAC Address: 00:04:4B:00:0C:87 (Nvidia)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

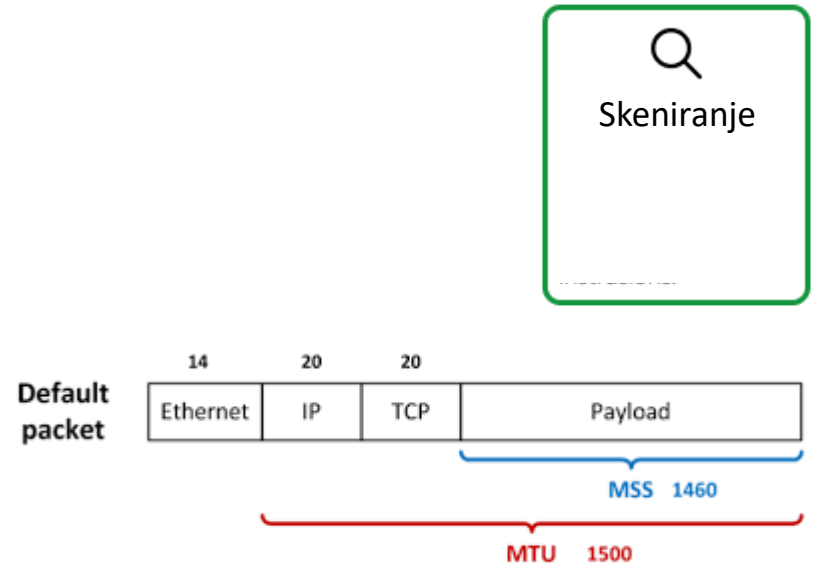
Prilagođeni MTU

NMAP skener sarži konfigurabilni MTU (Maximum transfer Unit)

Koristi se za zaobilaženje starijih firewall-ova i uređaja za detekciju proboja (IDS) jer oni mogu da smatraju da se radi samo o fragmentu a ne celom paketu i da na taj način propuste paket.

Moderni firewall sistemi rade defragmentaciju (sastavljaju paket koji je podeljen u manje fragmente) pre nego što ga pošalju na ciljnu mašinu.

MTU je višestruka vrednost od 8




```
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@bt:~# nmap --mtu 24 192.168.1.64

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-02 18:33 BST
Nmap scan report for Blackbox.home (192.168.1.64)
Host is up (0.00038s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
MAC Address: 00:04:4B:00:0C:87 (Nvidia)
```

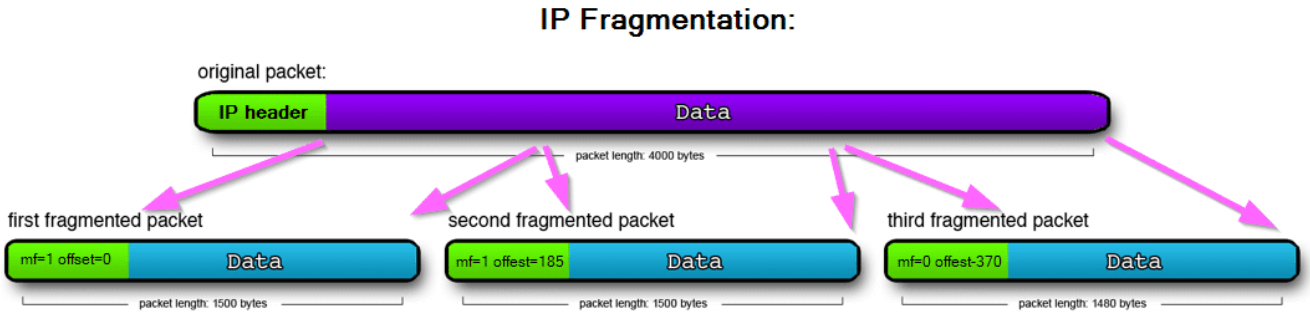
SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

Fragmentiranje paketa

Efikasan način za zaobilaženje starih firewall sistema je fragmentacija paketa

Paket je podeljen u više fragmenata

IDS senzori neće prepoznati zlonamerni paket jer paket nije kompletan




```
root@bt:~# nmap -f 192.168.1.64

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-02 13:56 BST
Nmap scan report for Blackbox.home (192.168.1.64)
Host is up (0.00049s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
MAC Address: 00:04:4B:00:0C:87 (Nvidia)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

SKENIRANJE – IZBEGAVANJE FIREWALL-A i IPS SISTEMA

Lažiranje MAC adrese

Za slučaj da u ciljnom okruženju postoje pravila samo za pakete sa određenih MAC adresa (mac filtering rule)

NMAP dozvoljava da se podesi određena MAC adresa (MAC spoofing)

```
root@bt:~# nmap -sT -Pn --spoof-mac Dell 192.168.1.64

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-02 01:01 BST
Spoofing MAC address 00:06:5B:4C:54:B2 (Dell Computer)
Nmap scan report for Blackbox.home (192.168.1.64)
Host is up (0.00049s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

SKENIRANJE

Identifikovanje Operativnog sistema

NMAP ima način da identifikuje OS pomoću TCP/IP otiska prsta (fingerprint).

OS Fingerprinting se odnosi na otkrivanje operativnog sistema krajnjeg hosta analizom paketa koji potiču iz tog sistema.

Nmap šalje seriju TCP i UDP paketa udaljenom hostu i ispituje svaki deo odgovora.

Određeni parametri unutar TCP/IP protokola su prepušteni implementaciji odgovarajućeg operativnog sistema.

Različiti operativni sistemi postavljaju različite podrazumevane vrednosti za ova polja.

Prikupljanjem i ispitivanjem ovih vrednosti, mogu se razlikovati operativni sistemi.

TTL , Veličina prozora, Veličina paketa, DF bit i TOS su samo neka od polja koja se koriste za određivanje OS-a .

```
E:\Temp>nmap -O -v 192.168.1.87

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-13 17:50 GMT Standard Time
Initiating ARP Ping Scan at 17:50
Scanning 192.168.1.87 [1 port]
Completed ARP Ping Scan at 17:50, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:50
Completed Parallel DNS resolution of 1 host. at 17:50, 0.01s elapsed
Initiating SYN Stealth Scan at 17:50
Scanning 192.168.1.87 [1000 ports]
Discovered open port 22/tcp on 192.168.1.87
Completed SYN Stealth Scan at 17:50, 0.59s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.87
Nmap scan report for 192.168.1.87
Host is up (0.015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 80:1F:02:82:C4:E3 (Edimax Technology Co.)
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: C:\Program Files (x86)\Nmap
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.25 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1017 (41.596KB)
```

PROFILISANJE SERVERA

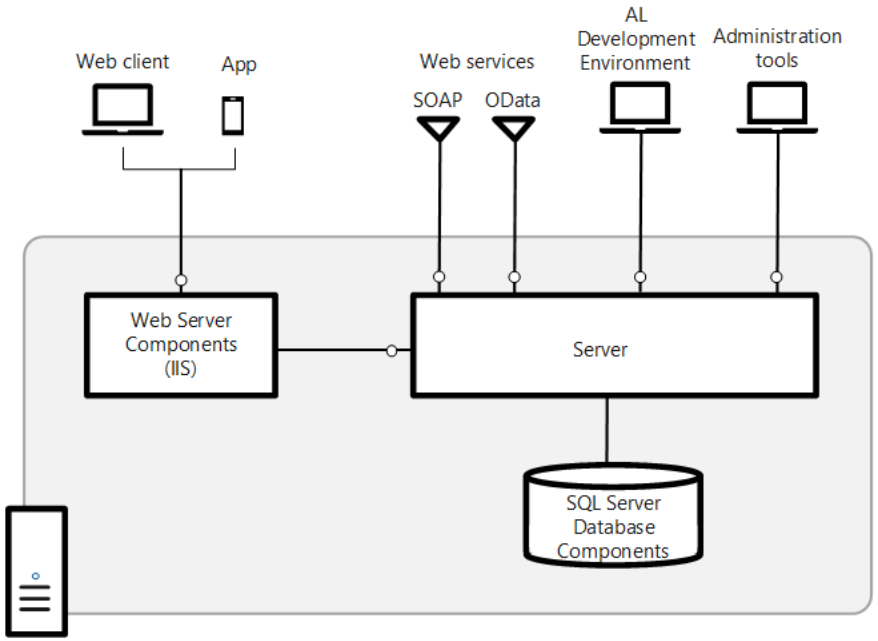
Identifikovanje aplikacija na otvorenim portovima

Skeniranjem web servera određuje se tip i verzija web servisa koji je pokrenut na OS-u.

- Web serveri obrađuju HTTP zahteve iz aplikacije kao što su Apache, IIS, Ngnix
- Razvoj Web aplikacija se oslanja na radne okvire (framework) i svaka web aplikacija će zahtevari drugačiji pristup (tehniku)

Identifikacija dodatnih komponenti koje podržavaju web aplikaciju

- Baza podataka
- Algoritmi enkripcije
- Raspoređivači opterećenja (load balancer)



PROFILISANJE SERVERA

Identifikovanje virtualnih hostova

Na jednom fizičkom web serveru može da se postavi više web sajtova

Svi web sajtovi dele resurse jednog fizičkog servera kao što je npr. IP adresa.

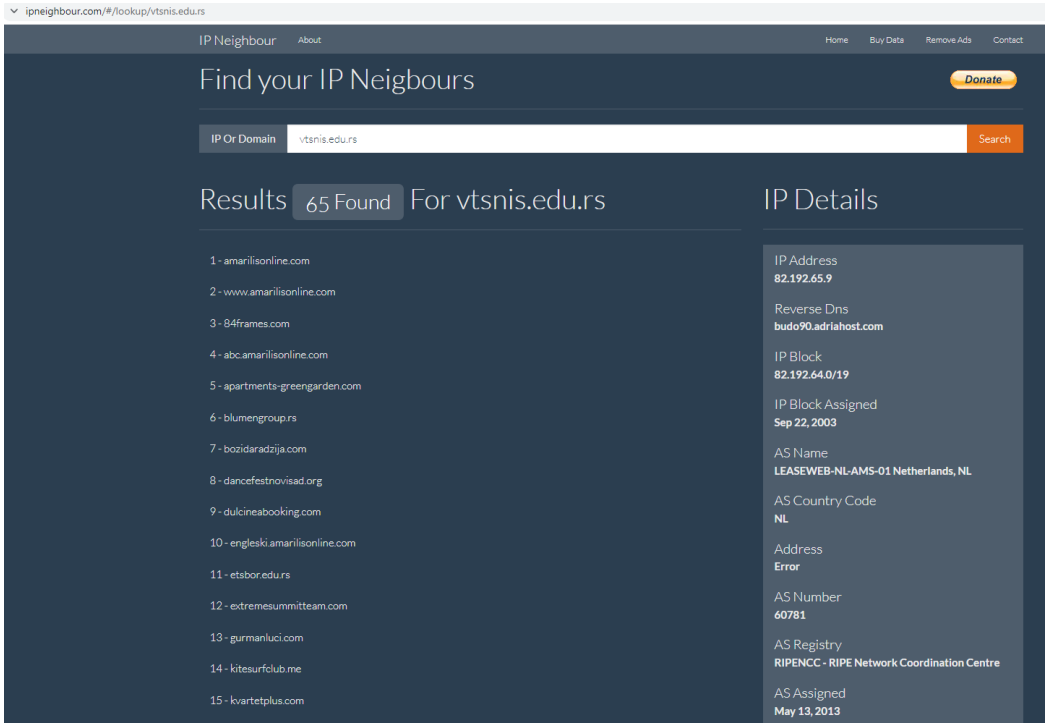
Virtualno hostovanje je zasnovano na nazivu i jedinstveno se identifikuju i razlikuju od drugih web sajtova koji sadrže istu IP adresu po vrednosti zaglavlja host-a.

Kada server primi zahtev on usmerava zahtev određenom hostu polja Host u zaglavlju zahteva.

Ako IP adresa hostuje više web sajtova treba da se upiše odgovarajući naziv za polje Host

Analizom DNS zapisa može da se utvrdi da li je više web sajtova hostovano na jednoj IP adresi.

Alati koji se koriste su nslookup, dig ili websajt https://www.ipneighbour.com/



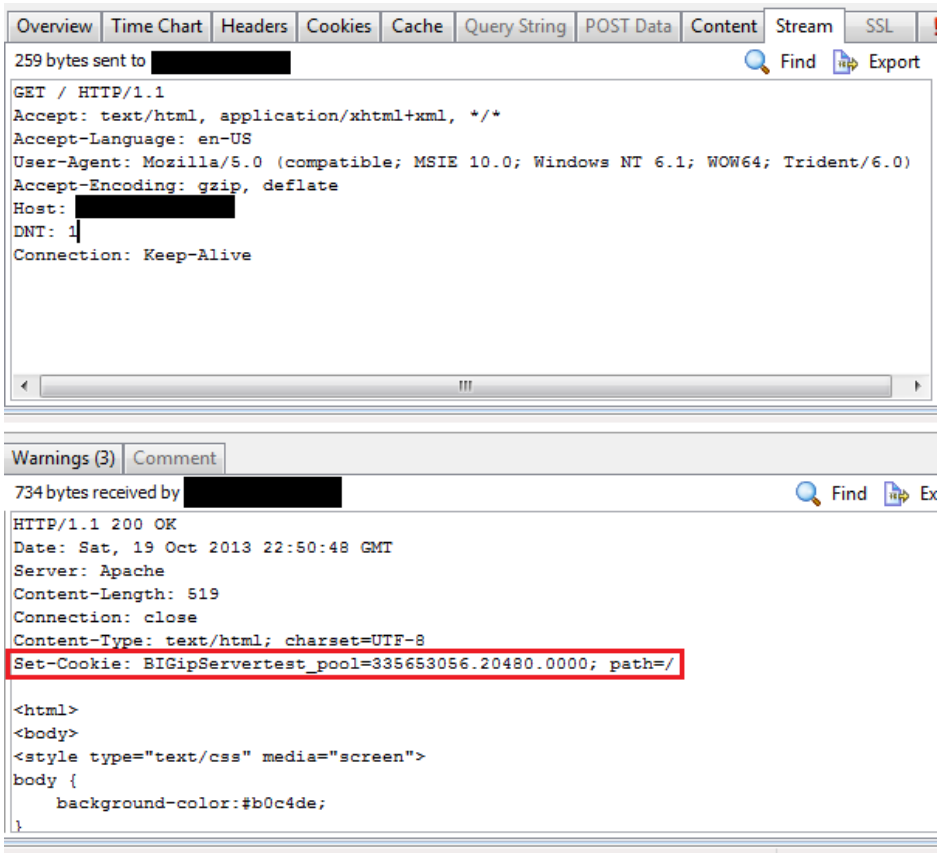
PROFILISANJE SERVERA

- Popularan metod koji koriste hardverski raspoređivači opterećenja je umetanje kolačića u pretraživač klijenta.
- Kolačić vezuje klijenta za određeni server.
- Metod omogućava ravnomerniju raspodelu opterećenja na serverima jer veliki broj klijenata koji se nalaze iza istog NAT servera imati istu izvornu IP adresu.
- Kolačići koje podesi load balanser mogu da otkriju poverljive informacije
- Kriptovana vrednost koja sadrži naziv skladišta, IP adresu web servera i port
- Kolačić za F5 load balanser koristi format:

BIGipServer<pool_name>=

<coded_server_IP> .<coded_server_port> .0000

RASPOREĐIVAČ OPTEREĆENJA ZASNOVAN NA KOLAČIĆU



PROFILISANJE SERVERA

DETEKTOVANJE RASPOREĐIVAČA OPTEREĆENJA

Pored umetanja kolačića postoje i drugi načini da se detektuje prisustvo load balansera.

- Analiza SSL razlika između servera
  - Mogu postojati male promene u SSL konfiguraciji na različitim web serverima, npr. vremenska oznaka na sertifikatu koja se izdaje web serverima može da varira.
- Preusmeravanje na drugi URL – preusmeravanje klijenta na drugi URL
  - Korisnik može da pretražuje web sajt www.xxx.com stim što se preusmerava na www2.xxx.com.
  - Zahtev od sledećeg korisnika će biti preusmeren na www1.xxx.com.
  - Ne primenjuje se često jer izaziva dodatno trošenje memorije za upravljanje i bezbedonosne probleme.
- DNS zapisi za raspoređivače opterećenja
- Detektor raspoređivača opterećenja
  - alat koji je uključen u Kali Linux
  - Komanda *lbd <ime web sajta>*

PROFILISANJE SERVERA

Nmap skeniranje verzije

Nmap ispituje cilj slanjem velikog broja paketa a zatim analizira odgovore za određivanje tačnog servisa i verzije

Skeniranje OS-a i verzije mogu zajedno da se kombinuju

Nmap prvo izvršava skeniranje portova na cilju koristeći standardnu listu od prvih 1000 portova

Nmap za otvorene portove šalje test upit za određivanje servisa koji se izvršava na otvorenom portu

Primljeni odgovor se upoređuje sa bazom podataka koja se nalazi u fajlu nmap-service-probes.

```
root@kali:~/Desktop# nmap -sS 192.168.1.38
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 21:01 EDT
Nmap scan report for 192.168.1.38
Host is up (0.00031s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
4848/tcp  open  appserv-http
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 08:00:27:DC:12:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds
```

PROFILISANJE SERVERA

Amap skeniranje verzije

Koristi sličan princip rada kao NMAP aplikacija

Proverava otvorene portove a zatim analizira odgovor za određivanje konkretnog servisa

Test koji je poslat se nalazi u fajlu *appdefs.trig* a primljeni odgovor je analiziran na osnovu potpisa u fajlu *appdefs.resp*

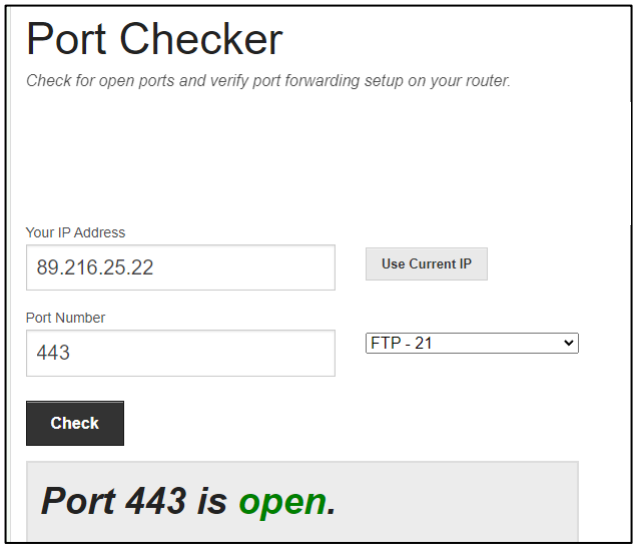
Važno je koristiti više alata koji testiraju istu stvar da bismo eleminisali lažno pozitivne i lažno negativne odgovore!!!

```
root@kali:~# amap -b -q 192.168.11.145 80 3306
amap v5.4 (www.thc.org/thc-amap) started at 2018-04-04 20:33:37 -
APPLICATION MAPPING mode

Protocol on 192.168.11.145:80/tcp matches http - banner: <!DOCTYPE
 HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n<title>40
0 Bad Request</title>\n</head><body>\n<h1>Bad Request</h1>\n<p>You
r browser sent a request that this server could not understand.<br
 />\n</p>\n</body></html>\n
Protocol on 192.168.11.145:80/tcp matches http-apache-2 - banner:
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n
<title>400 Bad Request</title>\n</head><body>\n<h1>Bad Request</h1
>\n<p>Your browser sent a request that this server could not under
stand.<br />\n</p>\n</body></html>\n
Protocol on 192.168.11.145:3306/tcp matches mysql - banner: GjHost
 '192.168.11.144' is not allowed to connect to this MySQL server
Protocol on 192.168.11.145:3306/tcp matches mysql-secured - banner
: GjHost '192.168.11.144' is not allowed to connect to this MySQL
server

amap v5.4 finished at 2018-04-04 20:33:48
```

PROFILISANJE SERVERA

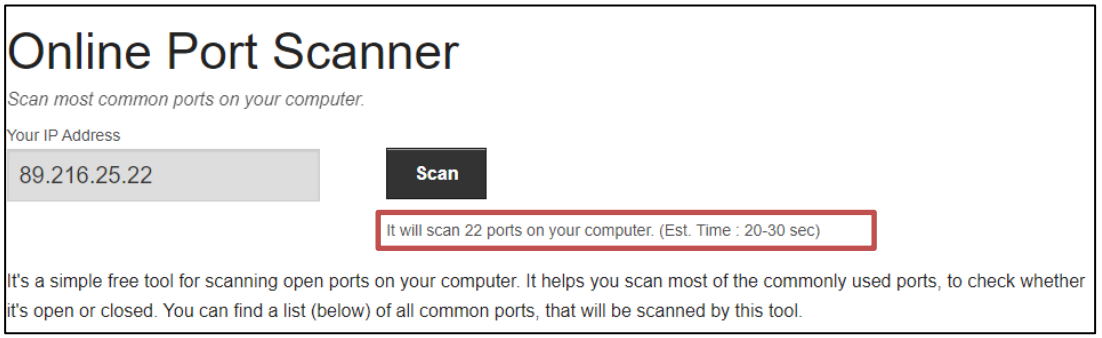
Online Port checker

https://portchecker.co/



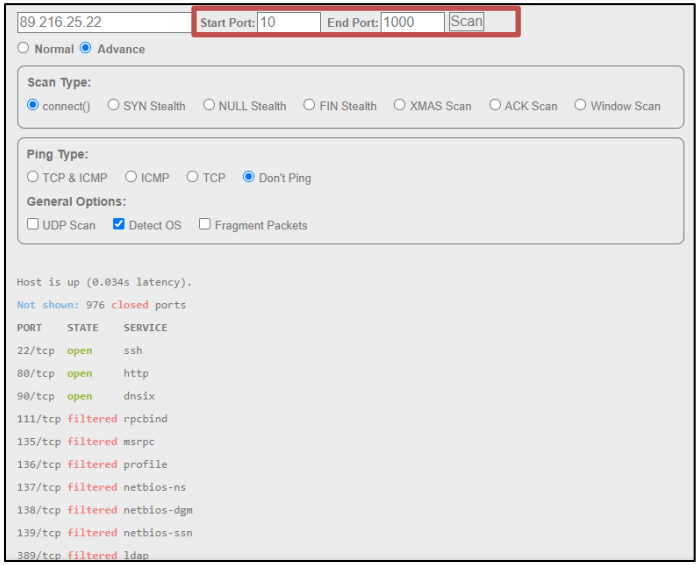
Online Port scaner

https://portchecker.co/online-port-scanner



Online Port scaner

https://www.ipfingerprints.com/portscan.php



PROFILISANJE SERVERA

Određivanje radnog okvira (framework) aplikacije

Poznavanje radnog okvira koji je korišćen u razvoju aplikacije mogu se otkriti potencijalne ranjivosti za određene verzije radog okvira

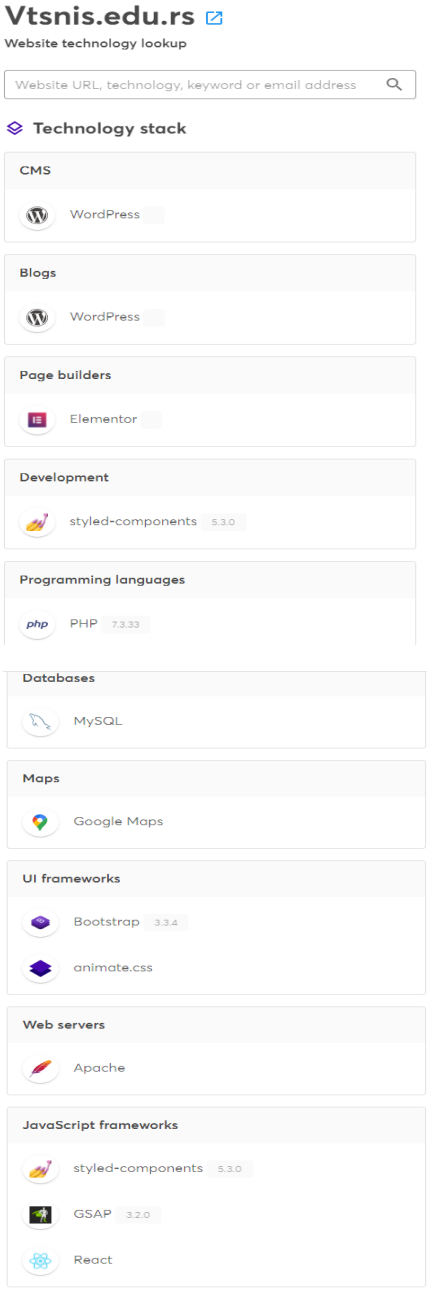
Većina radnih okvira u web aplikacijama ostavlja tragove koji mogu da se pronađu na web stranicama.

Radni okvir aplikacije često kreiraju kolačiće koji mogu da pojasne koji radni okvir je upotrebljen.

Komentari u izvornom kodu HTML stranice mogu da ukazuju na radni okvir koji je upotrebljen za razvoj web aplikacije.

Jedan od nnline alata koji otkriva tehnologije web sajta je

https://www.wappalyzer.com/lookup



PROFILISANJE SERVERA

WhatWeb Skener

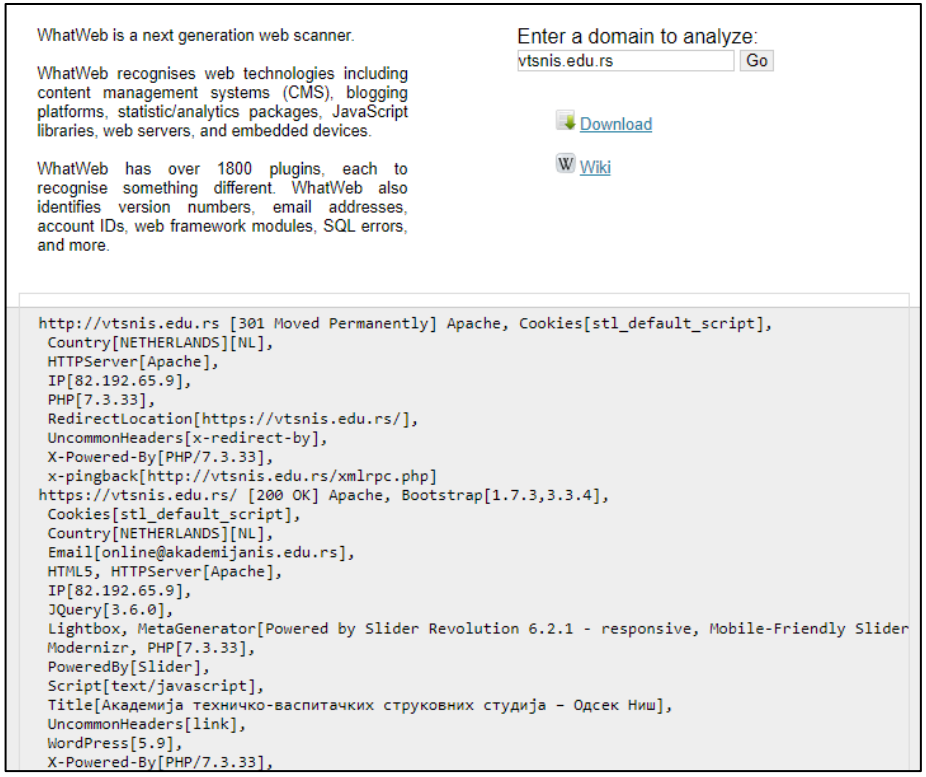
Alat za identifikaciju različitih web tehnologija koje koristi web sajt.

Alat identifikuje različite sisteme za upravljanje sadržajem (CMS) i JS biblioteke koje su upotrebljene za dizajniranje web aplikacije.

Alat ima više od 900 modula

Može da preuzme dovoljno informacija sa web stranice za određivanje tehnologije web sajtaili može rekurzivno da šalje upite web sajtu za određivanje upotrebljenih tehnologija

Online verzija alata je na adresi https://www.whatweb.net/



ISPITIVANJE RANJIVOSTI POGREŠNE KONFIGURACIJE WEB SERVERA

Identifikacija HTTP metoda pomoću NMAP alata

Web aplikacije koje su dizajnirane standardnom konfiguracijom i na starijim verzijama su ranjive na napade i mogu se eksploatisati pomoću automatizovanih alata

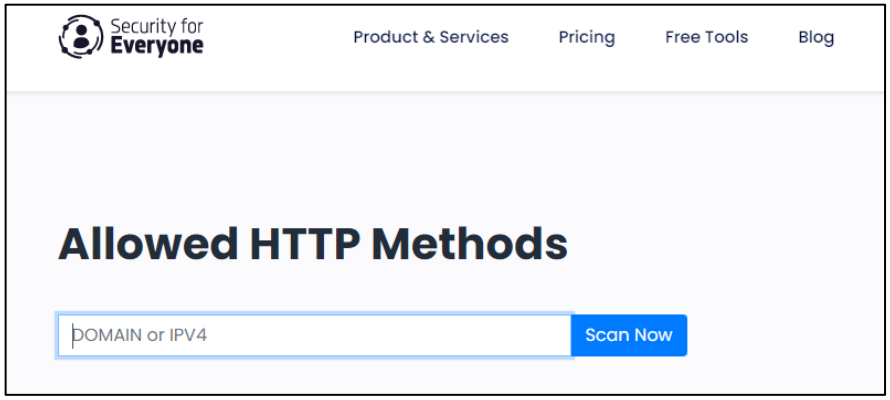
Alati za analizu web aplikacija za probleme u konfiguraciji identifikuju ranjivosti navigaciom kroz ceo web sajt tražeći konfiguraciona podešavanja, fajlove i direktorijume

Identifikacija metoda koje web server podržava koristeći Nmap alat izlistava omogućene HTTP metode na ciljnom uređaju i ukazuje na rizične metode.

Kali Linux Nmap alat

```
root@kali:~# nmap --script http-methods -p80,443,8080 10.7.7.5

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-02 14:50 CAT
Nmap scan report for 10.7.7.5
Host is up (-0.13s latency).

PORT     STATE SERVICE
80/tcp   open  http
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
443/tcp  open  https
8080/tcp open  http-proxy
MAC Address: 08:00:27:DA:00:19 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
```

https://securityforeveryone.com/tools/http-methods



ISPITIVANJE RANJIVOSTI POGREŠNE KONFIGURACIJE WEB SERVERA

Testiranje web servera u Metasploitu

dir_listing

Modul se povezje sa ciljnim web serverom sa ciljem da odredi da li je uključeno pretraživanje direktorijuma

dir_scanner

Skeniraju se interesatni web direktorijumi primenom standardnog rečinka ili posebno kreiranog rečnika

files_dir

Skenira podatke servera lociranjem rezernih kopija konfiguracionih fajlova i fajlova izvornog koda

http_login

Ako web stranica ima login formu može se pokušati pristup korišćenjem metasploit rečnika

robots.txt

Robot fajlovi koje koristi google bot mogu da sadrže URL adrese koje pretraživač nije indeksirao

Webdav scanner

Proverava da li je uključena ova opcija koja omogućava korisniku da preko ovog protokola (skup HTTP ekstenzija) udaljeno upravljaju fajlovima na web serveru tj web server se ponaša kao mrežni disk tj. server fajlova.

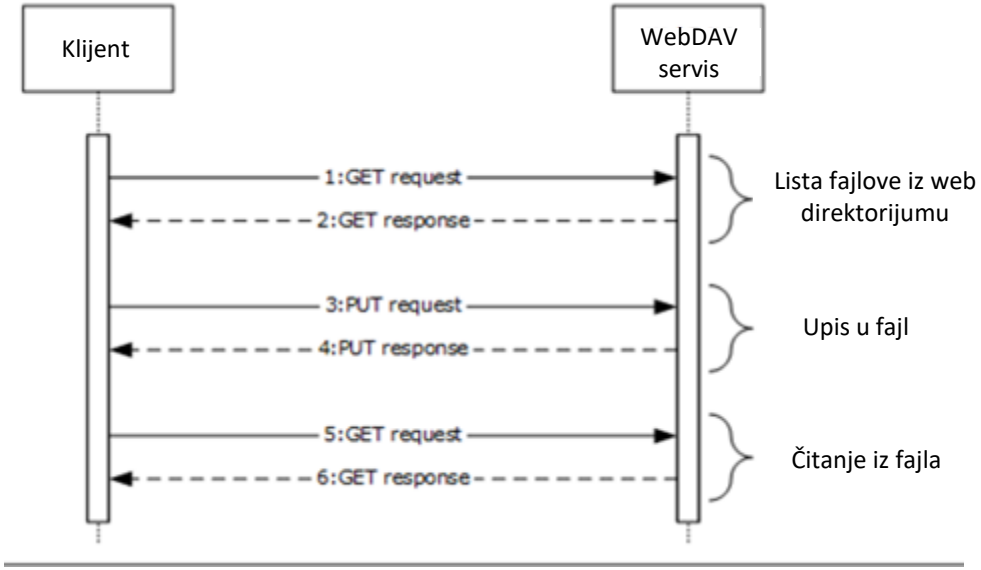
ISPITIVANJE RANJIVOSTI POGREŠNE KONFIGURACIJE WEB SERVERA

WebDAV protokol

Protokol pruža radni okvir korisnicima za kreiranje, menjanje i premeštanje dokumenata na serveru, pristup skladištu sistemu u oblaku,...

Proširuje standardni skup HTTP metoda za kreiranje, premeštanje i uređivanje datoteka, brisanje i kopiranje datoteka i foldera.

Koristi port 80 za običan, nešifrovan pristup i port 443 za kriptovan SSL/TLS protokol.



ISPITIVANJE RANJIVOSTI POGREŠNE KONFIGURACIJE WEB SERVERA

Ispitivanje WEB Aplikacije

Web aplikacija se sastoji od više web stranica koje su međusobno povezane

Mapiranje aplikacije nam pomaže da odredimo njenu veličinu

Klikom na svaki link možemo ručno da odredimo dostupne web stranice što je dug proces i sklon je propustima

Cilj je da pronađemo što više web stranica iz perspektive autorizovanog i neautorizovanog korisnika.

Automatizovani alati za ispitivanje WEB Aplikacije

Burp Spider

mapira aplikacije korišćenjem aktivnih i pasivnih metoda

Detaljno objašnjenje aplikacije https://www.youtube.com/watch?v=h2duGBZLEek