انظمة كشف الاختراق (IDS) هي أنظمة أمنية تُستخدم لاكتشاف النشاط الضار على الشبكة. يمكن أن تساعد أنظمة IDS في حماية الشبكة من مجموعة متنوعة من الهجمات، قد تبحث تقنية تحليل السلوك عن مستخدم يحاول تسجيل الدخول إلى حساب باستخدام كلمة مرور خاطئة عدة مرات. تقدم أنظمة IDS العديد من المزايا، الكشف المبكر: يمكن لأنظمة IDS اكتشاف الهجمات في وقت مبكر، السجلات: يمكن لأنظمة IDS إنشاء سجلات للنشاط المشبوهة، التكامل: يمكن دمج أنظمة IDS مع أنظمة أخرى، تتضمن بعض سلبيات أنظمة IDS ما يلي: التكلفة: يمكن أن تكون أنظمة IDS مكلفة. هناك عدة أنواع من أنظمة IDS، أنظمة كشف الاختراق المستندة إلى الشبكة (NIDS): تراقب أنظمة NIDS حركة مرور الشبكة بحثًا عن النشاط الضار. أنظمة كشف الاختراق المستندة إلى المضيف (HIDS): تراقب أنظمة HIDS النشاط على مستوى المضيف بحثًا عن النشاط الضار. أنظمة كشف الاختراق المستندة إلى السلوك (BIDS): تراقب أنظمة BIDS السلوكيات المريبة للمستخدمين والأنظمة بحثًا عن النشاط الضار. عند اختيار نظام IDS، حجم الشبكة: يجب اختيار نظام IDS قادر على التعامل مع حجم الشبكة. انظمة منع الاختراق (IPS) هي أنظمة أمنية تُستخدم لمنع النشاط الضار على الشبكة. أنظمة منع الاختراق (IPS) هي أداة أمنية مهمة يمكن استخدامها للحماية من مجموعة متنوعة من الهجمات الإلكترونية. مزايا أنظمة IPS بما في ذلك: مما يحمي الشبكة من الأضرار. سلبيات أنظمة IPS تتضمن بعض سلبيات أنظمة IPS ما يلي: التكلفة: يمكن أن تكون أنظمة IPS مكلفة. أنواع أنظمة IPS بما في ذلك: أنظمة منع الاختراق المستندة إلى الشبكة (NIPS): تراقب أنظمة NIPS حركة مرور الشبكة بحثًا عن النشاط الضار. أنظمة منع الاختراق المستندة إلى المضيف (HIPS): تراقب أنظمة HIPS النشاط على مستوى المضيف بحثًا عن النشاط الضار. اختيار نظام IPS يجب مراعاة العوامل التالية: الميزانية: تختلف تكلفة أنظمة IPS باختلاف الحجم والميزات. الاحتياجات الأمنية: يجب اختيار نظام IPS يلبي الاحتياجات الأمنية المحددة للمؤسسة. مقارنة أنظمة IDS و IPS أوجه التشابه كلاهما أنظمة أمنية تستخدم لمراقبة الشبكة بحثًا عن النشاط الضار. كلاهما يمكن أن يستخدم تحليل التوقيع أو تحليل السلوك لاكتشاف النشاط الضار.