هانی پات(Honeypots) چیست؟

هانی پات را میتوان یک حقه و کلک یا بهتر است بگوییم یک طعمه در نظر گرفت که میتواند بسیاری از نفوذگران را بخود جذب کند. عموما این طعمه ها میتوانند بصورت سیستم های فیزیکی و یا مجازی پیاده سازی شوند که نقش یک دیوایس واقعی و مهم را در شبکه از خود به نمایش میگذارند (در حالی که اینطور نیست). بر روی هانی پات ها مانیتورینگ و لاگینگ سنگینی را به اجرا میگذاریم تا بتوان عملکردهای نفوذگر را بر روی آن بدقت مورد بررسی و تحلیل قرار داد. اگرچه جذب عمدی یک نفوذگر در دسترسی به سیستمی از شبکه ممکن است از نظر یک فرد حرفه ای در زمینه امنیت متناقض به نظر برسد اما نباید از فواید راه اندازی و استفاده از هانی پات در شبکه نیز چشم پوشی نمود.

در واقع Honey pot یک سیستم اطلاعاتی است که ارزش آن به استفاده غیر مجاز و ممنوع دیگران از آن است.

در سازمان بایستی، Honey pot با مقاصد زیر قرار گیرد

۱- جلوگیری از حملات

۲- تشخیص حملات

۳- پاسخگویی به حملات

۴- استفاده برای مقاصد تحقیقاتی

- برای اکانت های مهم سرورها باید یک Admin قلابی با نام Administrator ایجاد گردد و یک رمز عبور مناسب و طولانی بر روی آن قرار گیرد
- در لبه اینترنت باید Honey pot قرار گیرد
- از ابزارهای مختلف و Honey pot های مختلف مانند La Brea Tar pit و یا Deception Toolkit برای مقاصد مختلف می توان استفاده نمود

یک Honey pot باید موارد زیر را در اختیار متخصص امنیت سازمان قرار دهد

۱) زمان نفوذ نفوذگر و یا هکر به سیستم

۲) پروتکلی که از آن استفاده کرده

۳) آدرس مبدا و مقصد

موارد زیر را برای نگهداری Honey pot باید در نظر گرفت

- سیستم باید دائماً تحت نظر باشد در غیر اینصورت نه تنها هیچ کمکی نمی کند بلکه خودش به عنوان یک نقطه خطر یا حفره امنیتی مطرح می شود.

- دارای ریسک بالا زیرا نفوذگر یک سیستم واقعی را در اختیار دارد و ممکن است به سیستم های اصلی شبکه صدمه بزند. بنابراین هیچ سیستمی بر روی شبکه را نمی توان امن در نظر گرفت

-کلیه موارد و تصمیم گیری چگونگی کار با متخصص امنیت سازمان باید باشد