Report z DVL2 – pokus číslo 2

DVL (Dawn Vulable Linux) nabízí kromě nástrojů pro scaning a případný průnik co cizího systému i mnoho služeb, které si může uživatel vyzkoušet v rámci svojí stanice bez nutnosti připojení počítačové stanice do místní sítě, či sítě internet.

Hlavním úkolem tedy bylo seznámit se většinou se službami, které mají za úkol zjistit informace o vzdáleném systému, případně umožnit minimálně jeden z webových útoků na něj. Dále bylo vhodné se seznámit s rozdílnými druhy webových útoků a případnou obranou proti nim. Jak již bylo zmíněno výše, DVL obsahuje mnoho nástrojů jak pro zjišťování důležitých informací o daném systému, tak i návody a speciálně připravené stránky a možností vyzkoušení mnoha typů útoků.

Před samotným útočením je však nutné v systému spustit apache server a příslušnou databázovou službu MySQL. Po spuštění těchto dvou služeb je uživateli umožněno používání obou balíků služeb a aplikací určených k webovým útokům.

V prvním ze dvou balíků s názvem „web exploitation package 01“ lze najít celkem pět výukových lekcí základního zabezpečení webových aplikací. Prvními dvěma lekcemi lze snadno proklouznout pomocí tutoriálu, který je k lekcím přiložen. V dalších lekcích již tento tutoriál chybí (což se domnívám, že je veliká škoda), avšak k lekci číslo 4 existuje videotutoriál s podrobným návodem. Právě v prvních dvou lekcích se uživatel seznamuje se základní bezpečností webových aplikací psaných v HTML kódu. Je zde nastíněn problém zcela otevřeného kódu včetně URL adresy na soubor resetující heslo daného uživatele. V lekci číslo 4 je uživatel seznámen s typem útoku zvaným Cross Site Scripting, v rámci něhož se požaduje po uživateli vložit příspěvek do imaginárního fóra a reakci na něj. Tuto lekci lze velice snadno absolvovat právě pomocí výše zmíněného videotutoriálu k této lekci.

Pomocí útoku Cross Site Scripting se nám podařilo do databáze „propašovat“ vlastní skript, který byl prováděn na straně serveru. Odpovědí serveru po přidání diskusního příspěvku ve tvaru: <script>alert(„XSS“);//<</script> bylo pouze nově otevřené okno obsahující text „XSS“. Jako útok nepoužitelné, avšak nádherně lze zde pozorovat sílu tohoto útoku.

Jako druhou demonstraci tohoto útoku bylo vložení tohoto textu:
< iframe src = http://www.example.com < , kde zpracováním na serveru náš příspěvek obsahoval frame s hláškou o nedostupnosti serveru (způsobeno odpojením lokální sítě od DVL). Opět zde platí, že jako útok je toto nepoužitelné, avšak s několika úpravami lze získat krásnou fishingovou stránku nejen pro klienty bank.

V druhém balíku se lze setkat s mnoha buď samostatně spustitelnými aplikacemi, nebo se službami zaměřujícími se na jeden z webových útoků. Námi vyzkoušená webová služba s názvem „Wordpress“ nás přesune na stránku obsahující téměř pouze jediné vyhledávací políčko. Návod jsme v distribuci nenašli, ale i zde platí, že videotutoriál pomůže i zde. Služba „Wordpress“ nabízí vyzkoušení útoku Injection Flow, kde do vyhledávacího políčka nevypisujeme hledaný text, ale vkládáme předem připravený kus kódu, na

který server odpoví tak, že například vrátí název uživatele, který má administrátorská práva vzdáleného systému.

Pokud se podíváme zpět do nabídky „Web Exploitation“, kterou nám distribuce nabízí, zjistíme, že jsou zde obsaženy další dvě položky. Jedna je samostatná aplikace, pro jejíž chod není nutný běh žádné další služby, a potom je tu obsažena služba „WebGoat“ která ke svému běhu potřebuje otevřený port 80 se službou http (případně funguje i na portu 8080).

Služba WebGoat, která má opět uživatele seznámit s různými typy útoků v rámci webových aplikací. Lze si zde ozkoušet jak útok Cross Site Scripting tak například několik druhů útoku SQL Injection. K této části jsem bohužel v DVL nenašel žádný tutoriál, avšak i zde platí, že internet obsahuje velké množství videotutoriálu k této službě. Nejen proto jsem úspěšně provedl svůj první SQL Injection útok a podařilo se nám z databáze dostat všechny její záznamy. Pomocí jednoduchého dotazu (Smith‘ or ‚0‘=‘0) databáze vrátila všechny její záznamy. Jednoduché, ale účinné.