

RE: DISA Security Readiness Review Evaluation Scripts

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0255.html>

techlists_at_comcast.net

Date: 11/26/05

To: "Smith, Michael J." <Michael.J.Smith@unisys.com>, "hannibal blog" <hannibalsec@gmail.com>, <p
Date: Sat, 26 Nov 2005 04:56:56 +0000

The Gold Disk itself runs very fast. It will scan your system in 2–3 minutes.

It allows you to apply the patches and recommended fixes very fast. If you blindly apply all of the recommended fixes, it will also break your system very fast, guaranteed. ("very fast" – do we see a pattern here?) There is even a "Platinum" level on the Gold Disk, even more restrictive than "Gold" level; now that one will break your system even more badly than the Gold.

It's good if you have a test lab that accurately represents your production network, so you can test the Gold Disk against your standard set of apps to see what is affected.

PG

- > *The SRR scripts are very good, but keep in mind that what they do is*
- > *check the configurations that are specified in the STIGs.*
- >
- > *It goes like this:*
- > *NSA creates Security Guides*
- > *Which begat:*
- > *DISA Security Technical Implementation Guides*
- > *Which begat:*
- > *DISA Manual Checklists*
- > *Which begat:*
- > *DISA SRR Scripts*
- >
- > *What the SRR Scripts are is an automated way to do the checks in the*
- > *manual checklists.*
- >
- > *A word of caution is that if an OS is configured according to the STIGS,*
- > *they will break. The good thing is that it's a fast tool to check for*
- > *vulnerabilities.*
- >
- > *The scripts for windows machines use winbatch as the script language.*
- > *They take about 15–20 minutes to run once you've figured out how to do*
- > *it. What we do is go into an office, select a random percentage of*
- > *computers to check, load the script, and start it. By the time we're*

SecurityFocus Penetration: RE: DISA Security Readiness Review Evaluation Scripts

> *done starting the script on the last computer, it's time to start*
> *retrieving results off the first ones.*
>
> *When DISA sends their audit team around, they run the SRR Scripts and an*
> *external scan with ISS or Retina.*
>
> *As for the .mil restriction, last time I looked at them, they allow*
> *anybody to download the STIGS but you need a .mil address to download*
> *the SRR Scripts. There is also the "gold disk" which has all the SRR*
> *Scripts on it.*
>
> *HTH*
> *--Mike*
>
>
>
> *Michael J Smith michael.j.smith@unisys.com*
> *Information Security Architect*
> *703.419.3109 W*
> *703.855.0890 C*
> *"Those who do not understand Unix are condemned to reinvent it, poorly."*
>
> *--Henry Spencer*
>
> > -----Original Message-----
> > *From: hannibal blog [mailto:hannibalsec@gmail.com]*
> > *Sent: Thursday, November 24, 2005 3:19 AM*
> > *To: pen-test@securityfocus.com*
> > *Subject: DISA Security Readiness Review Evaluation Scripts*
> >
> > *Hello*
> >
> > *did anyone try the publicly available disa SRR availble at*
> > *<http://iase.disa.mil/stigs/SRR/>*
> > *what is the diference between the publicly available ones and those*
> > *reserved to .mil ?*
> > *What do u think about using them to audit a customer win 2k server ?*
> >
> >
> >
> >

> >
> > -----
> > *Audit your website security with Acunetix Web Vulnerability Scanner:*
> >
> > *Hackers are concentrating their efforts on attacking applications on*
> > *your*
> > *website. Up to 75% of cyber attacks are launched on shopping carts,*
> > *forms,*
> > *login pages, dynamic content etc. Firewalls, SSL and locked-down*
> > *servers*

SecurityFocus Penetration: RE: DISA Security Readiness Review Evaluation Scripts

> > are
> > *futile against web application hacking. Check your website for*
> > *vulnerabilities*
> > *to SQL injection, Cross site scripting and other web attacks before*
> > *hackers do!*
> > *Download Trial at:*
> >
> > http://www.securityfocus.com/sponsor/pen-test_050831
> >
> >

> --
> > -----
>
>
>

> *Audit your website security with Acunetix Web Vulnerability Scanner:*
>
> *Hackers are concentrating their efforts on attacking applications on your*
> *website. Up to 75% of cyber attacks are launched on shopping carts, forms,*
> *login pages, dynamic content etc. Firewalls, SSL and locked-down servers are*
> *futile against web application hacking. Check your website for vulnerabilities*
> *to SQL injection, Cross site scripting and other web attacks before hackers do!*
> *Download Trial at:*
>
> http://www.securityfocus.com/sponsor/pen-test_050831
>
>

>

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
