**Week-05 Security+Penetration-Testing, Tools + how to practice**

**Agenda:**

1. Forklar security testing samt penetration testing
2. Forklar fordele og ulemper ved penetration testing.
3. Forklar hvordan man lovligt udøver pen testing.
4. Forklar konceptet af Juice Shop, Kali Linux og Metasploitable.
5. Forklar værktøjet nmap og hvad man kan få ud af brugen af denne.

**Explain briefly about the concept of Security Testing, and more thoroughly about Penetration Testing**

Security Testing er en test af et system, for svagheder med henblik på kunne eliminere disse, før de bliver udnyttet af en ondsindet hacker. Der er ikke nogen rigtig måde at gøre dette på, det vigtigste er blot at teste tidligt og ofte i en proces (Udviklings proces SDLC = Software Deveolpment Lifecycle).

Under Security Testing findes der Penetration Testing, også kaldet pen testing. Penetration Testing har været en almindelig teknik, der bruges til at teste netværkssikkerheder. Det er også almindeligt kendt som black box testing (tester hvad softwaren bør gøre, men ikke hvordan den gør det) eller etisk hacking. Penetration Testing er essentielt at teste en kørende applikation eksternt for at finde sikkerhedssårbarheder uden at kende de indre funktioner i selve applikationen.

Typisk ville penetrationstestteamet have adgang til en applikation, som om de var brugere. Testeren fungerer som en angriber og forsøger at finde og udnytte sårbarheder. I mange tilfælde får testeren en gyldig konto på systemet.

**Trin i Pen Testing:**

1. Planning
2. Gathering of information (information om en applikation og infrastruktur)
3. Discover vulnerabilities
4. Reporting

Derudover findes der under Securtity Testing: Code Review, Threat Modeling og Manuel Inspections and Reviews.

**Explain the pros & cons related to Penetration Testing**

**Fordele:**

* Kan være hurtig og derfor billig.
* Kræver et lavt teknisk niveau, i forhold til at lave Code Review.
* Tester den del af koden der faktisk anvendes/udsat.
* Kan identificere en række svagheder.
* Kan identificere høj-risiko svagheder, som et resultat af en kombination af små svagheder.

**Ulemper:**

* Testes for sent i SDLC.
* Tester kun angreb der kommer udefra.
* Hvis ikke testen udføres korrekt, kan den gøre mere skade end gavn.
* Kræver tillid til Pen Testeren.

**Explain a few (one or two) of the tools meant for Penetration Testing**

1. **Netdiscover** – bruges til at scanne efter enheder på et bestemt netværk.

sudo netdiscover -r <IP-address>/24

1. **Nmap** – bruges til at scanne en enhed, for relevante informationer, som f.eks. åbne porte eller OS.

nmap -v -A <IP-address>

1. **Nikto** – bruges til at scanne en enhed, med eller uden en specifik port, til at finde sårbare tjenester. Det er en open source-web-server scanner, der bruges til at udføre tests mod web servere for forskelligt indhold, f.eks. over 6700 potentielt farlige filer/programmer, søger efter udgåede versioner af over 1250 servere og versions specifikke problemer på over 270 servere. Derudover søger den efter server konfigurationer, som f.eks. http server options og den vil også forsøge at identificere samtlige installeret software.

sudo nikto -host <IP-address> -p <port-number>

1. **Postman** – teste endpoints, som ikke er tilgængelig i browseren, f.eks. POST
2. **Chrome Developer Tools** – bruges til at teste for eventuelle SQL Injections.

**Explain the purpose of NMap and what can be discovered with the tool, using one or more prepared samples**

Nmap bruges til at scanne en enhed, for relevante informationer, som at se hvilke hosts der er tilgængelige på netværket samt hvilke tjenester (applikationsnavn og version) disse tilbyder, hvilke operativsystemer der bruges (og OS-versioner), åbne porte og så videre.

Et billede, der indeholder tekst

Automatisk genereret beskrivelse

Vi har scannet salandt.dk med nmap og har fundet følgende:

1. Åbne porte (3306 SQL, 22 SSH, 443 HTTPS)
2. RSA-public key
3. OS = Linux
4. Apache Tomcat 9.0.21
5. OpenSSH
6. nginx 1.14.0 (Ubuntu)

**Explain “ways” to legally practice Penetration Tester Skills**

Pen Testing på andre/rigtige servere uden en meget specifik skriftlig aftale med ejeren, er ulovligt. Hvis man lovligt vil øve sin Pen Testing færdigheder, bør man kun scanne ens egen IP-adresse eller virtuelle IP-adresser sat op på ens egen computer. Der findes en lang liste med applikationer, der er bygget med formålet om at kunne hackes.

Måder hvorpå man kan øve sine Penetration Tester skills, er bl.a. igennem disse ”meant-to-be-hacked” applikationer, som f.eks. JuiceShop og Metasploitable2, som vi har arbejdet med.

**Explain the concepts (where do they fit in) Kali Linux, Metasploitable 2 (and 3) OWASP Juice Shop.**

Kali Linux er et styresystem, som man kan installere på en Virtuel Box på sin computer. Styresystemet har en række Pen Testing Tools, f.eks. nmap og wireshark til at finde svagheder på netværket, der kan udnyttes.

Metasploitable2 er en virtuel maskine, som man installerer på sin computer. Denne VM kan bruges til at gennemføre sikkerhedstræning, teste sikkerhedsværktøjer og praktisere teknikker på almindelig-kendte svagheder. Det er lovligt at scanne efter Metasploitable2 i sammenhæng med Kali Linux, inden for sit eget netværk.

Juice Shop er et open source-projekt, der er udviklet og vedligeholdt af frivillige. Det er en webapplikation, med et stort antal sikkerhedsmæssige sårbarheder og i sammenhæng med Google Developer Tools, giver applikationen mulighed for lovligt at træne sine Pen Testing færdigheder og udnytte de fundne sårbarheder. Sårbarhederne vedrører generelt top-10 OWASP.

Nedenstående er en måde at hacke sig ind på en profil uden at kende e-mail. Dette er sql injection.

Et billede, der indeholder skærmbillede, monitor, telefon, skærm

Automatisk genereret beskrivelse

Her får vi adgang til fortrolige dokumenter. Først klikkes på det grønne link.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

Herefter kommer dette dokument frem. Ved at slette legal.md, kommer man ind på…

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

… denne side, hvori der ligger flere dokumenter.

Et billede, der indeholder skærmbillede

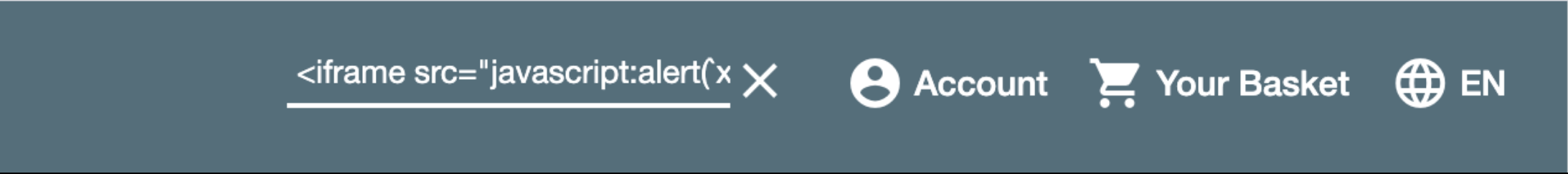
Automatisk genereret beskrivelse

Det fortrolige dokument er dette nedenstående.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

Et andet hack man kan lave på Juice Shop er DOM XXS, hvilket betyder at man i input felterne kan sætte ren JavaScript ind.



**Explain a possible test-setup using Kali Linux and Metasploitable x (or similar) and why testing/practising in this way “makes sense”**

Vi har installeret Kali Linux og metasploitable som virtuelle maskiner på vores egen computer. På den måde kan vi bruge redskaberne fra Kali Linux til at undersøge sårbarheder ved metasploitable uden at skulle have tilladelse fra nogen. Derudover kan vi lave alle test uden at være på nettet. På den måde undgår vi at scanne noget vi ikke må.

Dette test setup giver mening, da man ikke behøver tilladelse fra andre til at scanne efter sårbarheder, da alt er sat op på ens egen enhed.